



- Expert Verified, Online, **Free**.



## **CERTIFICATION TEST**

- [CertificationTest.net](https://CertificationTest.net) - Cheap & Quality Resources With Best Support

Which event is user interaction?

- A. gaining root access
- B. executing remote code
- C. reading and writing file permission
- D. opening a malicious file

**Suggested Answer: D**

Community vote distribution

D (100%)

🗳️ 👤 **marcosbude** 7 months, 3 weeks ago  
testoo  
upvoted 1 times

🗳️ 👤 **marcosbude** 7 months, 3 weeks ago  
testoo  
upvoted 1 times

🗳️ 👤 **marcosbude** 7 months, 3 weeks ago  
higjkl  
upvoted 1 times

🗳️ 👤 **marcosbude** 7 months, 3 weeks ago  
abcdefg  
upvoted 1 times

🗳️ 👤 **drdecker100** 9 months, 2 weeks ago  
**Selected Answer: D**

D. opening a malicious file is not necessarily an event that involves user interaction. The most common event that involves user interaction is opening a file or clicking on a link, which can lead to unintended consequences such as executing malicious code.

However, in the options given, none of them directly relate to user interaction.  
upvoted 3 times

🗳️ 👤 **kenbrewitt** 1 year ago  
**Selected Answer: D**  
Opening a malicious file  
upvoted 1 times

🗳️ 👤 **ZVerd** 1 year, 4 months ago  
**Selected Answer: D**  
Open a malicious file  
upvoted 1 times

🗳️ 👤 **dazzler0082** 1 year, 6 months ago  
**Selected Answer: D**  
D. Opening a malicious file  
upvoted 1 times

🗳️ 👤 **msg01** 1 year, 7 months ago  
**Selected Answer: D**  
D : open a malicious file  
upvoted 1 times

🗳️ 👤 **PrettyMs** 1 year, 7 months ago  
D. Opening a malicious file  
upvoted 1 times

🗄️ 👤 **WISDOM2080** 1 year, 10 months ago

D : open a malicious file

upvoted 1 times

🗄️ 👤 **ethhacker** 1 year, 10 months ago

**Selected Answer: D**

Like opening a macro embedded excel document

upvoted 1 times

🗄️ 👤 **chantips** 1 year, 11 months ago

D.open a malicious file

upvoted 1 times

🗄️ 👤 **RFSP** 3 years ago

d is response

upvoted 1 times

🗄️ 👤 **cloud88** 3 years ago

d response

upvoted 1 times

🗄️ 👤 **halamah** 3 years, 7 months ago

d is correct

upvoted 1 times

🗄️ 👤 **HARRYTULA** 3 years, 11 months ago

open a malicious file

upvoted 1 times

Which security principle requires more than one person is required to perform a critical task?

- A. least privilege
- B. need to know
- C. separation of duties
- D. due diligence

**Suggested Answer: C**

Community vote distribution

C (100%)

 **IT\_Master\_Tech** 8 months, 1 week ago

ChatGPT goes with B. Separation of duties refers to assigning tasks among different individuals to prevent conflict of interest or misuse of power.  
upvoted 1 times

 **IT\_Master\_Tech** 8 months, 1 week ago

Sorry, never mind.  
upvoted 1 times

 **anonymous1966** 9 months, 1 week ago

"C" is correct

---> Separation of duties is an administrative control dictating that a single individual should not perform all critical- or privileged-level duties. Additionally, important duties must be separated or divided among several individuals within the organization.

--> The principle of least privilege states that all users should be granted only the level of privilege they need to do their jobs, and no more.

Cisco CyberOps Associate CBROPS 200-201 Official Cert Guide

By Omar Santos  
upvoted 1 times

 **Proctored\_Expert** 9 months, 1 week ago

**Selected Answer: C**

The security principle that requires more than one person is required to perform a critical task is separation of duties.

Separation of duties is a security principle that involves dividing the responsibilities for a critical task among multiple individuals, so that no single person has complete control over the task. This helps to reduce the risk of errors, fraud, or abuse, and to ensure that the task is performed accurately and in accordance with established policies and procedures.

upvoted 1 times

 **drdecker100** 9 months, 1 week ago

**Selected Answer: C**

ere's why the other options are not the correct answer to the question:

A. Least privilege refers to the practice of limiting access to the minimum permissions necessary to perform a specific task. It helps to reduce the risk of unauthorized access or damage to critical systems and data.

B. Need to know refers to the principle that individuals should only have access to information that is necessary for them to perform their job duties. This helps to prevent the spread of sensitive information to those who don't need to know it.

D. Due diligence refers to the level of care and caution that is expected of individuals and organizations in order to protect themselves and others. It encompasses many different security principles and practices, including separation of duties.

So, while each of these principles is important for maintaining security, they are not directly related to the specific requirement of having more than one person perform a critical task.



upvoted 3 times

🗲️ 👤 **kenprewitt** 1 year ago

**Selected Answer: C**

Separation of duties is the only one of these is mandatory requirement of more than one

upvoted 1 times

🗲️ 👤 **msg01** 1 year, 7 months ago

**Selected Answer: C**

Separation of duties

upvoted 2 times

🗲️ 👤 **PrettyMs** 1 year, 7 months ago

C. Separation of duties

upvoted 1 times

🗲️ 👤 **WISDOM2080** 1 year, 10 months ago

C : separate of duties

upvoted 1 times

🗲️ 👤 **chantips** 1 year, 11 months ago

C. separation of duties

upvoted 1 times

🗲️ 👤 **[Removed]** 2 years, 11 months ago

C is correct

upvoted 1 times

🗲️ 👤 **evident** 3 years, 7 months ago

**Selected Answer: C**

C is correct

upvoted 1 times

🗲️ 👤 **halamah** 3 years, 7 months ago

c is correct

upvoted 1 times

🗲️ 👤 **Leo\_Visser** 4 years ago

Correct Answer

upvoted 1 times



How is attacking a vulnerability categorized?

- A. action on objectives
- B. delivery
- C. exploitation
- D. installation

**Suggested Answer:** C

Community vote distribution

C (100%)

  **anonymous1966** Highly Voted 9 months, 2 weeks ago

"C" is correct

Here are the steps of the Kill Chain Model.

The example are in the context of the question

- 1) Reconnaissance - identified vulnerabilities
- 2) Weaponization - prepare (in lab) the weapon, for example a file with malware code.
- 3) Delivery - transmit the file (e-mail, website, etc)
- 4) Exploitation - trigger the weapon (execute the code), exploiting the vulnerability
- 5) Installation - the weapon installs a backdoor (server)
- 6) Command and control (C2 or CnC) - connection to the treat actor
- 7) Actions on objectives - do the job (stealing information, for example)

upvoted 11 times

  **drdecker100** Most Recent 9 months, 1 week ago

**Selected Answer: C**

The correct answer is C. Exploitation, as it refers to the process of taking advantage of a weakness in a system or application in order to carry out some sort of malicious activity.

Here's why the other options are incorrect:

A. Action on objectives refers to the specific goals and objectives that an attacker is trying to achieve through their attack. For example, an attacker's objective might be to steal sensitive data, disrupt normal operations, or install malware on a target system.

B. Delivery refers to the method by which an attacker delivers their attack payload (such as malware or other malicious code) to the target system. This might involve phishing emails, drive-by downloads, or other types of social engineering tactics.

D. Installation refers to the process of actually installing the malicious payload onto the target system. This step in the attack process may involve running a malicious program or script, or modifying existing system files to enable continued access for the attacker.



upvoted 1 times

  **kenprewitt** 1 year ago

**Selected Answer: C**

C. exploitation

upvoted 1 times

  **msg01** 1 year, 7 months ago

**Selected Answer: C**

exploitation

upvoted 1 times

  **PrettyMs** 1 year, 7 months ago

C. Exploitation

upvoted 1 times

🗨️ 👤 **AhmedAbdalla** 1 year, 8 months ago

Here are the steps of the Kill Chain Model. The example are in the context of the question

- 1) Reconnaissance - identified vulnerabilities
- 2) Weaponization - prepare (in lab) the weapon, for example a file with malware code.
- 3) Delivery - transmit the file (e-mail, website, etc)
- 4) Exploitation - trigger the weapon (execute the code), exploiting the vulnerability
- 5) Installation - the weapon installs a backdoor (server)
- 6) Command and control (C2 or CnC) - connection to the treat actor
- 7) Actions on objectives - do the job (stealing information, for example)

upvoted 1 times

🗨️ 👤 **chantips** 1 year, 11 months ago

C.exploitation

upvoted 1 times

🗨️ 👤 **halamah** 3 years, 7 months ago

c is correct

upvoted 1 times

🗨️ 👤 **Leo\_Visser** 4 years ago

Reconnaissance: Intruder selects target, researches it, and attempts to identify vulnerabilities in the target network.

Weaponization: Intruder creates remote access malware weapon, such as a virus or worm, tailored to one or more vulnerabilities.

Delivery: Intruder transmits weapon to target (e.g., via e-mail attachments, websites or USB drives)

Exploitation: Malware weapon's program code triggers, which takes action on target network to exploit vulnerability.

Installation: Malware weapon installs access point (e.g., "backdoor") usable by intruder.

Command and Control: Malware enables intruder to have "hands on the keyboard" persistent access to target network.

Actions on Objective: Intruder takes action to achieve their goals, such as data exfiltration, data destruction, or encryption for ransom.

(source: [https://en.wikipedia.org/wiki/Kill\\_chain](https://en.wikipedia.org/wiki/Kill_chain))

So C is the right answer

upvoted 2 times

What is a benefit of agent-based protection when compared to agentless protection?

- A. It lowers maintenance costs
- B. It provides a centralized platform
- C. It collects and detects all traffic locally
- D. It manages numerous devices simultaneously

**Suggested Answer: C**

Community vote distribution

C (80%)


B (20%)

 **skysoft** Highly Voted 4 years, 6 months ago

Answer is C.

Host-based antivirus protection is also known as agent-based. Agent-based antivirus runs on every protected machine. Agentless antivirus protection performs scans on hosts from a centralized system. Agentless systems have become popular for virtualized environments in which multiple OS instances are running on a host simultaneously. Agent-based antivirus running in each virtualized system can be a serious drain on system resources. Agentless antivirus for virtual hosts involves the use of a special security virtual appliance that performs optimized scanning tasks on the virtual hosts. An example of this is VMware's vShield.

upvoted 20 times

 **anonymous1966** Highly Voted 3 years, 9 months ago

"B" is correct.

According to NIST SP 800-40r3, an enterprise patch management can use three typical deployment models:

Agent based: This model uses an agent, which is software installed on the system that communicates with a patch management server.

Agentless: This model includes one device that constantly scans the infrastructure and determines which host to patch.

Passive network monitoring: This model uses network traffic monitoring to determine which version of the operating system a host is running.


Keep in mind that "agent" is not antivirus or personal firewall. Agent's role is to communicate to a centralized server and "obey" its orders.

upvoted 10 times

 **omita** 3 years, 5 months ago

NO confusion... " Keep in mind that "agent" is not antivirus or personal firewall. Agent's role is to communicate to a centralized server and "obey" its orders." Hence, B is correct

upvoted 3 times

 **KYHO** Most Recent 9 months ago

**Selected Answer: B**

The benefit is that it provides a centralized platform! B~

upvoted 1 times

 **BlackDealth** 9 months, 1 week ago

Answer is C

Agentless systems are based on push technology and on a centralized design. A central authority is responsible for scanning the machines in the enterprise and for initiating all actions on those machines. Agentless systems have a number of advantages over agent-based systems. Strict agent-based systems can only report on machines that have the agent actively running. If the agent has been disabled the machine will appear to not exist. In addition, new machines can be introduced to a network and these rogue machines will not only be agentless, they may well be invisible. Agentless systems, on the other hand, can scan ranges of IP addresses and report on machines it finds. Even if it cannot access the system, the agentless scanner will at least report that a new IP address is present on the network. In many cases agentless systems lower the cost of ownership, reduce management overhead, and provide for quick and easy deployment. This is especially true in large enterprises managing 10,000 or more machines. An administrator can be scanning and fixing their network within minutes using an agentless system.

upvoted 2 times

 **Entivo** 9 months, 1 week ago

**Selected Answer: C**

The answer is C and here is why: The question asks what is a "benefit" of agent-based over agentless. BOTH systems utilise a central server to collate results, if they didn't you would have to examine every device to see what was going on. Hence "centralized admin" isn't a benefit. The benefit if agent-based protection is that devices will continue to be protected even if they lose connection with the centralized server. Agentless devices will not be scanned if they lose connection with the server because agentless uses "push" technology to scan hosts. So for me, the benefit here is that devices are scanned locally and thus remain protected at all times.

upvoted 8 times

  **drdecker100** 9 months, 1 week ago

**Selected Answer: C**

The correct answer is C. It collects and detects all traffic locally.

Here's why the other options are incorrect:



A. Agent-based protection can often result in higher maintenance costs compared to agentless protection, as there are additional software components that need to be installed, updated, and managed on each device.

B. While some centralized management platforms for agent-based protection may be available, this is not a direct benefit of using agent-based protection over agentless protection.

D. Agent-based protection may allow for the management of numerous devices simultaneously, but this is not a unique advantage when compared to agentless protection, as many agentless solutions also have centralized management capabilities.

So, the key advantage of agent-based protection over agentless protection is that it allows for the collection and detection of all traffic locally, which can lead to improved performance, greater accuracy, and more comprehensive security coverage. This is because the agent software runs directly on the device, allowing it to collect and analyze all traffic, including local and network traffic, without relying on any external systems.

upvoted 2 times

  **msg01** 1 year, 7 months ago

**Selected Answer: B**

It provides a centralized platform

upvoted 1 times

  **PrettyMs** 1 year, 7 months ago

Answer is C

upvoted 1 times

  **k10ud** 1 year, 9 months ago

Answer is D.



A benefit of agent-based protection when compared to agentless protection is:

D. It manages numerous devices simultaneously.

Agent-based protection allows for centralized management and control of security agents installed on individual devices. This centralized approach enables administrators to manage and monitor multiple devices, often across different platforms and locations, from a single management console or platform. It simplifies the management of security policies, updates, and configurations for all protected devices, making it easier to ensure that security measures are consistently applied and up to date across the organization.

In contrast, agentless protection typically relies on network-level security controls and may not provide the same level of centralized device management and control. This can make it more challenging to manage a large number of devices and ensure uniform security policies and configurations across the network.

upvoted 1 times

  **chantips** 1 year, 11 months ago

Answer is C

upvoted 1 times

  **evaline12** 2 years, 5 months ago

I think the confusion is coming from the word antivirus, Santos's book never explains agent-based/agentless antivirus only agent-based/agentless protections and in detail, the patch management agent based/less which is different

upvoted 1 times

🗨️ 👤 **evaline12** 2 years, 5 months ago

under the centralized platform, I think the test creators meant patch repository, "The server acts as the patch repository and process orchestrator"

I know it's not the sharpest answer, just don't overthink it!

upvoted 1 times

🗨️ 👤 **fyticez** 2 years, 8 months ago

It's clearly not A or D, but otherwise both B and C are ambiguous as answers.

upvoted 1 times

🗨️ 👤 **kyle942** 2 years, 9 months ago

Do not need a central host since they can perform tasks independently: Once installed, the agent will run its set of actions on demand without needing to establish a connection to a server beforehand – even when it is disconnected from the enterprise network.

upvoted 1 times

🗨️ 👤 **u170who** 2 years, 11 months ago

**Selected Answer: B**

The question isn't asking for a definition, it is asking what is the benefit. Working in a large company, you'll realize that they always want to save money and simplify things. The word Agent is usually associated with local AV, it is associated with a centrally managed server which cuts costs and management overhead. The answer is B.

upvoted 1 times

🗨️ 👤 **adodocletus** 3 years ago

Answer is C

agent-based protection is installed locally why agentless are not..Agent-based scan and detect on the local device because it has been installed example is Host-based antivirus.. Agentless is not installed locally and it is centralized.. so the answer can not be B.

upvoted 1 times

🗨️ 👤 **WillBui** 3 years, 3 months ago

**Selected Answer: C**

it's C

upvoted 1 times

🗨️ 👤 **[Removed]** 3 years, 3 months ago

It didnt ask which one was better, it asked whats the difference between agent and agentless, and agent is local..so C

upvoted 1 times

🗨️ 👤 **fyticez** 2 years, 8 months ago

It actually did, it asked "what is the benefit"...

upvoted 1 times

Which principle is being followed when an analyst gathers information relevant to a security incident to determine the appropriate course of action?

- A. decision making
- B. rapid response
- C. data mining
- D. due diligence

**Suggested Answer: D**

Community vote distribution

D (71%)

A (29%)

🗳️ 👤 **EVL87** 9 months, 1 week ago

**Selected Answer: D**

Due diligence is the process of gathering and analyzing all relevant information before making a decision or taking action. In the context of security incidents, due diligence involves gathering and analyzing all available information about the incident, such as the nature of the threat, the extent of the damage or potential damage, and the possible impact on the organization's operations and assets. This information is then used to determine the appropriate course of action, such as containing and mitigating the threat, restoring systems and data, and identifying and addressing any underlying vulnerabilities

upvoted 3 times

🗳️ 👤 **Proctored\_Expert** 9 months, 1 week ago

**Selected Answer: D**

The principle being followed when an analyst gathers information relevant to a security incident to determine the appropriate course of action is due diligence. Due diligence refers to the careful and thorough investigation and analysis of a particular situation or problem in order to make informed decisions or take appropriate action. In the context of security incidents, this may involve gathering and analyzing relevant data, studying the potential impact of the incident, and determining the most appropriate response based on the circumstances.

upvoted 2 times

🗳️ 👤 **drdecker100** 9 months, 1 week ago

**Selected Answer: D**

The correct answer is D. Due diligence.

Due diligence refers to the level of care and caution that is expected of individuals and organizations in order to protect themselves and others. In the context of security incidents, due diligence requires that analysts gather all relevant information about an incident in order to make informed decisions about the appropriate course of action. This involves carefully reviewing logs, network traffic, and other data sources to determine the scope and nature of the incident, and to identify any indicators of compromise.

upvoted 2 times

🗳️ 👤 **vvadas** 9 months, 1 week ago

A. decision making

When an analyst gathers information relevant to a security incident, their primary goal is to make informed decisions on how to proceed with the incident response. They need to assess the available data, understand the nature and severity of the incident, evaluate potential risks, and then decide on the appropriate course of action to contain, mitigate, and remediate the situation effectively.

"D. due diligence" is a broader concept that generally refers to the effort taken by a responsible party to avoid harm or potential risks to others. While due diligence is a critical part of the overall incident response process, the specific act of gathering information to determine the appropriate course of action more closely aligns with decision making (Option A) in this context.

upvoted 2 times

🗳️ 👤 **Sbonel0** 10 months, 3 weeks ago

D. due diligence

upvoted 1 times

🗳️ 👤 **fisher004** 1 year, 7 months ago

Decision making  
upvoted 1 times

🗨️ **msg01** 1 year, 7 months ago

**Selected Answer: A**

Decision making  
upvoted 2 times

🗨️ **PrettyMs** 1 year, 7 months ago

A. Decision making  
upvoted 1 times

🗨️ **Faio** 1 year, 9 months ago

A : decision making  
due diligence is appropriate to gathers information, now you need to decide on the course of action.  
upvoted 1 times

🗨️ **WISDOM2080** 1 year, 10 months ago

A : decision making  
upvoted 1 times

🗨️ **ShammaA** 2 years, 1 month ago

Dude diligence comes in before decision making, you first due and gather all information about an incident then you start working on it to make your decisions.  
upvoted 1 times

🗨️ **ShammaA** 2 years, 1 month ago

DUE diligence sorry for the typo  
upvoted 1 times

🗨️ **alhamry** 2 years, 2 months ago

Option A is the best answer because the principle being described is decision making. When an analyst gathers information relevant to a security incident, they are collecting data to help them make an informed decision on how to proceed. Rapid response is related to how quickly an organization can respond to a security incident once it has been detected, while data mining involves the process of discovering patterns in large datasets. Due diligence is a general term that refers to the effort that a reasonable person takes to avoid harm to others.  
upvoted 1 times

🗨️ **fyticez** 2 years, 8 months ago

**Selected Answer: D**

Cybersecurity due diligence is the process of anticipating, identifying, and addressing cyber risks across a company's network ecosystem.  
upvoted 3 times

🗨️ **isidrogg** 3 years, 2 months ago

Page29 on <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf>

The incident response team should work quickly to analyze and validate each incident, following a predefined process and documenting each step taken. When the team believes that an incident has occurred, the team should rapidly perform an initial analysis to determine the incident's scope, such as which networks, systems, or applications are affected; who or what originated the incident; and how the incident is occurring (e.g., what tools or attack methods are being used, what vulnerabilities are being exploited). The initial analysis should provide enough information for the team to prioritize subsequent activities, such as containment of the incident and deeper analysis of the effects of the incident.  
upvoted 1 times

🗨️ **Franky4** 3 years, 6 months ago

"Decision-making" comes up in NIST 800-600r2 in the Containment section, as well as the term "appropriate strategy" similar to "appropriate course of action" as written in the question.

"Organizations should create separate containment strategies for each major incident type, with criteria documented clearly to facilitate --decision-making----. Criteria for determining the appropriate strategy include...."  
upvoted 3 times

🗨️ **halamah** 3 years, 7 months ago

a is correct „since rapid response should be as the first step not after gather and detict



upvoted 2 times

  **BlackDealth** 3 years, 11 months ago

Decision making is correct answer

upvoted 3 times

One of the objectives of information security is to protect the CIA of information and systems.

What does CIA mean in this context?

- A. confidentiality, identity, and authorization
- B. confidentiality, integrity, and authorization
- C. confidentiality, identity, and availability
- D. confidentiality, integrity, and availability

**Suggested Answer: D**

Community vote distribution

D (100%)

🗳️ 👤 **[Removed]** 8 months, 2 weeks ago

This is from the CIA Triad model, which stands for confidentiality, integrity, and availability. For those that don't want to confuse this with that clandestine agency by the same initials, it is also referred to as the AIC Triad or availability, integrity, and confidentiality.

upvoted 1 times

🗳️ 👤 **drdecker100** 9 months, 1 week ago

**Selected Answer: D**

Confidentiality refers to the protection of sensitive information from unauthorized access or disclosure. This includes protecting the privacy of individuals and sensitive business information from unauthorized access or theft.

Integrity refers to the protection of information from unauthorized modification or destruction. This ensures that the information is accurate and complete, and that it is not tampered with in any way.

Availability refers to the ability of authorized users to access information and systems when they need to. This includes ensuring that systems and information are always accessible and functioning properly.

upvoted 1 times

🗳️ 👤 **kenprewitt** 9 months, 2 weeks ago

**Selected Answer: D**

This is from the CIA Triad model, which stands for confidentiality, integrity, and availability. For those that don't want to confuse this with that clandestine agency by the same initials, it is also referred to as the AIC Triad or availability, integrity, and confidentiality.

upvoted 1 times

🗳️ 👤 **msg01** 1 year, 7 months ago

**Selected Answer: D**

correct

upvoted 1 times

🗳️ 👤 **PrettyMs** 1 year, 7 months ago

The correct answer is D

upvoted 1 times

🗳️ 👤 **ahmeds113** 1 year, 8 months ago

D is the correct response

upvoted 1 times

🗳️ 👤 **WISDOM2080** 1 year, 10 months ago

D is the correct response

upvoted 1 times

🗳️ 👤 **Yulkata** 1 year, 11 months ago

D is the correct answer.

Check the CIA Triad for a reference.



upvoted 1 times

🗳️ 👤 **cy\_analyst** 2 years, 9 months ago

Selected Answer: D

D for correct

upvoted 1 times

  **Sarge** 3 years, 4 months ago

Selected Answer: D

D is correct


upvoted 1 times

  **tor\_nana** 3 years, 5 months ago

D is wrong

A is correct :p

upvoted 1 times

  **PanteLa\_26** 3 years, 5 months ago

A is incorrect, D is correct.

upvoted 3 times

  **halamah** 3 years, 7 months ago

d is correct

upvoted 2 times

  **Leo\_Visser** 4 years ago

Information security's primary focus is the balanced protection of the confidentiality, integrity, and availability of data (also known as the CIA triad) while maintaining a focus on efficient policy implementation, all without hampering organization productivity.

(source: [https://en.wikipedia.org/wiki/Information\\_security](https://en.wikipedia.org/wiki/Information_security))

So D is correct

upvoted 4 times

What is rule-based detection when compared to statistical detection?

- A. proof of a user's identity
- B. proof of a user's action
- C. likelihood of user's action
- D. falsification of a user's identity

**Suggested Answer: B**

Community vote distribution

B (100%)

🗳️ 👤 **Leo\_Visser** Highly Voted 🏆 4 years ago

A and D are not right because both detections have nothing to do with identity.

C is incorrect as statistical detection would concern with the likelihood so B is the correct answer.

upvoted 9 times

🗳️ 👤 **drdecker100** Most Recent 🕒 9 months, 1 week ago

**Selected Answer: B**

The correct answer is B. Proof of a user's action.

Statistical detection uses statistical algorithms and machine learning techniques to analyze patterns of behavior and determine the likelihood of a particular action being a security threat. But this likelihood can be used to determine whether an action was performed by a specific user, i.e. to prove the action was performed by the user. On the other hand, rule-based detection uses predefined rules to determine if a particular action is a security threat

upvoted 2 times

🗳️ 👤 **msg01** 1 year, 7 months ago

**Selected Answer: B**

proof of a user's action

upvoted 1 times

🗳️ 👤 **PrettyMs** 1 year, 7 months ago

B. Proof of a user's actions

upvoted 1 times

🗳️ 👤 **WISDOM2080** 1 year, 10 months ago

B. proof of a user's action

upvoted 1 times

🗳️ 👤 **Sarge** 3 years, 4 months ago

**Selected Answer: B**

B is correct

upvoted 2 times

🗳️ 👤 **halamah** 3 years, 7 months ago

B IS CORRECT

upvoted 2 times

An engineer configured regular expression ".\*\.[Dd][Oo][Cc][Xx][Ll][Ss][Pp][Pp][Tt] HTTP/1.[01]" on Cisco ASA firewall. What does this regular expression do?

- A. It captures .doc, .xls, and .pdf files in HTTP v1.0 and v1.1.
- B. It captures documents in an HTTP network session.
- C. It captures Word, Excel, and PowerPoint files in HTTP v1.0 and v1.1.
- D. It captures .doc, .xls, and .ppt files extensions in HTTP v1.0.

**Suggested Answer:** C

Community vote distribution

C (100%)

🗨️ 👤 **ImGonnaPassIt** 6 months, 2 weeks ago

**Selected Answer: A**

Hold on, bad guys may put anything into an .doc file. This is just ext. You can change it while keeping the content unchanged. Why not A?  
upvoted 3 times

🗨️ 👤 **kenbrewitt** 1 year ago

**Selected Answer: C**

Pretty self-explanatory, .doc is Word, .xls is Excel, and .ppt is Powerpoint and the two versions of HTTP  
upvoted 3 times

Which process is used when IPS events are removed to improve data integrity?

- A. data availability
- B. data normalization
- C. data signature
- D. data protection

**Suggested Answer: B**



Community vote distribution

B (100%)

  **Leo\_Visser** Highly Voted 4 years ago

By using data normalization duplicate data is removed and the overall memory/storage impact is reduced. This will make the data actionable. It's debatable if it really helps with the integrity of the data, but you could argue by removing the duplicates the data can be matched better with timestamps from other data sources in a forensic investigation.

So answer B is correct  
upvoted 12 times

  **affulinuha** 3 years, 10 months ago  
thank you for your explanation! it helps us to understanding more  
upvoted 2 times


  **anonymous1966** Highly Voted 9 months, 1 week ago

"B" is correct

Data normalization is the process of capturing, storing, and analyzing data (security-related events, in this case) so that it exists in only one form. One of the main goals of data normalization is to purge redundant data while maintaining data integrity. The normalized data is protected by making sure that any manifestation of the same data elsewhere is only making a reference to the data that is being stored.

Intrusion prevention systems (IPSs) focus on throughput for the most rapid and optimal inline performance. While doing so, in most cases, it is impossible for full normalization to take place. Traditional IPS devices often rely on shortcuts that only implement partial normalization and partial inspection. However, this increases the risk of evasions. Fragmentation handling is an example of such an evasion.

Cisco CyberOps Associate CBROPS 200-201 Official Cert Guide  
By Omar Santos  
upvoted 5 times

  **RolandoFiee** Most Recent 9 months, 1 week ago

Selected Answer: B

B is correct

Intrusion prevention systems (IPSs) focus on throughput for the most rapid and optimal inline performance. While doing so, in most cases, it is impossible for full normalization to take place. Traditional IPS devices often rely on shortcuts that only implement partial normalization and partial inspection  
upvoted 1 times

  **drdecker100** 9 months, 1 week ago

Selected Answer: B

The correct answer is B. Data normalization.

Data normalization is the process of organizing data in a database so that it is consistent and easily manageable. In the context of IPS events, data normalization refers to the process of removing redundant or unnecessary data to improve data integrity. By removing duplicates or inconsistent data, it ensures that the data stored is accurate and up-to-date.

The other options are incorrect because they do not accurately describe the process of removing IPS events to improve data integrity:

A. Data availability refers to the ability to access and retrieve data when it is needed.

C. Data signature refers to a unique identifier that is attached to data to verify its authenticity and integrity.

D. Data protection refers to the measures taken to secure and protect data from unauthorized access or loss.

So, the correct answer is B. Data normalization.



upvoted 1 times

  **kenprewitt** 1 year ago

**Selected Answer: B**

B. data normalization

upvoted 1 times

  **msg01** 1 year, 7 months ago

**Selected Answer: B**

data normalization

upvoted 2 times

  **PrettyMs** 1 year, 7 months ago

B. Data normalization

upvoted 1 times

  **WISDOM2080** 1 year, 10 months ago

B. data normalization

upvoted 1 times

  **Uzumaki\_Aliyy** 2 years, 10 months ago

**Selected Answer: B**

Data Normalization is correct B

upvoted 1 times

  **halamah** 3 years, 7 months ago

B IS CORRECT

upvoted 1 times

An analyst is investigating an incident in a SOC environment.  
Which method is used to identify a session from a group of logs?

- A. sequence numbers
- B. IP identifier
- C. 5-tuple
- D. timestamps

**Suggested Answer: C**

Community vote distribution

C (100%)

🗳️ 👤 **Proctored\_Expert** 9 months, 1 week ago

**Selected Answer: C**

In a security operations center (SOC) environment, one method that could be used to identify a session from a group of logs is the use of a 5-tuple. A 5-tuple consists of five pieces of information that can be used to identify a specific network session: the source IP address, source port, destination IP address, destination port, and protocol. By using this information, an analyst can identify a specific session from a group of logs and track its progress through the system. Other methods that could be used to identify a session from a group of logs include the use of sequence numbers, timestamps, or IP identifiers.

upvoted 4 times

🗳️ 👤 **kenbrewitt** 1 year ago

**Selected Answer: C**

5-tuple

upvoted 1 times

🗳️ 👤 **036e554** 1 year ago

The 5-tuple consists of five values: source IP address, source port, destination IP address, destination port and transport protocol. By examining the 5-tuple, analyst can determine the sequence events within a session and identify logs related to the session.

Together these five values uniquely identify a network session, by examining these attributes within a log data, an analyst can pinpoint and correlate activities related to a specific session, aiding in incident investigation within a SOC environment.

upvoted 3 times

🗳️ 👤 **msg01** 1 year, 7 months ago

**Selected Answer: C**

5- tuple

upvoted 1 times

🗳️ 👤 **PrettyMs** 1 year, 7 months ago

C. 5-tuple

upvoted 1 times

🗳️ 👤 **WISDOM2080** 1 year, 10 months ago

C . 5-tuple

upvoted 1 times

🗳️ 👤 **Yulkata** 1 year, 11 months ago

**Selected Answer: C**

The 5-Tuple, on first place, is a method, which matches the question. Second of all, with the help of 5-Tuple methodology, we can easily filter out logs based on the main elements of the method mentioned.

upvoted 1 times

🗳️ 👤 **IanR7** 2 years, 2 months ago

I actually think it's A. My logic being the question is to identify a session, surely a sequence number is unique. If the same computer connected to the same service a number of times they would have exactly the same 5-Tuple. So there is no way to identify a single session without also say a timestamp or a sequence number ?

upvoted 1 times



🗨️ 👤 **Eng\_ahmedyoussef** 2 years, 9 months ago

5-tuple is the correct answer as shown in given answer.

upvoted 1 times

🗨️ 👤 **SecurityGuy** 3 years, 4 months ago

A 5-tuple refers to a set of five different values that comprise a Transmission Control Protocol/Internet Protocol (TCP/IP) connection.

1. Layer 4 Protocol
2. Source IP address
3. Destination IP address
4. Source Port Number
5. Destination Source Port Number

upvoted 4 times

🗨️ 👤 **halamah** 3 years, 7 months ago

C IS CORRECT

upvoted 1 times

🗨️ 👤 **anonymous1966** 3 years, 9 months ago

"C" is correct.

Traditional firewalls typically provide security event logs that are mostly based on the 5-tuple.

A TCP session is a sequence of sockets with the same IP addresses, ports and protocol.

upvoted 4 times

🗨️ 👤 **germx** 4 years, 2 months ago

A -> Sequence Numbers

upvoted 2 times

🗨️ 👤 **Sun2sun** 3 years ago

How come A? Where is your evidence???

upvoted 1 times

🗨️ 👤 **beowolf** 4 years, 1 month ago

Read the question, which method?

sequence numbers is not a method. Given answer is correct

upvoted 7 times

What is a difference between SOAR and SIEM?

- A. SOAR platforms are used for threat and vulnerability management, but SIEM applications are not
- B. SIEM applications are used for threat and vulnerability management, but SOAR platforms are not
- C. SOAR receives information from a single platform and delivers it to a SIEM
- D. SIEM receives information from a single platform and delivers it to a SOAR

**Suggested Answer: A**

Community vote distribution



**Leo\_Visser** Highly Voted 4 years ago

Platforms based on SIEM (security information and event management) technology offer visibility and meaningful insights by collecting, aggregating, and analyzing information from different sources.

An upcoming platform in the security industry is based on SOAR (security orchestration, automation, and response) technology. SOAR platforms are similar to SIEMs in that they aggregate, correlate, and analyze alerts. However, SOAR technology goes a step further by integrating threat intelligence and automating incident investigation and response workflows based on playbooks developed by the security team.

Source: <https://www.cisco.com/c/en/us/products/security/what-is-a-security-platform.html#~types-of-security-platforms>

So answer A is correct

upvoted 15 times

**anonymous1966** Highly Voted 3 years, 9 months ago

"A" is correct

Unlike traditional SIEM platforms, SOAR solutions can also be used for threat and vulnerability management, security incident response, and security operations automation.

Example of products:

Log collection (SolarWinds Security Event Manager) -----> SIEM (IBM QRadar) -----> SOAR (IBM Resilient)

upvoted 8 times

**Hellome123** Most Recent 6 months, 1 week ago

**Selected Answer: D**

SIEM (Security Information and Event Management):

Primary Function: Collects, stores, and analyzes security event logs from various systems to detect threats, provide alerts, and help security teams with incident investigation.

Purpose: SIEM is focused on monitoring, logging, and event correlation. It helps with real-time threat detection and incident response by aggregating logs and providing insights based on the collected data.

SOAR (Security Orchestration, Automation, and Response):

Primary Function: Automates and orchestrates the security response process. It helps security teams respond to incidents quickly by automating tasks like blocking IP addresses, isolating systems, and executing predefined playbooks.

Purpose: SOAR is used to streamline workflows, automate repetitive actions, and integrate with various security tools (including SIEM) to ensure rapid and coordinated responses to incidents.

upvoted 1 times

**3000bd6** 7 months, 2 weeks ago

**Selected Answer: D**

I think the correct answer is D

upvoted 1 times

**msg01** 1 year, 7 months ago

**Selected Answer: A**

it is correct

upvoted 2 times

🗨️ 👤 **Hazem1234u** 1 year, 7 months ago

**Selected Answer: A**

"Unlike traditional SIEM platforms, SOAR solutions can also be used for threat and vulnerability management, security incident response, and security operations automation." This sentence is from the Official CertGuide book. pg 461 in the Tip box  
upvoted 3 times

🗨️ 👤 **Faio** 1 year, 8 months ago

The answer is D: but how can you say that this answer is right: SOAR platforms are used for threat and vulnerability management, but SIEM applications are not. So what is SIEM used for to peel potatoes?  
But who gave you these answers?  
upvoted 2 times

🗨️ 👤 **WISDOM2080** 1 year, 10 months ago

A. SOAR platforms are used for threat and vulnerability management, but SIEM applications are not  
upvoted 1 times

🗨️ 👤 **Topsecret** 1 year, 11 months ago

**Selected Answer: D**

D is the right answer  
upvoted 1 times

🗨️ 👤 **ethhacker** 1 year, 10 months ago

D is so wrong  
upvoted 1 times

🗨️ 👤 **sometacos** 2 years, 1 month ago

SIEMS are used for logging entry by applications, endpoints and servers, and makes a nice list for a tech to review,  
A SOAR go a step further by responding to security incidents  
upvoted 2 times

🗨️ 👤 **alhamry** 2 years, 2 months ago

The best answer is A. SOAR (Security Orchestration, Automation, and Response) platforms are used for threat and vulnerability management, while SIEM (Security Information and Event Management) applications are primarily used for log and event management. SOAR platforms integrate with SIEM systems to receive security event data and initiate automated responses based on defined playbooks.  
upvoted 1 times

🗨️ 👤 **drdecker100** 2 years, 4 months ago

**Selected Answer: B**

I think the correct answer is B.

A. SOAR platforms are used for threat and vulnerability management, but SIEM applications are not - This statement is not entirely accurate. SIEM applications are also used for threat and vulnerability management.

C. SOAR receives information from a single platform and delivers it to a SIEM - This statement is incorrect because SOAR platforms can integrate with multiple security tools, not just a single platform.

D. SIEM receives information from a single platform and delivers it to a SOAR - This statement is incorrect because SIEM applications collect and analyze security-related data from multiple sources, not just a single platform.

So, only option B correctly describes the relationship between SIEM and SOAR, where SIEM is used for threat and vulnerability management while SOAR is not.  
upvoted 2 times

🗨️ 👤 **Uzumaki\_Aliyy** 2 years, 10 months ago

**Selected Answer: A**

Correct Answer is A: SIEM vs SOAR - In short, SIEM aggregates and correlates data from multiple security systems to generate alerts while SOAR acts as the remediation and response. "Note SIEM from multiple security systems"  
upvoted 4 times

🗨️ 👤 **halamah** 3 years, 7 months ago

A IS CORRECT ,SOAR USE TO IDENTIFY AND MITIGATE THE VULNERABILITY IT CAN RESPONSE ,,,SIEM ONLY LOG MANAGMENT AND SECURITY MONITORING

upvoted 2 times

What is the difference between mandatory access control (MAC) and discretionary access control (DAC)?

- A. MAC is controlled by the discretion of the owner and DAC is controlled by an administrator
- B. MAC is the strictest of all levels of control and DAC is object-based access
- C. DAC is controlled by the operating system and MAC is controlled by an administrator
- D. DAC is the strictest of all levels of control and MAC is object-based access

**Suggested Answer: B**

Community vote distribution

B (100%)

🗳️ 👤 **Leo\_Visser** Highly Voted 🏆 4 years ago

B is correct, MAC is considered the strictest level of access control where information is classified in levels and users are given certain levels. With DAC the permissions are tied to an object and they are set by the owner.  
upvoted 11 times

🗳️ 👤 **drdecker100** Most Recent 🔍 9 months, 1 week ago

**Selected Answer: B**

The correct answer is B. MAC is the strictest of all levels of control and DAC is object-based access.

Mandatory Access Control (MAC) is a security mechanism in which the access to objects is restricted based on predefined rules established by an administrator or the system. These rules take precedence over the user's wishes or personal preferences.

Discretionary Access Control (DAC) is a security mechanism in which the owner of an object, such as a file or a process, decides who can access it and what they can do with it. The access is based on the discretion of the object's owner.

So, in summary, MAC is more restrictive and controlled by rules, while DAC is based on the discretion of the object owner.  
upvoted 4 times

🗳️ 👤 **WISDOM2080** 1 year, 10 months ago

B. MAC is the strictest of all levels of control and DAC is object-based access  
upvoted 2 times

🗳️ 👤 **Eng\_ahmedyoussef** 2 years, 9 months ago

B is correct  
upvoted 1 times

🗳️ 👤 **halamah** 3 years, 7 months ago

B IS CORRECT  
upvoted 1 times

What is the practice of giving employees only those permissions necessary to perform their specific role within an organization?

- A. least privilege
- B. need to know
- C. integrity validation
- D. due diligence

**Suggested Answer: A**

*Community vote distribution*

A (100%)

🗳️ 👤 **WISDOM2080** 10 months ago

A . least privilege  
upvoted 1 times

🗳️ 👤 **drdecker100** 1 year, 4 months ago

**Selected Answer: A**

The practice of giving employees only the necessary permissions to perform their specific role within an organization is called "least privilege". This is an important concept in information security because it reduces the risk of unauthorized access to sensitive information and systems. By giving employees the minimum amount of privileges they need to do their job, they are less likely to accidentally cause harm or intentionally misuse the information or systems they have access to. This helps to increase overall security and reduce the risk of security incidents.

upvoted 3 times

🗳️ 👤 **halamah** 2 years, 7 months ago

A IS CORRECT  
upvoted 1 times

🗳️ 👤 **Leo\_Visser** 3 years ago

Answer A is correct  
upvoted 1 times

What is the virtual address space for a Windows process?

- A. physical location of an object in memory
- B. set of pages that reside in the physical memory
- C. system-level memory protection feature built into the operating system
- D. set of virtual memory addresses that can be used

**Suggested Answer: D**

Community vote distribution

D (100%)

  **DPRamone** Highly Voted 4 years ago  
D is correct.

"The range of virtual addresses that is available to a process is called the virtual address space for the process",  
upvoted 7 times

  **anonymous1966** Highly Voted 9 months, 1 week ago  
"D" is correct (for the certification exam)

There is an exactly same question in book (chap 11):

13. What is a virtual address space in Windows?

- A - The physical memory allocated for processes
- B - A temporary space for processes to execute
- C - The set of virtual memory addresses that references the physical memory object a process is permitted to use
- D - The virtual memory address used for storing applications



Correct answer:



C. A virtual address space in Windows is the set of virtual memory addresses that references the physical memory object a process is permitted to use.



Cisco CyberOps Associate CBROPS 200-201 Official Cert Guide

By Omar Santos

upvoted 6 times

  **Andre70** Most Recent 1 year, 2 months ago  
Selected Answer: D  
is correct  
upvoted 1 times

  **WISDOM2080** 1 year, 10 months ago  
B. set of virtual memory addresses that it can use  
upvoted 1 times

  **drdecker100** 2 years, 4 months ago  
Selected Answer: D  
The answer is D. set of virtual memory addresses that can be used.

In a Windows operating system, each process has its own virtual address space, which is a range of virtual memory addresses that can be used by the process. This virtual address space provides an abstraction layer between the process and the physical memory, allowing the process to access memory as if it were contiguous and not shared with other processes. The virtual addresses are then translated to physical addresses by the operating system's memory management hardware.  
upvoted 1 times

  **Uzumaki\_Aliyy** 2 years, 10 months ago

Correct Answer D: the set of virtual memory addresses that it can use

upvoted 1 times

🗨️ 👤 **halamah** 3 years, 7 months ago

D IS CORRECT

upvoted 1 times

🗨️ 👤 **pmackin124** 3 years, 11 months ago

The virtual address space for a process is the set of virtual memory addresses that it can use. The address space for each process is private and cannot be accessed by other processes unless it is shared. Answer is D .

upvoted 2 times

🗨️ 👤 **cyberchick** 3 years, 11 months ago

The virtual address space for a process is the set of virtual memory addresses that it can use. The address space for each process is private and cannot be accessed by other processes unless it is shared.

upvoted 1 times

🗨️ 👤 **xoe123** 4 years ago

A virtual address space in Windows is the set of virtual memory addresses that references the physical memory object a process is permitted to use.

upvoted 2 times

🗨️ 👤 **Leo\_Visser** 4 years ago

Should be answer C

Virtual address space allows for process isolation and makes sure processes can't access each others memory (easily). So this should be considered a security measure. And it's also build in on OS level so that why C is correct. Answer D is what an application will get when it's using virtual address space but it's not a definition of the principle.

See also: [https://en.wikipedia.org/wiki/Virtual\\_address\\_space](https://en.wikipedia.org/wiki/Virtual_address_space)

upvoted 2 times



Which security principle is violated by running all processes as root or administrator?

- A. principle of least privilege
- B. role-based access control
- C. separation of duties
- D. trusted computing base

**Suggested Answer: A**

Community vote distribution

A (100%)

🗳️ 👤 **SecurityGuy** 9 months, 1 week ago

**Selected Answer: A**

Least Privilege vs. Separation of Duties

- "Separation of Duties" has to do with splitting tasks among employees to reduce the chance of one employee committing fraud.
- "Least Privilege" is when you only provide employees with the account privileges they need to complete their work.
- The principle of least privilege can support the separation of duties.

upvoted 2 times

🗳️ 👤 **drdecker100** 9 months, 1 week ago

**Selected Answer: A**

The security principle violated by running all processes as root or administrator is the "principle of least privilege." The principle of least privilege states that users and applications should only have the minimum permissions required to perform their necessary tasks, and no more. By running all processes as the root or administrator account, all processes are given full permissions, which could pose a security risk if a malicious process is executed.

upvoted 2 times

🗳️ 👤 **WISDOM2080** 1 year, 10 months ago

A. principle of least privilege

upvoted 1 times

🗳️ 👤 **SecurityGuy** 2 years, 7 months ago

Least Privilege vs. Separation of Duties

- "Separation of Duties" has to do with splitting tasks among employees to reduce the chance of one employee committing fraud.
- "Least Privilege" is when you only provide employees with the account privileges they need to complete their work.
- The principle of least privilege can support the separation of duties.

<https://www.cubcyber.com/what-is-the-difference-between-separation-of-duties-and-least-privilege#:~:text=Least%20Privilege%20vs%20Separation%20of,need%20to%20complete%20their%20work.>

upvoted 1 times

🗳️ 👤 **Kokain** 3 years, 2 months ago

A is correct

upvoted 1 times

🗳️ 👤 **[Removed]** 3 years, 4 months ago

page 73 of book talks about separation of duties, where 2 people in an organization can not have rights to the same thing.

upvoted 1 times

🗳️ 👤 **halamah** 3 years, 7 months ago

A IS CORRECT

upvoted 1 times

🗳️ 👤 **Leo\_Visser** 4 years ago

You could argue that A, B and C are all violated (but that would be very nitpicky). But principle of least privileges would surely be the right answer here.

upvoted 2 times

What is the function of a command and control server?

- A. It enumerates open ports on a network device
- B. It drops secondary payload into malware
- C. It is used to regain control of the network after a compromise
- D. It sends instruction to a compromised system

**Suggested Answer: D**

Community vote distribution

D (100%)


 **drdecker100** Highly Voted 1 year, 4 months ago

**Selected Answer: D**

The function of a command and control (C2) server is to send instructions to a compromised system, also known as a bot or a zombie. Once a system is compromised by malware such as a botnet, the C2 server acts as a central point of control for the attacker to send commands to the compromised systems. These commands could include downloading additional malware or executing specific commands on the compromised system, such as launching a distributed denial-of-service (DDoS) attack or stealing sensitive information.

Enumerating open ports on a network device is a network scanning technique that is not directly related to the function of a C2 server. Dropping secondary payloads into malware may be a function of a specific type of malware, but it is not a primary function of a C2 server. Regaining control of a network after a compromise is typically done through incident response procedures and is not a function of a C2 server.

upvoted 6 times

 **Leo\_Visser** Highly Voted 3 years ago

B could be considered correct but in the attack kill chain the malware is used to get access to the system. The command and Control server is then used to get "hand on the keyboard" and from there start performing actions. So answer D is the correct answer.

See also: [https://en.wikipedia.org/wiki/Kill\\_chain#Attack\\_phases\\_and\\_countermeasures](https://en.wikipedia.org/wiki/Kill_chain#Attack_phases_and_countermeasures)

upvoted 6 times

 **WISDOM2080** Most Recent 10 months ago

D. It sends instruction to a compromised system

upvoted 1 times

 **kyle942** 1 year, 9 months ago

page 546, Santos, listening to a beacon from the target.

upvoted 1 times

 **halamah** 2 years, 7 months ago

D IS CORRECT „THROUGH CALLOUT CONNECTION

upvoted 1 times

What is the difference between deep packet inspection and stateful inspection?

- A. Deep packet inspection is more secure than stateful inspection on Layer 4
- B. Stateful inspection verifies contents at Layer 4 and deep packet inspection verifies connection at Layer 7
- C. Stateful inspection is more secure than deep packet inspection on Layer 7
- D. Deep packet inspection allows visibility on Layer 7 and stateful inspection allows visibility on Layer 4

**Suggested Answer:** D

Community vote distribution

D (100%)

🗨️ 👤 **Leo\_Visser** Highly Voted 👍 4 years ago

Answer D is correct

Deep packet operates on layer 7 while statefull operates on layer 4 so A and C are incorrect as the methodes don't work on the same layer. B is incorrect because statefull doesn't do anything with contents.

upvoted 7 times

🗨️ 👤 **drdecker100** Most Recent ⌚ 9 months, 1 week ago

**Selected Answer: D**

The main difference between deep packet inspection and stateful inspection is the layer of the network stack at which they operate.

Stateful inspection works at the transport layer (Layer 4) of the network stack, and it verifies that the contents of each packet are allowed based on the state of the connection. It does this by keeping track of the state of each connection, and only allowing packets that match an established connection to pass through. Stateful inspection can provide basic security against network attacks, such as denial-of-service attacks and spoofing attacks.

Deep packet inspection, on the other hand, operates at the application layer (Layer 7) of the network stack. It inspects the contents of each packet in detail, looking for specific application-level information such as URLs, keywords, or file types. This allows it to identify and block specific types of traffic, such as malware or unwanted applications.

upvoted 3 times

🗨️ 👤 **WISDOM2080** 1 year, 10 months ago

D. Deep packet inspection allows visibility on Layer 7 and stateful inspection allows visibility on Layer 4

upvoted 1 times

🗨️ 👤 **u170who** 2 years, 10 months ago

**Selected Answer: D**

Packet inspection does not verify connections, it inspects them, that's why D is correct and B is not.

upvoted 2 times

🗨️ 👤 **halamah** 3 years, 7 months ago

D IS CORRECT LAYER 7 IS THE SITE TO SITE PROVIDE APPLICATION CONNECTION  
STATEFUL /LAYER 4

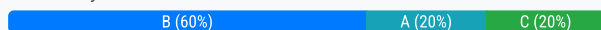
upvoted 1 times

Which evasion technique is a function of ransomware?

- A. extended sleep calls
- B. encryption
- C. resource exhaustion
- D. encoding

**Suggested Answer: B**

Community vote distribution



**alhamry** Highly Voted 2 years, 1 month ago

The correct answer is B. encryption.

Ransomware is a type of malware that encrypts a victim's files and demands payment in exchange for the decryption key. Encryption is the primary evasion technique used by ransomware to avoid detection and protect the malicious code from analysis or reverse-engineering. The other options listed as evasion techniques are not specific to ransomware.

upvoted 8 times

**drdecker100** Most Recent 9 months, 1 week ago

**Selected Answer: B**

The other options are not specific to ransomware. For example, extended sleep calls are used in a variety of malicious software to slow down the execution of the malware, resource exhaustion is used to overload systems and cause them to crash, and encoding is used to obfuscate payloads. B - encryption is the correct answer because ransomware often encrypts the data of an infected system and demands payment in exchange for the decryption key. This encryption technique is a key aspect of the ransomware threat and is used to evade detection and make it difficult for organizations to recover their data.

upvoted 2 times

**dunno\_** 9 months, 1 week ago

**Selected Answer: B**

The primary evasion technique used by ransomware is encryption. Ransomware encrypts the victim's files, making them inaccessible until a ransom is paid. This encryption is not only a means to hold the data hostage but also serves as an evasion technique because it prevents the data from being easily analyzed or recovered without the decryption key.

While extended sleep calls can be used by some malware for evasion, encryption is the hallmark technique of ransomware.

The Correct answer seems to be : B

upvoted 2 times

**Andre70** 1 year, 2 months ago

**Selected Answer: A**

Encryption is not an evasion technique. It is the primary function of ransomware. The evasion is the extended sleep, in my opinion

upvoted 1 times

**Coffeezw** 8 months, 2 weeks ago

The provided answer B is correct, the question asked for a function of Ransomware from the listed evasion techniques(answers).

upvoted 1 times

**WISDOM2080** 1 year, 10 months ago

B. encryption

upvoted 2 times

**Nav1999** 2 years, 2 months ago

I go with B

upvoted 3 times

**ASIDIBE** 2 years, 5 months ago

The correct is B

upvoted 2 times

🗨️ 👤 **MaliDong** 2 years, 8 months ago

**Selected Answer: C**

I go with C.

upvoted 1 times

🗨️ 👤 **MaliDong** 2 years, 8 months ago

typo, B is correct.

upvoted 1 times

🗨️ 👤 **joseph267** 2 years, 11 months ago

encryption is not used as an evasion technique for ransomware but... it is for other attacks such as trojans or malicious payloads to hide from security mechanisms

in ransomware encryption is used as the method to ask for a ransom

upvoted 1 times

🗨️ 👤 **halamah** 3 years, 7 months ago

B IS CORRECT

upvoted 2 times

🗨️ 👤 **vprollc** 3 years, 10 months ago

The study guide lists the following as evasion techniques against IDS and IPS devices: Fragmentation, low bandwidth attacks, address spoofing/proxying, pattern change evasion, and encryption. Based on that, I think the answer is correct.

upvoted 4 times

🗨️ 👤 **Leo\_Visser** 4 years ago

I think the question should be "which attack vector is used by ransomware". As most of the answers aren't really evasion techniques.

upvoted 4 times

Overview

Analysis

Policies

Devices

Objects

Content Explorer

Connections > Security Intelligence Events

Intrusions

Files

Hosts

Users

Vulnerabilities

Correlation

Custom

Search

Health

System

Help

Security Intelligence Events

(switch workflow)

Bookmark This Page

Report Designer

Dashboard

View Book

Security Intelligence with Application Details > Table View of Security Intelligence Events

2018-03-02 07:20:20 - 2018-03-07 13:47:20

Search Constraints (Edit Search Serve Search)

Expanding

Disabled Columns

Jump to...

	First Packet	Last Packet	Action	Reason	Initiator IP	Initiator Country	Initiator User	Responder IP	Responder Country	Security Intelligence Category	Ingress Security Zone	Egress Security Zone	Source Port/ICMP Type
2018-03-07 13:42:01	2018-03-07 13:42:01	Sinkhole	DNS Block	10.0.10.75		JERI LABORDE (DCLOUD-SOC-LDAP)	10.110.10.11		DNS Intelligence-CnC	External	Internal	54925 / udp	
2018-03-07 13:42:01	2018-03-07 13:42:01	Sinkhole	DNS Block	10.0.0.100		AMPARO GIVENS (DCLOUD-SOC-LDAP)	10.110.10.11		DNS Intelligence-CnC	External	Internal	54925 / udp	
2018-03-07 13:42:01	2018-03-07 13:42:01	Sinkhole	DNS Block	10.112.10.158		VERNETTA DONNEL (DCLOUD-SOC-LDAP)	192.168.1.153		DNS Intelligence-CnC	External	Internal	54925 / udp	

<< Page 1 of 1 >> | Displaying rows 1-3 of 3 rows

View

Delete

View All

Delete All

Refer to the exhibit. Which two elements in the table are parts of the 5-tuple? (Choose two.)

- A. First Packet
- B. Initiator User
- C. Ingress Security Zone
- D. Source Port
- E. Initiator IP

**Suggested Answer: DE**

Community vote distribution

DE (100%)

**Leo\_Visser** Highly Voted 3 years ago

5-Tuple: The tuple (source IP address, source port, destination IP address, destination port, transport protocol).

source: <https://www.ietf.org/rfc/rfc6146.txt>

So D, E are right answer

upvoted 8 times

**WISDOM2080** Most Recent 10 months ago

D. Source Port

E. Initiator IP

upvoted 2 times

**Eng\_ahmedyoussef** 1 year, 9 months ago

**Selected Answer: DE**

-SOURCE IP /PORT

-DESTINATION IP /PORT

-PROTOCOL

so D and E is Correct Answer

upvoted 2 times

**halamah** 2 years, 7 months ago

CORRECT

SOURCE IP /PORT-DESTINATION IP -PORT /PROTOCOL

upvoted 2 times

DRAG DROP -


Drag and drop the security concept on the left onto the example of that concept on the right.

Select and Place:

Risk Assessment	network is compromised
Vulnerability	lack of an access list
Exploit	configuration review
Threat	leakage of confidential information

Suggested Answer:

Risk Assessment	Threat
Vulnerability	Vulnerability
Exploit	Risk Assessment
Threat	Exploit

 **nataldogomes** Highly Voted 2 years, 9 months ago

network is compromised => Exploit

lack of an access list => Vulnerability

configuration review => Risk Assessment

leakage of confidential information => Threat

upvoted 34 times

 **Leo\_Visser** Highly Voted 2 years, 12 months ago

Answer is incorrect, Exploit and Threat should be switched.

upvoted 16 times

 **Leo\_Visser** 2 years, 12 months ago

Exploit = network is compromised

"[...] exploit means to take advantage of a vulnerability [...] an exploit refers to a tool, typically in the form of source or binary code."

So by taking advantage of the vulnerability the network is compromised.

Vulnerability - lack of an access list

"A vulnerability is any weakness (known or unknown) in a system, process, or other entity that could lead to its security being compromised by a threat."

So not having an ACL could be considered an vulnerability which is then compromised by the threat.

Risk Assessment - configuration review

"risk constitutes a specific vulnerability matched to a specific threat"

So risk assessment work to check for vulnerabilities so doing configuration review matches this.

Threat - leakage of confidential information

"A threat is any action that could disrupt, harm, destroy, or otherwise adversely affect an information system."

This will negatively affect the information system, none of the other options does this so this should be the threat.

upvoted 20 times

 **WISDOM2080** Most Recent 10 months ago



Vulnerability ==> Lack of an access list  
Exploit ==> Network is compromised  
Threat ==> leakage of confidential information  
Risk Assessment ==> Configuration review  
upvoted 2 times

🗨️ 👤 **drdecker100** 1 year, 4 months ago

Network is compromised: An exploit is a specific type of attack or technique that is used to take advantage of a vulnerability in a system or network. If an attacker successfully exploits a vulnerability, they may be able to compromise a network and gain unauthorized access to its resources.

Leakage of confidential information: A threat is any potential danger or risk to the confidentiality, integrity, or availability of a system or network. If confidential information is leaked, it represents a potential threat to the confidentiality of that information, as well as to the reputation and legal liability of the organization that owns it.

upvoted 2 times

🗨️ 👤 **Eng\_ahmedyoussef** 1 year, 9 months ago

Vulnerability ==> Lack of an access list  
Exploit ==> Network is compromised  
Threat ==> leakage of confidential information  
Risk Assessment ==> Configuration review  
upvoted 3 times

🗨️ 👤 **anonymous1966** 2 years, 9 months ago

For me the answer is correct, based on the definitions:

risk assessment

The process of identifying risks to organizational operations. Synonymous with risk analysis.

vulnerability

Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

An exploit is a piece of software, a chunk of data, or a sequence of commands that takes advantage of a bug or vulnerability.

Cyber Threat

Any circumstance or event with the potential to adversely impact organizational operations.

upvoted 3 times

🗨️ 👤 **anonymous1966** 2 years, 9 months ago

Network is compromised by a Cyber Threat  
Lack of an Access List is a Vulnerability of a system  
Risk assessment does Configuration Review  
An Exploit causes a Leakage of confidential information

Answer:

Network is compromised <--> Threat  
Lack of an Access List <--> Vulnerability  
Configuration Review <--> Risk assessment  
Leakage of confidential information <--> Exploit

upvoted 5 times

🗨️ 👤 **adodocletus** 2 years ago

A Threat is a consequence an organization faces when a vulnerability has been exploited.

So the leakage of confidential information is the threat and not the exploit.

upvoted 1 times

🗨️ 👤 **BlackDeath** 2 years, 11 months ago

E, V, R, T

upvoted 7 times

What is the difference between statistical detection and rule-based detection models?

- A. Rule-based detection involves the collection of data in relation to the behavior of legitimate users over a period of time
- B. Statistical detection defines legitimate data of users over a period of time and rule-based detection defines it on an IF/THEN basis
- C. Statistical detection involves the evaluation of an object on its intended actions before it executes that behavior
- D. Rule-based detection defines legitimate data of users over a period of time and statistical detection defines it on an IF/THEN basis

**Suggested Answer: B**

Community vote distribution

B (100%)

🗳️ 👤 **Leo\_Visser** Highly Voted 3 years ago

B is correct. Statistical checks over a period of time to see if it adheres to certain trends. Rulebased just checks for this specific moment.  
upvoted 9 times

🗳️ 👤 **WISDOM2080** Most Recent 10 months ago

A. Threat represents a potential danger that could take advantage of a weakness, while the risk is the likelihood of a compromise or damage of an asset.  
upvoted 1 times

🗳️ 👤 **WISDOM2080** 10 months ago

B. Statistical detection defines legitimate data of users over a period of time and rule-based detection defines it on an IF/THEN basis  
upvoted 1 times

🗳️ 👤 **alhamry** 1 year, 2 months ago

The answer is B. Statistical detection models use mathematical algorithms to define normal user behavior over a period of time, and deviations from this behavior are flagged as potential threats. Rule-based detection models, on the other hand, use a predefined set of rules to identify specific patterns or signatures of known attacks. Rule-based detection models operate on an IF/THEN basis, where if a certain condition is met, a threat is flagged.  
upvoted 1 times

🗳️ 👤 **drdecker100** 1 year, 4 months ago

**Selected Answer: B**

Rule-based detection models use a predefined set of rules to determine whether a particular behavior is normal or anomalous. These rules are typically based on the expected behavior of legitimate users, and are often expressed in an "if-then" format. For example, a rule-based system might flag any attempt to log in to a particular application from an unusual IP address as potentially suspicious.

Statistical detection models, on the other hand, use statistical analysis to identify patterns of behavior that deviate from the norm. These models are often based on machine learning algorithms that analyze large amounts of data to identify normal behavior and then flag any activity that deviates from that norm as potentially suspicious. For example, a statistical detection model might flag any attempt to transfer an unusually large amount of data from a particular user account as potentially suspicious.

upvoted 1 times

🗳️ 👤 **hansamaru** 1 year, 7 months ago

Agreed for B  
upvoted 1 times

🗳️ 👤 **halamah** 2 years, 7 months ago

B IS CORRECT STATIC OVER PERIOD OF TIME  
RULE BASED IDENTIFY POTENTIAL attack  
upvoted 1 times

What is the difference between a threat and a risk?

- A. Threat represents a potential danger that could take advantage of a weakness, while the risk is the likelihood of a compromise or damage of an asset.
- B. Risk represents the known and identified loss or danger in the system, while threat is a non-identified impact of possible risks.
- C. Risk is the unintentional possibility of damages or harm to infrastructure, while the threats are certain and intentional.
- D. Threat is a state of being exposed to an attack or a compromise, while risk is the calculation of damage or potential loss affecting the organization from an exposure.

**Suggested Answer: A**

  **hansamaru** Highly Voted 7 months, 2 weeks ago

Threat : potential danger to an asset

Vulnerability : a weakness in a system could be exploited by a threat

Exploit : mechanism that is used to leverage vulnerability to compromise an asset

Risk : likelihood that a threat will exploit vulnerability of an asset

(A)

upvoted 9 times

  **halamah** Most Recent 1 year, 7 months ago

correct

risk is the likelihood ./threat potential danger

upvoted 2 times

Which attack method intercepts traffic on a switched network?

- A. denial of service
- B. ARP cache poisoning
- C. DHCP snooping
- D. command and control

**Suggested Answer: B**

Community vote distribution

B (100%)

🗳️ 👤 **skysoft** Highly Voted 3 years, 6 months ago

Correct answer: B. ARP cache poisoning

DHCP snooping is a counter measure against attack.

wiki:

In computer networking, ARP spoofing, ARP cache poisoning, or ARP poison routing, is a technique by which an attacker sends (spoofed) Address Resolution Protocol (ARP) messages onto a local area network. Generally, the aim is to associate the attacker's MAC address with the IP address of another host, such as the default gateway, causing any traffic meant for that IP address to be sent to the attacker instead.

upvoted 30 times

🗳️ 👤 **fejec** 2 years, 9 months ago

from cert guide - Chapter 4:

ARP Cache Poisoning

Threat actors can attack hosts, switches, and routers connected to your Layer 2 network by poisoning the ARP caches of systems connected to the subnet and by intercepting traffic intended for other hosts on the subnet.

upvoted 4 times

🗳️ 👤 **ASIDIBE** 1 year, 5 months ago

<https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SXF/native/configuration/guide/swcg/snoodhcp.pdf>

upvoted 1 times

🗳️ 👤 **AhmedAbdalla** Most Recent 8 months, 3 weeks ago

ARP cache poisoning

ARP (Address Resolution Protocol) cache poisoning, also known as ARP spoofing, is an attack method that intercepts traffic on a switched network.

In an ARP cache poisoning attack, an attacker sends forged ARP messages to associate their MAC address with the IP address of another legitimate device on the network. As a result, traffic meant for the legitimate device is redirected to the attacker's system, allowing them to intercept and potentially modify the traffic.

upvoted 1 times

🗳️ 👤 **WISDOM2080** 10 months ago

B . ARP cache poisoning

upvoted 1 times

🗳️ 👤 **Faio** 1 year ago

Correct answer: B

DHCP snooping is a security mechanism used to prevent rogue DHCP (Dynamic Host Configuration Protocol) servers from providing incorrect or malicious IP configuration information to network clients. It does not directly intercept network traffic.

upvoted 1 times

🗳️ 👤 **jiri\_kurka** 1 year, 2 months ago

Selected Answer: B

...Switched network... = OSI Layer 2

ARP operates on Layer 2 to map IP address. Other answers are related to higher OSI Layers.

upvoted 2 times

🗨️ 👤 **drdecker100** 1 year, 4 months ago

**Selected Answer: B**

The attack method that intercepts traffic on a switched network is ARP cache poisoning, which is also known as ARP spoofing or ARP poisoning.

In a switched network, each device maintains an ARP cache that maps IP addresses to MAC addresses. When a device needs to communicate with another device on the same network, it looks up the MAC address in its ARP cache and uses that address to send the packet.

In an ARP cache poisoning attack, the attacker sends fake ARP messages to other devices on the network, claiming to be the owner of a particular IP address. This causes the other devices to update their ARP caches with the attacker's MAC address instead of the actual owner's MAC address. As a result, all traffic intended for the owner of that IP address is instead sent to the attacker, who can intercept and manipulate the traffic.

upvoted 1 times

🗨️ 👤 **ASIDIBE** 1 year, 5 months ago

<https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SXF/native/configuration/guide/swcg/snoodhcp.pdf> read this article for why C and not B is correct

upvoted 1 times

🗨️ 👤 **ASIDIBE** 1 year, 5 months ago

I don't think the correct is C. B is the likest answer.

upvoted 1 times

🗨️ 👤 **ASIDIBE** 1 year, 6 months ago

I choose B because of intercept and MITM attack be the answer was DHCP snooping.

upvoted 1 times

🗨️ 👤 **examtopicsfhrn2** 1 year, 6 months ago

**Selected Answer: B**

B. ARP cache poisoning is the correct answer

upvoted 1 times

🗨️ 👤 **fyticez** 1 year, 8 months ago

**Selected Answer: B**

arp cache poisoning == attack

dhcp snooping == counter-attack

upvoted 1 times

🗨️ 👤 **Eng\_ahmedyoussef** 1 year, 9 months ago

**Selected Answer: B**

B. ARP cache poisoning is the correct answer

upvoted 1 times

🗨️ 👤 **kyle942** 1 year, 9 months ago

The purpose of ARP is to translate between addresses at the data link layer – known as MAC Addresses – and addresses at the network layer, which are typically IP addresses (switch contains routing table), the fix is to enable DHCP snooping.

upvoted 1 times

🗨️ 👤 **Entivo** 1 year, 10 months ago

**Selected Answer: B**

The answer is B - see Skysoft response for explanation.

upvoted 1 times

🗨️ 👤 **adodocletus** 2 years ago

ARP cache poisoning is the correct answer and not C

upvoted 1 times

🗨️ 👤 **Oscar14258** 2 years, 1 month ago

**Selected Answer: B**

DHCP snooping is a countermeasure, not an attack.

upvoted 1 times

🗨️ 👤 **RolandoFiee** 2 years, 4 months ago

**Selected Answer: B**

B is correct

the attacker spoofs Layer 2 MAC addresses to make the devices on a LAN believe that the Layer 2 address of the attacker is the Layer 2 address of its default gateway. This is called ARP poisoning.

Obs:

DHCP snooping is used to prevent rogue DHCP servers on a network.

upvoted 1 times

What does an attacker use to determine which network ports are listening on a potential target device?

- A. man-in-the-middle
- B. port scanning
- C. SQL injection
- D. ping sweep

**Suggested Answer: B**

Community vote distribution

B (100%)

🗨️ 👤 **Leo\_Visser** Highly Voted 👍 3 years ago

"A port scanner is an application designed to probe a server or host for open ports. Such an application may be used by administrators to verify security policies of their networks and by attackers to identify network services running on a host and exploit vulnerabilities."

source: [https://en.wikipedia.org/wiki/Port\\_scanner](https://en.wikipedia.org/wiki/Port_scanner)

So B is the correct answer

upvoted 8 times

🗨️ 👤 **WISDOM2080** Most Recent ⌚ 10 months ago

B. port scanning

upvoted 1 times

🗨️ 👤 **AmirSA92** 2 years, 5 months ago

Selected Answer: B

The answer is B

upvoted 3 times

🗨️ 👤 **halamah** 2 years, 7 months ago

p is correct

upvoted 1 times

What is a purpose of a vulnerability management framework?

- A. identifies, removes, and mitigates system vulnerabilities
- B. detects and removes vulnerabilities in source code
- C. conducts vulnerability scans on the network
- D. manages a list of reported vulnerabilities

**Suggested Answer: A**

Community vote distribution

A (100%)

🗳️ 👤 **Leo\_Visser** Highly Voted 🏆 4 years ago

"Vulnerability management is the "cyclical practice of identifying, classifying, prioritizing, remediating, and mitigating" software vulnerabilities.[1]  
Vulnerability management is integral to computer security and network security, and must not be confused with Vulnerability assessment"

source: [https://en.wikipedia.org/wiki/Vulnerability\\_management](https://en.wikipedia.org/wiki/Vulnerability_management)

So A is the correct answer

upvoted 13 times

🗳️ 👤 **KYHO** Most Recent 🔍 9 months ago

The correct answer is A.

Attack vector refers to the path or means by which the attack is delivered <---

upvoted 1 times

🗳️ 👤 **ashlea** 9 months, 1 week ago

Selected Answer: A

A is the correct answer

upvoted 1 times

🗳️ 👤 **WISDOM2080** 1 year, 10 months ago

A. identifies, removes, and mitigates system vulnerabilities

upvoted 1 times

🗳️ 👤 **sh4dali** 3 years ago

Vulnerability management is the process of identifying, analyzing, prioritizing, and remediating vulnerabilities in software and hardware.

upvoted 1 times

🗳️ 👤 **halamah** 3 years, 7 months ago

a is correct

vulnerability management is internet exposed devices

upvoted 1 times

🗳️ 👤 **eggheadsv** 3 years, 7 months ago

What is a vulnerability management framework?

What is a vulnerability management program framework? ... Vulnerability management programs address today's modern cybersecurity challenges by instituting a comprehensive and continuous process for identifying, classifying, remediating, and mitigating vulnerabilities before attackers can take advantage of them.

So A is the correct answer

upvoted 1 times



A network engineer discovers that a foreign government hacked one of the defense contractors in their home country and stole intellectual property. What is the threat agent in this situation?

- A. the intellectual property that was stolen
- B. the defense contractor who stored the intellectual property
- C. the method used to conduct the attack
- D. the foreign government that conducted the attack

**Suggested Answer: C**

Community vote distribution

D (50%)

C (50%)

  **jlmadvig** Highly Voted 4 years, 2 months ago

I think is C. the method used to conduct the attack



The entity that takes advantage of the vulnerability is known as the malicious actor, and the path used by this actor to perform the attack is known as the threat agent or threat vector.

Source: Official cert Guide Cisco CyberOps Associate CBROPS 200-201

Chapter1: Cybersecurity Fundamentals

Author: Omar Santos

upvoted 21 times

  **Mevijil** 3 years, 4 months ago

This is the correct answer according to the book - page 10. Threat agent refers to the method, threat actor refers to the attacker. Agent and Actor are not synonyms here - the answer is C.

upvoted 4 times

  **Frog\_Man** 10 months, 3 weeks ago

Read the book, page 10 and it is "C".

upvoted 1 times

  **beowolf** 4 years, 1 month ago

threat agent AKA threat actor . Given answer is correct

upvoted 10 times

  **ethhacker** 1 year, 10 months ago

Not the same. Read the book

upvoted 1 times

  **Leo\_Visser** Highly Voted 4 years ago

Threat agent and Threat actor are the same (see [https://itlaw.wikia.org/wiki/Threat\\_agent](https://itlaw.wikia.org/wiki/Threat_agent))

And the threat actor is the organization/person performing the attack. (<https://orangematter.solarwinds.com/2018/07/18/cybersecurity-fundamentals-threat-attack-terminology/>)

So D is the correct answer

upvoted 12 times

  **Chris1971** 2 years, 5 months ago

A threat agent is an active entity motivated to attack our mobile devices and activities. We may identify threat agents as specific organizations or individuals like Anonymous, or we may classify them by goals or methods of operation (MOs). For example, shoplifters are a class of threat agent that attacks retail :

[https://cryptosmith.com/2016/01/31/threat-agents-and-levels-of-](https://cryptosmith.com/2016/01/31/threat-agents-and-levels-of-motivation/#:~:text=A%20threat%20agent%20is%20an%20active%20entity%20motivated,class%20of%20threat%20agent%20that%20attacks%20retail%20)

[motivation/#:~:text=A%20threat%20agent%20is%20an%20active%20entity%20motivated,class%20of%20threat%20agent%20that%20attacks%20retail%20](https://cryptosmith.com/2016/01/31/threat-agents-and-levels-of-motivation/#:~:text=A%20threat%20agent%20is%20an%20active%20entity%20motivated,class%20of%20threat%20agent%20that%20attacks%20retail%20)

upvoted 2 times

 **CyberGrog**  3 months, 2 weeks ago

**Selected Answer: D**

The correct answer is:

D. the foreign government that conducted the attack

Explanation:


A threat agent is an entity responsible for carrying out an attack or exploiting vulnerabilities. In this scenario, the foreign government is the actor responsible for orchestrating the attack and stealing the intellectual property.

Here's why the other options are incorrect:

- A. the intellectual property that was stolen: This is the target or asset, not the threat agent.
- B. the defense contractor who stored the intellectual property: This is the victim or entity impacted by the attack, not the agent causing it.
- C. the method used to conduct the attack: This refers to the attack vector or technique, not the entity executing the attack.

The threat agent is always the actor or group initiating the malicious activity—in this case, the foreign government.

upvoted 1 times

 **Willieearl1k** 3 months, 2 weeks ago

**Selected Answer: D**

Threat Actor = Threat Agent. The term is very similar.

upvoted 1 times

 **ImGonnaPassIt** 6 months, 2 weeks ago

**Selected Answer: C**

According to the book: "The entity that takes advantage of the vulnerability is known as the malicious actor, and the path used by this actor to perform the attack is known as the threat agent or threat vector."

upvoted 1 times

 **Coffeezw** 8 months ago


The correct answer is D, the question didn't specify how the attack was accomplished and it asked what is the threat agent "in this situation?". So D definitely is the correct answer in this context.

upvoted 1 times

 **KYHO** 9 months ago


In this context, the threat agent is the entity responsible for carrying out the attack. A threat agent is the actor or group that intentionally causes harm or poses a risk.

upvoted 1 times

 **Sbonel0** 10 months, 3 weeks ago

The correct answer is D.

upvoted 1 times

 **Frog\_Man** 11 months, 2 weeks ago

D>. External threat agents are individuals or groups that originate from outside the target organization.

upvoted 1 times

 **c79ecd3** 12 months ago

**Selected Answer: D**

Threat agents, also known as threat actors, are individuals or entities that intentionally cause harm or pose a risk to the cyber sphere.

upvoted 1 times

 **fisher004** 1 year, 7 months ago

It should be C. Method used to conduct the attack. In the certguide, a threat agent is the path used by the threat actor to perform an attack

upvoted 1 times

 **Mulema** 1 year, 7 months ago

The answer is D

In cybersecurity, a threat agent is any entity that can exploit vulnerabilities or conduct other damaging activities to a system or organization. This can include individuals, groups, organizations, or even nation-states. Threat agents can be motivated by various factors, such as financial gain, political

ideology, or personal vendettas.

<https://bard.google.com/chat/283439dd3b271707>

upvoted 1 times

🗨️ **jorgeaaq** 1 year, 8 months ago

**Selected Answer: D**

In summary:

A threat is a negative event that can lead to an undesired outcome.

A threat actor is the entity (individual or group) that performs the attack.

A threat agent is the means by which a threat actor carries out an attack.

upvoted 1 times

🗨️ **jorgeaaq** 1 year, 8 months ago

Sorry, Wrong Answer selected... C is correct

upvoted 1 times

🗨️ **Faio** 1 year, 9 months ago

Selected Answer: D

What is a threat agent in cyber security?

An individual or group that acts, or has the power to, exploit a vulnerability or conduct other damaging activities.

The method used to conduct the attack is also not the threat agent, as it is simply a tool used by the threat agent to achieve their goal.

upvoted 1 times

🗨️ **WISDOM2080** 1 year, 10 months ago

D. the foreign government that conducted the attack

upvoted 1 times

🗨️ **Savann** 1 year, 11 months ago

**Selected Answer: C**

Threat Agent = path/method used

upvoted 1 times

🗨️ **Swordfishtaco** 1 year, 12 months ago

**Selected Answer: D**

The threat Agent is the person doing the attack

upvoted 2 times

What is the practice of giving an employee access to only the resources needed to accomplish their job?

- A. principle of least privilege
- B. organizational separation
- C. separation of duties
- D. need to know principle

**Suggested Answer: A**

🗲️ 👤 **036e554** 1 year ago

ANS: A

Least privilege focus on minimizing potential system damage, ensuring that each employee should have minimum resources to perform their task, e.g files, network, application.

While, need to know focus on restricting access to sensitive information like personal data, sensitive data, classified document, and providing them with information they need to know to perform their tasks.

upvoted 2 times

🗲️ 👤 **WISDOM2080** 1 year, 10 months ago

A. principle of least privilege

upvoted 2 times

🗲️ 👤 **cryptonite** 2 years, 1 month ago

The answer is D.

Somewhat related to the principle of least privilege is the concept of "need to know," which means that users should get access only to data and systems that they need to do their job, and no other. (From Cisco Press)

upvoted 1 times

🗲️ 👤 **evra** 3 years, 2 months ago

D is the correct.

The Need-to-know security principle: This principle states that a user shall only have access to the information that their job function requires, regardless of their security clearance level or other approvals.

upvoted 1 times

🗲️ 👤 **halamah** 3 years, 7 months ago

correct

upvoted 1 times

🗲️ 👤 **Leo\_Visser** 4 years ago

See also: <https://www.ciscopress.com/articles/article.asp?p=2783637>

A is the correct answer

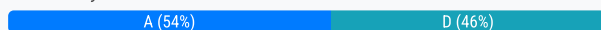
upvoted 4 times

Which metric is used to capture the level of access needed to launch a successful attack?

- A. privileges required
- B. user interaction
- C. attack complexity
- D. attack vector

**Suggested Answer: A**

Community vote distribution



**Torvalds** Highly Voted 4 years, 2 months ago

i Think is "D. attack vector".

Attack Vector ( AV) represents the level of access an attacker needs to have to exploit a vulnerability. It can assume four values: Network, Adjacent, Local and Physical.

Source: Official cert Guide Cisco CyberOps Associate CBROPS 200-201

Chapter7: Introduction to Security Operations Management.

Author: Omar Santos

upvoted 23 times

**Leo\_Visser** 4 years ago

According to cisco:

<https://tools.cisco.com/security/center/resources/understanding-terminology.html#exploitability>

The attack vector metric describes the shortest distance from the attacker to the target. So the privileges required are something else. So A is correct.

upvoted 12 times

**Dunky** 4 years, 1 month ago

There is little difference that I can see in the description of privileges and attack vector <https://www.balbix.com/insights/base-cvss-scores/>

upvoted 1 times

**alocin** Highly Voted 3 years, 8 months ago

According with OFFICIAL Cert Guide Cisco O.Santos, correct is D.

According with tool.cisco.com terminology, correct is A.

Good question ... for me, my opinion, the question means not vector but privileges.

Free interpretation .

upvoted 11 times

**Sbonel0** Most Recent 10 months, 3 weeks ago

A. privileges required

upvoted 3 times

**Sbonel0** 10 months, 3 weeks ago

Privileges Required (PR) is a metric in the Common Vulnerability Scoring System (CVSS), which assesses the level of access or privileges an attacker needs before attempting an attack.

upvoted 1 times

**036e554** 1 year ago

ANS: A

Privilege required is the metric that refers to the level of access an attacker needs to execute an attack

User interaction: This metric assess whether an attack requires a human action to be successful

Attack complexity: It is a metric used to measure how difficult it is for an attacker to successfully exploit a vulnerability or execute attack

Attack Vector: It refers to specific path uses to gain unauthorized access to a system or network

upvoted 2 times

🗨️ 👤 **cevahiroglu** 1 year, 1 month ago

Answer is A. Privileges required: This is a metric that captures the level of access that is required for a successful exploit of the vulnerability.  
upvoted 1 times

🗨️ 👤 **RoBery** 1 year, 5 months ago

A is correct

From official Cisco course:

Privileges required: This is a metric that captures the level of access that is required for a successful exploit of the vulnerability.

Attack vector: This is a metric that reflects the proximity of the threat actor to the vulnerable component. The more remote the threat actor is to the component, the higher the severity. Threat actors close to your network or inside your network are easier to detect and mitigate.

upvoted 1 times

🗨️ 👤 **Max\_DeJaV** 1 year, 9 months ago

**Selected Answer: D**

From Official cert Guide Cisco CyberOps Associate CBROPS 200-201:

The base group defines exploitability metrics that measure how the vulnerability can be exploited, and impact metrics that measure the impact on confidentiality, integrity, and availability. In addition to these two, a metric called scope change (S) is used to convey the impact on systems that are affected by the vulnerability but do not contain vulnerable code.

Exploitability metrics include the following:

- Attack Vector (AV): Represents the level of access an attacker needs to have to exploit a vulnerability. It can assume four values:

- Network (N)

- Adjacent (A)

- Local (L)

- Physical (P)

upvoted 2 times

🗨️ 👤 **WISDOM2080** 1 year, 10 months ago

A . privileges required

upvoted 1 times

🗨️ 👤 **Faio** 1 year, 10 months ago

The answer is A. privileges required.

upvoted 1 times

🗨️ 👤 **Faio** 2 years ago

Correct Answer: A privileges required.

The "attack vector" (D) refers to the path or method used by an attacker to exploit a vulnerability. It describes how the attacker gains access to the target system, but it does not specifically capture the level of access needed to launch the attack.

upvoted 1 times

🗨️ 👤 **KC21** 2 years ago

**Selected Answer: D**

Attack Vector (AV): Represents the level of access an attacker needs to have to exploit a vulnerability. It can assume four values:

- Network (N)

- Adjacent (A)

- Local (L)

- Physical (P)

upvoted 3 times

🗨️ 👤 **KC21** 2 years ago

Privileges Required (PR): Represents the level of privileges an attacker must have to exploit the vulnerability. The values are as follows:

- None (N)

- Low (L)

- High (H)

upvoted 2 times

🗨️ 👤 **slippery31** 2 years ago

Correct ANS=D

upvoted 1 times

🗨️ 👤 **ShammaA** 2 years, 1 month ago

Attack Vector simply is --> a way for attackers to enter the system (exploiting vulnerabilities)

Whilst the question talks about privileges --> answer PRIVILEGE

upvoted 1 times

🗨️ 👤 **slippery31** 2 years, 1 month ago

Correct Answer=D

upvoted 1 times

🗨️ 👤 **Stevens0103** 2 years, 1 month ago

**Selected Answer: A**

Source: <https://contenthub.netacad.com/legacy/CyberOps/1.1/en/index.html#10.2.2.3>

Privileges required – This is a metric that captures the level of access that is required for a successful exploit of the vulnerability.

upvoted 1 times

🗨️ 👤 **alhamry** 2 years, 2 months ago

The best answer is A. privileges required.

"Privileges required" is a metric used in the Common Vulnerability Scoring System (CVSS) to measure the level of access an attacker needs to successfully exploit a vulnerability. The other metrics mentioned, such as user interaction, attack complexity, and attack vector, are also used in CVSS to score the severity of a vulnerability, but they do not specifically measure the level of access required.

upvoted 1 times

🗨️ 👤 **itousattud** 2 years, 3 months ago

**Selected Answer: A**

The correct answer is A. privileges required.

The metric "privileges required" is used to capture the level of access needed to launch a successful attack. This metric refers to the level of permissions or access that an attacker would need to have in order to exploit a vulnerability and carry out an attack.

For example, an attack that requires administrative privileges to execute would have a higher "privileges required" metric than an attack that can be carried out with only user-level permissions. The higher the level of access required, the more difficult the attack is to carry out and the more severe the potential impact.

The other options, user interaction, attack complexity, and attack vector, are also important metrics used in assessing the severity of a vulnerability or attack, but they do not specifically capture the level of access required for a successful attack.

upvoted 2 times

What is the difference between an attack vector and an attack surface?

- A. An attack surface identifies vulnerabilities that require user input or validation; and an attack vector identifies vulnerabilities that are independent of user actions.
- B. An attack vector identifies components that can be exploited; and an attack surface identifies the potential path an attack can take to penetrate the network.
- C. An attack surface recognizes which network parts are vulnerable to an attack; and an attack vector identifies which attacks are possible with these vulnerabilities.
- D. An attack vector identifies the potential outcomes of an attack; and an attack surface launches an attack using several methods against the identified vulnerabilities.

**Suggested Answer: C**

Community vote distribution

C (100%)

🗳️ 👤 **036e554** 1 year ago

ANS: C

Attack Vector refers to specific path uses to gain unauthorized access to a system or network, while An attack surface recognizes which network parts are vulnerable to an attack.

upvoted 1 times

🗳️ 👤 **WISDOM2080** 1 year, 10 months ago

C. An attack surface recognizes which network parts are vulnerable to an attack; and an attack vector identifies which attacks are possible with these vulnerabilities.

upvoted 1 times

🗳️ 👤 **alhamry** 2 years, 2 months ago

Option C is partially correct, as it correctly defines an attack surface as recognizing which network parts are vulnerable to an attack. However, it does not accurately define an attack vector. An attack vector is not just about identifying which attacks are possible with the vulnerabilities, but it also identifies the specific method or path used to exploit the vulnerability.

Option B is the best answer, as it correctly defines an attack vector as identifying the components that can be exploited and an attack surface as identifying the potential path an attack can take to penetrate the network.

upvoted 1 times

🗳️ 👤 **drdecker100** 2 years, 4 months ago

**Selected Answer: C**

An attack surface represents the overall set of vulnerabilities that an attacker could potentially exploit to launch an attack. This can include hardware, software, network protocols, configurations, and user accounts. By identifying and assessing the attack surface, defenders can understand the overall security posture of their system or network and take steps to reduce its exposure to potential attacks.

An attack vector, on the other hand, refers to the specific method or path that an attacker uses to exploit a particular vulnerability within the attack surface. An attacker may use multiple attack vectors to reach their goal, such as social engineering, malware, or exploiting a specific software flaw.

upvoted 4 times

🗳️ 👤 **SecurityGuy** 2 years, 7 months ago

**Selected Answer: C**

Attack Vector, Attack Surface and Threat Vector

Vector - It is a quantity having direction as well as magnitude

Attack Vector - is a "method" of gaining unauthorized access to a network or computer system. It takes many forms such as malware, ransomware, compromise pop-ups etc; basically any method that intends to compromise a system.

Attack Surface - is the total number of attack vectors an attacker can use to manipulate or compromise a network or system. Can also be defined as the total network or system.



Threat Vector - can be used interchangeably with attack vector and generally describes the potential ways a hacker can gain access to data or other confidential

[https://www.upguard.com/blog/attack-](https://www.upguard.com/blog/attack-vector#:~:text=minimize%20cybersecurity%20risk.%,What%20is%20the%20Difference%20Between%20an%20Attack%20Vector%2C%20Attack%20Surface,com)

[vector#:~:text=minimize%20cybersecurity%20risk.%,What%20is%20the%20Difference%20Between%20an%20Attack%20Vector%2C%20Attack%20Surface,com](https://www.upguard.com/blog/attack-vector#:~:text=minimize%20cybersecurity%20risk.%,What%20is%20the%20Difference%20Between%20an%20Attack%20Vector%2C%20Attack%20Surface,com)  
upvoted 1 times

🗳️ 👤 **kyle942** 2 years, 9 months ago

The 17 most common attack vectors are:

Compromised Credentials

Weak Credentials

Uneducated Employees

Insider Threats

Poor Encryption

Unpatched Software

Security Vulnerabilities

Third-party Vendors

Phishing Attacks

Ransomware

Brute Force Attacks

Distributed Denial of Service (DDoS) Attacks

SQL Injections

Trojans

Session Hijacking

Cross-Site Scripting (XSS)

Man-in-the-Middle Attacks

upvoted 2 times

🗳️ 👤 **[Removed]** 2 years, 9 months ago

**Selected Answer: C**

C is better answer but B is also correct right?

upvoted 1 times

🗳️ 👤 **halamah** 3 years, 7 months ago

correct

upvoted 1 times

🗳️ 👤 **eggheadsv** 3 years, 7 months ago

Correct Answer: C

The attack surface of a software environment is the sum of the different points (for "attack vectors") where an unauthorized user (the "attacker") can try to enter data to or extract data from an environment.[1][2] Keeping the attack surface as small as possible is a basic security measure.[3]

[https://en.wikipedia.org/wiki/Attack\\_surface](https://en.wikipedia.org/wiki/Attack_surface)

In computer security, an attack vector is a specific path, method, or scenario that can be exploited to break into an IT system, thus compromising its security. The term was derived from the corresponding notion of vector in biology. An attack vector may be exploited manually, automatically, or through a combination of manual and automatic activity.

[https://en.wikipedia.org/wiki/Attack\\_vector](https://en.wikipedia.org/wiki/Attack_vector)

upvoted 1 times

Which metric in CVSS indicates an attack that takes a destination bank account number and replaces it with a different bank account number?

- A. integrity
- B. confidentiality
- C. availability
- D. scope

**Suggested Answer: A**

Community vote distribution

A (100%)

🗳️ 👤 **Leo\_Visser** Highly Voted 🏆 2 years, 12 months ago

Correct answer is A

"2.3.2. Integrity (I)

This metric measures the impact to integrity of a successfully exploited vulnerability. Integrity refers to the trustworthiness and veracity of information. The Base Score is greatest when the consequence to the impacted component is highest."

source: <https://www.first.org/cvss/specification-document>

upvoted 7 times

🗳️ 👤 **Leo\_Visser** 2 years, 12 months ago

But you could read the question in a way where the goal of this attack might be to overload the storage of the server or something like that, and if that would be the case it could be that this the Actions on Objective phase because it's targeting multiple places which have things create so it could very well be that it might tries to exhaust the storage and by that take the site down. But this is not an attack which is seen often and therefore I wouldn't say this to be the right answer.

It could also indeed be answer C where the goal is to install several files but this would be more an delivery step then a installation step. Normally you would use the installed files to create a better RCE exploit which allows you to install something malicious on the system itself and from there work on.

So I think A is the best answer as it looks more like the threat actor is just trying different sites to see where the code will work.

upvoted 2 times

🗳️ 👤 **WISDOM2080** Most Recent 🕒 10 months ago

A. integrity

upvoted 1 times

🗳️ 👤 **ShammaA** 1 year, 1 month ago

Simplest question -- anything that changes has to do with the integrity.

upvoted 2 times

🗳️ 👤 **drdecker100** 1 year, 4 months ago

**Selected Answer: A**

The "Integrity" metric in CVSS measures the impact that a successful attack would have on the integrity of the system or data. This metric is based on the potential for unauthorized modification or destruction of data, which includes actions such as changing bank account numbers.

In this scenario, an attacker is modifying the destination bank account number, which could lead to financial loss and the unauthorized transfer of funds. This attack would impact the integrity of the system, as it involves unauthorized modification of data.

upvoted 2 times

🗳️ 👤 **halamah** 2 years, 7 months ago

correct

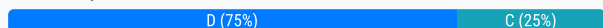
upvoted 1 times

A security specialist notices 100 HTTP GET and POST requests for multiple pages on the web servers. The agent in the requests contains PHP code that, if executed, creates and writes to a new PHP file on the webserver. Which event category is described?

- A. reconnaissance
- B. action on objectives
- C. installation
- D. exploitation

**Suggested Answer: D**

Community vote distribution



**anonymous1966** Highly Voted 3 years, 9 months ago

The correct answer should be Delivery.

But, in this case, I would choose "C" - instalation.

Here are the steps of the Kill Chain Model:

Reconnaissance --> Weaponization --> Delivery --> Exploitation --> Installation --> Command and control (C2 or CnC) --> Actions on objectives

- 1) Reconnaissance: research on a target, search vulnerabilities. Ex: nmap
- 2) Weaponization: develop and test how the attack will be executed. Buld the "weapon". Ex: a file trojan.
- 3) Delivery: deliver the weapon against target. Ex: phishing
- 4) Exploitation: launch the weapon against a vulnerability. Ex: user open a trojan file.
- 5) Installation: instalation of the weapon in the target: Ex: a backdoor server
- 6) Command and control (C2 or CnC): the attacker accesses the breached system. Ex: orchestration of zumbi hosts
- 7) Actions on objectives: launching the attack. Ex: stole credit card number/password.

Cisco CyberOps Associate CBROPS 200-201 Official Cert Guide

By Omar Santos

upvoted 15 times

**Leo\_Visser** Highly Voted 3 years, 12 months ago

Read more: [https://en.wikipedia.org/wiki/Kill\\_chain#Attack\\_phases\\_and\\_countermeasures](https://en.wikipedia.org/wiki/Kill_chain#Attack_phases_and_countermeasures)

I think A would be the best answer here as they threat actor is trying several different places to see where it works. This sounds more like Reconnaissance then actual installation already. If it was in the installation phase the threat actor would know where to exploit and therefore do a more targeted attack.

upvoted 9 times

**Frontal** Most Recent 2 months, 2 weeks ago

**Selected Answer: D**

C. Installation - NO - That's after exploitation, when malware/backdoors get installed. We're seeing the exploit now. ✗

✓ D. Exploitation - Yes — the attacker is sending malicious payloads with PHP code to trigger code execution and write a new file = Exploitation phase. ✓

upvoted 1 times

**maclovio** 4 months, 1 week ago

**Selected Answer: C**

While it is true that the attacker could be exploiting a vulnerability in the server to write and execute PHP code, the act of writing the malicious PHP code and creating the PHP file itself is more in line with an installation action. The attacker is trying to establish a persistent tool on the system (such as a backdoor or web shell), which corresponds to the installation stage of the attack.

upvoted 1 times

🗨️ **3000bd6** 7 months, 2 weeks ago

**Selected Answer: C**

I also think it's C .The goal of the action described in the question is "install a new PHP file" on the web server.

upvoted 1 times

🗨️ **3000bd6** 7 months, 2 weeks ago

Disregard, I think the best answer is D as the code HASN'T been executed yet.

upvoted 1 times

🗨️ **Faio** 1 year, 9 months ago

The correct answer is D.

In this case, the attacker is clearly trying to exploit a vulnerability on the web server in order to gain control of it. Therefore, the event category is exploitation.

upvoted 2 times

🗨️ **WISDOM2080** 1 year, 10 months ago

C. installation

upvoted 1 times

🗨️ **SecurityGuy** 1 year, 10 months ago

**Selected Answer: C**

Recon - Can't be

Action on Objectives - No actions, data exfiltration etc. has been made yet.

Installation - Keyword: "creates and writes"

Exploitation - No indications of taking advantage yet.

upvoted 4 times

🗨️ **Faio** 2 years ago

The correct answer is D exploitation.

Installation (C) typically refers to the stage where an attacker establishes a foothold or installs malware on a compromised system. However, in the given scenario, the focus is on the exploitation of the web servers rather than the installation of persistent access or malware.

upvoted 2 times

🗨️ **ShammaA** 2 years, 1 month ago

At first thought I went for exploitation -- like typical but when you look back at the Kill chain model the exploitation already happened through the vulnerability of HTTP-- all that's left is the actual installation because the payload is already there now

So this is strictly "installation".

upvoted 1 times

🗨️ **alhamry** 2 years, 2 months ago

the HTTP requests with the PHP code are attempting to create and write to a new PHP file on the webserver, which is a form of exploiting a vulnerability. Therefore, the correct answer is D.

upvoted 2 times

🗨️ **itousattud** 2 years, 3 months ago

**Selected Answer: D**

The event category described in the scenario is "exploitation" (option D).

The scenario describes a situation where an attacker is attempting to exploit a vulnerability in the webserver by injecting malicious PHP code in the HTTP requests. The purpose of this code is to create and write to a new PHP file on the server, which could potentially allow the attacker to take control of the server or steal sensitive information.

Reconnaissance (option A) refers to the initial stage of an attack where the attacker gathers information about the target system. Action on objectives (option B) refers to the stage of an attack where the attacker achieves their goals, such as stealing data or disrupting services. Installation (option C) refers to the stage of an attack where the attacker installs their tools or malware on the target system. None of these stages accurately describe the situation in the scenario.

upvoted 2 times

🗨️ **drdecker100** 2 years, 4 months ago

**Selected Answer: D**

The event category that is described in this scenario is "exploitation."

The HTTP GET and POST requests, along with the presence of malicious PHP code in the user agent, suggest that an attacker is attempting to exploit a vulnerability in the web server. The creation and writing of a new PHP file on the server could be an attempt to establish persistent access to the system or to install a backdoor that would allow the attacker to maintain control even after the initial attack.

Therefore, this scenario is consistent with an "exploitation" event category, where the attacker is attempting to take advantage of a vulnerability in the system to gain unauthorized access or control.

upvoted 1 times

🗨️ 👤 **MaliDong** 2 years, 8 months ago

**Selected Answer: D**

' for multiple pages' , then D.

upvoted 2 times

🗨️ 👤 **cy\_analyst** 2 years, 8 months ago

**Selected Answer: D**

D --> because it simply exploits the possibility to copy the script every time, to create a new page, nothing more.

upvoted 1 times

🗨️ 👤 **WillBui** 3 years, 3 months ago

**Selected Answer: D**

I think it's D

upvoted 1 times

🗨️ 👤 **[Removed]** 3 years, 3 months ago

It says "IF executed" which is before installation, so whats before installation? Exploitation

upvoted 4 times

What specific type of analysis is assigning values to the scenario to see expected outcomes?

- A. deterministic
- B. exploratory
- C. probabilistic
- D. descriptive

**Suggested Answer: A**

Community vote distribution

A (100%)

🗳️ 👤 **Leo\_Visser** Highly Voted 👍 3 years, 12 months ago

"In deterministic models, the output of the model is fully determined by the parameter values and the initial values, whereas probabilistic (or stochastic) models incorporate randomness in their approach. Consequently, the same set of parameter values and initial conditions will lead to a group of different outputs. "

<https://www.preventionweb.net/disaster-risk/concepts/deterministic-probabilistic/>

So A seems to be correct

upvoted 10 times

🗳️ 👤 **anonymous1966** Highly Voted 👍 3 years, 9 months ago

"A" is correct.

Deterministic: Cause --> Effect.

Probabilistic: behavior

In deterministic analysis, all data used for the analysis is known beforehand. Probabilistic analysis, on the other hand, is done assuming the likelihood that something will or has happened, but you don't know exactly when or how.

Probabilistic methods institute powerful tools for use in many kinds of decision-making problems—in this case, cybersecurity event analysis. In this type of analysis, the analysis components suggest a "probabilistic answer" to the results of the investigation, which is not a definitive result.

Cisco CyberOps Associate CBROPS 200-201 Official Cert Guide

By Omar Santos

upvoted 6 times

🗳️ 👤 **Frontal** Most Recent 🕒 2 months, 2 weeks ago

Selected Answer: C

The keyword "expected outcomes" directly implies:

C. Probabilistic

Dont @ me hoes

upvoted 1 times

🗳️ 👤 **3000bd6** 7 months, 1 week ago

Selected Answer: C

"expected outcomes" more commonly refers to the average or most likely result derived from probabilistic

upvoted 1 times

🗳️ 👤 **RoBery** 1 year, 5 months ago

C is correct.

What is a characteristic of a probabilistic analysis in an alert evaluation?

random variables that create difficulty in knowing the outcome of any given event with certainty.

Explanation: Statistical techniques can be used to evaluate the risk that exploits will be successful in a given network. This type of analysis can help decision makers to better evaluate the cost of mitigating a threat and the damage that an exploit could cause. Two general approaches used to do this are as follows:

Deterministic Analysis: For an exploit to be successful, all prior steps in the exploit must also be successful. The cybersecurity analyst knows the steps for a successful exploit.

Probabilistic Analysis: Statistical techniques are used to determine the probability that a successful exploit will occur based on the likelihood that each step in the exploit will succeed.

upvoted 1 times

🗳️ 👤 **RoBery** 1 year, 5 months ago

C is the correct,

What is a characteristic of a probabilistic analysis in an alert evaluation?

each event an inevitable result of antecedent causes

precise methods that yield the same result every time by relying on predefined conditions

random variables that create difficulty in knowing the outcome of any given event with certainty analysis of applications that conform to application/networking standards

Explanation: Statistical techniques can be used to evaluate the risk that exploits will be successful in a given network. This type of analysis can help decision makers to better evaluate the cost of mitigating a threat and the damage that an exploit could cause. Two general approaches used to do this are as follows:

Deterministic Analysis: For an exploit to be successful, all prior steps in the exploit must also be successful. The cybersecurity analyst knows the steps for a successful exploit.

Probabilistic Analysis: Statistical techniques are used to determine the probability that a successful exploit will occur based on the likelihood that each step in the exploit will succeed.

upvoted 1 times

🗳️ 👤 **WISDOM2080** 1 year, 10 months ago

D. descriptive

upvoted 1 times

🗳️ 👤 **drdecker100** 2 years, 4 months ago

**Selected Answer: A**

Deterministic analysis involves using mathematical equations to determine a specific outcome based on fixed inputs. In a cybersecurity context, this might involve using a formula to calculate the potential loss from a specific type of attack based on known variables such as the value of the data that could be stolen or the cost of system downtime.

In contrast, probabilistic analysis involves assigning probabilities to potential outcomes based on known variables. This might involve assessing the likelihood of a specific type of attack succeeding and calculating the expected value of the potential loss.

upvoted 1 times

🗳️ 👤 **itousattud** 2 years, 3 months ago

ChatGPT

upvoted 1 times

🗳️ 👤 **kyle942** 2 years, 9 months ago

a deterministic algorithm is an algorithm that, given a particular input, will always produce the same output,

upvoted 1 times

🗳️ 👤 **gkp\_br** 2 years, 9 months ago

**Selected Answer: A**

A. deterministic models

upvoted 2 times

🗳️ 👤 **halamah** 3 years, 7 months ago

A IS CORRECT

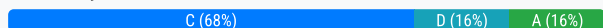
upvoted 1 times

When trying to evade IDS/IPS devices, which mechanism allows the user to make the data incomprehensible without a specific key, certificate, or password?

- A. fragmentation
- B. pivoting
- C. encryption
- D. stenography

**Suggested Answer: C**

Community vote distribution



**evra** Highly Voted 4 years, 2 months ago

It is A

[https://en.wikipedia.org/wiki/Intrusion\\_detection\\_system\\_evasion\\_techniques](https://en.wikipedia.org/wiki/Intrusion_detection_system_evasion_techniques)

upvoted 22 times

**Leo\_Visser** 3 years, 12 months ago

I would agree

C and D both need keys to work and B is only used to go to another network but won't evade the IDS perse.

more info:

<https://www.ciscopress.com/articles/article.asp?p=3100055&seqNum=3>

upvoted 3 times

**fyticez** 2 years, 8 months ago

Even if ste(ga)nography needs a key to decode the embedded secret, it still relates to discernible (vs. incomprehensible) output.

upvoted 1 times

**anonymous1966** Highly Voted 3 years, 10 months ago

By the Book, I believe Fragmentation would be correct.

Traditional IDS and IPS devices also suffer from many evasion attacks. The following are some of the most common evasion techniques against traditional IDS and IPS devices:

Fragmentation: Attackers can evade the IPS box by sending fragmented packets.

Using low-bandwidth attacks: Attackers can use techniques that use low-bandwidth or a very small number of packets to evade the system.

Address spoofing/proxying: Attackers can use spoofed IP addresses or sources, as well as intermediary systems such as proxies to evade inspection.

Pattern change evasion: Attackers may use polymorphic techniques to create unique attack patterns.

Encryption: Attackers can use encryption to hide their communication and information.

upvoted 11 times

**anonymous1966** 3 years, 10 months ago

Steganography is used for hiding text. I believe that it is not the question.

Steganography is the practice of hiding a secret message inside of (or even on top of) something that is not secret. That something can be just about anything you want. These days, many examples of steganography involve embedding a secret piece of text inside of a picture. Or hiding a secret message or script inside of a Word or Excel document.

<https://www.comptia.org/blog/what-is-steganography>

upvoted 4 times

**Twphill** Most Recent 3 months, 3 weeks ago

**Selected Answer: A**

Fragmentation is the only method that evades IPS without key, etc.



upvoted 1 times

🗨️ **abbeyade** 5 months, 2 weeks ago

**Selected Answer: A**

C and D required key

upvoted 1 times

🗨️ **3000bd6** 7 months, 1 week ago

**Selected Answer: D**

I believe it's D

upvoted 1 times

🗨️ **d503c75** 9 months, 2 weeks ago

Answer is the option D.

Incomprehensible = hidden

Steganography can be used to "hide" virtually any type of digital content, including text, image, video, or audio content. And to do this, you don't need a specific key, certificate or password.

upvoted 2 times

🗨️ **WISDOM2080** 1 year, 10 months ago

C. encryption

upvoted 1 times

🗨️ **Faio** 1 year, 10 months ago

The answer is C. encryption.

Encryption is the process of converting data into a form that is unreadable without a specific key. This can be used to evade IDS/IPS devices by making the data incomprehensible to them.

upvoted 3 times

🗨️ **drdecker100** 2 years, 4 months ago

**Selected Answer: C**

When an attacker is trying to evade detection by IDS/IPS devices, they may use encryption to make their communication unreadable to the security tools that are monitoring the network. By encrypting their data, the attacker can make it more difficult for the IDS/IPS devices to detect and analyze the content of their communication.

Fragmentation involves splitting up data into smaller packets, which can also be used to evade IDS/IPS devices, but it doesn't make the data incomprehensible.

upvoted 2 times

🗨️ **SecurityGuy** 2 years, 5 months ago

**Selected Answer: C**

After months of studying, I realized that C - Encryption is the correct answer.

- The question is "Evading IDS/IPS" and there is no way to use Stenography to evade IDS/IPS.

Intrusion Detection Evasive Techniques:

Most attackers are aware of IDSs and use evasive techniques to dodge them. These evasive techniques include flooding, fragmentation, encryption, and obfuscation.

[https://www.pearsonitcertification.com/articles/article.aspx?](https://www.pearsonitcertification.com/articles/article.aspx?p=174342&seqNum=3#:~:text=Most%20attackers%20are%20aware%20of,fragmentation%2C%20encryption%2C%20and%20obfuscation.)

[p=174342&seqNum=3#:~:text=Most%20attackers%20are%20aware%20of,fragmentation%2C%20encryption%2C%20and%20obfuscation.](https://www.pearsonitcertification.com/articles/article.aspx?p=174342&seqNum=3#:~:text=Most%20attackers%20are%20aware%20of,fragmentation%2C%20encryption%2C%20and%20obfuscation.)

upvoted 3 times

🗨️ **youssssef** 2 years, 5 months ago

**Selected Answer: C**

encryption

upvoted 1 times

🗨️ **aaawnd** 2 years, 6 months ago

**Selected Answer: C**

just encryption need a key, certificate or password to see this info and is an evasion technique

upvoted 2 times

🗨️ **Chris1971** 2 years, 5 months ago

but the question is "data incomprehensible without a specific key,"

so "C" is wrong

upvoted 2 times

🗨️ **SecurityGuy** 2 years, 9 months ago

**Selected Answer: D**

I believe the correct answer is "D"

Stenography is writing on a different way, which can be used to hide the true meaning of the subject.

The purpose of steganography is to conceal and deceive. It is a form of covert communication and can involve the use of any medium to hide messages. It's not a form of cryptography, because it doesn't involve scrambling data or using a key. Instead, it is a form of data hiding and can be executed in clever ways.

[https://www.comptia.org/blog/what-is-](https://www.comptia.org/blog/what-is-steganography#:~:text=The%20purpose%20of%20steganography%20is,be%20executed%20in%20clever%20ways.)

[steganography#:~:text=The%20purpose%20of%20steganography%20is,be%20executed%20in%20clever%20ways.](https://www.comptia.org/blog/what-is-steganography#:~:text=The%20purpose%20of%20steganography%20is,be%20executed%20in%20clever%20ways.)

upvoted 3 times

🗨️ **Giacomius** 2 years, 10 months ago

I would agree on A -->

"Traditional IDS and IPS devices also suffer from many evasion attacks. The following are some of the most common evasion techniques against traditional IDS and IPS devices:

- Fragmentation: Attackers can evade the IPS box by sending fragmented packets.
- Using low-bandwidth attacks: Attackers can use techniques that use low-bandwidth or a very small number of packets to evade the system.
- Address spoofing/proxying: Attackers can use spoofed IP addresses or sources, as well as intermediary systems such as proxies to evade inspection.
- Pattern change evasion: Attackers may use polymorphic techniques to create unique attack patterns.
- Encryption: Attackers can use encryption to hide their communication and information."

Ref: Cisco CyberOps Associate

CBROPS 200-201 Official

Cert Guide

Omar Santos

upvoted 1 times

🗨️ **[Removed]** 2 years, 11 months ago

I might be wrong but encryption is used by threat actors as a method of evasion and obfuscation <https://www.ciscopress.com/articles/article.asp?p=3100055&seqNum=2>

From here I agree with answer C.

upvoted 1 times

🗨️ **Nhendy** 2 years, 11 months ago

**Selected Answer: C**

Incomprehensible without decryption, then answer is encryption

upvoted 1 times

🗨️ **Kane4555** 3 years ago

**Selected Answer: C**

Both C and D are correct, as both fulfill the requirements, but C is on the exam objectives and D is not, so C. These questions are fairly terrible. People saying A need reading comprehension.

upvoted 2 times

Why is encryption challenging to security monitoring?

- A. Encryption analysis is used by attackers to monitor VPN tunnels.
- B. Encryption is used by threat actors as a method of evasion and obfuscation.
- C. Encryption introduces additional processing requirements by the CPU.
- D. Encryption introduces larger packet sizes to analyze and store.

**Suggested Answer: B**

🗨️ 👤 **WISDOM2080** 10 months ago

B . Encryption is used by threat actors as a method of evasion and obfuscation.  
upvoted 2 times

🗨️ 👤 **RolandoFiee** 2 years, 4 months ago

B is correct  
Encryption can be challenging to security monitoring because it can be used by threat actors as a method of evasion and obfuscation, and security monitoring tools might not be able to inspect encrypted traffic  
upvoted 2 times

🗨️ 👤 **halamah** 2 years, 7 months ago

B IS CORRECT  
upvoted 1 times

🗨️ 👤 **Leo\_Visser** 2 years, 12 months ago

B is the correct answer  
"On the other hand, those same mechanisms can be used by threat actors as a method of evasion and obfuscation. "  
<https://www.ciscopress.com/articles/article.asp?p=3100055&seqNum=2>  
upvoted 4 times

An employee reports that someone has logged into their system and made unapproved changes, files are out of order, and several documents have been placed in the recycle bin. The security specialist reviewed the system logs, found nothing suspicious, and was not able to determine what occurred. The software is up to date; there are no alerts from antivirus and no failed login attempts. What is causing the lack of data visibility needed to detect the attack?

- A. The threat actor used a dictionary-based password attack to obtain credentials.
- B. The threat actor gained access to the system by known credentials.
- C. The threat actor used the teardrop technique to confuse and crash login services.
- D. The threat actor used an unknown vulnerability of the operating system that went undetected.

**Suggested Answer: B**

Community vote distribution

B (100%)

🗳️ 👤 **WISDOM2080** 10 months ago

B. The threat actor gained access to the system by known credentials.

upvoted 1 times

🗳️ 👤 **Antari8** 1 year ago

I think 'B' because if the threat actor know the right credential he can also delete logs file and seem to be never entered in to the system

upvoted 2 times

🗳️ 👤 **alhamry** 1 year, 2 months ago

the question stated clearly that the suspicious activity "made unapproved changes, files are out of order, and several documents have been placed in the recycle bin." If the attacker used known credentials, then this will appear in the system logs under that credential. I am going with answer D

upvoted 1 times

🗳️ 👤 **drdecker100** 1 year, 4 months ago

**Selected Answer: B**

If the attacker used valid credentials to access the employee's system, it would explain why there were no failed login attempts in the logs, and why there were no alerts from antivirus. In this scenario, the attacker would not need to use a dictionary-based password attack to obtain credentials or exploit an unknown vulnerability in the operating system.

The fact that the security specialist found nothing suspicious in the system logs could also suggest that the attacker used legitimate credentials to access the system, making it difficult to detect the attack through traditional security monitoring methods.

upvoted 1 times

🗳️ 👤 **SecurityGuy** 1 year, 9 months ago

**Selected Answer: B**

B is the correct answer for me.

Certification exams are always tricky. Cisco wants you to overthink. So, I always go for the simplest but sensible answer during an exam.

upvoted 1 times

🗳️ 👤 **DLukynskyy** 2 years, 3 months ago

I guess Cisco believes B to be the right answer

upvoted 2 times

🗳️ 👤 **halamah** 2 years, 7 months ago

D IS CORRECT

ZERO DAY ATTACK

upvoted 3 times

🗳️ 👤 **anonymous1966** 2 years, 10 months ago

The simplest is almost always the right answer.

Think of the real world.

An user complaining this: two options: a cat on the keyboard (I know because I have one) or another person/bot with user credentials.

upvoted 2 times

🗨️ 👤 **SecurityGuy** 1 year, 9 months ago

I agree with this, certification exams are always tricky. Cisco wants you to overthink. So, I always go for the simplest but sensible answer during an exam.

upvoted 1 times

🗨️ 👤 **anonymous1966** 2 years, 10 months ago

So (B) is correct

upvoted 4 times

🗨️ 👤 **Kapside** 3 years ago

A lot of these questions are horrible and could go either way in my opinion. I really hate the way these certs word questions and answers

upvoted 2 times

🗨️ 👤 **beowolf** 3 years, 1 month ago

I think answer is D - zero day exploit

upvoted 4 times

🗨️ 👤 **Msal1134** 3 years, 1 month ago

Zero day exploits can give you access... but not always undetected.... unless you're already know the credentials

upvoted 1 times

🗨️ 👤 **Leo\_Visser** 2 years, 12 months ago

But it says in the question the engineer investigated the system logs, so if any logins were done with known credentials it would show up in there. So only conclusion can be that the attacker used an unknown way of entry which isn't captured in the system logs and monitoring software.

So I agree D should be the right answer.

upvoted 5 times

🗨️ 👤 **jb372** 2 years, 11 months ago

the question says "The security specialist reviewed the system logs, found nothing suspicious, and was not able to determine what occurred. The software is up to date; there are no alerts from antivirus and no failed login attempts." which means that a successful login with known credentials would have been ignored as valid system usage, and not inspected as malicious. I believe the Given answer of \_"KNOWN CREDENTIALS" is the correct answer

upvoted 13 times

🗨️ 👤 **alhamry** 1 year, 2 months ago

the question stated clearly that the suspicious activity "made unapproved changes, files are out of order, and several documents have been placed in the recycle bin." If the attacker used known credentials, then this will appear in the system logs under that credential. I am going with answer D

upvoted 1 times

A company receptionist received a threatening call referencing stealing assets and did not take any action assuming it was a social engineering attempt. Within


48 hours, multiple assets were breached, affecting the confidentiality of sensitive information. What is the threat actor in this incident?

- A. company assets that are threatened
- B. customer assets that are threatened
- C. perpetrators of the attack
- D. victims of the attack

**Suggested Answer: C**

Community vote distribution

C (100%)

  **anonymous1966** Highly Voted 2 years, 9 months ago

"C" is correct.

Threat actors are the individuals (or a group of individuals) who perform an attack or are responsible for a security incident that impacts or has the potential of impacting an organization or individual. There are several types of threat actors:

Script kiddies, Organized crime groups, State sponsors and governments, Hacktivists, Terrorist groups.

Cisco CyberOps Associate CBROPS 200-201 Official Cert Guide

By Omar Santos

upvoted 6 times

  **WISDOM2080** Most Recent 10 months ago

C. perpetrators of the attack

upvoted 1 times

  **SecurityGuy** 1 year, 9 months ago

Selected Answer: C

C is the correct answer.

For those people who don't know this word.

Perpetrator is a person who carries out a harmful, illegal, or immoral act.

upvoted 1 times

  **BobbyYarush** 2 years, 3 months ago

Three different dumps.... three different answers on this question....

upvoted 1 times

  **BobbyYarush** 2 years, 3 months ago

C makes total sense to me....

upvoted 1 times

  **saakovv** 2 years, 5 months ago

what does it have to do with this " perpetrators of the attack" ??

upvoted 1 times

  **halamah** 2 years, 7 months ago

C IS CORRECT

upvoted 1 times

  **Leo\_Visser** 2 years, 12 months ago

C is the right answer

"A threat actor or malicious actor is a person or entity responsible for an event or incident that impacts, or has the potential to impact, the safety or security of another entity"

[https://en.wikipedia.org/wiki/Threat\\_actor](https://en.wikipedia.org/wiki/Threat_actor)

upvoted 3 times

What is the relationship between a vulnerability and a threat?

- A. A threat exploits a vulnerability
- B. A vulnerability is a calculation of the potential loss caused by a threat
- C. A vulnerability exploits a threat
- D. A threat is a calculation of the potential loss caused by a vulnerability

**Suggested Answer: A**

Community vote distribution

A (100%)

🗳️ 👤 **Leo\_Visser** Highly Voted 👍 1 year, 12 months ago

A vulnerability refers to a known weakness of an asset (resource) that can be exploited by one or more attackers.

A threat refers to a new or newly discovered incident that has the potential to harm a system or your company overall.

So a threat exploits a vulnerability so A is right

upvoted 13 times

🗳️ 👤 **anonymous1966** Highly Voted 👍 1 year, 9 months ago

"A" is correct

A threat is any potential danger to an asset.

A vulnerability is a weakness in the system design, implementation, software, or code or the lack of a mechanism.

A threat actor (criminal) uses a threat (a malware) to explore a vulnerability (OS not updated) to achieve his objectives (stole information)

upvoted 7 times

🗳️ 👤 **Eng\_ahmedyoussef** Most Recent 🕒 9 months ago

Selected Answer: A

"A" is correct

upvoted 1 times

🗳️ 👤 **halamah** 1 year, 7 months ago

A IS CORRECT

upvoted 3 times

🗳️ 👤 **Madkayo** 1 year, 10 months ago

What's the difference between answer A and B? The same.

upvoted 1 times

🗳️ 👤 **JJt4x** 2 years ago

answer is C

upvoted 1 times

🗳️ 👤 **tsabee** 1 year, 8 months ago

Nope :)

upvoted 3 times



What is the principle of defense-in-depth?

- A. Agentless and agent-based protection for security are used.
- B. Several distinct protective layers are involved.
- C. Access control models are involved.
- D. Authentication, authorization, and accounting mechanisms are used.

**Suggested Answer:** B

Community vote distribution

B (100%)

🗳️ 👤 **anonymous1966** Highly Voted 👍 2 years, 10 months ago

B is correct.

By the book:

If you are a cybersecurity expert, or even an amateur, you probably already know that when you deploy a firewall or an intrusion prevention system or install antivirus or advanced malware protection on your machine, you cannot assume you are now safe and secure. A layered and cross-boundary "defense-in-depth" strategy is what is needed to protect your network and corporate assets. One of the primary benefits of a defense-in-depth strategy is that even if a single control (such as a firewall or IPS) fails, other controls can still protect your environment and assets.

upvoted 12 times

🗳️ 👤 **Leo\_Visser** Highly Voted 👍 2 years, 12 months ago

B is correct answer.

more info: <https://www.ciscopress.com/articles/article.asp?p=2783637&seqNum=2>

upvoted 6 times

🗳️ 👤 **WISDOM2080** Most Recent 🕒 10 months ago

B. Several distinct protective layers are involved.

upvoted 2 times

🗳️ 👤 **Eng\_ahmedyoussef** 1 year, 9 months ago

Selected Answer: B

B is correct answer - This is a layered security

upvoted 2 times

🗳️ 👤 **AVT** 2 years, 6 months ago

This is a layered security: when you use different security measures at different layers.

Security in depth is when you use different security products within the same layer.

upvoted 2 times

🗳️ 👤 **halamah** 2 years, 7 months ago

b is correct

upvoted 2 times

DRAG DROP -

Drag and drop the uses on the left onto the type of security system on the right.

Select and Place:

ensures protection of individual devices	Endpoint
detects intrusion attempts	
monitors host for suspicious activity	
monitors incoming traffic and connections	Network

Suggested Answer:

ensures protection of individual devices	Endpoint
detects intrusion attempts	ensures protection of individual devices
monitors host for suspicious activity	monitors host for suspicious activity
monitors incoming traffic and connections	Network
	detects intrusion attempts
	monitors incoming traffic and connections

🗨️ **WISDOM2080** 10 months ago

Answer is correct.

upvoted 2 times

🗨️ **Eng\_ahmedyoussef** 1 year, 9 months ago

Answer is correct.

upvoted 1 times

🗨️ **halamah** 2 years, 7 months ago

1 and 3 are endpoint

upvoted 1 times

🗨️ **anonymous1966** 2 years, 9 months ago

Answer is correct.

Keywords:

"individual devices" --> endpoint

"host" --> endpoint

upvoted 4 times

🗨️ **Leo\_Visser** 2 years, 12 months ago

Answer is correct.

upvoted 3 times

What is the difference between the rule-based detection when compared to behavioral detection?

- A. Rule-Based detection is searching for patterns linked to specific types of attacks, while behavioral is identifying per signature.
- B. Rule-Based systems have established patterns that do not change with new data, while behavioral changes.
- C. Behavioral systems are predefined patterns from hundreds of users, while Rule-Based only flags potentially abnormal patterns using signatures.
- D. Behavioral systems find sequences that match a particular attack signature, while Rule-Based identifies potential attacks.

**Suggested Answer: B**

Community vote distribution



**beowolf** 3 years, 7 months ago

Behavioral is not signature based detection. Correct answer is C

An IDS when placed inline it will become an IPS, initially the IDS will analyze user data for sometime to understand the pattern so it can determine what is normal / abnormal in the network, based on this it will create a baseline.

upvoted 17 times

**Leo\_Visser** 3 years, 5 months ago

Isn't the correct answer B, it says it has a predefined collection of patterns which it uses to detect the attack but as far as I know the Behavioral Detection keeps analysing the network and changes the baseline accordingly.

Here (<https://www.cisco.com/c/en/us/products/security/what-is-network-detection-response.html>) it says "NDR solutions continuously monitor and analyze raw enterprise network traffic to generate a baseline of normal network behavior."

So that would suggest that answer B is more correct because C would suggest that after the baseline is generated it doesn't change at all anymore. It also says this in the stealthwatch documentation

"After the initial 7 days, Stealthwatch tracks 14 key attributes to create a rolling 28-day baseline. This baseline is the average of the daily attribute values for the past 28 days, heavily weighted for the last 7 days. Since the baseline incorporates the last seven days, these are used to represent weekly values. Therefore, the baseline includes values for the previous month, but is heavily weighted to the most recent week. "

So I would really say B is the right answer.

upvoted 26 times

**anonymous1966** 3 years, 3 months ago

For me "B" is correct.

In a behavioral model, the focus is on user or application behavior and not on a specific attack pattern. The goal is to distinguish between malicious and nonmalicious behaviors. The promise of such systems is great: Theoretically, this type of solution can deal with all attacks, both known and unknown. Moreover, it promises to free the user from having to keep the system updated, since there is no use of attack signatures.

A signature is actually a fingerprint of a given attack. The signature captures the actions, which are unique to a given attack. This pragmatic approach is focused on specific attacks and is very accurate at lowering the rate of false positives.

ref: <https://www.computerworld.com/article/2581345/behavioral-rules-vs-signatures-which-should-you-use-.html>

upvoted 15 times

**dunno\_** 7 months, 1 week ago

**Selected Answer: B**

B is correct.

Rule-based detection relies on static, predefined patterns that do not change, while behavioral detection adapts and changes based on new data and observed behaviors.

upvoted 1 times

**jorgeaaq** 1 year, 2 months ago

I think is B because

A.- behavioral is identifying per signature is wrong (per signature is rule based)

C.- Behavioral systems are predefined patterns... behavioral could not be predefined

D.- Behavioral systems find sequences that match a particular attack signature ... is wrong because behavioral not look for signatures look for anomalies...

so the correct Answer is B

upvoted 3 times

  **WISDOM2080** 1 year, 4 months ago

D . Behavioral systems find sequences that match a particular attack signature, while Rule-Based identifies potential attacks.

upvoted 1 times

  **Topsecret** 1 year, 5 months ago

The correct answer is D. Behavioral systems find sequences that match a particular attack signature, while Rule-Based identifies potential attacks.

Rule-based detection involves searching for patterns that are linked to specific types of attacks. These patterns are predefined and do not change with new data. When a specific pattern is detected, the system flags it as a potential attack. Rule-based detection relies on known signatures or patterns to identify threats.

On the other hand, behavioral detection focuses on identifying sequences of behavior that match a particular attack signature. It analyzes the behavior of users or systems and looks for deviations or anomalies from expected patterns. Behavioral detection systems are designed to adapt and learn from new data, allowing them to detect novel or previously unseen attacks based on deviations from normal behavior.

Therefore, the correct answer is D, as it accurately describes the difference between rule-based and behavioral detection.

upvoted 3 times

  **alhamry** 1 year, 7 months ago

The best answer is "B. Rule-Based systems have established patterns that do not change with new data, while behavioral changes."

Rule-based detection and behavioral detection are two different approaches used in intrusion detection and prevention systems.

Rule-based detection involves searching for specific patterns that are linked to known types of attacks. These patterns are represented as signatures, and the system checks incoming data against these signatures to detect potential attacks. Rule-based systems have established patterns that do not change with new data. Therefore, they may be less effective at detecting new or unknown attacks that do not match the established patterns.

Behavioral detection, on the other hand, involves monitoring system behavior and identifying anomalies that may indicate an attack. It uses machine learning algorithms to analyze normal patterns of system behavior and detect deviations from those patterns. Behavioral systems are designed to adapt and learn from new data and can detect new or unknown attacks that do not match established patterns.

upvoted 4 times

  **drdecker100** 1 year, 10 months ago

**Selected Answer: B**

Rule-Based systems have established patterns that do not change with new data, while behavioral detection is more dynamic and adapts to new data.

Rule-based systems use pre-defined rules or signatures to detect known types of attacks. These rules are based on static patterns or behaviors that are known to be associated with specific attacks. Therefore, rule-based detection is less adaptable to new or unknown threats, and it may miss sophisticated attacks that use novel techniques.

In contrast, behavioral detection is based on dynamic analysis of system behavior and can adapt to new or previously unknown threats.

upvoted 4 times

  **cy\_analyst** 2 years, 2 months ago

**Selected Answer: C**

C because behavioral patterns being predefined when creating the baseline of the network.

upvoted 1 times

  **SecurityGuy** 2 years, 3 months ago

**Selected Answer: D**

### Behavior-Based

A behavior or anomaly-based IDS solution goes beyond identifying particular attack signatures to detect and analyze malicious or unusual patterns of behavior.

This type of system applies Statistical, AI and machine learning to analyze giant amounts of data and network traffic and pinpoint anomalies.

### Rule-Based

Rule based IDS looks for the specific pattern which is defined as malicious.

In a Rule-based intrusion detection system, an attack can either be detected if a rule is found in the rule base or goes undetected if not found.

If this is combined with FIDS, the intrusions went undetected by RIDS can further be detected.

Rule-Based identifies potential attacks based on the set of rules configured on the system

<https://mesadeestudo.com/what-is-the-difference-between-the-rule-based-detection-when-compared-to-behavioral-detection>

upvoted 3 times

🗲️ 👤 **Entivo** 2 years, 4 months ago

The answer is (C) Behavioral systems are predefined patterns from hundreds of users, while Rule-Based only flags potentially abnormal patterns using signatures.

upvoted 2 times

🗲️ 👤 **WillBui** 2 years, 9 months ago

**Selected Answer: C**

It's C

upvoted 2 times

🗲️ 👤 **WillBui** 2 years, 9 months ago

My bad, correct answer is B

upvoted 3 times

🗲️ 👤 **halamah** 3 years, 1 month ago

d is correct

Behavioral summarize existing data

upvoted 2 times



A security incident occurred with the potential of impacting business services. Who performs the attack?

- A. threat actor
- B. malware author
- C. direct competitor
- D. bug bounty hunter

**Suggested Answer: A**

Reference:

[https://www.paubox.com/blog/what-is-threat-actor/#:~:text=The%20term%20threat%20actor%20refers,CTA\)%20when%20referencing%20cybersecurity%20issues](https://www.paubox.com/blog/what-is-threat-actor/#:~:text=The%20term%20threat%20actor%20refers,CTA)%20when%20referencing%20cybersecurity%20issues)

  **halamah** 7 months, 2 weeks ago

a is correct

upvoted 4 times



How does a certificate authority impact security?

- A. It authenticates domain identity when requesting an SSL certificate.
- B. It validates client identity when communicating with the server.
- C. It authenticates client identity when requesting an SSL certificate.
- D. It validates the domain identity of the SSL certificate.

**Suggested Answer:** *D*

Reference:

[https://en.wikipedia.org/wiki/Certificate\\_authority](https://en.wikipedia.org/wiki/Certificate_authority)

  **halamah** 7 months, 2 weeks ago

d is correct it validate certificate domain identity

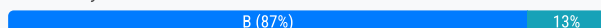
upvoted 2 times

Which data type is necessary to get information about source/destination ports?

- A. statistical data
- B. session data
- C. alert data
- D. connectivity data

**Suggested Answer: B**

Community vote distribution



**VividBot** **Highly Voted** 2 years, 8 months ago

Shouldn't the answer be session data? Session data provides information about the five tuples; source IP address/port number, destination IP address/port number and the protocol  
upvoted 17 times

**aiglart** **Highly Voted** 2 years, 4 months ago

**Selected Answer: B**

Session Data is the right answer.  
upvoted 5 times

**ethhacker** **Most Recent** 10 months ago

5 tuple session data. A is correct  
upvoted 1 times

**ethhacker** 10 months ago

sorry, B  
upvoted 2 times

**Topsecret** 11 months, 4 weeks ago

The correct answer is B. session data.

To obtain information about source/destination ports, you need to analyze session data. Session data refers to the information associated with a network session or connection between two devices. This data typically includes details such as source IP address, destination IP address, source port, destination port, protocol used, and other relevant information.

By examining session data, you can identify the specific ports being used by the source and destination devices. This information is crucial for network administrators and security professionals to understand network traffic patterns, identify potential vulnerabilities, and investigate network-related issues.  
upvoted 1 times

**Faio** 1 year ago

B.

To get information about source/destination ports, you need session data. Session data typically includes information about the network connections established between different devices or systems, including the source and destination IP addresses, as well as the corresponding source and destination ports.

Connectivity data generally refers to information about the availability and status of network connections. It may include details like whether a connection is active or inactive, but it may not specifically focus on source/destination ports.  
upvoted 1 times

**drdecker100** 1 year, 4 months ago

**Selected Answer: B**

Session data typically includes information about the communication session between two devices, including the source and destination IP addresses and port numbers. Port numbers are an important part of network communication because they allow different services to use the same IP address while still maintaining unique communication channels. By analyzing session data, network administrators can gain insight into the types of traffic on their network and identify potential security risks or performance issues.



C. Alert data is generated by security tools and indicates the detection of a specific event, such as an attempted intrusion or malware infection. While alerts can provide valuable information about security incidents, they do not necessarily include details about the ports used in the attack.

D. Connectivity data may include information about the availability or performance of network connections, but it typically does not include detailed information about the ports used for communication.

upvoted 1 times

🗨️ 👤 **SecurityGuy** 1 year, 7 months ago

**Selected Answer: D**

I believe "Connectivity Data" or "Connection Data" is correct. Knowing Cisco, the most simplest and sensible answer is always correct.

Let's define "Flow" first.

It is a unidirectional sequence of packets between two network endpoints that have the following 7 things in common:

1. Source IP Address
2. Destination IP Address
3. L3 Protocol Type
4. Source Port
5. Destination Port
6. Type of Service
7. Input Interface

Connection - It is a bidirectional flow.

Session - Many Connections between the same source and destination.

Socket - Single unidirectional flow

Connection Data already have source/destination ports present. Session is just multiple flows, the simplest one would be Connection Data.

<https://community.cisco.com/t5/application-networking/difference-between-session-connections-socket/td-p/2417074>

<https://community.cisco.com/t5/network-security/difference-between-session-and-connection/td-p/1846129>

upvoted 3 times

🗨️ 👤 **Neruneruuu** 1 year, 8 months ago

**Selected Answer: B**

Session data is correct

upvoted 1 times

🗨️ 👤 **gkp\_br** 1 year, 9 months ago

**Selected Answer: B**

B. "Session data".

upvoted 1 times

🗨️ 👤 **Entivo** 1 year, 11 months ago

**Selected Answer: B**

Got to be the TCP Session data surely?

upvoted 3 times

🗨️ 👤 **sakih** 1 year, 11 months ago

SESSION DATA

upvoted 2 times

🗨️ 👤 **Nhendy** 1 year, 11 months ago

**Selected Answer: B**

session data

upvoted 3 times

🗨️ 👤 **KKIIMM123** 2 years, 1 month ago

**Selected Answer: B**

i think its session

upvoted 3 times

🗨️ 👤 **Oscar14258** 2 years, 1 month ago

**Selected Answer: B**



Session data is required

upvoted 3 times

  **h821715** 2 years, 4 months ago

There is no connectivity data in the course, only session data is right here. Answer is B.


upvoted 4 times

  **Case** 2 years, 6 months ago

The Transport and Session layers keep track of all new connections, established connections and connections that are in the process of being torn down, which explains how Host A remembers that it's expecting a reply from the Internet Server.

Answer is "B" Session Data.

upvoted 2 times

  **halamah** 2 years, 7 months ago

c is correct its session

upvoted 1 times



Which event is a vishing attack?

- A. obtaining disposed documents from an organization
- B. using a vulnerability scanner on a corporate network
- C. impersonating a tech support agent during a phone call
- D. setting up a rogue access point near a public hotspot

**Suggested Answer:** C

Reference:

<https://www.cisco.com/c/en/us/products/security/email-security/what-is-phishing.html#~types-of-phishing-attacks>

  **halamah** 7 months, 2 weeks ago

c is correct

upvoted 2 times

  **eggheadsv** 7 months, 2 weeks ago

Answer is C.

A vishing attack, which is voice phishing, is a type of social engineering attack in which the threat actor makes a telephone call to the potential victim. The threat actor will pretend to be or impersonate someone who has the authority to convince the potential victim into performing an action, or even revealing sensitive information

upvoted 4 times

## DRAG DROP -

Drag and drop the security concept from the left onto the example of that concept on the right.

Select and Place:

threat	anything that can exploit a weakness that was not mitigated
risk	a gap in security or software that can be utilized by threats
vulnerability	possibility for loss and damage of an asset or information
exploit	taking advantage of a software flaw to compromise a resource

## Suggested Answer:

	threat
	vulnerability
	risk
	exploit

 **ethhacker** 10 months ago

Answer is correct

upvoted 2 times

 **SecurityGuy** 1 year, 5 months ago

Threat - Can exploit a weakness

Vulnerability - Gap in security

Risk - "Possibility" for loss and damage

Exploit - Attacking or "Compromising" a flaw or vulnerability.

upvoted 1 times

 **halamah** 2 years, 7 months ago

threat can exploit the weakness

gap is vulnerabikity

possibility is risk

compromis is exploit

upvoted 3 times



What is a difference between SIEM and SOAR?

- A. SIEM predicts and prevents security alerts, while SOAR checks attack patterns and applies the mitigation.
- B. SIEM's primary function is to collect and detect anomalies, while SOAR is more focused on security operations automation and response.
- C. SOAR's primary function is to collect and detect anomalies, while SIEM is more focused on security operations automation and response.
- D. SOAR predicts and prevents security alerts, while SIEM checks attack patterns and applies the mitigation.

**Suggested Answer:** *B*

Reference:

<https://www.cisco.com/c/en/us/products/security/what-is-a-security-platform.html>

  **halamah** 7 months, 2 weeks ago

correct

siem is log managment

soar is vulnerability managment that automat and response

upvoted 4 times

What is vulnerability management?

- A. A process to identify and remediate existing weaknesses.
- B. A process to recover from service interruptions and restore business-critical applications.
- C. A security practice of performing actions rather than acknowledging the threats.
- D. A security practice focused on clarifying and narrowing intrusion points.

**Suggested Answer: A**

Reference:

<https://www.brinqa.com/vulnerability-management-primer-part-2-challenges/>

🗨️ 👤 **Uzumaki\_Aliyy** 1 year ago

A is correct:

based on Cisco CyberOps Official Cert Guide by Omar Santos Page: 461.

upvoted 4 times

🗨️ 👤 **halamah** 1 year, 1 month ago

a is correct

upvoted 2 times

🗨️ 👤 **eggheadsv** 1 year, 1 month ago

Correct Answer: A

Vulnerability management is simply defined as the processes, techniques, and tools involved in discovering, prioritizing, assessing, remediating, and mitigating vulnerabilities on a system

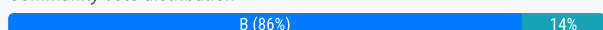
upvoted 2 times

What is a difference between signature-based and behavior-based detection?

- A. Signature-based identifies behaviors that may be linked to attacks, while behavior-based has a predefined set of rules to match before an alert.
- B. Behavior-based identifies behaviors that may be linked to attacks, while signature-based has a predefined set of rules to match before an alert.
- C. Behavior-based uses a known vulnerability database, while signature-based intelligently summarizes existing data.
- D. Signature-based uses a known vulnerability database, while behavior-based intelligently summarizes existing data.

**Suggested Answer: B**

Community vote distribution



**drdecker100** Highly Voted 1 year, 10 months ago

**Selected Answer: B**

Signature-based detection and behavior-based detection are two common approaches used in cybersecurity to detect and prevent attacks. The main difference between these two methods is how they identify potential threats.

Signature-based detection involves using a predefined set of rules, or signatures, to identify known patterns of malicious activity. These signatures are often based on specific characteristics of a known threat, such as a particular virus or malware strain. When a signature-based system detects a pattern that matches one of these predefined rules, it generates an alert or takes some other action to prevent the attack.

On the other hand, behavior-based detection focuses on identifying abnormal behavior that may indicate an attack. Instead of using predefined rules or signatures, behavior-based systems analyze patterns of activity to identify anomalies that may be indicative of an attack. For example, a behavior-based system might flag an unusual amount of network traffic from a particular device or identify a user accessing a critical system outside of normal business hours.

upvoted 8 times

**RoBery** Most Recent 11 months, 3 weeks ago

B is correct.

in D, it talks about known vulnerabilities, not known threats.

upvoted 1 times

**itmonkey1** 1 year, 9 months ago

I agree the answer is B because signature-based detection is only known threats. Known threats mean it most certainly has rules established already and detected based on pre-established rules.

upvoted 2 times

**trigger4848** 2 years, 1 month ago

**Selected Answer: D**

The answer is "D" and is correct. Read "B" carefully it says "Behavior-based identifies behaviors that may be linked to attacks" ---- this is not behavior based...this is almost the definition of signature based. Behavior based identifies anomalies

upvoted 3 times

**Nhendy** 2 years, 5 months ago

**Selected Answer: B**

vote for B too

upvoted 3 times

**anonymous1966** 2 years, 6 months ago

**Selected Answer: B**

Behavior is statistical, and can use AI and ML. "Summarize" is not correct


upvoted 1 times

**adodocletus** 2 years, 6 months ago

D is correct

the signature base uses a know vulnerability table, which means a vulnerability is already known and signed as a vulnerability. In contrast, the behavior base looks through already existing data and sees if there is abnormal behavior.



upvoted 4 times

  **PanteLa\_26** 2 years, 11 months ago

**Selected Answer: B**

Should be B imho

upvoted 3 times

  **DaveEly** 2 years, 11 months ago

I think it could be also B.

upvoted 1 times

  **Samuelpn96** 2 years, 11 months ago

**Selected Answer: B**

Instead of searching for patterns linked to specific types of attacks, behavior-based IDS solutions monitor behaviors that may be linked to attacks, increasing the likelihood of identifying and mitigating a malicious action before the network is compromised.

<https://accedian.com/blog/what-is-the-difference-between-signature-based-and-behavior-based-ids/>

upvoted 4 times

  **halamah** 3 years, 1 month ago

d is correct

upvoted 1 times



When communicating via TLS, the client initiates the handshake to the server and the server responds back with its certificate for identification. Which information is available on the server certificate?

- A. server name, trusted subordinate CA, and private key
- B. trusted subordinate CA, public key, and cipher suites
- C. trusted CA name, cipher suites, and private key
- D. server name, trusted CA, and public key

**Suggested Answer:** D

Community vote distribution

D (100%)

🗳️ 👤 **Leo\_Visser** Highly Voted 👍 2 years, 5 months ago

The server won't ever share its private key, so A and C are not right, and the cipher suite is in the handshake, not the certificate so B isn't right either. so D is correct.

upvoted 8 times

🗳️ 👤 **drdecker100** Most Recent 🕒 10 months, 2 weeks ago

**Selected Answer: D**

When a client initiates a TLS handshake with a server, the server sends its certificate to the client. The server certificate typically includes the server's domain name (i.e., server name), the public key of the server, and the name of the trusted Certificate Authority (CA) that issued the certificate.

The client uses the public key in the server certificate to encrypt a random value and send it back to the server, which can then decrypt it with its private key. This step establishes a secure channel between the client and server that they can use to exchange encrypted data.

upvoted 3 times

🗳️ 👤 **halamah** 2 years, 1 month ago

d is correct

server not share private key

upvoted 1 times

How does an SSL certificate impact security between the client and the server?

- A. by enabling an authenticated channel between the client and the server
- B. by creating an integrated channel between the client and the server
- C. by enabling an authorized channel between the client and the server
- D. by creating an encrypted channel between the client and the server

**Suggested Answer:** D

Community vote distribution

D (63%)

A (38%)

🗳️ 👤 **RoBery** 11 months, 3 weeks ago

.... impact security between.. = encryption

D is correct

upvoted 3 times

🗳️ 👤 **Faio** 1 year, 5 months ago

Selected Answer: D

An SSL certificate is a security credential that binds a public key to a website's identity. When a user visits a website that uses SSL, the browser will verify the website's certificate and establish an encrypted connection between the client and the server. This ensures that all data exchanged between the client and the server is protected from eavesdropping and tampering.

upvoted 4 times

🗳️ 👤 **drdecker100** 1 year, 10 months ago

Selected Answer: D

An SSL/TLS certificate is a digital certificate that is used to secure communications between a client and a server. When a client connects to a server using SSL/TLS, the server presents its SSL/TLS certificate, which includes a public key. The client then uses this public key to encrypt data that is sent to the server.

The SSL/TLS certificate provides assurance to the client that they are communicating with the intended server, and that the communication is encrypted and secure. This helps to prevent man-in-the-middle attacks, eavesdropping, and data tampering.

upvoted 2 times

🗳️ 👤 **SecurityGuy** 2 years, 1 month ago

Selected Answer: D

Secure Sockets Layer (SSL) is a standard security technology for establishing an encrypted link between a server and a client.

[https://www.digicert.com/what-is-an-ssl-certificate#:~:text=Secure%20Sockets%20Layer%20\(SSL\)%20is,client%20\(e.g.%2C%20Outlook\).](https://www.digicert.com/what-is-an-ssl-certificate#:~:text=Secure%20Sockets%20Layer%20(SSL)%20is,client%20(e.g.%2C%20Outlook).)

upvoted 2 times

🗳️ 👤 **cy\_analyst** 2 years, 2 months ago

Selected Answer: D

D ...creates an "encrypted channel" between client and server

upvoted 3 times

🗳️ 👤 **trigger4848** 2 years, 2 months ago

Selected Answer: D

SSL Certificates DO identify the server for Authentication, however I dont like the use of the term "Authentication Channel" in answer A. So I would go with encryption in this case

upvoted 3 times

🗳️ 👤 **fyticez** 2 years, 2 months ago

Selected Answer: A

"The server certificate is used for server authentication (by the client) and ensures that server can be trusted."

upvoted 3 times

🗳️ 👤 **Vano1** 2 years, 4 months ago

**Selected Answer: D**

IMHO - authenticated channel :)

D- correct answer

upvoted 3 times

🗨️ 👤 **netzbus** 2 years, 5 months ago

**Selected Answer: A**

SSL/TLS is an encryption protocol but certificate is for authentication so A is correct

upvoted 4 times

🗨️ 👤 **sh4dali** 2 years, 9 months ago

**Selected Answer: D**

D is correct

upvoted 3 times

🗨️ 👤 **[Removed]** 2 years, 10 months ago

in the book pg 207 it talks bout client to server authentication to web server. and that would then be A correct?

upvoted 2 times

🗨️ 👤 **sh4dali** 2 years, 9 months ago

No this is talking about SSL which is an encryption protocol

upvoted 2 times

🗨️ 👤 **halamah** 3 years, 1 month ago

d is correct

upvoted 2 times

Which attack is the network vulnerable to when a stream cipher like RC4 is used twice with the same key?

- A. forgery attack
- B. plaintext-only attack
- C. ciphertext-only attack
- D. meet-in-the-middle attack

**Suggested Answer: C**

Community vote distribution

C (100%)

 **drdecker100** 10 months, 2 weeks ago

**Selected Answer: C**

In a ciphertext-only attack, an attacker intercepts two ciphertexts encrypted using the same key and tries to obtain information about the plaintext or the key. With two ciphertexts encrypted using the same key, an attacker can XOR the two ciphertexts together to obtain the XOR of the two plaintexts. If the attacker can guess or obtain some of the plaintext, they can use it to recover the other plaintext by XORing it with the XOR of the two ciphertexts. This can allow the attacker to obtain the key and decrypt other messages encrypted using the same key.

Therefore, it is important to use a unique key for each encryption operation when using a stream cipher like RC4 to avoid such vulnerabilities.

upvoted 4 times

 **Samuelnpn96** 1 year, 11 months ago

**Selected Answer: C**

Early versions of Microsoft's PPTP virtual private network software used the same RC4 key for the sender and the receiver (later versions solved this problem but may still have other problems). In any case where a stream cipher like RC4 is used twice with the same key, it is open to ciphertext-only attack.

[https://simple.wikipedia.org/wiki/Ciphertext-](https://simple.wikipedia.org/wiki/Ciphertext-only_attack#:~:text=In%20cryptography%2C%20a%20ciphertext%20only,%2C%20even%20better%2C%20the%20key.)

[only\\_attack#:~:text=In%20cryptography%2C%20a%20ciphertext%20only,%2C%20even%20better%2C%20the%20key.](https://simple.wikipedia.org/wiki/Ciphertext-only_attack#:~:text=In%20cryptography%2C%20a%20ciphertext%20only,%2C%20even%20better%2C%20the%20key.)

upvoted 1 times

 **halamah** 2 years, 1 month ago

c is correct

cipher text is known cipher attach

upvoted 1 times

 **anonymous1966** 2 years, 3 months ago

"C" is correct.

RC4 is a Symmetric Algorithm (like DES, 3DES, AES, IDEA, RC2, RC4, RC5, RC6, Blowfish).

The aim of the ciphertext-only attack is to discover the cipher key because it was used twice the same key.

upvoted 3 times

 **anonymous1966** 2 years, 3 months ago

Early versions of Microsoft's PPTP virtual private network software used the same RC4 key for the sender and the receiver (later versions had other problems). In any case where a stream cipher like RC4 is used twice with the same key it is open to ciphertext-only attack.

Stream ciphers are vulnerable to attack if the same key is used twice (depth of two) or more.

Source: [https://en.wikipedia.org/wiki/Ciphertext-only\\_attack](https://en.wikipedia.org/wiki/Ciphertext-only_attack)

[https://en.wikipedia.org/wiki/Stream\\_cipher\\_attacks](https://en.wikipedia.org/wiki/Stream_cipher_attacks)

upvoted 1 times

 **Leo\_Visser** 2 years, 5 months ago

C is the right answer.

See the examples provided here:

[https://en.wikipedia.org/wiki/Ciphertext-only\\_attack](https://en.wikipedia.org/wiki/Ciphertext-only_attack)

upvoted 4 times

Which list identifies the information that the client sends to the server in the negotiation phase of the TLS handshake?

- A. ClientStart, ClientKeyExchange, cipher-suites it supports, and suggested compression methods
- B. ClientStart, TLS versions it supports, cipher-suites it supports, and suggested compression methods
- C. ClientHello, TLS versions it supports, cipher-suites it supports, and suggested compression methods
- D. ClientHello, ClientKeyExchange, cipher-suites it supports, and suggested compression methods

**Suggested Answer:** C

Community vote distribution

C (100%)

🗳️ 👤 **drdecker100** 10 months, 2 weeks ago

**Selected Answer: C**

During the negotiation phase of the TLS handshake, the client sends a ClientHello message to the server, which includes information about the TLS versions it supports, cipher-suites it supports, suggested compression methods, and other information. Therefore, the list that identifies the information that the client sends to the server in the negotiation phase of the TLS handshake is: ClientHello, TLS versions it supports, cipher-suites it supports, and suggested compression methods.

Option D is incorrect because ClientKeyExchange is sent later in the handshake, after the negotiation phase.

upvoted 4 times

🗳️ 👤 **SecurityGuy** 11 months, 1 week ago

**Selected Answer: C**

C is correct

Refer to: <https://www.cloudflare.com/learning/ssl/what-happens-in-a-tls-handshake/#:~:text=A%20TLS%20handshake%20is%20the,and%20agree%20on%20session%20keys>.

upvoted 1 times

🗳️ 👤 **Eng\_ahmedyoussef** 1 year, 2 months ago

**Selected Answer: C**

C is correct

upvoted 1 times

🗳️ 👤 **joseph267** 1 year, 5 months ago

C is correct

upvoted 1 times

🗳️ 👤 **halamat** 2 years, 1 month ago

c is correct

upvoted 1 times

🗳️ 👤 **anonymous1966** 2 years, 3 months ago

"C" is correct.

Reference: <https://www.ibm.com/docs/en/ibm-mq/7.5?topic=ssl-overview-tls-handshake>

upvoted 3 times

Severity	Date	Time	Sig ID	Source IP	Source Port	Dest IP	Dest Port	Description
6	Jan 15 2020	05:15:22	33883	62.5.22.54	22557	198.168.5.22	53	*

Refer to the exhibit. Which type of log is displayed?

- A. IDS
- B. proxy
- C. NetFlow
- D. sys

**Suggested Answer: A**

Community vote distribution

A (100%)

**andrewdh** Highly Voted 3 years ago

No - This is a IDS/IPS log. Look at the Signature ID  
upvoted 40 times

**samismayilov** 2 years, 9 months ago

agreed  
upvoted 5 times

**bren\_** Highly Voted 2 years, 12 months ago

Sig. ID is there, therefore the answer could be A: IDS  
upvoted 13 times

**slippery31** Most Recent 7 months, 1 week ago

Correct ANS= A  
upvoted 1 times

**alhamry** 8 months ago

The answer is D (IDS)

The log entry contains information about a signature ID, source and destination IP addresses, source and destination ports, and a severity rating. These are characteristics typically found in IDS logs (Intrusion Detection System). IDS logs provide information about security events detected by an IDS system, which monitors network traffic for signs of unauthorized activity or security policy violations. On the other hand, proxy logs record client connections to a proxy server, NetFlow logs capture network traffic data, and syslogs are a type of system log that captures messages from various components of a computer system.

upvoted 2 times

**alhamry** 8 months ago

sorry it's A (IDS)  
upvoted 2 times

**drdecker100** 10 months, 2 weeks ago

Selected Answer: A

"Sig ID" typically refers to a Signature ID, which is a unique identifier assigned to a particular security threat or event by an intrusion detection or prevention system (IDS/IPS). A log message that includes a Sig ID would suggest that the message is related to an alert triggered by the IDS/IPS in response to a security event.

upvoted 2 times

**cy\_analyst** 1 year, 3 months ago

Selected Answer: A

IDS and firewalls uses signatures.  
upvoted 1 times

**Entivo** 1 year, 4 months ago

**Selected Answer: A**

Looks more like an IDS/IPS log to me. Syslog doesn't have a Signature ID field so it can't be that.

upvoted 1 times

  **addpro7** 1 year, 8 months ago

**Selected Answer: A**

You also see the 5-tuple in IPS events, NetFlow records, and other event data. In fact, on the exam you may need to differentiate between a firewall log versus a traditional IPS or IDS event. One of the things to remember is that traditional IDS and IPS use signatures, so an easy way to differentiate is by looking for a signature ID (SigID). If you see a signature ID, then most definitely the event is a traditional IPS or IDS event.



Cisco CyberOps Associate\_P861

CBROPS 200-201 Official

Cert Guide



Omar Santos

upvoted 4 times

  **Dunky** 1 year, 9 months ago

OK - so what has the severity got to do with and IDS. Severity 6 is a syslog feature and means informational and represents a normal event. Why would a normal even have a sig id?

upvoted 1 times

  **aiglart** 1 year, 10 months ago

**Selected Answer: A**

A should be the answer, signature ID.

upvoted 1 times

  **CiscoTerminator** 2 years, 1 month ago

**Selected Answer: A**

SIG ID is present so IDS/IPS

upvoted 3 times

  **halamah** 2 years, 1 month ago

a is corrects

ids log

upvoted 2 times

  **alocin** 2 years, 2 months ago

you are right there is the signature ID column, but the first column is Severity

upvoted 2 times

  **Fafabeans** 3 years ago

Agreed.

upvoted 8 times

## Top 10 Src IP Addr ordered by flows:

Date first seen	Duration	Src IP Addr	Flows	Packets	Bytes	pps	bps	bpp
2019-11-30 06:45:50.990	1147.332	192.168.12.234	109183	202523	13.1 M	176	96116	68
2019-11-30 06:45:02.928	1192.834	10.10.151.203	62794	219715	25.9 M	184	182294	123
2019-11-30 06:59:24.563	330.110	192.168.28.173	27864	47943	2.2 M	145	55769	48

Refer to the exhibit. What information is depicted?

- A. IIS data
- B. NetFlow data
- C. network discovery event
- D. IPS event data

**Suggested Answer:** *B*

  **halamah**  7 months, 2 weeks ago

b is correct

alwyes duration is indicater for net flow

upvoted 8 times



What is the difference between the ACK flag and the RST flag in the NetFlow log session?

- A. The RST flag confirms the beginning of the TCP connection, and the ACK flag responds when the data for the payload is complete
- B. The ACK flag confirms the beginning of the TCP connection, and the RST flag responds when the data for the payload is complete
- C. The RST flag confirms the receipt of the prior segment, and the ACK flag allows for the spontaneous termination of a connection
- D. The ACK flag confirms the receipt of the prior segment, and the RST flag allows for the spontaneous termination of a connection

**Suggested Answer:** *D*

🗨️ 👤 **Eng\_ahmedyoussef** 8 months, 4 weeks ago

D is correct

upvoted 3 times

🗨️ 👤 **halamah** 1 year, 7 months ago

d is correct

ack (confirm received)

reset-termination

upvoted 4 times

Date	Flow Start	Duration	Proto	Src IP Addr:Port	Dst IP Addr:Port	Packets	Bytes	Flows
2020-01-05	21:15:28.389	0.000	UDP	127.0.0.1:25678	→ 192.168.0.1:20521	1	82	1

Refer to the exhibit. Which type of log is displayed?

- A. proxy
- B. NetFlow
- C. IDS
- D. sys

**Suggested Answer: B**

Community vote distribution

B (100%)

Eng\_ahmedyoussef **Highly Voted** 8 months, 4 weeks ago

**Selected Answer: B**

Duration ==> Netflow

upvoted 5 times

shibli\_zahir **Most Recent** 1 year, 6 months ago

**Selected Answer: B**

B is correct

upvoted 1 times

halamah 1 year, 7 months ago

b is correct

upvoted 1 times

How is NetFlow different from traffic mirroring?

- A. NetFlow collects metadata and traffic mirroring clones data.
- B. Traffic mirroring impacts switch performance and NetFlow does not.
- C. Traffic mirroring costs less to operate than NetFlow.
- D. NetFlow generates more data than traffic mirroring.

**Suggested Answer: A**

*Community vote distribution*

A (100%)

🗳️ 👤 **drdecker100** 10 months, 2 weeks ago

**Selected Answer: A**

NetFlow is a protocol developed by Cisco that allows network administrators to collect metadata about network traffic, such as source and destination IP addresses, traffic volumes, and protocols used. NetFlow works by capturing traffic at the network layer and generating flow records, which are then exported to a collector for further analysis. NetFlow data is typically used for network traffic analysis, capacity planning, and security monitoring.

Traffic mirroring, on the other hand, involves copying network traffic from a switch port and sending it to another port for analysis. This allows administrators to capture and inspect all of the data contained in the mirrored traffic, including payload content.

upvoted 2 times

🗳️ 👤 **Eng\_ahmedyoussef** 1 year, 2 months ago

**Selected Answer: A**

A. is correct

NetFlow ==> collects metadata.

traffic mirroring ==> clones data.

upvoted 1 times

🗳️ 👤 **halamah** 2 years, 1 month ago

a is correct

upvoted 2 times

What makes HTTPS traffic difficult to monitor?

- A. SSL interception
- B. packet header size
- C. signature detection time
- D. encryption

**Suggested Answer:** D

*Community vote distribution*

D (100%)

  **drdecker100** 10 months, 2 weeks ago

**Selected Answer: D**

HTTPS traffic is difficult to monitor because it is encrypted, which makes it more difficult for network administrators and security systems to inspect the contents of the traffic. The encryption used by HTTPS, which is typically based on SSL/TLS, ensures that data transmitted between the client and server is secure and cannot be easily intercepted or tampered with by third parties. However, this also means that anyone trying to monitor or inspect the traffic would need to decrypt it first in order to see its contents.

upvoted 3 times

  **halamah** 2 years, 1 month ago

d is correct

upvoted 1 times

How does an attacker observe network traffic exchanged between two users?

- A. port scanning
- B. man-in-the-middle
- C. command injection
- D. denial of service

**Suggested Answer: B**

*Community vote distribution*

B (100%)

🗨️ 👤 **Eng\_ahmedyoussef** 8 months, 4 weeks ago

**Selected Answer: B**

B is Correct

man in the middle ==> traffic exchanged between two users?

upvoted 1 times

🗨️ 👤 **halamah** 1 year, 7 months ago

b is correct

upvoted 1 times


Which type of data consists of connection level, application-specific records generated from network traffic?

- A. transaction data
- B. location data
- C. statistical data
- D. alert data

**Suggested Answer: A**

Community vote distribution

A (100%)

 **itmonkey1** 9 months, 1 week ago

Transaction is also the only option that makes sense  
upvoted 1 times

 **drdecker100** 10 months, 2 weeks ago

**Selected Answer: A**

ransaction data, also known as session data, is information generated by network connections between devices and servers, such as IP addresses, ports, protocols, and other metadata. It also includes details about the specific applications or services being used, such as URLs, HTTP headers, and other application-specific data.  
upvoted 2 times

 **SecurityGuy** 11 months, 1 week ago

**Selected Answer: A**

A is correct

Transactional Data:

It is the actual data that is exchanged during a session.

This type of data can be captured using a protocol analyzer such as TCP Dump or Wireshark.

Application-Specific records generated from network traffic. Logs deeper connection-level information, which may span multiple packets within a connection.

Must have predefined templates for protocol formatting. Common for logging HTTP header/request information, SMTP command data, etc.

[https://vwannabe.com/2017/02/07/ccna-cyber-ops-5-0-security-](https://vwannabe.com/2017/02/07/ccna-cyber-ops-5-0-security-monitoring/#:~:text=Security%20Monitoring)%20data-.5.2.,multiple%20packets%20within%20a%20connection.)

[monitoring/#:~:text=Security%20Monitoring\)%20data-.5.2.,multiple%20packets%20within%20a%20connection.](https://vwannabe.com/2017/02/07/ccna-cyber-ops-5-0-security-monitoring/#:~:text=Security%20Monitoring)%20data-.5.2.,multiple%20packets%20within%20a%20connection.)

[https://www.linkedin.com/learning/cisco-certified-cyberops-associate-200-201-cert-prep-2-security-monitoring/visualizing-session-and-transactional-](https://www.linkedin.com/learning/cisco-certified-cyberops-associate-200-201-cert-prep-2-security-monitoring/visualizing-session-and-transactional-data)  
data

upvoted 1 times

 **halamah** 2 years, 1 month ago

a is correct

upvoted 2 times

An engineer receives a security alert that traffic with a known TOR exit node has occurred on the network. What is the impact of this traffic?

- A. ransomware communicating after infection
- B. users downloading copyrighted content
- C. data exfiltration
- D. user circumvention of the firewall

**Suggested Answer:** D

Community vote distribution



**anonymous1966** Highly Voted 2 years, 3 months ago

Correct answer = D

A Tor exit node is basically the last Tor node or the gateway where the Tor encrypted traffic exits to the Internet. A Tor exit node can be targeted to monitor Tor traffic. Many organizations block Tor exit nodes in their environment. The Tor project has a dynamic list of Tor exit nodes that makes this task a bit easier. This Tor exit node list can be downloaded from <https://check.torproject.org/exit-addresses>.

upvoted 12 times

**drdecker100** Most Recent 10 months, 2 weeks ago

Selected Answer: D

The TOR (The Onion Router) network is often used to anonymize traffic on the internet, which can be beneficial for protecting privacy, but it can also be used to circumvent network security measures, such as firewalls. When traffic with a known TOR exit node occurs on a network, it means that a user is likely attempting to use TOR to bypass network restrictions and access restricted content or services.

Ransomware communicating after infection, users downloading copyrighted content, and data exfiltration are all potential security threats that could occur on a network, but they are not directly related to traffic with a known TOR exit node.

upvoted 1 times

**SecurityGuy** 11 months, 1 week ago

Selected Answer: D

TOR (The Onion Router)

It is an open-source privacy network that enables anonymous web browsing.

The Tor browser enables people to have access to the dark web.

TOR Exit Node

Tor moves encrypted traffic across a network of Tor servers and provides anonymity to users.

A Tor exit node is the final node that routes Tor traffic to a destination.

Circumvention

The process of avoiding something, especially cleverly or illegally.

Circumvention Tools

They are designed to bypass online censorship such as simple web proxies, virtual private network service, and so on.

Frequently used in countries whose governments impose heavy Internet censorship.

upvoted 2 times

**Binx** 11 months, 2 weeks ago

The question is What is the Impact?

NIST states "The magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system availability." To me the biggest

IMPACT here from TOR traffic is , Data Exfiltration. As an analyst, I would be more concerned with untraceable traffic like TOR, stealing data. I say Data Exfiltration.

upvoted 2 times

  **Binx** 11 months, 2 weeks ago

NIST states "Impact" as The magnitude of harm.... we need an edit tab with this post system.

upvoted 1 times

  **trigger4848** 1 year, 2 months ago

**Selected Answer: D**

I think D. Bc if the if the TOR exit node "is known" the only way there should be rules/firewalls in place to make sure that traffic never enters or is even allowed out of the network, so if its on the network D makes sense

upvoted 1 times

  **cy\_analyst** 1 year, 3 months ago

**Selected Answer: C**

I will use TOR exit to exfiltrate data from the network bypassing the firewall and the company rules.

upvoted 1 times

  **halamah** 2 years, 1 month ago

d is correct

tor unknown the identity of the browser ip

upvoted 1 times

  **[Removed]** 2 years, 3 months ago

It looks like that user used TOR browser to download content.

So it seems that the correct answer is:

B. users downloading copyrighted content

upvoted 1 times

  **skysoft** 3 years ago



This is a strange question. Detecting the address of a tor EXITnode means someone is using TOR to initiate communication with your network (server probably). When a user IN the network is connecting via TOR to circumvent the firewall, he is connecting to a "guard" node. (aka entry node).

Answer D is not the correct answer. For the same reason "B" is not correct either.

because of the inbound nature of the traffic, A or C are possible but should be blocked by the firewall.

I don't know the aswer, anyone ?

upvoted 2 times

  **tsabee** 2 years, 2 months ago

Funny... Actually every answer is correct from different aspect...

Only the C answer may be the weakest, beacuse the traffice come from TOR Exit node - so the traffic towards to firewall, it is received traffic, and the data exfiltration is rather than an upload traffic.

I'm hesitating between B and D, but the D is more "official" than the B. The B is only a type of using to TOR, not a definition.

I know it isn't so convincing argument, but may be this is the reason why I choose D.

Of course a firewall can block it, but as you know it is only a possibility. :)

upvoted 1 times

  **hoek** 2 years, 12 months ago

You probably answered yourself :) "A or C are possible but should be blocked by the firewall."

So firewall is not blocking the connection from TOR.

upvoted 1 times


  **Aimismynname** 2 years, 7 months ago

A user circumventing firewalls may connect to a guard node, but I think the data response will be considered to come from an exit node. I feel this is the answer.

Ransomware communicating from host to server would connect to guard node as you say. Same for data exfiltrating to a server on TOR.

I would say downloading copyrighted data is not strictly an "impact".

upvoted 1 times

  **bren\_** 2 years, 12 months ago

imho D is the only valid answer here. to use a TOR exit node could implicitly mean you're somehow finding a way around a firewall.



upvoted 12 times

  **anonymous1966** 2 years, 3 months ago

Agreed

upvoted 1 times

What is an example of social engineering attacks?

- A. receiving an unexpected email from an unknown person with an attachment from someone in the same company
- B. receiving an email from human resources requesting a visit to their secure website to update contact information
- C. sending a verbal request to an administrator who knows how to change an account password
- D. receiving an invitation to the department's weekly WebEx meeting

**Suggested Answer: B**

Community vote distribution



**JoJanathan** Highly Voted 4 years, 3 months ago

Not A. Because A is about an unexpected email from an unknown person. It's not C. Because C simply states a verbal request to an admin and anyone can pull that card. I doubt it's D anyone can receive a webex invite. But B. for sure picks a high level target you're the most likely to respond to. HR. I think B is correct.

upvoted 17 times

**MartinRB** 2 years, 4 months ago

I don't think it's B see ...to their secure website. Attacker would not send you HR's secure website.

upvoted 4 times

**anonymous1966** Highly Voted 3 years, 9 months ago

"B" is correct.

According to the book, Phishing is a social engineering technique. The first listed.

So the question is to identify which alternative is Phishing.

upvoted 8 times

**3000bd6** Most Recent 7 months, 1 week ago

I think B is the best answer

upvoted 1 times

**imbatnom** 8 months, 2 weeks ago

**Selected Answer: B**

Definitely B. It is tricking the victim into providing sensitive information, which is the main purpose of social engineering.

upvoted 1 times

**Twphill** 8 months, 2 weeks ago

**Selected Answer: A**

A is most likely, B,C,D are all routine business practices with no hint of malfeasance.

upvoted 1 times

**Faio** 1 year, 11 months ago

It's B

Social engineering attacks are based on tricking the victim into providing sensitive information or taking an action that is harmful to themselves or their organization. In this case, the attacker is trying to trick the victim into visiting a fake website that looks like the HR website. Once the victim enters their contact information on the fake website, the attacker can steal it.

The other options are not examples of social engineering attacks. Option A is an example of a phishing attack, but it is not a social engineering attack because the attacker is not trying to trick the victim into doing anything. Option C is an example of a legitimate request, and option D is an invitation to a meeting.

upvoted 2 times

**Topsecret** 1 year, 11 months ago

The correct answer for an example of a social engineering attack is:

B. receiving an email from human resources requesting a visit to their secure website to update contact information

This example represents a common social engineering technique known as phishing. The attacker impersonates a trusted entity (in this case, human resources) and tricks the recipient into visiting a fraudulent website to update their contact information. The purpose is to deceive the individual into divulging sensitive information or credentials, which can then be exploited for unauthorized access or other malicious purposes.

upvoted 1 times

🗳️ 👤 **drdecker100** 2 years, 4 months ago

**Selected Answer: B**

"B" is correct. Receiving an unexpected email from an unknown person with an attachment from someone in the same company is an example of a phishing email or a malware attack.

Sending a verbal request to an administrator who knows how to change an account password is an example of a legitimate request, assuming the requester is authorized to make the change.

Receiving an invitation to the department's weekly WebEx meeting is an example of a routine business communication and not an attack.

upvoted 3 times

🗳️ 👤 **MartinRB** 2 years, 4 months ago

**Selected Answer: C**

Social engineering sounds more like C.

A seems like phishing, B and D sounds legit.

upvoted 1 times

🗳️ 👤 **SecurityGuy** 2 years, 5 months ago

**Selected Answer: B**

B would be the most sensible answer.

upvoted 2 times

🗳️ 👤 **weganos** 2 years, 6 months ago

In other dumps this question appears a little different: Which two activities are examples of social engineering?

Which two activities are examples of social engineering? (Choose two)

A. receiving call from the IT department asking you to verify your username/password to maintain the account

B. receiving an invite to your department's weekly WebEx meeting

C. sending a verbal request to an administrator to change the password to the account of a user the administrator does know

D. receiving an email from MR requesting that you visit the secure HR website and update your contract information

E. receiving an unexpected email from an unknown person with an uncharacteristic attachment from someone in the same company

Correct Answer: AD

upvoted 2 times

🗳️ 👤 **CyberLogner** 2 years, 8 months ago

**Selected Answer: B**

Social Engineering is the key here, I think. Social Engineering implies that an action is taken to obtain information. the only option here that relates to information being obtained is B. A can be a good answer as well the only thing that does not line up for me is that it only states there is an attachment. this could be a DELIVERY sure but of what? an attachment could mean a lot of things. I'm voting for B as it is the only option that refers to information being requested which is in line with social engineering

upvoted 3 times

🗳️ 👤 **Lo\_Ma** 2 years, 9 months ago

I think B is correct.

Phishing attack definition :A threat actor sends fraudulent email which is disguised as being from a legitimate, trusted source to trick the recipient into installing malware on their device, or to share personal or financial information.

And in answer B Human resources looks legitimate and want you to share your information .

upvoted 1 times

🗳️ 👤 **knowone** 2 years, 10 months ago

**Selected Answer: A**

Its A because B implies the request is from your HR department and doesnt say its a spoofed email address. The question doesnt have enough information to make an accurate decision but with the given in A is the better answer.

upvoted 1 times

🗳️ 👤 **adodocletus** 3 years ago

Not B, I think A is the better answer... the email contains an attachment from some one in the same company

upvoted 1 times

🗳️ 👤 **DLukynskyy** 3 years, 3 months ago

Selected Answer: A

Not B: normal practice in large companies with HR applications available over web.

Not D: obviously

Why C: who is sending? Even if sent (say one left voicemail because his/her account is blocked), this is a normal case with procedure to follow.

A: Highly possible. Email may look like from the company, but not be one or company's account could be used. This is HoxHunt is for.

upvoted 1 times

  **carr1146** 3 years, 4 months ago

What are examples of social engineering attacks?

Image result for social engineering attack and phishing attack

Social engineering attack techniques

Baiting. As its name implies, baiting attacks use a false promise to pique a victim's greed or curiosity. ...

Scareware. Scareware involves victims being bombarded with false alarms and fictitious threats. ...

Pretexting. ...

Phishing. ...

Spear phishing.

upvoted 2 times

Interface: 192.168.1.29 --- 0x11		
Internet Address	Physical Address	Type
192.168.1.10	d8-a7-56-d7-19-ea	dynamic
192.168.1.67	d8-a7-56-d7-19-ea	dynamic
192.168.1.1	01-00-5e-00-00-16	static

Refer to the exhibit. What is occurring in this network?

- A. ARP cache poisoning
- B. DNS cache poisoning
- C. MAC address table overflow
- D. MAC flooding attack

**Suggested Answer: A**

Community vote distribution

A (100%)

🗳️ 👤 **SecurityGuy** 11 months, 1 week ago

**Selected Answer: A**

ARP Spoofing

Also known as ARP poisoning, is a Man in the Middle (MitM) attack that allows attackers to intercept communication between network devices.

The attack works as follows:

The attacker must have access to the network. They scan the network to determine the IP addresses of at least two devices.

The attacker uses a spoofing tool such as Arpspoof or Driftnet, to send out forged ARP responses.

The forged responses advertise that the correct MAC address for both IP addresses, belonging to the router and workstation, is the attacker's MAC address. This fools both router and workstation to connect to the attacker's machine, instead of to each other.

The two devices update their ARP cache entries and from that point onwards, communicate with the attacker instead of directly with each other.

The attacker is now secretly in the middle of all communications.

<https://www.imperva.com/learn/application-security/arp-spoofing/>

upvoted 3 times

🗳️ 👤 **Eng\_ahmedyoussef** 1 year, 2 months ago

**Selected Answer: A**

A. ARP cache poisoning is correct answer.

upvoted 2 times

🗳️ 👤 **halamah** 2 years, 1 month ago

A IS CORRECT

upvoted 2 times

Which data format is the most efficient to build a baseline of traffic seen over an extended period of time?

- A. syslog messages
- B. full packet capture
- C. NetFlow
- D. firewall event logs

**Suggested Answer: C**

Community vote distribution

C (89%)

11%

🗨️ **alhamry** 7 months, 3 weeks ago

The best answer is "C. NetFlow."

NetFlow is a protocol developed by Cisco for collecting IP traffic information as it enters or exits an interface of a router or switch. It provides detailed information about traffic flows, including the source and destination IP addresses, ports, protocols, and the amount of data transferred.

NetFlow data is a compact format that summarizes the network traffic data and is therefore an efficient way to build a baseline of traffic seen over an extended period of time. It can help detect patterns of network traffic that may be indicative of security threats or other abnormal activity.

In contrast, full packet capture and firewall event logs can provide more detailed information about network traffic but can be less efficient in terms of storage and processing requirements. Syslog messages can also provide valuable information, but may not provide the level of detail needed for building a baseline of traffic over an extended period of time.

upvoted 1 times

🗨️ **drdecker100** 10 months, 2 weeks ago

**Selected Answer: C**

NetFlow is a feature that provides network traffic information for network analysis, monitoring, and security. It is a protocol used to collect and record information about IP network traffic flows, including source and destination IP addresses, source and destination ports, protocol types, and other relevant information. NetFlow data can be stored and analyzed over time to gain insights into network usage and identify changes in traffic patterns.

Compared to full packet capture, which captures all packets in their entirety and can quickly become very large, NetFlow data is more compact and summarizes network traffic data.

upvoted 1 times

🗨️ **MartinRB** 10 months, 2 weeks ago

**Selected Answer: C**

This is a Cisco exam and NetFlow is Cisco product, they always root for theirs even if other products are better

upvoted 2 times

🗨️ **SecurityGuy** 11 months, 1 week ago

**Selected Answer: C**

Netflow

- It is a protocol developed by Cisco that is used to collect and record all IP Traffic going to and from a Cisco router or switch that is Netflow enabled.
- Keyword is "most efficient".

upvoted 3 times

🗨️ **hansamaru** 1 year, 1 month ago

The keywords is "most efficient", must be netflow

upvoted 2 times

🗨️ **cy\_analyst** 1 year, 2 months ago

**Selected Answer: B**

B because in the official book says: the details provided by capturing packets are necessary for establishing baselines as well as security requirements and therefore is the best approach versus what limited data NetFlow can provide. Throughput-546-Omar Santos.

upvoted 1 times

🗨️ 👤 **Eng\_ahmedyoussef** 1 year, 2 months ago

**Selected Answer: C**

Netflow ==> traffic seen over an extended #period of time#

upvoted 2 times

🗨️ 👤 **halamat** 2 years, 1 month ago

NET FLOW

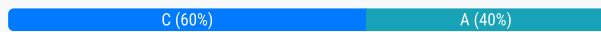
upvoted 2 times

Which action prevents buffer overflow attacks?

- A. variable randomization
- B. using web based applications
- C. input validation
- D. using a Linux operating system

**Suggested Answer: C**

Community vote distribution



🗳️ 👤 **Twphill** 8 months, 2 weeks ago

**Selected Answer: C**

Buffer overflow attacks are prevented by input validation.

upvoted 2 times

🗳️ 👤 **RoBery** 1 year, 5 months ago

c

Buffer overflow attacks can be prevented by implementing proper input validation & boundary checking in software, using secure coding practices, applying compiler-based protections like stack canaries & Address Space Layout Randomization [ASLR] & keeping software up to date with security patches.

upvoted 2 times

🗳️ 👤 **Faio** 1 year, 8 months ago

The answer is: C. input validation.

upvoted 3 times

🗳️ 👤 **Topsecret** 1 year, 11 months ago

The action that can help prevent buffer overflow attacks is:

C. input validation

Buffer overflow attacks occur when a program or application attempts to write data beyond the boundaries of a buffer, leading to overwriting adjacent memory areas. This can be exploited by an attacker to inject and execute malicious code.

Input validation refers to the process of checking and validating user input to ensure it meets the expected criteria and does not exceed the allocated buffer size. By implementing proper input validation techniques, such as length checks, input sanitization, and boundary checks, developers can prevent buffer overflow vulnerabilities.

upvoted 3 times

🗳️ 👤 **Isuckatexams** 2 years ago

**Selected Answer: A**

Several measures can be taken to prevent buffer overflows. These include address space layout randomization (ASLR), data execution prevention, and operating system runtime protections. ASLR is a technique that makes it harder for an attacker to predict where code will be executed in memory

upvoted 2 times

🗳️ 👤 **Eng\_ahmedyoussef** 2 years, 8 months ago

**Selected Answer: C**

C is correct (input sanitization)

upvoted 3 times

🗳️ 👤 **halamah** 3 years, 7 months ago

C IS CORRECT (input validation)


upvoted 2 times

🗳️ 👤 **Dion\_Weby** 3 years, 8 months ago

Input validation or input sanitization?



upvoted 3 times

  **joseph267** 2 years, 11 months ago

both are kind of similar however

What is input sanitisation?

Input sanitisation checks data that is entered and removes anything that might be potentially dangerous. A good example of this is on a website form. A hacker might try to gain access to a website's data through a SQL injection attack.

What is input validation?

Input validation is the process of testing input received by the application for compliance against a standard defined within the application. It can be as simple as strictly typing a parameter and as complex as using regular expressions or business logic to validate input.

upvoted 3 times

Which type of attack occurs when an attacker is successful in eavesdropping on a conversation between two IP phones?

- A. known-plaintext
- B. replay
- C. dictionary
- D. man-in-the-middle

**Suggested Answer:** D

Community vote distribution

D (100%)

🗨️ **abbeyade** 5 months, 2 weeks ago

**Selected Answer: A**

D is the correct answer

The attacker position himself between the two conversations to capture the traffic...

upvoted 1 times

🗨️ **Eng\_ahmedyoussef** 8 months, 4 weeks ago

**Selected Answer: D**

D. is correct answer

man in the middle ==> conversation #between# two IP phones.

upvoted 2 times

🗨️ **halamah** 1 year, 7 months ago

d is correct

upvoted 1 times

```
- Internet Protocol version 4, Src: 192.168.122.100 (192.168.122.100), Dst: 81.179.179.69 (81.179.179.69)
  Version: 4
  Header Length: 20 bytes
+ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
  Total Length: 538
  Identification: 0x6bse (27534)
+ Flags: 0x02 (Don't Fragment)
  Fragment offset: 0
  Time to live: 128
  Protocol: TCP (6)
+ Header checksum: 0x000 [Validation disabled]
  Source: 192.168.122.100 (192.168.122.100)
  Destination: 81.179.179.69 (81.179.179.69)
  [Source GeoIP: Unknown]

+ Transmission control protocol. src port: 50272 (50272) Dst Port: 80 (80).
  Seq: 419451624. Ack: 970444123. Len: 490
```

Refer to the exhibit. What should be interpreted from this packet capture?

- A. 81.179.179.69 is sending a packet from port 80 to port 50272 of IP address 192.168.122.100 using UDP protocol.
- B. 192.168.122.100 is sending a packet from port 50272 to port 80 of IP address 81.179.179.69 using TCP protocol.
- C. 192.168.122.100 is sending a packet from port 80 to port 50272 of IP address 81.179.179.69 using UDP protocol.
- D. 81.179.179.69 is sending a packet from port 50272 to port 80 of IP address 192.168.122.100 using TCP protocol.

**Suggested Answer: B**

Community vote distribution

B (100%)

Eng\_ahmedyoussef 8 months, 4 weeks ago

**Selected Answer: B**

B is correct answer

upvoted 2 times

halamah 1 year, 7 months ago

b is correct

tcp protoco; has flag and segment offset

upvoted 1 times

What are the two characteristics of the full packet captures? (Choose two.)

- A. Identifying network loops and collision domains.
- B. Troubleshooting the cause of security and performance issues.
- C. Reassembling fragmented traffic from raw data.
- D. Detecting common hardware faults and identify faulty assets.
- E. Providing a historical record of a network transaction.

**Suggested Answer:** CE

Community vote distribution



**evra** Highly Voted 4 years, 2 months ago

It is BE

upvoted 12 times

**harshi** 3 years, 12 months ago

why not C ? P Reassembly is a feature in Wireshark and TShark to automatically reassemble all fragmented IP Datagrams into a full IP packet before ... This feature will require a lot of extra memory to be consumed by wireshark in order to store the ... You have captured packets with a SnapLen less than the MTU of the ...

upvoted 1 times

**3000bd6** Most Recent 7 months, 1 week ago

Selected Answer: BE

B and E is the better answer

upvoted 2 times

**d503c75** 9 months, 2 weeks ago

BE is the correct answer.

About B: Packet capture enables teams to deal with complex network issues with ease and efficiency. - <https://www.solarwinds.com/resources/it-glossary/pcap>

upvoted 1 times

**RoBery** 1 year, 5 months ago

BD

Not only are network protocol analyzers used for security analysis. They are also very useful for network troubleshooting, software and protocol development, and education. For instance, in security forensics, a security analyst may attempt to reconstruct an incident from relevant packet captures.

upvoted 1 times

**sheyshey** 1 year, 6 months ago

Selected Answer: BE

B and E for me

upvoted 1 times

**toirdem** 1 year, 10 months ago

Selected Answer: BE

agree it is BE

upvoted 1 times

**Topsecret** 1 year, 11 months ago

The two characteristics of full packet captures are:

- B. Troubleshooting the cause of security and performance issues.
- E. Providing a historical record of a network transaction.

Options A, C, and D are not characteristics of full packet captures

upvoted 1 times


  **drdecker100** 2 years, 4 months ago

**Selected Answer: BE**

Option C is not necessarily wrong, but it is not one of the two characteristics of full packet captures that the question is asking for.

Reassembling fragmented traffic from raw data is a capability of full packet capture and can be useful for analyzing and understanding network traffic. However, the question is specifically asking for the two main characteristics of full packet capture.

upvoted 3 times

  **SecurityGuy** 2 years, 5 months ago

**Selected Answer: CE**

Let's start from the word itself. "Characterstics"

Characteristics - a feature or quality belonging typically to a person, place, or thing and serving to identify it.

>>Characteristics<<

- Reassembling fragmented traffic from raw data.
- Providing a historical record of a Network Transaction.

>>Use cases or Diagnostics<<

- Identifying network loops and Collision Domains.
- Troubleshooting the cause of security and performance issues.
- Detecting common hardware faults and identify faulty assets.

upvoted 3 times

  **cy\_analyst** 2 years, 8 months ago

**Selected Answer: CE**

Clearly bc we are here for cybersecurity, the other answers can be for net engineers.

upvoted 2 times

  **SecurityGuy** 2 years, 5 months ago

Yes, that makes sense. We should be thinking as Security / SOC Engineers and not as a Network Engineer.

upvoted 1 times

  **cy\_analyst** 2 years, 8 months ago

**Selected Answer: BE**

BE for right answer.

upvoted 1 times

  **cy\_analyst** 2 years, 8 months ago

not the right choice. If can please delete the comment.

upvoted 1 times

  **theodorrrr** 2 years, 8 months ago

So C E is the correct?

upvoted 1 times

  **Eng\_ahmedyoussef** 2 years, 8 months ago

**Selected Answer: CE**

C & E seems to be the correct answer .

upvoted 1 times

  **evra** 3 years, 2 months ago

It is BE. The question is about full packet capture and not about packet analysers.

"Full Packet Capture (FPC) provides a network defender an after-the-fact investigative capability that other security tools cannot provide. Uses include capturing malware samples, network exploits and determining if data exfiltration has occurred. Full packet captures are a valuable troubleshooting tool for operations and security teams alike."

<https://sansorg.egnyte.com/dl/v6XafdW96e>

upvoted 1 times

  **halamah** 3 years, 7 months ago

correct

it can ressample the data that in the same session

upvoted 2 times

🗨️ 👤 **alocin** 3 years, 9 months ago

C and E seem me correct answers.

I don't exclude B because for Troubleshooting often use Wireshark.

ops .. but this is third.

upvoted 1 times

🗨️ 👤 **[Removed]** 3 years, 9 months ago

I agree with anonymous1966. I think that correct answer is CE.

C. Reassembling fragmented traffic from raw data.

There is reassembly feature in Wireshark.

[https://wiki.wireshark.org/IP\\_Reassembly#](https://wiki.wireshark.org/IP_Reassembly#)

E. Providing a historical record of a network transaction.

Packet captures provide a full historical record of a

network transaction or an attack. It is important to

recognize that no other data source offers this level

of detail.

From Book:Omar Santos - Cisco CyberOps Associate CBROPS 200-201 Official Cert Guide

upvoted 1 times

🗨️ 👤 **anonymous1966** 3 years, 9 months ago

"C" is correct.

IP Reassembly

IP Reassembly is a feature in Wireshark and TShark to automatically reassemble all fragmented IP Datagrams into a full IP packet before calling the higher layer dissector.

Ref: [https://wiki.wireshark.org/IP\\_Reassembly](https://wiki.wireshark.org/IP_Reassembly)

This feature will require a lot of extra memory to be consumed by wireshark in order to store the reassembly buffers and is disabled by default.

"E" is correct.

By the book:

Packet captures provide a full historical record of a network transaction or an attack. It is important to recognize that no other data source offers this level of detail.

There are many study of cases of using Wireshark to troubleshooting the cause of security and performance issues. So, "B" would also be right. But the other options are more direct.

upvoted 4 times

<b>File name</b>	CVE-2009-4324 PDF 2009-11-30 note200911.pdf
<b>File size</b>	400918 bytes
<b>File type</b>	PDF document, version 1.6
<b>CRC32</b>	11638A9B
<b>MD5</b>	61baabd6fc12e01ff73ceacc07c84f9a
<b>SHA1</b>	0805d0ae62f5358b9a3f4c1868d552f5c3561b17
<b>SHA256</b>	27cced58a0fcbb0bbe3894f74d3014611039fefdf3bd2b0ba7ad85b18194c
<b>SHA512</b>	5a43bc7eef279b209e2590432cc3e2eb480d0f78004e265f00b98b4afdc9a
<b>Ssdeep</b>	1536:p0AAH2KthGBjcdBj8VETeePxsT65ZZ3pdx/ves/SQR/875+:prahGV6B
<b>PEiD</b>	None matched
<b>Yara</b>	<ul style="list-style-type: none"> <li>• embedded_pe (Contains an embedded PE32 file)</li> <li>• embedded_win_api (A non-Windows executable contains win32 API)</li> <li>• vmdetect (Possibly employs anti-virtualization techniques)</li> </ul>
<b>Virus Total</b>	<a href="#">Permalink</a> VirusTotal Scan Date: 2013-12-27 06:51:52 Detection Rate: 32/46 ( <a href="#">collapse</a> )

Refer to the exhibit. An engineer is analyzing this Cuckoo Sandbox report for a PDF file that has been downloaded from an email. What is the state of this file?

- A. The file has an embedded executable and was matched by PEiD threat signatures for further analysis.
- B. The file has an embedded non-Windows executable but no suspicious features are identified.
- C. The file has an embedded Windows 32 executable and the Yara field lists suspicious features for further analysis.
- D. The file was matched by PEiD threat signatures but no suspicious features are identified since the signature list is up to date.

**Suggested Answer: C**

Community vote distribution

C (100%)

🗳️ **abrahamberhanu** 10 months ago

**Selected Answer: C**

C is correct

upvoted 1 times

🗳️ **Eng\_ahmedyoussef** 2 years, 8 months ago

**Selected Answer: C**

c is correct answer

upvoted 2 times

🗳️ **halamah** 3 years, 7 months ago

correct

pe related to ext files

upvoted 2 times

## DRAG DROP -

Drag and drop the technology on the left onto the data type the technology provides on the right.

Select and Place:

tcpdump	session data
Cisco Umbrella	full packet capture
stateful firewall	transaction data
Snort	connection event

**Suggested Answer:**

tcpdump	stateful firewall
Cisco Umbrella	tcpdump
stateful firewall	Snort
Snort	Cisco Umbrella

 **anonymous1966** Highly Voted 3 years, 3 months ago

The correct answer is: StateFull Firewall, TCPDUMP, Cisco Umbrella, Snort

StateFull Firewall --> Session data

Session data is data about a network session that is usually established between two devices either on the same network or remote networks.

Session data contains the following elements, which are used to identify the details within the network session:

Source and destination IP addresses

Source and destination service ports

Layer 3 protocol details and code

TCPDUMP --> full packet capture

Cisco Umbrella (DNS) --> Transaction Data

The actual data that is exchanged during a session is known as transaction data. The actual data that is being sent across the network.

Snort (IDS) --> connection event

Connection events – These events are generated when a device establishes a session with another device on the network. When a session is detected by NGIPS, it creates a connection log that contains all the information about the session/connection itself.

Reference: Book Cisco Certified CyberOps Associate 200-201 Certification Guide - By Glen D. Singh

upvoted 23 times

 **anonymous1966** 3 years, 3 months ago


session data --> Statefull Firewall

full packet capt --> tcpdump

transaction data --> Cisco Umbrella

connection event --> Snort

upvoted 9 times

 **JoJanathan** Highly Voted 3 years, 9 months ago

Q95 Cleary shows Stateful firewall as connection event and TCP Dump as Full Packet Capture . But i have no idea on the other 2 items

<https://vwanabee.com/2017/02/07/ccna-cyber-ops-5-0-security-monitoring/>

upvoted 5 times



🗨️ 👤 **ivlis\_27** 3 years, 1 month ago

you should base it on that question, for me i think stateful firewall is session by this sentence

Session data: Session data is the summary of the communication between two network devices. Also known as a conversation or a flow, this summary data is one of the most flexible and useful forms of NSM (Network Security Monitoring) data.

meanwhile snort is connection event by this context:

Connection event: Connection events are the records of any connection that occurs in a monitored network.

upvoted 1 times

🗨️ 👤 **Dunky** 2 years, 9 months ago

From book by Singh "This firewall maintains a state of connections that are originating from the inside zone (internal) to the outside zone (the internet)."

upvoted 1 times

🗨️ 👤 **ivlis\_27** 3 years, 1 month ago

shouldnt

upvoted 1 times

🗨️ 👤 **Msal1134** 3 years, 7 months ago

Snort -> session data

Cisco umbrella -> transaction data

upvoted 6 times

🗨️ 👤 **RoBery** Most Recent 11 months, 3 weeks ago

the answer is correct.

Snort is IDS, as Zeek, which has a transaction data.

Umbrella is a DNS security tool that monitor the connections of urls.

upvoted 1 times

🗨️ 👤 **Topsecret** 1 year, 5 months ago

Session data is associated with stateful firewalls.

Full packet capture can be performed using tools like tcpdump.

Transaction data is a more general term and is not specifically associated with Cisco Umbrella.

Snort is an intrusion detection/prevention system and can detect connection events among other types of network activity.

upvoted 2 times

🗨️ 👤 **drdecker100** 1 year, 10 months ago

Session data: Session data refers to information about network sessions, including data such as the source and destination IP addresses, source and destination ports, protocol used, and the duration of the session. This type of data is typically generated by stateful firewalls, which keep track of the state of network connections.

Full packet capture: Full packet capture refers to capturing all the data that is transmitted over a network, including the packet headers and payloads.

This type of data is typically captured using packet capture software or appliances such as Wireshark or tcpdump.

Transaction data: Transaction data refers to data generated by a network application when a transaction occurs, such as a web server log recording a user's access to a website.

Connection event: A connection event refers to an event in which a device initiates or receives a connection attempt, such as a TCP SYN packet. This type of event is typically captured by network flow analysis tools like NetFlow or sFlow collectors or Snort.

upvoted 1 times

🗨️ 👤 **Eng\_ahmedyoussef** 2 years, 2 months ago

I think that correct answer is

\* tcp dump ==> full packet capture.

\* stateful firewall ==> session data.

\* cisco Umbrella (DNS) ==> transaction data.

\* snort ==> connection event.

upvoted 1 times

🗨️ 👤 **evra** 2 years, 8 months ago

Tcpdump -> full packet capture

Cisco Umbrella -> transaction data

Traditional stateful firewall -> connection event

Snort -> session data

Connection events – These events are generated when a device establishes a session with another device on the network. When a

session is detected by NGIPS, it creates a connection log that contains all the information about the session/connection itself. Each connection log will contain essential data, such as date and timestamps, source and destination IP addresses, and any other additional information that can be used to identify the session. Additionally, if an ACL blocks traffic on a router or firewall, the name of the ACL is also inserted within the connection event log on the device.

Reference: Book Cisco Certified CyberOps Associate 200-201 Certification Guide - By Glen D. Singh

upvoted 3 times

🗳️ 👤 **halamah** 3 years, 1 month ago

snort is session

umbrella is web data filtering so transaction

statfull firewall connection data

tcpdump-open source full packet capture

upvoted 4 times

🗳️ 👤 **tsabee** 3 years, 2 months ago

Snort is an IDS, so it should be provide alarm data...

TCPdump & Umbrella are clear, but the firewall provide I think connection data. Later in the question #110 it seems clearer.

Finally the session and IDS remains only..

upvoted 2 times

🗳️ 👤 **[Removed]** 3 years, 3 months ago

Session data = protocol, source ip, source port, destination ip, destination port, timestamps, packet count,

bytes transferred, 5-tuple information

Transaction data = data exchanged during session, for example email transfers, kerberos ticket information for active directory

upvoted 1 times

🗳️ 👤 **[Removed]** 3 years, 3 months ago

I think that correct answer is:

Session Data -> stateful firewall

full packet capture -> tcpdump (or it could be also wireshark)

transaction data -> cisco umbrella, it includes includes secure web gateway,

firewall, and cloud access security broker (CASB) functionality.

snort -> connection event

Session Data = information about client/server connections, the details of a session between two hosts

Transaction Data = "application data" that are exchanged during connection.

upvoted 2 times

🗳️ 👤 **xoe123** 3 years, 6 months ago

cisco umbrella does content filtering using DNS it makes sense that it uses session data and SNORT uses transaction data

upvoted 2 times

🗳️ 👤 **xoe123** 3 years, 6 months ago

It is easier to store large amounts of

NetFlow data because it is only a transactional record.

upvoted 1 times

🗳️ 👤 **xoe123** 3 years, 6 months ago

NetFlow provides information about network

session data, and NetFlow records take less space

than a full packet capture.

upvoted 1 times

🗳️ 👤 **JohnBB** 3 years, 7 months ago


According to <https://vwannabe.com/2017/02/07/ccna-cyber-ops-5-0-security-monitoring/>

NextGen IPS (Snort) -> Connection event

Session data - data is the summary of the communication between two network devices. -> hence FIREWALL

And then Umbrella - Transaction data: application-specific

upvoted 2 times

  **BigSwinger44** 2 years, 8 months ago

DNS functions at Application level = Transaction data:application specific  
upvoted 1 times

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.0.0.2	10.128.0.2	TCP	54	3341 → 80 [SYN] Seq=0 Win=512 Len=0
2	0.003987	10.128.0.2	10.0.0.2	TCP	58	80 → 3222 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 NSS=1460
3	0.005514	10.128.0.2	10.0.0.2	TCP	58	80 → 3341 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 NSS=1460
4	0.008429	10.0.0.2	10.128.0.2	TCP	54	3342 → 80 [SYN] Seq=0 Win=512 Len=0
5	0.010233	10.128.0.2	10.0.0.2	TCP	58	80 → 3220 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 NSS=1460
6	0.014072	10.128.0.2	10.0.0.2	TCP	58	80 → 3342 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 NSS=1460
7	0.016830	10.0.0.2	10.128.0.2	TCP	54	3343 → 80 [SYN] Seq=0 Win=512 Len=0
8	0.022220	10.128.0.2	10.0.0.2	TCP	58	80 → 3343 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
9	0.023496	10.128.0.2	10.0.0.2	TCP	58	80 → 3219 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
10	0.025243	10.0.0.2	10.128.0.2	TCP	54	3344 → 80 [SYN] Seq=0 Win=512 Len=0
11	0.026672	10.128.0.2	10.0.0.2	TCP	58	80 → 3218 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
12	0.028038	10.128.0.2	10.0.0.2	TCP	58	80 → 3221 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
13	0.030523	10.128.0.2	10.0.0.2	TCP	58	80 → 3344 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460

Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)  
 Ethernet II, Src: 42:01:0a:f0:00:17 (42:01:0a:f0:00:17), Dst: 42:01:0a:f0:00:01 (42:01:0a:f0:00:01)  
 Internet Protocol Version 4, Src: 10.0.0.2, Dst: 10.128.0.2  
 Transmission Control Protocol, Src Port: 3341, Dst Port: 80, Seq: 0, Len: 0

Source Port: 3341  
 Destination Port: 80  
 [Stream index: 0]  
 [TCP Segment Len: 0]  
 Sequence number: 0 (relative sequence number)  
 [Next sequence number: 0 (relative sequence number)]  
 Acknowledgement number: 1023350804  
 0101.... = Header Length: 20 bytes (5)  
 Flags: 0x002 (SYN)  
 Window size value: 512  
 [Calculated window size: 512]  
 Checksum: 0x8d5a [unverified]  
 [Checksum Status: Unverified]  
 Urgent pointer: 0  
 [Timestamps]

Refer to the exhibit. What is occurring in this network traffic?

- A. High rate of SYN packets being sent from a multiple source towards a single destination IP.
- B. High rate of ACK packets being sent from a single source IP towards multiple destination IPs.
- C. Flood of ACK packets coming from a single source IP to multiple destination IPs.
- D. Flood of SYN packets coming from a single source IP to a single destination IP.

**Suggested Answer: D**

Community vote distribution

D (100%)

**c79ecd3** 12 months ago

**Selected Answer: D**

The correct answer: D - Flood of SYN packets coming from a single source IP to a single destination IP.

upvoted 1 times

**AhmedAbdalla** 1 year, 8 months ago

In the provided network traffic capture, there is a flood of SYN packets (Synchronize) coming from a single source IP (10.128.0.2) to a single destination IP (10.0.0.2) on port 80. This is indicative of an attempt to establish multiple TCP connections.

Therefore, the correct answer is D. Flood of SYN packets coming from a single source IP to a single destination IP

upvoted 2 times

**surforlife** 2 years, 11 months ago

This is a loop in the network! Indeed is Flood of Syn and no final 3 way handshake as packet returns back to the source from the single destination.

upvoted 1 times

**BigSwinger44** 3 years, 2 months ago

What about the fact that the SYNS are coming from multiple ports?

upvoted 1 times

**halamah** 3 years, 7 months ago

yes its sync flood

upvoted 1 times

**[Removed]** 3 years, 9 months ago

The correct answer:D. Flood of SYN packets coming from a single source IP to a single destination IP.

upvoted 3 times





An engineer needs to have visibility on TCP bandwidth usage, response time, and latency, combined with deep packet inspection to identify unknown software by its network traffic flow. Which two features of Cisco Application Visibility and Control should the engineer use to accomplish this goal? (Choose two.)

- A. management and reporting
- B. traffic filtering
- C. adaptive AVC
- D. metrics collection and exporting
- E. application recognition

**Suggested Answer: DE**

Community vote distribution

DE (100%)

  **anonymous1966** Highly Voted 2 years, 3 months ago



Correct D and E

AVC can do many things. Attention to the question. The engineering needs:

visibility on several parameters - metrics collection and exporting (D)

identify unknown software by its network traffic flow - application recognition (E)

upvoted 10 times

  **drdecker100** Most Recent 10 months, 2 weeks ago

**Selected Answer: DE**

E. Application recognition: This feature allows the engineer to identify the type of application running on the network by analyzing its traffic flow. It can help identify unknown software and monitor the usage of known applications.

D. Metrics collection and exporting: This feature allows the engineer to collect and export network performance metrics such as TCP bandwidth usage, response time, and latency. These metrics can provide insights into the overall network performance and can help the engineer to identify and troubleshoot performance issues.

upvoted 2 times

  **pmackin124** 2 years, 4 months ago

DPI feature = Application Recognition

TCP performance = Metrics Collection and Exporting

upvoted 3 times

  **pmackin124** 2 years, 4 months ago


D and E are correct .

upvoted 3 times

  **harshi** 2 years, 5 months ago

Cisco Application Visibility and Control (AVC) uses deep packet inspection found in Layers 3 and 7 to recognize, analyse, and control over 1000 Applications that include voice and video, email, file sharing, gaming, peer-to-peer (P2P), and cloud-based Applications. AVC combines several Cisco IOS/IOS XE components, as well as communicating with external tools, to integrate the functions of Application Recognition; Metrics Collection and Exporting; Management and Reporting Systems; and Control, i.e. prioritization and management of application bandwidth, functionality into their firewall.

upvoted 2 times

  **harshi** 2 years, 5 months ago

why not A ?

upvoted 1 times

Which security technology guarantees the integrity and authenticity of all messages transferred to and from a web application?

- A. Hypertext Transfer Protocol
- B. SSL Certificate
- C. Tunneling
- D. VPN

**Suggested Answer:** B

*Community vote distribution*

B (100%)

🗳️ 👤 **Eng\_ahmedyoussef** 8 months, 4 weeks ago

**Selected Answer: B**

B is correct

SSL Certificate ==> is security technology guarantees the #integrity and #authenticity of all messages transferred to and from a #web application?  
upvoted 1 times

🗳️ 👤 **AVT** 1 year, 7 months ago

B is right yes

upvoted 1 times

🗳️ 👤 **halamah** 1 year, 7 months ago

yes its b

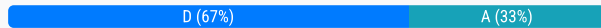
upvoted 1 times

An engineer is investigating a case of the unauthorized usage of the `Tcpdump` tool. The analysis revealed that a malicious insider attempted to sniff traffic on a specific interface. What type of information did the malicious insider attempt to obtain?

- A. tagged protocols being used on the network
- B. all firewall alerts and resulting mitigations
- C. tagged ports being used on the network
- D. all information and data within the datagram

**Suggested Answer: D**

Community vote distribution



**anonymous1966** Highly Voted 2 years, 9 months ago

The correct is "D"

Sniffing traffic on a specific interface sends to agent the full information.

upvoted 16 times

**fejec** 2 years, 9 months ago

using verbose parameter (-v or -vv) increases the amount of detail shown in the output, showing more than tagged protocols.

upvoted 3 times

**ivlis\_27** 2 years, 7 months ago

i think D correct because sniffing on specific interface doesn't mean you only get the tagged protocol, if you try you still get many information beside tagged protocol

upvoted 2 times

**CCNPTT** Most Recent 7 months, 2 weeks ago

**Selected Answer: D**

"Datagram" is NOT only related to UDP, I'm surprised people mentioning it.

Just read latest version of the TCP RFC, RFC 9293:

"TCP segments are sent as internet datagrams. The Internet Protocol (IP) header carries several information fields, including the source and destination host addresses."

"datagram: A message sent in a packet-switched computer communications network."

Answer is D.

upvoted 1 times

**Faio** 11 months, 1 week ago

The answer is D.

Tcpdump is a command-line tool used to capture and analyze network traffic in real-time. By sniffing traffic on a specific interface, the malicious insider could potentially obtain all information and data within the datagram, including:

The source and destination IP addresses

The source and destination ports

The protocol type

The payload data

he other options are not correct. Option A is incorrect because tagged protocols are not part of the datagram. Option B is incorrect because firewall alerts and resulting mitigations are not captured by tcpdump. Option C is incorrect because tagged ports are not part of the datagram.

upvoted 1 times

**Topsecret** 11 months, 3 weeks ago



D. all information and data within the datagram

Tcpdump is a packet capture tool that allows users to capture and analyze network packets in real-time. By capturing network traffic on a specific interface, the malicious insider would have been able to intercept and inspect the contents of the captured packets. This includes the payload data, headers, and any other information contained within the network datagrams.

upvoted 1 times

🗨️ 👤 **Isuckatexams** 1 year ago

**Selected Answer: D**

You could use NMAP for tagged protocols. Why use TCPDUMP or Wireshark for anything other than packet inspection?

upvoted 1 times

🗨️ 👤 **drdecker100** 1 year, 4 months ago

**Selected Answer: D**

The malicious insider attempted to obtain D. all information and data within the datagram by using the Tcpdump tool to sniff the traffic on a specific interface. Tcpdump is a powerful tool that can capture and display the contents of network packets, including the data within the datagram. By analyzing the captured data, the malicious insider can potentially obtain sensitive information such as login credentials, financial data, or confidential business information. This type of unauthorized network monitoring is a serious security threat, and appropriate measures should be taken to prevent it from happening in the future.

upvoted 1 times

🗨️ 👤 **aaawnd** 1 year, 6 months ago

**Selected Answer: D**

Datagram is not exclusive of UDP

upvoted 2 times

🗨️ 👤 **cy\_analyst** 1 year, 8 months ago

**Selected Answer: A**

A is correct, D uses the word datagram which is a UDP only concept. Tcpdump can take full packet capture.

upvoted 1 times

🗨️ 👤 **CCNPTT** 7 months, 2 weeks ago

Datagram \*IS NOT\* UDP only.

upvoted 1 times

🗨️ 👤 **aplicacion101** 1 year, 11 months ago

**Selected Answer: A**

No, the answer is good, in D the word datagrama damages the answer. It is most wise to select protocols, so A is the best answer

upvoted 3 times

🗨️ 👤 **tor\_bap** 2 years, 6 months ago

**Selected Answer: D**

The answer should be D

upvoted 3 times

🗨️ 👤 **halamah** 2 years, 7 months ago

Correct ID full data

upvoted 2 times

At a company party a guest asks questions about the company's user account format and password complexity. How is this type of conversation classified?

- A. Phishing attack
- B. Password Revelation Strategy
- C. Piggybacking
- D. Social Engineering

**Suggested Answer:** D

Community vote distribution

D (100%)

🗨️ 👤 **036e554** 11 months, 1 week ago

The answer is D

Social engineering involve manipulating individuals into divulging confidential information or performing actions that are against security policies.  
upvoted 1 times

🗨️ 👤 **Eng\_ahmedyoussef** 2 years, 8 months ago

**Selected Answer: D**

yes, it is social engineering strategy.

i think D is correct Answer.

upvoted 1 times

🗨️ 👤 **DLukynskyy** 3 years, 3 months ago

a variation of phishing attack is the social engineering attack. These identity attacks use the social conventions of the workplace to fool users  
upvoted 1 times

🗨️ 👤 **halamah** 3 years, 7 months ago

yes its d

upvoted 1 times

Which security monitoring data type requires the largest storage space?

- A. transaction data
- B. statistical data
- C. session data
- D. full packet capture

**Suggested Answer:** D

*Community vote distribution*

D (100%)

Eng\_ahmedyoussef 8 months, 4 weeks ago

**Selected Answer: D**

D. Full packet Capture .

upvoted 2 times

halamah 1 year, 7 months ago

yes its d

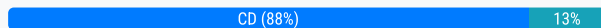
upvoted 1 times

What are two denial of service attacks? (Choose two.)

- A. MITM
- B. TCP connections
- C. ping of death
- D. UDP flooding
- E. code red

**Suggested Answer:** CD

Community vote distribution



**beowolf** Highly Voted 3 years, 7 months ago

Ping of death and UDP flooding are correct.

Code Red was a computer worm observed on the Internet in 2001

upvoted 34 times

**VegasBF** 3 years, 5 months ago

Agree with you!

upvoted 4 times

**anonymous1966** Highly Voted 3 years, 3 months ago

C and D are correct

A UDP flood is a type of denial-of-service attack in which a large number of User Datagram Protocol (UDP) packets are sent to a targeted server with the aim of overwhelming that device's ability to process and respond.

A Ping of death (PoD) attack is a denial-of-service (DoS) attack, in which the attacker aims to disrupt a targeted machine by sending a packet larger than the maximum allowable size, causing the target machine to freeze or crash.

<https://www.cloudflare.com/pt-br/learning/ddos/udp-flood-ddos-attack/>

<https://www.cloudflare.com/pt-br/learning/ddos/ping-of-death-ddos-attack/>

upvoted 10 times

**fejec** 3 years, 3 months ago

Agree, because UDP flooding is used for reflected or amplifications DoS attacks (DDoS), for example using protocols DNS, NTP.

upvoted 1 times

**Faio** Most Recent 1 year, 3 months ago

The two denial of service attacks are C. ping of death and D. UDP flooding.

upvoted 2 times

**Faio** 1 year, 5 months ago

The correct answers are C. ping of death and D. UDP flooding.

upvoted 2 times

**slippery31** 1 year, 6 months ago

CORRECT ANS = C D

upvoted 1 times

**drdecker100** 1 year, 10 months ago

Selected Answer: CD

The two denial of service attacks are:

C. Ping of death: This is a type of denial of service attack where an attacker sends a ping packet that is larger than the maximum size allowed by the IP protocol. When the target system receives this oversized packet, it can crash or become unresponsive. This type of attack exploits a vulnerability in the target system's network stack and can affect a wide range of systems.

D. UDP flooding: This is a type of denial of service attack where an attacker floods a target system with a large number of User Datagram Protocol

(UDP) packets. The target system becomes overwhelmed with the flood of incoming packets, and as a result, legitimate traffic cannot get through. This type of attack can be particularly effective against applications that rely heavily on UDP traffic, such as online gaming or VoIP applications.

upvoted 2 times

🗨️ 👤 **SecurityGuy** 1 year, 11 months ago

Selected Answer: CD

Correct Answer: Ping of Death and UDP Flooding

- Code Red was initially written to deface the infected computer's Web site and to perform a "Distributed Denial of Service (DDoS) Attack" against the numerical Internet address used by www.whitehouse.gov.

- Two subsequent versions of Code Red do not deface Web pages but still launch the DDoS attack.

Explanation: The question only asks DOS Attack and not DDOS Attack.

upvoted 2 times

🗨️ 👤 **Silexis** 11 months, 1 week ago

I think that you have answered to my doubts. I was on CD and now I realize it is CE - thank you! The idea is the UDP Flood is a DDOS. A pure DOS will crash a service through a flaw in that service so both PoD and CR were exactly what they were doing. I remember the days of Windows 98 when a ICMP with big size was generating a blue screen.....

upvoted 1 times

🗨️ 👤 **Eng\_ahmedyoussef** 2 years, 2 months ago

Selected Answer: CD

I am Sure C & D is the correct answer

Denial of service attack caused by /

\* Ping of Death

\* UDP Flooding

upvoted 2 times

🗨️ 👤 **Eng\_ahmedyoussef** 2 years, 2 months ago

Selected Answer: CD

I am Sure C & D is the correct answer

Denial of service attach caused by /

\* Ping of Death

\* UDP Flooding

upvoted 1 times

🗨️ 👤 **cy\_analyst** 2 years, 2 months ago

Selected Answer: CD

Ping of death & UDP flooding

upvoted 1 times

🗨️ 👤 **fjcsanchez** 2 years, 3 months ago

C and D are correct.

<https://openwebinars.net/blog/top-10-de-ataques-dos-denial-of-service-o-denegacion-de-servicios/>

upvoted 1 times

🗨️ 👤 **Vano1** 2 years, 4 months ago

Selected Answer: CD

C and D are correct

upvoted 1 times

🗨️ 👤 **PraygeForPass** 2 years, 5 months ago

Selected Answer: CD

C and D.

The question does not state "Distributed" DoS, just DoS.

Code Red is a DDoS attack, where as ping of death and UDP floods can be just DoS attacks.

upvoted 1 times

🗨️ 👤 **Alvesbtc** 2 years, 5 months ago

Ping of death and UDP flooding are some of the many DoS attack types while Code Red was a computer worm observed on the internet in the year 2001. So C and D are correct

upvoted 1 times

🗨️ 👤 **DLukynskyy** 2 years, 9 months ago

**Selected Answer: CD**

"flooding" is the keyword

upvoted 1 times

🗨️ 👤 **tor\_bap** 3 years ago

**Selected Answer: CD**

It's Should be C&D

upvoted 3 times

🗨️ 👤 **afifulinuha** 3 years ago

**Selected Answer: CE**

Code Red is a worm that was discovered on 13 July 2001. It is famously known for its (DDoS) Denial of Service attack on the USA White house web server and for its famous "Hacked by Chinese" signature. The virus targeted computers with Microsoft IIS Web installed particularly the Windows NT and Windows 2000 systems.

source: [www.computersdemystified.com/code-red-virus/](http://www.computersdemystified.com/code-red-virus/)

upvoted 2 times

An engineer needs to discover alive hosts within the 192.168.1.0/24 range without triggering intrusive portscan alerts on the IDS device using Nmap. Which command will accomplish this goal?

- A. `nmap --top-ports 192.168.1.0/24`
- B. `nmap -sP 192.168.1.0/24`
- C. `nmap -sL 192.168.1.0/24`
- D. `nmap -sV 192.168.1.0/24`

**Suggested Answer: B**

Community vote distribution

B (92%)

8%

 **JohnBB** Highly Voted 3 years ago

Correct answer is C. `nmap -sL 192.168.1.0/24`  
<https://nmap.org/book/host-discovery-controls.html>  
<https://nmap.org/book/man-briefoptions.html>  
`-sL`: List Scan - simply list targets to scan  
 upvoted 14 times

 **Entivo** 1 year, 10 months ago

With respect you are wrong. The `-sL` switch simply lists which hosts to perform a port scan against, which will trigger your IDS/IPS. You need the `-sP` switch to skip port scanning and check for live hosts.  
 upvoted 6 times

 **AhmedAbdalla** Most Recent 8 months, 3 weeks ago

`Nmap -sP 192.168.1.0/24`

This command will perform a simple ping scan to identify hosts that are alive in the specified IP range without performing a detailed port scan, which is less likely to trigger intrusive alerts on IDS devices.  
 upvoted 1 times

 **alhamry** 1 year, 2 months ago

The best answer is B.

The engineer needs to discover alive hosts within the 192.168.1.0/24 range without triggering intrusive portscan alerts on the IDS device using Nmap. The `--sP` option in Nmap sends an ICMP echo request, TCP SYN to port 443, TCP ACK to port 80, and ICMP timestamp request probes to determine if a host is up. This is a non-intrusive method of host discovery and does not send any probes to specific ports that could trigger alerts on an IDS device.

Option A (`--top-ports`) is used to scan the top N most frequently used ports on a host, and is not used for host discovery.

Option C (`-sL`) sends a list scan and does not send any probes to determine if a host is up. This option simply lists the targets that would be scanned by Nmap.

Option D (`-sV`) is used for version detection and does not send any probes to determine if a host is up.  
 upvoted 1 times

 **drdecker100** 1 year, 4 months ago

Selected Answer: B

The `"-sP"` option instructs Nmap to perform a simple ping scan to determine which hosts are alive on the network. This type of scan does not send any packets to the target hosts' ports, so it should not trigger any intrusive portscan alerts on the IDS device. The output of this command will list the IP addresses of the live hosts found on the network.  
 upvoted 2 times

 **cy\_analyst** 1 year, 9 months ago

Selected Answer: B

-sn (No port scan) This option tells Nmap not to do a port scan after host discovery, and only print out the available hosts that responded to the host discovery probes.

In previous releases of Nmap, -sn was known as -sP.

upvoted 4 times

🗳️ 👤 **weganos** 1 year, 9 months ago

**Selected Answer: B**

I think the answer is B from what I read in all the links below.

upvoted 1 times

🗳️ 👤 **Entivo** 1 year, 10 months ago

**Selected Answer: B**

The answer is B. The -sP option skips port scanning and checks for live hosts in the network. See this link [https://www.golinuxcloud.com/nmap-command-in-](https://www.golinuxcloud.com/nmap-command-in-linux/#:~:text=nmap%20command%20allows%20you%20to%20scan%20a%20system,by%20using%20an%20IP%20address%20with%20nmap%20command.)

[linux/#:~:text=nmap%20command%20allows%20you%20to%20scan%20a%20system,by%20using%20an%20IP%20address%20with%20nmap%20command.](https://www.golinuxcloud.com/nmap-command-in-linux/#:~:text=nmap%20command%20allows%20you%20to%20scan%20a%20system,by%20using%20an%20IP%20address%20with%20nmap%20command.)

upvoted 1 times

🗳️ 👤 **momoamek** 1 year, 11 months ago

B is correct

-sP allows light reconnaissance of a target network

without attracting much attention. Knowing how many hosts are up is more valuable to attackers than the list provided by list scan of every single IP and host name.

upvoted 1 times

🗳️ 👤 **BigSwinger44** 2 years, 2 months ago

B is correct.

Supported here. [https://linuxhint.com/nmap\\_ping\\_sweep/](https://linuxhint.com/nmap_ping_sweep/)

upvoted 1 times

🗳️ 👤 **J8Ryan** 2 years, 4 months ago

**Selected Answer: B**

-sP solo realizar ping (igual que con -PP -PM -PS443 -PA80), descubriendo así los host vivos de la red sin escaneo de puertos, tal y como dice la pregunta.

upvoted 1 times

🗳️ 👤 **mariodesa** 2 years, 5 months ago

**Selected Answer: B**

-sL (List Scan)

The list scan is a degenerate form of host discovery that simply lists each host of the network(s) specified, without sending any packets to the target hosts. By default, Nmap still does reverse-DNS resolution on the hosts to learn their names. It is often surprising how much useful information simple hostnames give out.

-sn (No port scan)

This option tells Nmap not to do a port scan after host discovery, and only print out the available hosts that responded to the host discovery probes.

This is often known as a "ping scan", but you can also request that traceroute and NSE host scripts be run. This is by default one step more intrusive than the list scan, and can often be used for the same purposes. It allows light reconnaissance of a target network WITHOUT ATTRACTING MUCH ATTENTION. Knowing how many hosts are up is more valuable to attackers than the list provided by list scan of every single IP and host name.

IN PREVIOUS RELEASES OF NMAP, -sn WAS KNOWN AS -sP.

Correct answer is B

Source: <https://nmap.org/book/man-host-discovery.html>

upvoted 2 times

🗳️ 👤 **DubDubDub** 2 years, 5 months ago

B is correct: <https://explainshell.com/explain?cmd=nmap+-sP>

upvoted 2 times

🗳️ 👤 **tor\_bap** 2 years, 6 months ago

**Selected Answer: C**

ans should be C

upvoted 1 times



🗨️ 👤 **alocin** 2 years, 9 months ago

from NMAP Cheat Sheet

-sn: Probe only (host discovery, not port scan)

-sS: SYN Scan

-sT: TCP Connect Scan

-sU: UDP Scan

-sV: Version Scan

-O: Used for OS Detection/fingerprinting

--scanflags: Sets custom list of TCP using URG ACK PSH RST SYN FIN in any order

upvoted 1 times

🗨️ 👤 **Alannn** 2 years, 9 months ago

nmap 192.168.1.1-3 -sL

No Scan. List targets only

nmap 192.168.1.1/24 -sn

Disable port scanning. Host discovery only.

So -Sn is the correct answer seeing the question is asking about alive hosts.

upvoted 1 times

🗨️ 👤 **Alannn** 2 years, 9 months ago

But seeing this is not an option the next best thing is -sL

upvoted 2 times

🗨️ 👤 **fejec** 2 years, 9 months ago

The -sP is the ping sweep, this parameter don't make a port scanning. Try by your self on your network.

upvoted 1 times

🗨️ 👤 **qz999** 2 years, 10 months ago

The -sL list scan still scans the listed targets. Though not given an an answer choice, the -sn options causes nmap to ping sweep only without any port scanning.

upvoted 1 times

Which open-sourced packet capture tool uses Linux and Mac OS X operating systems?

- A. NetScout
- B. tcpdump
- C. SolarWinds
- D. netsh

**Suggested Answer:** B

*Community vote distribution*

B (100%)

🗳️ 👤 **AhmedAbdalla** 8 months, 4 weeks ago  
tcpdump

Tcpdump is an open-source packet capture tool primarily used on Unix-like operating systems, including Linux and macOS. It allows users to capture and analyze network traffic for troubleshooting, monitoring, and security analysis purposes. Netsh is a Windows command-line utility, and SolarWinds and NetScout are software solutions that provide network monitoring and management but are not packet capture tools like tcpdump.

upvoted 2 times

🗳️ 👤 **Eng\_ahmedyoussef** 1 year, 8 months ago

**Selected Answer: B**

TCP Dump ==> open-sourced packet capture tool uses Linux and Mac OS X operating systems.

upvoted 1 times

🗳️ 👤 **Uzumaki\_Aliyy** 2 years, 6 months ago

B is correct. check cisco cyberops associate by Omar Santos pg-683/684

upvoted 2 times

```
<IMG SRC=j%41vascript:alert('attack')>
```

Refer to the exhibit. Which kind of attack method is depicted in this string?

- A. cross-site scripting
- B. man-in-the-middle
- C. SQL injection
- D. denial of service

**Suggested Answer: A**

Community vote distribution

A (100%)

🗲️ 👤 **SecurityGuy** 11 months ago

**Selected Answer: A**

Cross-site scripting works by manipulating a vulnerable web site so that it returns malicious JavaScript to users.

Key word: Java

upvoted 3 times

🗲️ 👤 **Eng\_ahmedyoussef** 1 year, 2 months ago

**Selected Answer: A**

A. cross-site scripting

upvoted 2 times

🗲️ 👤 **JayPEI** 1 year, 6 months ago

**Selected Answer: A**

A is correct

upvoted 2 times

Which two components reduce the attack surface on an endpoint? (Choose two.)

- A. secure boot
- B. load balancing
- C. increased audit log levels
- D. restricting USB ports
- E. full packet captures at the endpoint

**Suggested Answer:** AD

Community vote distribution

AD (100%)

🗨️ 👤 **AhmedAbdalla** 8 months, 4 weeks ago

The two components that reduce the attack surface on an endpoint are:

Secure boot: Secure boot is a process that ensures the integrity and authenticity of the firmware and operating system that are loaded on an endpoint device when it starts up. It helps prevent malicious code from being executed during the boot process, reducing the attack surface by ensuring only trusted software is run.

Restricting USB ports: By restricting or disabling USB ports on an endpoint device, you can reduce the risk of malware being introduced through external devices like USB drives. This limits the attack surface by preventing unauthorized or potentially malicious USB devices from being connected to the endpoint.

(full packet captures at the endpoint), (increased audit log levels), and (load balancing) are not directly related to reducing the attack surface on an endpoint.

upvoted 2 times

🗨️ 👤 **Eng\_ahmedyoussef** 1 year, 8 months ago

**Selected Answer:** AD

- A. secure boot
- D. restricting USB ports

upvoted 1 times

🗨️ 👤 **anonymous1966** 2 years, 9 months ago

The keyword here is "endpoint". The only two items related to endpoint is secure boot and USB port restriction.

upvoted 4 times

🗨️ 👤 **anonymous1966** 2 years, 9 months ago

Full packet at endpoint is not recommended and do not influence surface

upvoted 4 times

What is an attack surface as compared to a vulnerability?

- A. any potential danger to an asset
- B. the sum of all paths for data into and out of the environment
- C. an exploitable weakness in a system or its design
- D. the individuals who perform an attack

**Suggested Answer: B**

Community vote distribution

B (88%)



13%

  **beowolf**  2 years, 9 months ago

B. is attack vector not attack surface. C is the correct answer.

An attack surface is the total sum of vulnerabilities that can be exploited to carry out a security attack. Attack surfaces can be physical or digital. The term attack surface is often confused with the term attack vector, but they are not the same thing. The surface is what is being attacked; the vector is the means by which an intruder gains access.

upvoted 9 times


  **Jack\_B** 2 years, 8 months ago

Correct me if I am wrong, but this question is asking about attack surface.

Hence, looking at the options available, I would simply eliminate option A because it is defined as a risk, option D because it is defined as a threat actor. Which leaves me with option B and C. Option C sounds more like describing a vulnerability which then leaves me with option B as the answer.



Please do correct me if I am incorrect. Thank you.

upvoted 11 times

  **beowolf** 2 years, 7 months ago

@Jack\_B, the surface is what is being attacked so C should be correct, please see my comment above, let me know if you have any more info. cheers mate.

upvoted 1 times

  **beowolf** 2 years, 7 months ago

From wikipedia,

The attack surface of a software environment is the sum of the different points (for "attack vectors") where an unauthorized user (the "attacker") can try to enter data to or extract data from an environment.[1][2] [3]Keeping the attack surface as small as possible is a basic security measure.

So as you said B is correct then, sorry for the confusion.

upvoted 12 times

  **tsabee**  2 years, 2 months ago

My opinion:

- a - this is the Threat
- b - Correct Answer (only may be incorrect wording)
- c - Vulnerabilities
- d - Threat Actor

According to the Cisco "Understanding Cisco Cybersecurity Operations Fundamentals" course the "B" should be the right answer. One of the test question in this topics:

Q: What best describes an attack surface?

A: The sum of the different points ("attack vectors") in a given computing device or network that are accessible to an unauthorized user ("attacker")

upvoted 7 times

🗨️ 👤 **Stevens0103** Most Recent 7 months, 2 weeks ago

**Selected Answer: B**

source: <https://contenthub.netacad.com/legacy/CyberOps/1.1/en/index.html#6.1.1.1>

Vulnerability and Attack Surface – A weakness in a system or its design that could be exploited by a threat. An attack surface is the total sum of the vulnerabilities in a given system that is accessible to an attacker. The attack surface describes different points where an attacker could get into a system, and where they could get data out of the system. For example, your operating system and web browser could both need security patches. They are each vulnerable to attacks. Together, they create an attack surface the threat actor can exploit.

upvoted 2 times

🗨️ 👤 **alhamry** 7 months, 3 weeks ago

The best answer is "B. the sum of all paths for data into and out of the environment."

An attack surface refers to the sum of all paths through which an attacker can gain access to a system or environment to carry out an attack. This includes not only the hardware and software components of the system but also the interfaces, networks, and protocols that allow data to enter and leave the system.

A vulnerability, on the other hand, is an exploitable weakness or flaw in a system or its design that can be used by an attacker to compromise the system's security and gain unauthorized access. Vulnerabilities can exist in hardware, software, network configurations, or even in human behavior.

In summary, while a vulnerability is a specific weakness or flaw that can be exploited by an attacker, an attack surface is the sum of all possible avenues an attacker can use to gain access to a system or environment and carry out an attack.

upvoted 2 times

🗨️ 👤 **drdecker100** 10 months, 2 weeks ago

**Selected Answer: B**

B. Attack surface: The sum of all paths, entry points, and vulnerabilities through which an attacker can access an environment, system, or application.

upvoted 2 times

🗨️ 👤 **cy\_analyst** 1 year, 2 months ago

**Selected Answer: C**

From the book CCNA cybersecurity Operations Companion Guide.:

Recall that a vulnerability is a weakness in a system or its design that could be exploited by a threat. An attack surface is the total sum of the vulnerabilities in a given system that is accessible to an attacker. The attack surface can consist of open ports on servers or hosts, software that runs on Internet-facing servers, wireless network protocols, and even users.

upvoted 1 times

🗨️ 👤 **joseph267** 1 year, 5 months ago

for me answer C seems to talk about 1 thing but option B talks about many so I think B is the one here

upvoted 1 times

🗨️ 👤 **ivlis\_27** 2 years, 1 month ago

**Selected Answer: B**

because it's a surface

upvoted 3 times

An intruder attempted malicious activity and exchanged emails with a user and received corporate information, including email distribution lists. The intruder asked the user to engage with a link in an email. When the link launched, it infected machines and the intruder was able to access the corporate network.

Which testing method did the intruder use?

- A. social engineering
- B. eavesdropping
- C. piggybacking
- D. tailgating

**Suggested Answer: A**

Community vote distribution

A (100%)

🗨️ **AhmedAbdalla** 8 months, 3 weeks ago

The intruder used "social engineering" to trick the user into clicking a harmful link in an email, which allowed them to access the corporate network. Social engineering involves manipulating people to gain unauthorized access or information.

upvoted 1 times

🗨️ **Eng\_ahmedyoussef** 1 year, 8 months ago

**Selected Answer: A**

A. Social Engineering Method (Phishing Attack)

upvoted 2 times

🗨️ **weganos** 1 year, 9 months ago

Since Phishing is not an answer I think social Engineering is the best option.

Also there's a typo in the question "fink" should be "link".

upvoted 1 times

🗨️ **joseph267** 1 year, 11 months ago

here I think would be phishing but yeah A is the best option

upvoted 1 times

🗨️ **anonymous1966** 2 years, 9 months ago

The only problem here is that Social Engineering is not a "testing method" it is an attack.

But the other alternatives are wrong, so (A) is correct.

Social engineering attacks leverage the weakest link, which is the human user. If the attacker can get the user to reveal information, it is much easier for the attacker to cause harm rather than use some other method of reconnaissance. This could be done through email or misdirection of web pages, which results in the user clicking something that leads to the attacker gaining information. Social engineering can also be done in person by an insider or outside entity or over the phone.

upvoted 3 times

What are two social engineering techniques? (Choose two.)

- A. privilege escalation
- B. DDoS attack
- C. phishing
- D. man-in-the-middle
- E. pharming

**Suggested Answer:** CE

Community vote distribution

CE (100%)

🗨️ **anonymous1966** Highly Voted 2 years, 3 months ago

From the book:

Other social engineering techniques include the following: Phishing, Spear phishing, Pharming (is the term used to describe a threat actor redirecting a victim from a valid website or resource to a malicious one that could be made to appear as the valid site to the user. From there, an attempt is made to extract confidential information from the user or to install malware in the victim's system. Pharming can be done by altering the host file on a victim's system, through DNS poisoning, or by exploiting a vulnerability in a DNS server.), Malvertising, SMS phishing, Voice phishing (or vishing), Whaling, Elicitation, interrogation, and impersonation (Pretexting)

upvoted 6 times

🗨️ **drdecker100** Most Recent 10 months, 2 weeks ago

**Selected Answer:** CE

C. phishing - Phishing is the practice of sending emails or messages to deceive individuals into providing sensitive information such as usernames, passwords, and credit card details.

E. pharming - Pharming is a type of cyber attack where an attacker redirects website traffic from a legitimate website to a fraudulent website that looks similar to the legitimate one, with the aim of stealing personal or financial information.

upvoted 1 times

🗨️ **fyticez** 1 year, 2 months ago

Not actually clear why the book considers Pharming as a social engineering type of attack (threat actor doesn't need to communicate with the victim), since it's actually more of an end-point(workstation/server/online dns resolver) based attack revolving around the manipulation of DNS entries...

upvoted 1 times

🗨️ **Eng\_ahmedyoussef** 1 year, 2 months ago

**Selected Answer:** CE

C. phishing (Phishing is when attackers attempt to trick users into doing 'the wrong thing', such as clicking a bad link that will download malware, or direct them to a dodgy website)

E. pharming (Pharming is a form of online fraud involving malicious code and fraudulent websites. Cybercriminals install malicious code on your computer or server. The code automatically directs you to bogus websites without your knowledge or consent)

upvoted 1 times



```
# nmap -sV 172.18.104.139

Starting Nmap 7.01 ( https://nmap.org ) at 2020-03-07 11:36 EST
Nmap scan report for 172.18.104.139
Host is up (0.000018s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.4 (Ubuntu Linux; protocol 2.0)
25/tcp    open  smtp      Postfix smtpd
110/tcp   open  pop3      Dovecot pop3d
143/tcp   open  imap      Dovecot imapd
Service Info: Host: 172.18.108.139; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Refer to the exhibit. What does the output indicate about the server with the IP address 172.18.104.139?

- A. open ports of a web server
- B. open port of an FTP server
- C. open ports of an email server
- D. running processes of the server

**Suggested Answer: C**

 **SecurityGuy** 10 months ago

Some facts that may be helpful.

IMAP (Internet Messaging Access Protocol)

- It allows you to access your email wherever you are, from any device.
- When you read an email message using IMAP, you aren't actually downloading or storing it on your computer; instead, you're reading it from the email service.


POP (Post Office Protocol)

- It works by contacting your email service and downloading all of your new messages from it.
  - Once they are downloaded onto your PC or Mac, they are deleted from the email service.
- This means that after the email is downloaded, it can only be accessed using the same computer.

<https://support.microsoft.com/en-us/office/what-are-imap-and-pop-ca2c5799-49f9-4079-aefe-ddca85d5b1c9>  
upvoted 3 times

 **Eng\_ahmedyoussef** 1 year, 2 months ago

- \* SMTP ==> sending mail
  - \*IMAP & POP3 ==> Receiving mail
  - \* SSH ==> secure remote connection
- upvoted 2 times

 **joseph267** 1 year, 5 months ago

I think it should be D since ssh is also open  
upvoted 1 times

 **hansamaru** 1 year, 1 month ago

the capture is not talking about the process  
upvoted 1 times

 **Templar** 2 years ago

C is correct  
upvoted 2 times

What does the Zero Trust security model signify?

- A. Zero Trust security means that no one is trusted by default from inside or outside the network.
- B. Zero Trust addresses access control and states that an individual should have only the minimum access privileges necessary to perform specific tasks.
- C. Zero Trust states that no users should be given enough privileges to misuse the system on their own.
- D. Zero Trust states that unless a subject is given explicit access to an object, it should be denied access to that object.

**Suggested Answer: A**

Community vote distribution

A (100%)

🗳️ 👤 **c79ecd3** 12 months ago

**Selected Answer: A**

Zero Trust - trust no one so answer A

upvoted 1 times

🗳️ 👤 **2StepsFromHell** 1 year, 3 months ago

**Selected Answer: A**

The correct answer is 'A'

Zero Trust is a security framework that requires all users to be authenticated, authorized, and continuously validated before being granted access to the network/systems.

Crowdstrike | What is Zero Trust Security?

upvoted 1 times

🗳️ 👤 **RoBery** 1 year, 5 months ago

I am not sure but I found that:

Zero Trust security means that no one is trusted by default from inside or outside the network, and verification is required from everyone trying to gain access to resources on the network. This added layer of security has been shown to prevent data breaches.

Zero Trust security | What is a Zero Trust network? | Cloudflare

upvoted 1 times

🗳️ 👤 **fisher004** 1 year, 7 months ago

I think it should be A. Whilst Zero Trust applies the principle of least privilege, it primarily assumes by default that no one is trusted.

upvoted 4 times

🗳️ 👤 **sheyshey** 1 year, 7 months ago

Amen bro, or sis lol

upvoted 2 times

🗳️ 👤 **sheyshey** 1 year, 7 months ago

**Selected Answer: A**

should the answer be A?

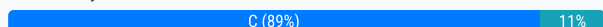
upvoted 3 times

An engineer needs to configure network systems to detect command and control communications by decrypting ingress and egress perimeter traffic and allowing network security devices to detect malicious outbound communications. Which technology should be used to accomplish the task?

- A. static IP addresses
- B. cipher suite
- C. digital certificates
- D. signatures

**Suggested Answer: C**

Community vote distribution



**Faio** 1 year, 5 months ago

The answer is B. c

A cipher suite is a set of cryptographic algorithms that are used to secure network communications. By configuring network systems to use a cipher suite that supports decryption, the engineer can inspect the traffic for malicious activity, including command and control communications.

The other options are not correct. Option A, static IP addresses, is not a technology that can be used to decrypt traffic. Option C, digital certificates, are used to verify the identity of a sender, but they do not provide encryption. Option D, signatures, are used to verify the integrity of a message, but they do not provide encryption.

upvoted 5 times

**Silexis** 11 months, 1 week ago

I think that you are wrong.

Digital Certificates are used for encryption as well. Inspecting SSL traffic, will make a firewall appliance to behave like a man in the middle. It will terminate one side of the SSL connection and it will start another one with its own certificate. This is why, the firewall certificate will have to be trusted by all clients in Trusted Root CA store. Of course that a private key and a digital certificate in the end have a suite of ciphers but you need a digital certificate for this, to have a match and not the cipher suite used for that certificate because if you are going on this logic path, ANY certificate issued with the same cypher will work, which is very wrong.....

upvoted 2 times

**Twphill** 3 months, 3 weeks ago

**Selected Answer: B**

Cipher suite is the only answer that provides encryption/decryption of network traffic.

upvoted 1 times

**alhamry** 1 year, 8 months ago

Digital certificates are used to authenticate and establish trust between two communicating parties, but they do not provide the ability to decrypt traffic. The process of decrypting traffic involves using a decryption key, which is not related to digital certificates. Therefore, digital certificates are not the appropriate technology to use to accomplish the task of detecting command and control communications by decrypting ingress and egress perimeter traffic.

The best answer is B, cipher suite. Cipher suites are sets of cryptographic algorithms that determine how secure network connections are established and data is encrypted. By configuring the network systems to decrypt ingress and egress perimeter traffic using a cipher suite, network security devices can inspect the traffic for command and control communications and other malicious outbound communications.

upvoted 2 times

**Silexis** 11 months, 1 week ago

A private key is an end result of running a cypher algorithm on something - the secret. So please note that the private key is not the algorithm itself! When you configure SSL decryption on security appliances (NGFW, WSA, etc) you need to import the certificate of the appliance in Trusted ROOT CAs of clients, as the appliance in fact is doing a ssl break-through (it terminates the SSL connection to itself and starts a new one on the other side). In between, the traffic is no longer encrypted so it can be parsed for malware inspection. This being said, in my opinion, it is not the cypher you need to configure but a Digital Certificate

upvoted 1 times

🗳️ 👤 **mozaki** 1 year, 9 months ago

**Selected Answer: C**

Answer: is Digital certificates

The Digital Certificate can be used to encrypt the cleartext into a ciphertext, which is sent from the sending party to the other party. From cisco Modules

upvoted 2 times

🗳️ 👤 **SecurityGuy** 1 year, 10 months ago

**Selected Answer: B**

As based on [https://en.wikipedia.org/wiki/Cipher\\_suite](https://en.wikipedia.org/wiki/Cipher_suite)

The key exchange algorithm is used to exchange a key between two devices. This key is used to encrypt and "decrypt" the messages being sent between two machines.

upvoted 1 times

🗳️ 👤 **trigger4848** 2 years, 1 month ago

**Selected Answer: C**

Enabling SSL decryption uses the root certificate on client machines, acting as certificate authority for SSL requests. This process makes it possible for SSL decryption to decrypt, perform a detailed inspection, and then re-encrypt SSL traffic before sending it off to its destination. This helps ensure that only authorized SSL traffic is traversing the network, and that malware hidden in SSL/TLS sessions is detected and remediated within the SSL decryption process.

upvoted 3 times

🗳️ 👤 **evaline12** 1 year, 11 months ago

but it not only uses certificates to encrypt/decrypt traffic, for that it needs a cipher suit "They define the method in which specific algorithms will be used to encrypt and decrypt data exchanged between a client (typically a browser) and a server (mostly a web server)." "client"=WSA "Web Server"=C&C

upvoted 1 times

🗳️ 👤 **Silexis** 11 months, 1 week ago

The cipher suites are negotiated during the SSL/TLS handshake. What you can configure is a set of ciphers which are not prone to known attacks but this will never make possible the decryption of the packets for inspection!!! trigger4848 is right - Digital Certificates are needed because in a security appliance you have ssl break-through between client and server. The simple fact that all Digital Certificates are using ciphers is not relevant in this context

upvoted 1 times

🗳️ 👤 **fvanderschmudt** 2 years, 5 months ago

**Selected Answer: C**

With SSL/TLS inspection, you can 'break open' traffic to inspect it.

A cipher suite is used in encryption, but that is not relevant here (is a detail of the implementation) Hence, answer C is correct.

upvoted 3 times

🗳️ 👤 **joseph267** 2 years, 5 months ago

C is the one here using Dcert to decrypt using ssl proxy

upvoted 3 times

🗳️ 👤 **Dunky** 2 years, 9 months ago

You must use a Root certificate, also referred to as a Certificate Authority (CA) Signing certificate, for HTTPS decryption on the WSA.

upvoted 2 times

🗳️ 👤 **saakovv** 2 years, 11 months ago

is it not about SSL inspection?

upvoted 2 times

🗳️ 👤 **omita** 3 years ago

Cipher suites dictate which of these algorithms the server should use to make a secure and reliable connection. But it's important to remember that cipher suites do not just ensure the security, but also the compatibility and performance of HTTPS connections. So, you should choose yours wisely.

upvoted 1 times

🗳️ 👤 **Dinhkk** 3 years ago



c is correct

upvoted 1 times

🗳️ 👤 **CiscoTerminator** 3 years ago

I think answer is C as well. Cipher suite is just a set of available ciphers that can be used by a device for encryption.

upvoted 2 times

  **akustic** 3 years, 2 months ago

C. digital certificates - the traffic need to be decrypted for further analysis. This technology is used in proxy/WSA.

upvoted 2 times

What is indicated by an increase in IPv4 traffic carrying protocol 41?

- A. deployment of a GRE network on top of an existing Layer 3 network
- B. attempts to tunnel IPv6 traffic through an IPv4 network
- C. unauthorized peer-to-peer traffic
- D. additional PPTP traffic due to Windows clients

**Suggested Answer:** B

Reference:

[https://simple.wikipedia.org/wiki/Protocol\\_41](https://simple.wikipedia.org/wiki/Protocol_41)

*Community vote distribution*

B (100%)

🗲️ 👤 **Templar** Highly Voted 🍌 2 years, 6 months ago

B is correct.

Protocol 41 is a communication protocol which embeds internet protocol version 6 (IPv6) packets inside Internet protocol version 4 (IPv4) packets.

upvoted 6 times

🗲️ 👤 **cliefan** Most Recent 🕒 9 months ago

Sneaky – GRE is protocol 47

upvoted 1 times

🗲️ 👤 **Eng\_ahmedyoussef** 1 year, 8 months ago

**Selected Answer: B**

B is correct

Protocol 41 is a communication protocol which embeds internet protocol version 6 (IPv6) packets inside Internet protocol version 4 (IPv4) packets. It is usually used to allow a computer or router with only an IPv4 address to obtain an IPv6 address (or maybe more than one address, to serve more than one computer). Most IPv6 tunnel providers support Protocol 41, including Hurricane Electric and SixXS. 6to4, 6rd, and 6in4 are all different ways of using Protocol 41. Protocol 41 does not use TCP or UDP (although the IPv6 packets inside can carry TCP and UDP traffic). It is not to be confused with TCP or UDP port number 41.

[https://simple.wikipedia.org/wiki/Protocol\\_41](https://simple.wikipedia.org/wiki/Protocol_41)

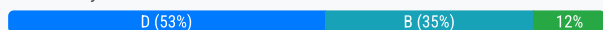
upvoted 2 times

When an event is investigated, which type of data provides the investigate capability to determine if data exfiltration has occurred?

- A. firewall logs
- B. full packet capture
- C. session data
- D. NetFlow data

**Suggested Answer: D**

Community vote distribution



**akustic** Highly Voted 3 years, 8 months ago

B. full packet capture. Other data could be an indicators of data exfiltration. But only packet insight could gives answer.  
upvoted 22 times

**3000bd6** Most Recent 7 months, 1 week ago

**Selected Answer: B**

"data exfiltration" points directly to the need for a data type that allows detailed inspection of transferred content, which is why full packet capture is the best answer.  
upvoted 2 times

**ppsilva** 1 year, 6 months ago

**Selected Answer: B**

"Provides the investigate capability" . To me it is B)  
upvoted 4 times

**fisher004** 1 year, 7 months ago

Correct answer should is session data. While session data is very simple, it can be used to answer many important questions that arise regularly in the SOC. Threat intelligence reports may provide a list of suspicious external IP addresses. Session data can be consulted to see if any internal systems have communicated with any of the suspicious external IP addresses. Similarly, if a particular TCP port is associated with an active malware campaign command and control, session data can be consulted to see if any internal systems are communicating by using that TCP port. If an internal host has been identified as being compromised, session data can identify other internal systems that it has communicated with (potential lateral movement) and any external systems that it has communicated with (potential data exfiltration). This is from the Cisco U CyberOps Course  
upvoted 1 times

**CCNPTT** 1 year, 7 months ago

**Selected Answer: D**

Full packet capture is NOT an option.

The question is about if data exfiltration has occurRED, past tense.

upvoted 2 times

**CCNPTT** 1 year, 7 months ago

Full packet capture is NOT an option.

The question is about if data exfiltration has occurRED, past tense.

upvoted 1 times

**Faio** 1 year, 9 months ago

The answer is B. full packet capture.

Full packet capture is the most comprehensive type of data that can be used to investigate an event. It captures all of the data that is transmitted over a network, including the header and payload of each packet. This allows investigators to see exactly what data was sent and received, and by whom.

Firewall logs, session data, and NetFlow data are all less comprehensive than full packet capture

upvoted 3 times

🗳️ 👤 **Faio** 1 year, 11 months ago

B.

Full packet capture is the most comprehensive type of data that can be used to investigate a data exfiltration event. It captures all of the data that is transmitted over a network, including the headers, payload, and metadata. This data can be used to identify the source and destination of the traffic, the type of data that is being transferred, and the time and date of the transfer.

Firewall logs, session data, and NetFlow data can also be used to investigate data exfiltration events, but they provide less information than full packet capture.

upvoted 2 times

🗳️ 👤 **Topsecret** 1 year, 11 months ago

B. full packet capture 100%

upvoted 1 times

🗳️ 👤 **drdecker100** 2 years, 4 months ago

**Selected Answer: B**

In the context of data exfiltration, full packet capture can be used to identify the source and destination of any data that is being transferred out of the network. It can also provide insight into the type of data that is being exfiltrated, the frequency and duration of the transfers, and any other characteristics that may be relevant to the investigation.

upvoted 2 times

🗳️ 👤 **evaline12** 2 years, 5 months ago

"determine if data exfiltration has occurred" basically you don't want to look into the packets just want to determine high bandwidth use, the size of these packets, best thing is to look at the metadata

upvoted 2 times

🗳️ 👤 **evaline12** 2 years, 5 months ago

ignore this one, wsa is one dlp solution that indeed does deep content inspection

upvoted 1 times

🗳️ 👤 **hansamaru** 2 years, 7 months ago

**Selected Answer: B**

B should be the correct one

upvoted 3 times

🗳️ 👤 **cy\_analyst** 2 years, 8 months ago

**Selected Answer: C**

C & D is the same data. The question says to see if data exfiltrate, so you don't need to see the actual data with full packet capture but only if it happened. So you need only session data to get the answer. Net flow "sees" session data so both answers might be correct.

upvoted 2 times

🗳️ 👤 **SecurityGuy** 2 years, 4 months ago

I agree with this, although Full Packet Capture provides a more comprehensive output, the question just asks if Data Exfiltration has occurred and Session Data if enough. No need to complicate things.

On a certification exam, sometimes the most simplest or provides the bare minimum is the correct one.

upvoted 1 times

🗳️ 👤 **fyticez** 2 years, 8 months ago

**Selected Answer: B**

Official Cert Guide - "Another product family that integrates with other DLP solutions is the Cisco WSA, which redirects all outbound traffic to a third-party DLP appliance, allowing deep content inspection for regulatory compliance and data exfiltration protection. It enables an administrator to inspect web content by title, metadata, and size and even to prevent users from storing files to cloud services such as Dropbox and Google Drive." ... I think the keyword here should be "all outbound traffic", hence B.

upvoted 2 times


🗳️ 👤 **fyticez** 2 years, 8 months ago

Then again, on the other hand, D is also a possibility (NetFlow data could also provide the investigation capability). According to <https://www.plixer.com/blog/netflow-and-internet-data-loss-prevention-alarms/> "The effort to prevent data loss is a top priority for many organizations. Identifying odd traffic patterns and suspicious data transfers has become a concern for many data security professionals. Flow



Analytics, an add on to our NetFlow collector, allows administrators to detect odd traffic patterns, such as servers communicating to unauthorized hosts on the Internet." This suggests the solution does not actually implement DLP (outgoing traffic doesn't get inspected for social security numbers, credit card, resumes etc.), just helps detecting it, by alerting when certain network baseline breaches occur (eg. larger amount of exiting traffic than usual, external connections initiated outside working hours etc.)



upvoted 1 times

  **weganos** 2 years, 9 months ago

**Selected Answer: D**



I also think the answer should be D "Netflow"

upvoted 2 times

  **surforlife** 2 years, 12 months ago

Netflow is used for network performance analysis and behavioral analytics for security. The flows do not contain actual packet data, but rather the metadata for communications. It is a standard form of session data that details who, what, when, and where of network traffic It is similar to the call records in a phone bill, but in real time. Every network transaction typically gets two flows, one in each direction. If you were to do full capture on each interface is extraordinarily expensive. The best practice is to look at session data in the flows. Cisco Stealthwatch is such a tool and Plixer Scrutinizer! After you see the behavior then you know where to put the full capture filter!

upvoted 4 times

  **DYKO** 3 years, 1 month ago

**Selected Answer: D**

NetFlow

upvoted 2 times

Which attack represents the evasion technique of resource exhaustion?

- A. SQL injection
- B. bluesnarfing
- C. denial-of-service
- D. man-in-the-middle

**Suggested Answer:** C

Reference:

<https://www.ciscopress.com/articles/article.asp?p=3100055&seqNum=3>

*Community vote distribution*

C (100%)

🗳️ 👤 **abrahamberhanu** 10 months ago

**Selected Answer: C**

Denial of Service (DoS) Attacks

upvoted 1 times

🗳️ 👤 **AhmedAbdalla** 1 year, 8 months ago

Denial-of-service

The attack that represents the evasion technique of resource exhaustion is a denial-of-service (DoS) attack. In a DoS attack, the attacker overwhelms a target system or network with a flood of traffic or resource requests, causing the system to become unavailable to legitimate users by exhausting its resources such as bandwidth, CPU, memory, or network connections. This evasion technique aims to disrupt the normal operation of a system or service by consuming all available resources

upvoted 1 times

🗳️ 👤 **Eng\_ahmedyoussef** 2 years, 8 months ago

**Selected Answer: C**

C. is the correct answer.

Denial of service ==> evasion technique of resource exhaustion.

upvoted 1 times

🗳️ 👤 **surforlife** 2 years, 12 months ago

DoS and DDoS

upvoted 1 times

🗳️ 👤 **Uzumaki\_Aliyy** 3 years, 6 months ago

C - correct check cyber ops by Omar Santos page; 836

upvoted 3 times

```
$ cuckoo submit --machine cuckoo1 /path/to/binary
```

Refer to the exhibit. Which event is occurring?

- A. A binary named "submit" is running on VM cuckoo1.
- B. A binary is being submitted to run on VM cuckoo1
- C. A binary on VM cuckoo1 is being submitted for evaluation
- D. A URL is being evaluated to see if it has a malicious binary

**Suggested Answer: B**

*Community vote distribution*

B (100%)

 **skysoft** Highly Voted 4 years, 6 months ago

Agreed. B is the correct answer.

<https://cuckoo.readthedocs.io/en/latest/usage/submit/>

upvoted 32 times

 **Kaddi** Highly Voted 4 years, 6 months ago

"B" should be the right answer.

upvoted 17 times

 **d503c75** Most Recent 9 months, 2 weeks ago


The answer is B.

<https://cuckoo.readthedocs.io/en/latest/usage/submit/>

Example: submit a local binary to be run on virtual machine cuckoo1:

```
$ cuckoo submit --machine cuckoo1 /path/to/binary
```

upvoted 1 times

 **SecurityGuy** 2 years, 3 months ago

Selected Answer: B

Example: submit a local binary to be run on virtual machine cuckoo1:

```
$ cuckoo submit --machine cuckoo1 /path/to/binary
```

Source: <https://cuckoo.sh/docs/usage/submit.html>

upvoted 1 times

 **Chris1971** 2 years, 5 months ago

c could be also correct, what's the reason to send a file or a url?

to analyse (evaluate) them


upvoted 1 times

 **Eng\_ahmedyoussef** 2 years, 8 months ago

Selected Answer: B

B. A binary is being submitted to run on VM cuckoo1

upvoted 1 times

 **kyle942** 2 years, 9 months ago

Example: submit a local binary to be run on virtual machine cuckoo1:

```
$ cuckoo submit --machine cuckoo1 /path/to/binary
```

upvoted 1 times

 **weganos** 2 years, 9 months ago

Selected Answer: B

The answer is B, it is in the examples on the documentation page.

<https://cuckoo.readthedocs.io/en/latest/usage/submit/>

upvoted 1 times

🗨️ **surforlife** 2 years, 11 months ago

Correct, submit a local binary to be run on virtual machine cuckoo1

upvoted 1 times

🗨️ **ESTHER\_97** 3 years, 1 month ago

**Selected Answer: B**

B is correct

upvoted 1 times

🗨️ **KKIIMM123** 3 years, 1 month ago

**Selected Answer: B**

b is correct

upvoted 2 times

🗨️ **OmarXtream** 3 years, 3 months ago

**Selected Answer: B**

B is correct

upvoted 1 times

🗨️ **RolandoFiee** 3 years, 5 months ago

submit a local binary to be run on virtual machine cuckoo1:

`$ cuckoo submit --machine cuckoo1 /path/to/binary`

upvoted 1 times

🗨️ **saakovv** 3 years, 5 months ago

This is B

<https://cuckoo.sh/docs/usage/submit.html>

upvoted 2 times

🗨️ **eggheadsv** 3 years, 7 months ago

One well-known open source sandbox is Cuckoo. This sandbox allows a security professional to implement Cuckoo on a local system and execute malicious files and malware within a safe environment.

upvoted 2 times

🗨️ **nataldogomes** 3 years, 9 months ago

Submit a local binary to be run on virtual machine cuckoo1:

`$ cuckoo submit --machine cuckoo1 /path/to/binary`

upvoted 4 times

```
Mar 6 10:35:34 user sshd[12900]: pam_unix(sshd:auth):authentication failure;
logname= uid=0 euid=0 tty=ssh ruser= rhost=127.0.0.1
Mar 6 10:35:36 user sshd[12900]: Failed password for invalid user not_bill from
127.0.0.1 port 38346 ssh2
```

Refer to the exhibit. In which Linux log file is this output found?

- A. /var/log/authorization.log
- B. /var/log/dmesg
- C. var/log/var.log
- D. /var/log/auth.log

**Suggested Answer: D**

Community vote distribution

D (100%)

Eng\_ahmedyoussef 8 months, 3 weeks ago

**Selected Answer: D**

D. /var/log/auth.log  
upvoted 2 times

Uzumaki\_Aliyy 1 year, 6 months ago

- c) /var/log/btmp – This file contains information about failed login attempts. Use the last command to view the btmp file. For example, “last -f /var/log/btmp | more”
  - d) /var/log/wtmp or /var/log/utmp – Contains login records. Using wtmp you can find out who is logged into the system. who command uses this file to display the information.
  - e) /var/log/faillog – Contains user failed login attempts. Use faillog command to display the content of this file.
  - f) /var/log/secure – Contains information related to authentication and authorization privileges. For example, sshd logs all the messages here, including unsuccessful login.
- upvoted 1 times

Uzumaki\_Aliyy 1 year, 6 months ago

1. The main log file
    - a) /var/log/messages – Contains global system messages, including the messages that are logged during system startup. There are several things that are logged in /var/log/messages including mail, cron, daemon, kern, auth, etc.
  2. Access and authentication
    - a) /var/log/auth.log – Contains system authorization information, including user logins and authentication machinsm that were used.
    - b) /var/log/lastlog – Displays the recent login information for all the users. This is not an ascii file. You should use lastlog command to view the content of this file.
- upvoted 1 times

Uzumaki\_Aliyy 1 year, 6 months ago

D - correct based on the below:

<https://www.netsurion.com/articles/top-5-linux-log-file-groups-in-var>

log#:~:text=There%20are%20several%20things%20that,%2C%20kern%2C%20auth%2C%20etc.&text=a)%20%2Fvar%2Flog%2Fauth.,information%20for%20all%  
upvoted 2 times

An engineer runs a suspicious file in a sandbox analysis tool to see the outcome. The analysis report shows that outbound callouts were made post infection.

Which two pieces of information from the analysis report are needed to investigate the callouts? (Choose two.)

- A. signatures
- B. host IP addresses
- C. file size
- D. dropped files
- E. domain names

**Suggested Answer:** BE

*Community vote distribution*

BE (100%)

  **drdecker100** 10 months, 1 week ago

**Selected Answer:** BE

The two pieces of information from the analysis report that are needed to investigate the outbound callouts are:

B. Host IP addresses - this will give information about the destination of the callouts and can be used to identify potential malicious hosts.

E. Domain names - this will give information about the domains contacted during the outbound callouts and can be used to identify potential command-and-control servers or other malicious infrastructure.

upvoted 4 times

  **Eng\_ahmedyoussef** 1 year, 2 months ago

**Selected Answer:** BE

B & E

host IP addresses and Domain names.

upvoted 1 times

  **cvetica** 2 years ago

B,E - IP address and domain name

upvoted 1 times

An analyst is exploring the functionality of different operating systems.

What is a feature of Windows Management Instrumentation that must be considered when deciding on an operating system?

- A. queries Linux devices that have Microsoft Services for Linux installed
- B. deploys Windows Operating Systems in an automated fashion
- C. is an efficient tool for working with Active Directory
- D. has a Common Information Model, which describes installed hardware and software

**Suggested Answer: D**

Community vote distribution

D (100%)

anonymous1966 **Highly Voted** 2 years, 3 months ago

"D" is correct.

Windows Management Instrumentation (WMI) consists of a set of extensions to the Windows Driver Model that provides an operating system interface through which instrumented components provide information and notification. WMI is Microsoft's implementation of the Web-Based Enterprise Management (WBEM) and Common Information Model (CIM) standards from the Distributed Management Task Force (DMTF).

[https://en.wikipedia.org/wiki/Windows\\_Management\\_Instrumentation](https://en.wikipedia.org/wiki/Windows_Management_Instrumentation)

upvoted 10 times

SecurityGuy **Most Recent** 9 months, 3 weeks ago

**Selected Answer: D**

WMI uses the Common Information Model (CIM) industry standard to represent systems, applications, networks, devices, and other managed components.

Windows Management Instrumentation (WMI)

- WMI is a Windows protocol.
- It has a running service that can be viewed on services.msc
- WMI uses TCP Port 135
- WMI provides users with information about the status of local or remote computer systems.
- The purpose of WMI is to help administrators manage different Windows operational environments, including remote systems.
- WMI provides admins with a powerful tool for monitoring remote processes and machines and can be utilized when building a EUMA to provide automatic alerts on suspicious user activity.

Common Information Model (CIM)

- It is a "Computer Industry Standard" or "Open Standard" that defines device and application characteristics so system administrators and management programs can control devices and applications from different manufacturers.

upvoted 1 times

Eng\_ahmedyoussef 1 year, 2 months ago

**Selected Answer: D**

D is Correct

WMI ==> has a Common Information Model, which describes installed hardware and software.

upvoted 1 times

cy\_analyst 1 year, 2 months ago

**Selected Answer: D**

WMI uses the Common Information Model (CIM) industry standard to represent systems, applications, networks, devices, and other managed components.

From Omar's book.

upvoted 2 times

What causes events on a Windows system to show Event Code 4625 in the log messages?

- A. The system detected an XSS attack
- B. Someone is trying a brute force attack on the network
- C. Another device is gaining root access to the system
- D. A privileged user successfully logged into the system

**Suggested Answer: B**

Community vote distribution

B (100%)

Eng\_ahmedyoussef **Highly Voted** 8 months, 3 weeks ago

**Selected Answer: B**

B is correct answer

Event ID 4625 (viewed in Windows Event Viewer) documents every failed attempt at logging on to a local computer. This event is generated on the computer from where the logon attempt was made.

so attacker my use brute force attack tools to gain access.

upvoted 5 times

RolandoFiee **Most Recent** 1 year, 5 months ago

This event is generated when a logon request fails. It is generated on the computer where access was attempted.

The Subject fields indicate the account on the local system which requested the logon.

<https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventID=4625#:~:text=Examples%20of%204625&text=Failure%20Reason%3A%20Unknown%20user%20name%20or%20bad%20password.&text=This%20even>

upvoted 2 times

anonymous1966 1 year, 9 months ago

"B" is correct

4625(F): An account failed to log on.

Event Description:

This event generates if an account logon attempt failed when the account was already locked out. It also generates for a logon attempt after which the account was locked out.

It generates on the computer where logon attempt was made, for example, if logon attempt was made on user's workstation, then event will be logged on this workstation.

This event generates on domain controllers, member servers, and workstations.

<https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4625>

upvoted 4 times



```
10.44.101.23 - - [20/Nov/2017:14:18:06 -0500] "GET / HTTP/1.1"
200 1254 "-" "Mozilla/5.0(X11; Ubuntu; Linux x86_64; rv:54.0)
Gecko/20100101 Firefox/54.0"
```

Refer to the exhibit. What does the message indicate?

- A. an access attempt was made from the Mosaic web browser
- B. a successful access attempt was made to retrieve the password file
- C. a successful access attempt was made to retrieve the root of the website
- D. a denied access attempt was made to retrieve the password file

**Suggested Answer: C**

Community vote distribution

C (100%)

Eng\_ahmedyoussef 8 months, 3 weeks ago

**Selected Answer: C**

C. a successful access attempt was made to retrieve the root of the website  
upvoted 1 times

CiscoTerminator 1 year, 9 months ago

To be honest I dont get the whole "root of the website" int his question. I do get that it is a retrieve attempt.  
upvoted 3 times

HarryPotter69 1 year, 9 months ago

I believe C then B... you would like to get to the root directory first, then try to get a password. My thinking... I would stick with the answer as C  
upvoted 1 times

anonymous1966 1 year, 9 months ago

The HTTP 200 OK success status response code indicates that the request has succeeded.

The meaning of a success depends on the HTTP request method:

GET: The resource has been fetched and is transmitted in the message body.

<https://developer.mozilla.org/en-US/docs/Web/HTTP/Status/200>

So we stay between "B" and "C".

Anybody can explain why "C" is correct?

upvoted 2 times

anonymous1966 1 year, 9 months ago

"C" is correct.

Apache log format: LogFormat "%h %l %u %t \"%r\" %>s %b"

Now let's break down what each section of that log means.

%h The IP address of the client.

%l The identity of the client determined by identd on the client's machine. Will return a hyphen (-) if this information is not available.

%u The userid of the client if the request was authenticated.

%t The time that the request was received.

\"%r\" The request line that includes the HTTP method used, the requested resource path, and the HTTP protocol that the client used.

%>s The status code that the server sends back to the client.

%b The size of the object requested.

Pay attention at \"%r\". The resource path is "-" that means "empty". So, the root of the site was requested.

upvoted 29 times

```
GET /item.php?id=34' or sleep(10)
```

Refer to the exhibit. This request was sent to a web application server driven by a database.  
Which type of web server attack is represented?

- A. parameter manipulation
- B. heap memory corruption
- C. command injection
- D. blind SQL injection

**Suggested Answer: D**

Community vote distribution

D (100%)

 **gnuga** Highly Voted 2 years, 4 months ago

I think blind sql injection is correct

Blind SQL (Structured Query Language) injection is a type of SQL Injection attack that asks the database true or false questions and determines the answer based on the applications response.


[https://owasp.org/www-community/attacks/Blind\\_SQL\\_Injection](https://owasp.org/www-community/attacks/Blind_SQL_Injection)

upvoted 14 times

 **anonymous1966** 2 years, 3 months ago

Agreed. "D" is correct

upvoted 2 times

 **SecurityGuy** Most Recent 9 months, 3 weeks ago

**Selected Answer: D**

SQL Injection

- SQL injection usually occurs when you ask a user for input, like their username/userid, and instead of a name/id, the user gives you an SQL statement that you will unknowingly run on your database.

Time-Based Blind SQL Injection:

- If the website does not return an immediate response, it indicates a vulnerability to blind SQL injection. The most popular time-intensive operation is a sleep operation.


- Based on the example above, the attacker would benchmark the web server response time for a regular SQL query, and then would issue the request below:

- <http://www.webshop.local/item.php?id=14> and `if(1=1, sleep(15), false)`

- The website is vulnerable if the response is delayed by 15 seconds.

<https://brightsec.com/blog/blind-sql-injection/>

upvoted 1 times

 **SecurityGuy** 9 months, 3 weeks ago

SLEEP is a query that pauses the MySQL process for a given duration

upvoted 1 times

 **Eng\_ahmedyoussef** 1 year, 2 months ago

**Selected Answer: D**

i agree with answer D



i think blind SQL injection is correct

upvoted 1 times

 **surforlife** 1 year, 5 months ago

C. command injection

upvoted 1 times

  **JohnBB** 2 years, 7 months ago

I think it's "Command injection" is a tright answer.

[https://owasp.org/www-community/attacks/Command\\_Injection](https://owasp.org/www-community/attacks/Command_Injection)

upvoted 4 times

A SOC analyst is investigating an incident that involves a Linux system that is identifying specific sessions.

Which identifier tracks an active program?

- A. application identification number
- B. active process identification number
- C. runtime identification number
- D. process identification number

**Suggested Answer: D**

Community vote distribution

D (100%)


 **gnuga** Highly Voted 2 years, 4 months ago

Answer is correct.

The process identifier (process ID or PID) is a number used by Linux or Unix operating system kernels. It is used to uniquely identify an active process.

<https://www.cyberciti.biz/faq/linux-find-process-name/>

upvoted 10 times

 **SecurityGuy** Most Recent 9 months, 3 weeks ago

**Selected Answer: D**

Process Identifier (PID)

- PIDs are unique values that are automatically assigned to processes on a Linux system.
- PIDs start from 0. The process that has the id 0 is part of the kernel and is not regarded as a normal user-mode process.
- The process with the ID of the value 1 is the init process.

[https://www.baeldung.com/linux/identifiers#:~:text=Process%20identifiers%20\(PIDs\)%20are%20unique,1%20is%20the%20init%20process.](https://www.baeldung.com/linux/identifiers#:~:text=Process%20identifiers%20(PIDs)%20are%20unique,1%20is%20the%20init%20process.)

upvoted 4 times

 **Eng\_ahmedyoussef** 1 year, 2 months ago

**Selected Answer: D**

D. is correct answer.

PID (Process identification number) ==> is Linux system that is identifying specific sessions.

upvoted 2 times

An offline audit log contains the source IP address of a session suspected to have exploited a vulnerability resulting in system compromise. Which kind of evidence is this IP address?

- A. best evidence
- B. corroborative evidence
- C. indirect evidence
- D. forensic evidence

**Suggested Answer: B**

Community vote distribution

B (100%)

🗳️ 👤 **anonymous1966** Highly Voted 2 years, 3 months ago

"B is correct.

There are 3 types of evidences:

Best: Do not need anything else.

Corroborating: evidence that tends to support a theory or an assumption deduced by some initial evidence.

Indirect: extrapolation to a conclusion of fact (such as fingerprints, DNA evidence, and so on)

In this case the IP address would corroborate to some other evidence.

upvoted 8 times

🗳️ 👤 **qz999** Highly Voted 2 years, 4 months ago

Corroborative evidence supports some other evidence, yet the question does not state that there is any other evidence than this log entry and a suspicion. Seems more like this would be circumstantial evidence at the very most and may not even be 'evidence' at all - it's just a log entry.

upvoted 5 times

🗳️ 👤 **SecurityGuy** Most Recent 9 months, 3 weeks ago

**Selected Answer: B**

Three types of Evidence:

Best Evidence

- Original, unaltered evidence. In court, this is preferred over secondary evidence.

- The best evidence rule is a legal principle that holds an original copy of a document as superior evidence.

Corroborative Evidence

- It is an evidence that strengthens or confirms already existing evidence.

Indirect Evidence (Circumstantial Evidence)

- It is an evidence that relies on an inference to connect it to a conclusion of fact. Like a fingerprint, DNA etc. at the scene of a crime.

[https://vwannabe.com/2018/01/02/ccna-cyber-ops-secops-1-](https://vwannabe.com/2018/01/02/ccna-cyber-ops-secops-1-0/#:~:text=Corroborative%20evidence%3A%20(or%20corroboration),therefore%20confirming%20the%20original%20proposition.)

[0/#:~:text=Corroborative%20evidence%3A%20\(or%20corroboration\),therefore%20confirming%20the%20original%20proposition.](https://vwannabe.com/2018/01/02/ccna-cyber-ops-secops-1-0/#:~:text=Corroborative%20evidence%3A%20(or%20corroboration),therefore%20confirming%20the%20original%20proposition.)

upvoted 1 times

🗳️ 👤 **Eng\_ahmedyoussef** 1 year, 2 months ago

**Selected Answer: B**

i think B. is correct answer.

Corroborating evidence ==> is evidence that strengthens or confirms already existing evidence.

\*\* in this case ==> ip address would corroborate the current evidence.

upvoted 3 times


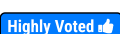
Which system monitors local system operation and local network access for violations of a security policy?

- A. host-based intrusion detection
- B. systems-based sandboxing
- C. host-based firewall
- D. antivirus

**Suggested Answer: A**

Community vote distribution

A (100%)

 **Torvalds**  3 years, 2 months ago

i think that "A.host-based intrusion detection".

HIDS is capable of monitoring the internals of a computing system as well as the network packets on its network interfaces.

Host-based firewall is a piece of software running on a single Host that can restrict incoming and outgoing Network activity for that host only.

upvoted 22 times

 **anonymous1966**  2 years, 9 months ago

"A" is correct.

The question is copy and past of Wikipedia definition:

An intrusion detection system (IDS)[1] is a device or software application that monitors a network or systems for malicious activity or policy violations. Any intrusion activity or violation is typically reported either to an administrator or collected centrally using a security information and event management (SIEM) system. A SIEM system combines outputs from multiple sources and uses alarm filtering techniques to distinguish malicious activity from false alarms.

[https://en.wikipedia.org/wiki/Intrusion\\_detection\\_system](https://en.wikipedia.org/wiki/Intrusion_detection_system)

upvoted 9 times

 **Faio**  11 months, 1 week ago

The answer is A.

Host-based intrusion detection (HIDS) is a security system that monitors a computer system for malicious activity or policy violations. HIDSs can be used to detect a variety of threats, including unauthorized access, malware, and data exfiltration.

Systems-based sandboxing is a security technique that isolates applications in a controlled environment to prevent them from causing harm to the host system.

Host-based firewall is a security system that controls incoming and outgoing network traffic on a host system.

Antivirus is a software application that detects and removes malware from a computer system.

upvoted 1 times

 **SecurityGuy** 1 year, 3 months ago

**Selected Answer: A**

Keyword: "Monitors" - It is an IDS function.

- An Intrusion Detection System (IDS) is a device or software application that monitors a network or systems for malicious activity or policy violations.

- A host based firewall does not monitor local system operations. A firewall is no more than an ACL matching traffic in and out of a system based on how it's configured.

upvoted 1 times

 **Eng\_ahmedyoussef** 1 year, 8 months ago

**Selected Answer: A**

A. is the best answer

HIDS is capable of monitoring the internals of a computing system as well as the network packets on its network interfaces. Host-based firewall is a

piece of software running on a single Host that can restrict incoming and outgoing Network activity for that host only.

upvoted 2 times

🗨️ 👤 **kyle942** 1 year, 9 months ago

**Selected Answer: A**

A host intrusion detection system uses rules and policies in order to search your log files, flagging those with events or activity the rules have determined could be indicative of potentially malicious behavior.

upvoted 1 times

🗨️ 👤 **Tobds234** 2 years, 1 month ago

**Selected Answer: A**

Host-based firewall is a piece of software running on a single Host that can restrict incoming and outgoing Network activity for that host only.

upvoted 1 times

🗨️ 👤 **PanteLa\_26** 2 years, 4 months ago

**Selected Answer: A**

Should be A imho, key word "monitors"

upvoted 1 times

🗨️ 👤 **hukkaru** 2 years, 5 months ago

**Selected Answer: A**

HIDS monitors local system, firewall not. Answer is A

upvoted 1 times

🗨️ 👤 **HarryPotter69** 2 years, 9 months ago

Answer is A

An intrusion detection system (IDS) is a device or software application that monitors a network or systems for malicious activity or policy violations.

upvoted 6 times

🗨️ 👤 **Alannn** 2 years, 9 months ago

A host based firewall does not monitor local system operations. A firewall is no more than an ACL matching traffic in and out of a system based on how it's configured. A significant advantage of HIPS is that it can monitor operating system processes. "A HIPS often monitors memory, kernel, and network state, log files, ... protects system integrity by detecting changes to critical operating system files."

upvoted 4 times

🗨️ 👤 **Alannn** 2 years, 9 months ago

In this case its HIDS and not HIPS, which one could argue would only make choice A even stronger seeing that a HIDS only monitors (both network and system files) whilst a firewall monitors network only but also intervene and blocks, which is more then just monitoring.

upvoted 1 times

🗨️ 👤 **affulinuha** 2 years, 10 months ago

IDS Global detection, Firewall Local.. and i agree with the answer.. no doubt bro make it simple

upvoted 1 times

🗨️ 👤 **mrodriguez** 2 years, 11 months ago

It says security policies. In the firewall the concept of security policies is handled. I agree with the answer

upvoted 2 times

🗨️ 👤 **JohnBB** 3 years ago

The key word is "monitors". And it's IDS work.

upvoted 3 times



An analyst received an alert on their desktop computer showing that an attack was successful on the host. After investigating, the analyst discovered that no mitigation action occurred during the attack. What is the reason for this discrepancy?

- A. The computer has a HIPS installed on it.
- B. The computer has a NIPS installed on it.
- C. The computer has a HIDS installed on it.
- D. The computer has a NIDS installed on it.

**Suggested Answer: C**

Community vote distribution

C (100%)

🗳️ 👤 **anonymous1966** Highly Voted 2 years, 3 months ago

"C" is correct.

Remember:

H = host

N = network

D = detect

P = prevent

upvoted 17 times

🗳️ 👤 **weganos** 1 year, 3 months ago

Maybe I read the question wrong but shouldn't it be HIPS?

Since it has been prevented and not just detected?

upvoted 2 times

🗳️ 👤 **weganos** 1 year ago

Nevermind, C is correct indeed.

upvoted 1 times

🗳️ 👤 **SecurityGuy** Most Recent 9 months, 3 weeks ago

**Selected Answer: C**

Detection - This means that the protection system will be able to detect and alert upon a possible security event, but it will not attempt to block anything.

Prevention - This means that when the protection system detects a possible security event, it will automatically try to block it.

The alert was received on the "desktop computer" which means that the IDS was installed on the host thus the answer is Host-based Intrusion Detection System.

upvoted 1 times

🗳️ 👤 **griszadwa** 10 months, 3 weeks ago

"host-based security systems function as both detection and prevention systems because they prevent known attacks and detect unknown potential attacks"

from cisco netacad 22.2.3

upvoted 1 times

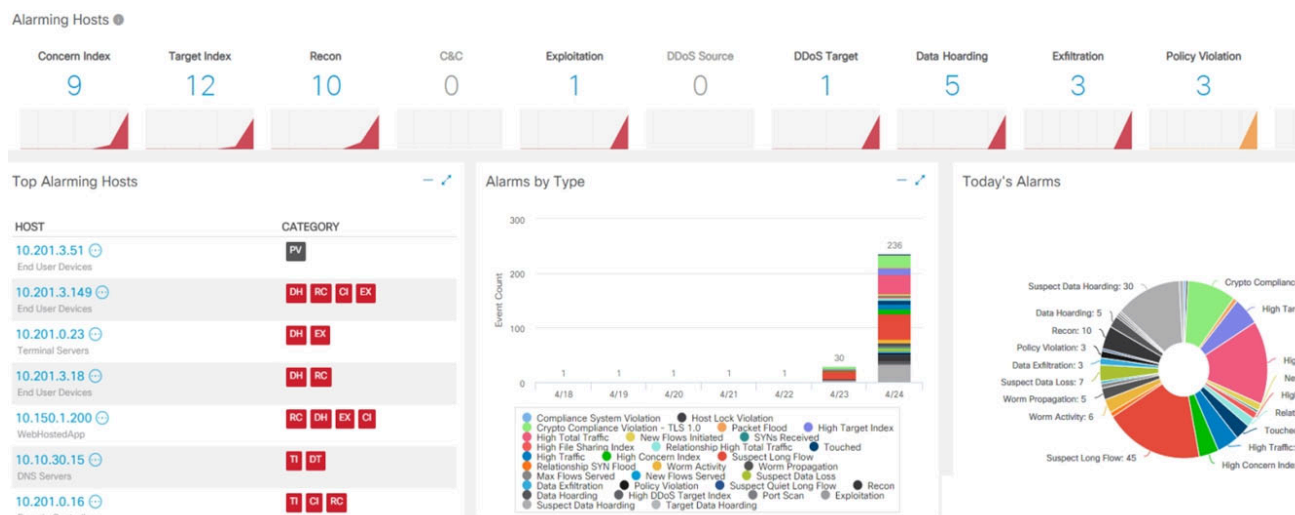
🗳️ 👤 **Eng\_ahmedyoussef** 1 year, 2 months ago

C. is correct answer

The computer has a HIDS installed on it.

HIDS ==> Detects only attacks and don't take action or mitigation.

upvoted 2 times



Refer to the exhibit. What is the potential threat identified in this Stealthwatch dashboard?

- A. A policy violation is active for host 10.10.101.24.
- B. A host on the network is sending a DDoS attack to another inside host.
- C. There are three active data exfiltration alerts.
- D. A policy violation is active for host 10.201.3.149.

**Suggested Answer: C**

Community vote distribution

C (100%)

**s1m0n** Highly Voted 2 years, 3 months ago

Believe should be C --> How can a (one) host send a DDoS that should be DoS  
upvoted 24 times

**beowolf** 2 years, 3 months ago

you are right, I too vote for C  
upvoted 7 times

**fejec** 1 year, 9 months ago

also "Source DDoS" counter is zero.  
"C" is correct.  
upvoted 7 times

**anonymous1966** Highly Voted 1 year, 9 months ago

Obviously is "C"  
"EX" = exfiltration  
And there are three.  
Also the "suspect long flow" and "suspect data heading" suggest, for example, DNS exfiltration  
upvoted 8 times

**Eng\_ahmedyoussef** Most Recent 8 months, 3 weeks ago

**Selected Answer: C**

C is the correct answer.  
there are 3 EX (exfiltration)  
upvoted 2 times

**weganos** 9 months, 4 weeks ago

**Selected Answer: C**

I think the answer is C.  
upvoted 1 times

🗨️ 👤 **adodocletus** 1 year ago

"C" is correct

upvoted 1 times

🗨️ 👤 **tor\_bap** 1 year, 6 months ago

**Selected Answer: C**

it's should be C

upvoted 2 times

🗨️ 👤 **qz999** 1 year, 10 months ago

The question requires a single answer, and clearly there are three active exfiltration alerts. So a second choice cannot be made, and as mentioned by s1m0n below, a single host by definition would not be the sole machine in a DDoS attack. Answer choice C is best.

upvoted 4 times

🗨️ 👤 **snahta** 1 year, 11 months ago

Thanks for the useful information.

I am searching this type of information about this from long time but didn't find the exact one that i wanted.

upvoted 2 times

🗨️ 👤 **gnuga** 1 year, 11 months ago

DDoS attacker should have DS attribute, and it is not there

DDoS Source

Alarm Category Index: DS

Indicates that a host has been identified as the source of a DDoS attack.

The following security events are associated with the DDoS Source alarm.

[https://www.cisco.com/c/dam/en/us/td/docs/security/stealthwatch/management\\_console/smc\\_users\\_guide/SW\\_6\\_9\\_0\\_SMC\\_Users\\_Guide\\_DV\\_1\\_2.pdf](https://www.cisco.com/c/dam/en/us/td/docs/security/stealthwatch/management_console/smc_users_guide/SW_6_9_0_SMC_Users_Guide_DV_1_2.pdf)  
page 177.

I vote for C.

upvoted 2 times

🗨️ 👤 **gnuga** 1 year, 11 months ago

There is one with DT flagged, indicated as a target.

Alarm Category Index: DT

Indicates that a host has been identified as the target of a DDoS attack

upvoted 1 times



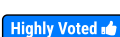
What is a difference between tampered and untampered disk images?

- A. Tampered images have the same stored and computed hash.
- B. Untampered images are deliberately altered to preserve as evidence.
- C. Tampered images are used as evidence.
- D. Untampered images are used for forensic investigations.

**Suggested Answer:** D

Community vote distribution

D (100%)

  **beowolf**  3 years, 1 month ago

D is the correct answer.

upvoted 23 times

  **anonymous1966**  2 years, 9 months ago

"D" is correct.

The disk image must be intact for forensics analysis.

As a cybersecurity professional, you may be given the task of capturing an image of a disk in a forensic manner. Imagine a security incident has occurred on a system and you are required to perform some forensic investigation to determine who and what caused the attack. Additionally, you want to ensure the data that was captured is not tampered with or modified during the creation of a disk image process.

Ref: Cisco Certified CyberOps Associate 200-201 Certification Guide

By Glen D. Singh

upvoted 12 times

  **lemin05**  9 months, 3 weeks ago

The right question is a D: untampered images used for the investigation process

but I don't understand why you don't put the right question or justify your reason because when I looked up all the resources related all agree for D choice

upvoted 1 times

  **Faio** 11 months, 1 week ago

The answer is D. Untampered images are used for forensic investigations.

Tampered images are not used for forensic investigations because they cannot be trusted as evidence. Tampered images may have been modified or altered in a way that changes their content or meaning. This can make it difficult or impossible to use them to reconstruct the events that led to the creation of the image.

upvoted 1 times

  **Faio** 11 months, 1 week ago

The answer is D. Untampered images are used for forensic investigations.

upvoted 2 times

  **Faio** 11 months, 1 week ago

D is the correct answer.

upvoted 2 times

  **Topsecret** 11 months, 3 weeks ago

The correct answer is D. Untampered images are used for forensic investigations.

When referring to disk images in the context of digital forensics, a tampered image refers to an image that has been modified or altered in some way, potentially compromising its integrity and reliability as evidence. On the other hand, an untampered image is one that has not been altered and is considered a faithful representation of the original source.

upvoted 2 times

  **macxwhale** 12 months ago

Tampered evidence will of course be challenged in court and thrown out... Did they mean it?

upvoted 1 times

🗨️ 👤 **evaline12** 1 year, 5 months ago

who the hell clicked on C

upvoted 5 times

🗨️ 👤 **Eng\_ahmedyoussef** 1 year, 8 months ago

**Selected Answer: D**

D is the correct answer

tampered with or modified during the creation of a disk image process. Ref: Cisco Certified

upvoted 1 times

🗨️ 👤 **[Removed]** 1 year, 10 months ago

**Selected Answer: D**

D should be the answer

upvoted 1 times

🗨️ 👤 **EmmaDer** 1 year, 11 months ago

**Selected Answer: D**

D is correct

upvoted 1 times

🗨️ 👤 **J8Ryan** 2 years ago

Respuesta B.

Yo tengo una imagen de disco, y un atacante me manipula la imagen. La evidencia de que he sufrido un ataque es la imagen manipulada por el atacante, o sea mi imagen manipulada.

upvoted 2 times

🗨️ 👤 **J8Ryan** 2 years ago

Perdón la RESPUESTA C

upvoted 1 times

🗨️ 👤 **KKIIMM123** 2 years, 1 month ago

**Selected Answer: D**

D is the correct answer.

upvoted 1 times

🗨️ 👤 **PanteLa\_26** 2 years, 4 months ago

**Selected Answer: D**

D without any doubt

upvoted 2 times

🗨️ 👤 **Fringe** 2 years, 5 months ago

**Selected Answer: D**

D is the correct answer.

upvoted 1 times

🗨️ 👤 **DaveEly** 2 years, 5 months ago

**Selected Answer: D**

D. Untampered images are used for forensic investigations.

upvoted 3 times

What is a sandbox interprocess communication service?

- A. A collection of rules within the sandbox that prevent the communication between sandboxes.
- B. A collection of network services that are activated on an interface, allowing for inter-port communication.
- C. A collection of interfaces that allow for coordination of activities among processes.
- D. A collection of host services that allow for communication between sandboxes.

**Suggested Answer: C**

Community vote distribution

C (75%)

A (25%)


 **Pwned** Highly Voted 2 years, 8 months ago

C is correct

IPC is a collection of programming interfaces that allows the coordination of activities among different program processes that can run concurrently in an operating system.

Cisco CyberOps Associate CBROPS 200-201 Official Cert Guide by Omar Santos


upvoted 11 times

 **[Removed]** Highly Voted 2 years, 9 months ago

I think that correct answer is:

C. A collection of interfaces that allow for coordination of activities among processes.

upvoted 5 times

 **tsabee** 2 years, 8 months ago

Yes the correct answer is the C.

Inter-process communication (IPC) allows communication between different processes. A process is one or more threads running inside its own, isolated address space.

[https://docs.legato.io/16\\_10/basicIPC.html](https://docs.legato.io/16_10/basicIPC.html)

upvoted 1 times

 **Topsecret** Most Recent 11 months, 3 weeks ago

The correct answer is C. A collection of interfaces that allow for coordination of activities among processes.

A sandbox interprocess communication (IPC) service refers to a set of interfaces or mechanisms that enable communication and coordination between processes running within a sandboxed environment. Sandboxing is a technique used to isolate and restrict the execution of applications or processes, often for security purposes.

The sandbox IPC service provides a controlled and secure means for processes within the sandbox to interact with each other, exchange data, or coordinate activities. It allows for communication while maintaining the security and integrity of the sandboxed environment. The IPC mechanisms could include interprocess messaging, shared memory, or other methods for inter-process coordination.

upvoted 3 times

 **drdecker100** 1 year, 4 months ago

**Selected Answer: C**

IPC services within a sandbox allow for controlled and secure communication between processes running inside the same sandbox. This can enable features such as interprocess coordination, data sharing, and other forms of collaboration between sandboxed processes, while still maintaining the overall security of the sandbox environment.

upvoted 2 times

 **Eng\_ahmedyoussef** 1 year, 8 months ago

**Selected Answer: C**

C is the correct answer

Inter-process communication (IPC) ==> A collection of interfaces that allow for coordination of activities among processes.

upvoted 3 times

🗉 👤 **cy\_analyst** 1 year, 9 months ago

**Selected Answer: C**

C by the book.

upvoted 2 times

🗉 👤 **EmmaDer** 1 year, 11 months ago

**Selected Answer: A**

Google says A

upvoted 1 times

🗉 👤 **addpro7** 2 years, 2 months ago

**Selected Answer: C**

Correct Answer C !!!

Host the sandbox interprocess communication service to the target processes. IPC is a collection of programming interfaces that allows the coordination of activities among different program processes that can run concurrently in an operating system.

Cisco CyberOps Associate CBROPS 200-201 Official Cert Guide by Omar Santos P810

upvoted 3 times

🗉 👤 **OmarXtream** 2 years, 3 months ago

**Selected Answer: A**

just by google this the answer is A

upvoted 1 times

🗉 👤 **Uzumaki\_Aliyy** 2 years, 6 months ago

C- correct based on ;

Cisco CyberOps Associate CBROPS 200-201 Official Cert Guide by Omar Santos page 810

upvoted 1 times

```

File      Actions      Edit      View      Help

  48 41.270348133 185.199.111.153 → 192.168.88.164 TLSv1.2 123 Application Data
  49 41.270348165 185.199.111.153 → 192.168.88.164 TLSv1.2 104 Application Data
  50 41.270356290 192.168.88.164 → 185.199.111.153 TCP 66 44736 → 443 [ACK]
Seq=834 Ack=3104 Win=64128 Len=0 TSval=3947973757 TSecr=2989424849
  51 41.270369874 192.168.88.164 → 185.199.111.153 TCP 66 44736 → 443 [ACK]
Seq=834 Ack=3142 Win=64128 Len=0 TSval=3947973757 TSecr=2989424849
  52 41.270430171 192.168.88.164 → 185.199.111.153 TLSv1.2 104 Application Data
  53 41.271767772 185.199.111.153 → 192.168.88.164 TLSv1.2 2854 Application Data
  54 41.271767817 185.199.111.153 → 192.168.88.164 TLSv1.2 904 Application Data
  55 41.271788996 192.168.88.164 → 185.199.111.153 TCP 66 44736 → 443 [ACK]
Seq=872 Ack=6768 Win=62592 Len=0 TSval=3947973758 TSecr=2989424849
  56 41.271973293 192.168.88.164 → 185.199.111.153 TLSv1.2 97 Encrypted Alert
  57 41.272411701 192.168.88.164 → 185.199.111.153 TCP 66 44736 → 443 [FIN, ACK]
Seq=903 Ack=6768 Win=64128 Len=0 TSval=3947973759 TSecr=2989424849
  58 41.283301751 185.199.111.153 → 192.168.88.164 TCP 66 443 → 44736 [ACK]
Seq=6768 Ack=903 Win=28160 Len=0 TSval=2989424852 TSecr=3947973757
  59 41.283301808 185.199.111.153 → 192.168.88.164 TLSv1.2 97 Encrypted Alert
  60 41.283321947 192.168.88.164 → 185.199.111.153 TCP 54 44736 → 443 [RST]
Seq=903 Win=0 Len=0
  61 41.283939151 185.199.111.153 → 192.168.88.164 TCP 66 443 → 44736 [FIN, ACK]
Seq=6799 Ack=903 Win=28160 Len=0 TSval=2989424852 TSecr=3947973757
  62 41.283945760 192.168.88.164 → 185.199.111.153 TCP 54 44736 → 443 [RST]
Seq=903 Win=0 Len=0
  63 41.284635561 185.199.111.153 → 192.168.88.164 TCP 66 443 → 44736 [ACK]
Seq=6800 Ack=904 Win=28160 Len=0 TSval=2989424853 TSecr=3947973759
  64 41.284642324 192.168.88.164 → 185.199.111.153 TCP 54 44736 → 443 [RST]
Seq=904 Win=0 Len=0

```

An analyst is investigating a host in the network that appears to be communicating to a command and control server on the Internet. After collecting this packet capture, the analyst cannot determine the technique and payload used for the communication.


Which obfuscation technique is the attacker using?

- A. Base64 encoding
- B. transport layer security encryption
- C. SHA-256 hashing
- D. ROT13 encryption

**Suggested Answer: B**

Community vote distribution

B (89%) 11%

 **mariodesa** Highly Voted 1 year, 5 months ago

**Selected Answer: B**

B is the correct answer.

ROT13 is considered weak encryption and is not used with TLS (HTTPS:443).

Source: <https://en.wikipedia.org/wiki/ROT13>

upvoted 7 times

 **Eng\_ahmedyoussef** Most Recent 8 months, 3 weeks ago

**Selected Answer: B**

B. is the correct answer

TLS encryption == HTTPS protocol with port number : 443


upvoted 1 times

 **cy\_analyst** 9 months ago

**Selected Answer: B**

B for obvious.

upvoted 1 times

 **Mevijil** 1 year, 4 months ago

**Selected Answer: B**



Clearly says TLS right in the output

upvoted 4 times

  **seriously5000** 1 year, 5 months ago

**Selected Answer: B**

TLS is visible in the dump

upvoted 4 times

  **tor\_nana** 1 year, 5 months ago

**Selected Answer: D**

Halarput D is correct

upvoted 2 times

An OSINT team scans the target hosts, gathers information regarding the adversary online services, and equips the red team with the obtained information. Which step in the kill chain is this activity?

- A. weaponization
- B. installation
- C. delivery
- D. reconnaissance

**Correct Answer:** *D*

Currently there are no comments in this discussion, be the first to comment!

During which phase of the forensic process is data that is related to a specific event labeled and recorded to preserve its integrity?

- A. examination
- B. investigation
- C. collection
- D. reporting

**Suggested Answer:** C

*Community vote distribution*

C (100%)

🗉 👤 **AhmedAbdalla** 8 months, 3 weeks ago

During the forensic process, data that is related to a specific event is typically labeled and recorded to preserve its integrity during the "collection" phase. This phase involves the gathering and preservation of potential evidence, ensuring that it is properly documented, secured, and maintained to maintain its evidentiary value for later analysis and reporting.

upvoted 2 times

🗉 👤 **Eng\_ahmedyoussef** 1 year, 8 months ago

**Selected Answer: C**

C is correct

in Collection phase in forensic process ==> specific event labeled and recorded to preserve its integrity.

upvoted 2 times

🗉 👤 **Pwned** 2 years, 8 months ago

C is Correct

<https://csrc.nist.gov/publications/detail/sp/800-86/final>

upvoted 1 times

Which step in the incident response process researches an attacking host through logs in a SIEM?

- A. detection and analysis
- B. preparation
- C. eradication
- D. containment

**Suggested Answer: A**

Community vote distribution

A (88%)

13%

🗳️ 👤 **drdecker100** Highly Voted 👍 10 months, 2 weeks ago

**Selected Answer: A**

The incident response process typically includes the following phases: preparation, detection and analysis, containment, eradication, and recovery. The detection and analysis phase is focused on identifying and assessing the scope and severity of the incident, and this includes analyzing logs and other data to identify the source and nature of the attack.

upvoted 8 times

🗳️ 👤 **hansamaru** Most Recent ⌚ 1 year, 1 month ago

**Selected Answer: A**

Supposed to be A

upvoted 1 times

🗳️ 👤 **MaliDong** 1 year, 1 month ago

**Selected Answer: D**

D should be the answer.

upvoted 2 times

🗳️ 👤 **trigger4848** 1 year, 1 month ago

**Selected Answer: A**

these questions are tricky but the key here " researches an attacking host through logs in a SIEM?" -- This should be done in Detection and Analysis -- A

upvoted 3 times

🗳️ 👤 **Eng\_ahmedyoussef** 1 year, 2 months ago

**Selected Answer: A**

A is correct answer.

Preparation --> Detection and Analysis --> Containment, Eradication and Recovery --> Post-Incident Activity

upvoted 2 times

🗳️ 👤 **[Removed]** 1 year, 4 months ago

sorry NIST SP 800-61...

upvoted 1 times

🗳️ 👤 **[Removed]** 1 year, 4 months ago

According to NIST SP 800-31 3.3 Identifying the Attacking Hosts - incident handlers should generally stay focused on containment, eradication, and recovery. Could be C and D

upvoted 1 times

🗳️ 👤 **adodocletus** 1 year, 6 months ago

Identifying the attacking host is done during containment

so the correct answer is "D"

upvoted 1 times

🗳️ 👤 **Dunky** 1 year, 9 months ago

It is done during Containment, eradication and recovery which is considered a single phase.

As per the course guide

"Containment, Eradication, and Recovery

The containment, eradication, and recovery phase includes the following activities:

- Gathering and handling evidence
- Identifying the attacking hosts
- Choosing a containment strategy to effectively contain and eradicate the attack, as well as to successfully recover from it"

upvoted 2 times

🗨️ 👤 **[Removed]** 1 year, 9 months ago

page 303 in cyberops book, states Containment, eradication and recovery, - identify the attacking host,, which is bad wording because that means answer could be containment or eradication since they are both possible answers. horrible test writing for cisco here .

upvoted 2 times

🗨️ 👤 **bn1234** 1 year, 9 months ago

<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf> section 3.3.3 shows "Identifying the Attacking Hosts" under "Containment, Eradication, and Recovery"

upvoted 2 times

🗨️ 👤 **alocin** 2 years, 2 months ago

From Cisco CyberOps Associate CBROPS 200-201 Official Cert Guide  
chapter 8 page 303

The containment, eradication, and recovery phase includes the following activities:

- Gathering and handling evidence
- Identifying the attacking hosts
- Choosing a containment strategy to effectively contain and eradicate the attack, as well as to successfully recover from it

upvoted 3 times

🗨️ 👤 **ivlis\_27** 2 years, 1 month ago

for me, i think the right answer is A, because in eradication process you identify the attacked hosts not the attacking hosts, meanwhile in detection analysis you profile the network and system, so you can get a clue for the attacking hosts

upvoted 1 times

🗨️ 👤 **aplicacion101** 1 year, 5 months ago

attacked hosts - recovery

attacking hosts - containment

upvoted 1 times

🗨️ 👤 **anonymous1966** 2 years, 3 months ago

Preparation --> Detection and Analysis --> Containment, Erradicaion and Recovery --> Post-Incident Activity

Detection and Analysis --> Profile networks and systems, Understand normal behaviors, Create a log retention policy, Perform event correlation. Maintain and use a knowledge base of information. Use Internet search engines for research. Run packet sniffers to collect additional data. Filter the data. Seek assistance from others. Keep all host clocks synchronized. Know the different types of attacks and attack vectors. Develop processes and procedures to recognize the signs of an incident. Understand the sources of precursors and indicators. Create appropriate incident documentation capabilities and processes. Create processes to effectively prioritize security incidents. Create processes to effectively communicate incident information (internal and external communications).

Ref: Cisco CyberOps Associate CBROPS 200-201 Official Cert Guide

upvoted 3 times

🗨️ 👤 **anonymous1966** 2 years, 3 months ago

Correct = A

upvoted 4 times

A malicious file has been identified in a sandbox analysis tool.

Which piece of information is needed to search for additional downloads of this file by other hosts?

- A. file type
- B. file size
- C. file name
- D. file hash value

**Suggested Answer:** D

Community vote distribution

D (100%)

🗳️ 👤 **drdecker100** 10 months, 2 weeks ago

**Selected Answer: D**

A file hash value is a unique digital signature that is calculated based on the contents of a file. Even a small change to the contents of the file will result in a different hash value. By comparing the hash value of a file that is known to be malicious with the hash values of other files on other hosts, it is possible to identify other instances of the same malicious file, even if the file has a different name, size, or type.

upvoted 2 times

🗳️ 👤 **Eng\_ahmedyoussef** 1 year, 2 months ago

**Selected Answer: D**

File hash value ==> represents the malicious file.

upvoted 1 times

🗳️ 👤 **Cristhian9** 1 year, 7 months ago

yes, it is!

upvoted 1 times

**Stealthwatch** Dashboards Monitor Analyze Jobs

### Flow Search Results (1,166)

[Edit Search](#) 05/06/2020 06:00 AM - 05/06/2020 1:20 PM (Time Range) 2,000 (Max Records)

Subject: 10.201.3.149 Client (Orientation)

Connection: All (Flow Direction)

Peer: Outside Hosts (Host Groups)

START	DURATION	SUBJECT IP AD...	SUBJECT PORT...	SUBJECT HOST...	SUBJECT BYTES	APPLICATION	TOTAL BYTES	PEER IP ADDR...
Ex. 06/09/20	Ex. <=50min40s	Ex. 10.10.10.10	Ex. 57100/UDP	Ex. "catch All"	Ex. <=50M	Ex. "Corporate"	Ex. <=50M	Ex. 10.255.255
May 6, 2020 6:46:42 AM (9hr 14 min 19s ago)	15min 13s	10.201.3.149	52599/UDP	End User Devices, Desktops, Atlanta, Sales and Marketing	6.42 M	Undefined UDP	132.53 M	152.46.6.91

**General**

[View URL Data](#)

Subject	Totals	Peer
Packets: 60.06 K	Packets: 165.87 K	Packets: 105.81 K
Packet Rate: 65.78 pps	Packet Rate: 181.67 pps	Packet Rate: 115.89 pps
Bytes: 6.42 MB	Bytes: 132.53 MB	Bytes: 126.11 MB
Byte Rate: 7.37 Kbps	Byte Rate: 152.2 Kbps	Byte Rate: 144.83 Kbps
Percent Transfer: 4.84%	Subject Byte Ratio: 4.84%	Percent Transfer: 95.16%
Host Groups: End User Devices, Desktops, Atlanta, Sales and Marketing	RTT: --	Host Groups: United States
Payload: --	SRT: --	Payload: --

May 6, 2020 9:44:05 AM (6hr 16min 56s ago)	55 min 56s	10.201.3.149	52599/UDP	End User Devices, Desktops, Atlanta, Sales and Marketing	4.13 M	Undefined UDP	96.26 M	152.46.6.91
---	------------	--------------	-----------	--	--------	---------------	---------	-------------

Refer to the exhibit. What is the potential threat identified in this Stealthwatch dashboard?

- A. Host 10.201.3.149 is sending data to 152.46.6.91 using TCP/443.
- B. Host 152.46.6.91 is being identified as a watchlist country for data transfer.
- C. Traffic to 152.46.6.149 is being denied by an Advanced Network Control policy.
- D. Host 10.201.3.149 is receiving almost 19 times more data than is being sent to host 152.46.6.91.

**Suggested Answer: D**

**anonymous1966** Highly Voted 3 years, 9 months ago

The question is very simple.

"D" is correct.

Subject = 10.201.3.149

Peer = 152.46.6.91

1st search:

Subject --- 6.42 MB --> Peer

Peer --- 132.53 MB --> Subject

2nd search:

Subject --- 4.13 MB --> Peer

Peer --- 96.26 MB --> Subject

$132.53/6.42 = 20.64$

$96.26/4.13 = 22.34$

upvoted 10 times

**AVT** 3 years, 7 months ago

Great explanation, just to clarify:

1st search:

Subject --- 6.42 MB --> Peer

Peer --- 126.11 MB --> Subject

Total Bytes on 1st search: 132.53 MB

2nd search:

Subject --- 4.13 MB --> Peer


Peer --- 92.13 MB --> Subject

Total Bytes on 2nd search: 96.26 MB

$126.11/6.42 = 19.64$



$92.13/4.13 = 22.30$

upvoted 9 times

  **andrewdh**  4 years, 6 months ago

Is it just me or is Answer D the only feasible answer but the wrong way around? It is Host 152.46.6.149 that is receiving 19 times more data than the "subject" at 10.201.3.149

upvoted 8 times

  **bren\_** 4 years, 5 months ago

are you sure the byte and bytes rate are about the download and not about the upload?

upvoted 1 times

  **d3vm3t**  10 months, 3 weeks ago

A. Host 10.201.3.149 is sending data to 152.46.6.91 using TCP/443.

Incorrect: The application shown is UDP, not TCP/443.

B. Host 152.46.6.91 is being identified as a watchlist country for data transfer.

Incorrect: The dashboard doesn't indicate anything about a watchlist country. The peer IP shows "United States" as the host group, which doesn't imply a threat.

C. Traffic to 152.46.6.149 is being denied by an Advanced Network Control policy.

Incorrect: The dashboard does not show any indication of traffic being denied by an Advanced Network Control policy.

upvoted 1 times

  **macxwhale** 1 year, 12 months ago

at <https://www.youtube.com/watch?v=Yvp1hapurj4&t=9s> for the answer D

upvoted 2 times

  **hoek** 4 years, 5 months ago

I also think this is B.

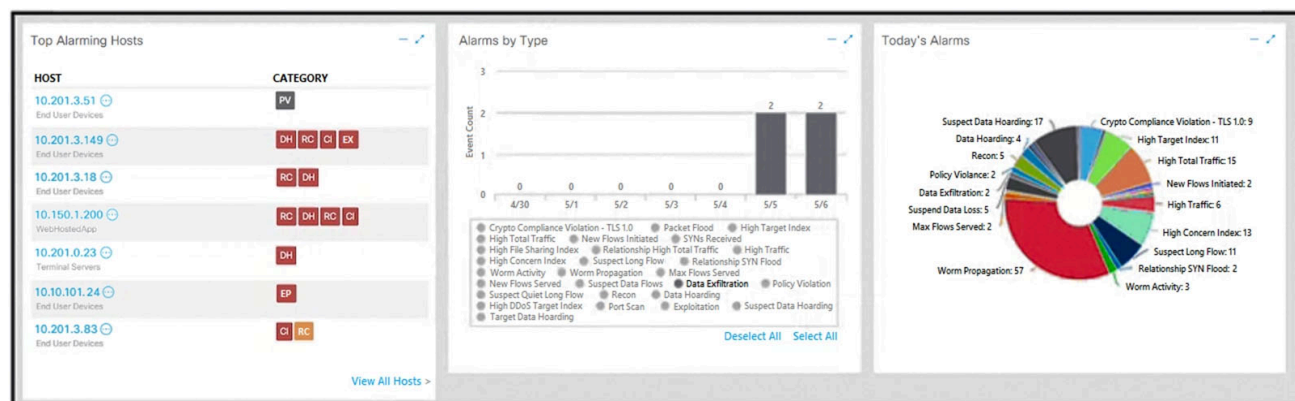
upvoted 3 times

  **Fafabeans** 4 years, 6 months ago

Could it be the watchlist country answer? Maybe because the host group listed is the United States?

upvoted 3 times





Refer to the exhibit. What is the potential threat identified in this Stealthwatch dashboard?

- A. A policy violation is active for host 10.10.101.24.
- B. A host on the network is sending a DDoS attack to another inside host.
- C. There are two active data exfiltration alerts.
- D. A policy violation is active for host 10.201.3.149.

**Suggested Answer: C**

Community vote distribution

C (100%)

Eng\_ahmedyoussef 8 months, 3 weeks ago

**Selected Answer: C**

c is best answer

upvoted 2 times

adodocletus 1 year ago

I think there is no correct answer to this question, I can only see one Ex on the stealth watch and option C says there is two data Exfiltration threat, so the answer can not be C... Please if anyone can explain why C was chosen I will appreciate it...For me, I don't see any correct answer there.

upvoted 1 times

AndyBrian 1 year ago

Look at the middle column, data exfiltration is highlighted (in bold) and the graph displays 2 event counts. Of all the choices its the only one that makes sense.

upvoted 5 times

adodocletus 1 year ago

I just found it... so "C" is correct, Thanks

upvoted 2 times

Which security technology allows only a set of pre-approved applications to run on a system?

- A. application-level blacklisting
- B. host-based IPS
- C. application-level whitelisting
- D. antivirus

**Suggested Answer:** C

*Community vote distribution*

C (100%)

 **AhmedAbdalla** 8 months, 3 weeks ago

Application-level whitelisting is a security practice where only a predefined list of approved applications or processes are allowed to execute on a system. Any other application or process not on the whitelist is blocked or denied from running. This approach provides strong control over the software that can run on a system, enhancing security by preventing the execution of unauthorized or potentially malicious software

upvoted 2 times

 **Eng\_ahmedyoussef** 1 year, 8 months ago

**Selected Answer: C**

C is correct answer

Application level whitelisting ==> security technology allows only a set of pre-approved applications to run on a system.

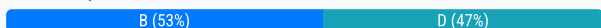
upvoted 1 times

An investigator is examining a copy of an ISO file that is stored in CDFS format.  
What type of evidence is this file?

- A. data from a CD copied using Mac-based system
- B. data from a CD copied using Linux system
- C. data from a DVD copied using Windows system
- D. data from a CD copied using Windows

**Suggested Answer: B**

Community vote distribution



🗨️ **anonymous1966** Highly Voted 3 years, 9 months ago

CDfs is a virtual file system for Unix-like operating systems; it provides access to data and audio tracks on Compact Discs. When the CDfs driver mounts a Compact Disc, it represents each track as a file. This is consistent with the Unix convention "everything is a file".

Source: <https://en.wikipedia.org/wiki/CDfs>

upvoted 9 times

🗨️ **anonymous1966** 3 years, 9 months ago

So, "B" is correct

upvoted 7 times

🗨️ **3000bd6** Most Recent 7 months, 1 week ago

**Selected Answer: B**

The answer is B

upvoted 1 times

🗨️ **d503c75** 9 months, 2 weeks ago

CDfs (Compact Disc File System) - is a virtual file system for Unix-like operating systems;

upvoted 2 times

🗨️ **thisguyfucks** 1 year, 4 months ago

**Selected Answer: D**

Here's the breakdown:

- ISO file - This refers to an image file format that represents the contents of an entire disc, such as a CD or DVD. ISO files are commonly used to back up disc contents or distribute software/data on discs.

- CDFS format - CDFS stands for CD File System. It's a file system used to organize files and metadata on CD and DVD discs.

- So in this case, we have an ISO file, which contains a full disc image, and that disc image uses the CDFS format internally.

The CDFS format is used by Windows natively to organize CD/DVD discs. ISO files are a common format used across Windows, Mac and Linux to back up and distribute disc contents.

Therefore, the ISO file being in CDFS format implies it is an image of a CD that was originally copied or created on a Windows system, using the native CDFS file system.

The answer is D - data from a CD copied using Windows.

upvoted 2 times

🗨️ **sheyshey** 1 year, 6 months ago

**Selected Answer: B**

The answer is B.. linux

upvoted 2 times

🗨️ 👤 **Faio** 1 year, 11 months ago

The answer is D.

CDFS is a file system for CD-ROMs that was developed by Microsoft. It is the most common file system for CD-ROMs, and it is used by both Windows and Linux systems. However, Mac systems do not use CDFS. Therefore, the ISO file must have been created by a Windows system.

Operating System File System

Windows CDFS

Linux ISO 9660

Mac HFS+

upvoted 2 times

🗨️ 👤 **Topsecret** 1 year, 11 months ago

**Selected Answer: D**

The correct answer is D. data from a CD copied using Windows.

An ISO file stored in CDFS (Compact Disc File System) format typically contains data that was originally from a CD. CDFS is a file system commonly used for CDs, and it is compatible with Windows operating systems.

upvoted 2 times

🗨️ 👤 **Isuckatexams** 2 years ago

**Selected Answer: B**

NIST Publication 800-86 defines all file systems for linux, and under the file system category falls CDFS (not CDfs).

defined as "Compact Disk File System (CDFS). As the name indicates, the CDFS filesystem is used for

CDs" If we investigate CDFS further, it was first introduced between 1985 and 1986 on Linux and it exports all tracks and boot images on a CD as normal files.

CDFS is a write-once-read-only file system (ISO 9660). The Question is asking where the ISO came from. not what operating system is examining the copy, which could be windows.

In my opinion, the ISO data came from a UNIX based system stored on a CD in the CDFS format

upvoted 4 times

🗨️ 👤 **Isuckatexams** 2 years ago

**Selected Answer: D**

CDFS is windows

upvoted 2 times

🗨️ 👤 **Isuckatexams** 2 years ago

i am wrong look at other comment

upvoted 2 times

🗨️ 👤 **Stevens0103** 2 years, 1 month ago

**Selected Answer: D**

CDFS is a file system used by Windows operating systems for CD-ROMs and DVDs. It provides a hierarchical file system structure and is used for reading discs that conform to the ISO 9660 standard.

CDfs, on the other hand, is a file system used by Unix-like operating systems for mounting CD-ROMs and DVDs. It allows the disc to be treated like any other file system, and files can be accessed by their names and paths.

upvoted 2 times

🗨️ 👤 **StutiKandpal** 2 years, 5 months ago

**Selected Answer: D**

Windows based

upvoted 3 times

🗨️ 👤 **Eng\_ahmedyoussef** 2 years, 8 months ago

**Selected Answer: B**

B is correct



CDfs is a virtual file system for Linux operating systems

upvoted 2 times

🗨️ 👤 **BobbyYarush** 3 years, 3 months ago



CDFS is not specific to a single Operating System, it means that a disc burned on Macintosh using CDFS can be read on a Windows or Linux based computer. So, what's the answer??

upvoted 3 times

  **Dunky** 3 years, 3 months ago

CDFs is a file system for Linux systems that `exports' all tracks and boot images on a CD as normal files. These files can then be mounted (e.g. for ISO and boot images), copied, played (audio tracks), etc. The primary goal for developing this file system was to `unlock' information in old ISO sessions.

upvoted 1 times

  **Briley** 3 years, 5 months ago

I thought CDFs was unix-based? Doesn't that mean that it's a cd from a mac system?

upvoted 1 times

Which piece of information is needed for attribution in an investigation?

- A. proxy logs showing the source RFC 1918 IP addresses
- B. RDP allowed from the Internet
- C. known threat actor behavior
- D. 802.1x RADIUS authentication pass and fail logs

**Suggested Answer:** C

Community vote distribution

C (100%)

🗳️ 👤 **SecurityGuy** 10 months, 4 weeks ago

**Selected Answer: C**

Attribution

- The action of regarding something as being caused by a person or thing; identifies a source or cause of something.
- Synonym: Attribute, Characteristic, Feature, Trait, Quality

upvoted 2 times

🗳️ 👤 **Eng\_ahmedyoussef** 1 year, 8 months ago

**Selected Answer: C**

C is the best answer

upvoted 1 times

🗳️ 👤 **kyle942** 1 year, 9 months ago

The private IP address of the attacker is what you want for the police, to map the attack to your device on the internet.

upvoted 1 times

🗳️ 👤 **1z** 2 years, 8 months ago

RFC1918 is for Address Allocation for Private Internets so I doubt that it would serve to any attribution...

upvoted 4 times

🗳️ 👤 **tsabee** 2 years, 8 months ago

Sure! Correct answer is C. Actually this is the most important thing: know who, what, how, why, etc.. attack the network.

upvoted 2 times

🗳️ 👤 **[Removed]** 2 years, 9 months ago

It seems to me that correct answer is A. proxy logs showing the source RFC 1918 IP addresses.

upvoted 1 times

What does cyber attribution identify in an investigation?

- A. cause of an attack
- B. exploit of an attack
- C. vulnerabilities exploited
- D. threat actors of an attack

**Suggested Answer: D**

Community vote distribution

D (100%)

🗳️ 👤 **SecurityGuy** 10 months, 4 weeks ago

**Selected Answer: D**

Attribution

- The action of regarding something as being caused by a person or thing; identifies a source or cause of something.
- Synonym: Attribute, Characteristic, Feature, Trait, Quality

upvoted 3 times

🗳️ 👤 **drdecker100** 1 year, 4 months ago

**Selected Answer: D**

Cyber attribution in an investigation is the process of identifying the threat actors who are responsible for an attack.

Cyber attribution involves collecting and analyzing various types of data, including network logs, malware samples, social media activity, and other intelligence sources, to identify the individuals, groups, or nations responsible for the attack. The process of cyber attribution can help identify the motives, methods, and capabilities of the attackers, which can be useful in preventing future attacks and in pursuing legal action against the perpetrators.

upvoted 2 times

🗳️ 👤 **Eng\_ahmedyoussef** 1 year, 8 months ago

**Selected Answer: D**

D. threat actors of an attack

upvoted 1 times

🗳️ 👤 **[Removed]** 2 years, 3 months ago

i think D is correct also. Page 17 omar book

upvoted 1 times

🗳️ 👤 **Uzumaki\_Aliyy** 2 years, 6 months ago

D - correct based on this:

<https://www.techtarget.com/searchsecurity/definition/cyber-attribution>

upvoted 3 times

A security engineer has a video of a suspect entering a data center that was captured on the same day that files in the same data center were transferred to a competitor.

Which type of evidence is this?

- A. best evidence
- B. prima facie evidence
- C. indirect evidence
- D. physical evidence

**Suggested Answer: C**

Community vote distribution

C (100%)

🗳️ 👤 **SecurityGuy** 10 months, 3 weeks ago

**Selected Answer: C**

Prima Facie Evidence

- Sometimes called presumptive evidence, uses other types of evidence gathered from a crime scene to make a plausible or reasonable assumption.

Indirect or Circumstantial Evidence

- It describes information that doesn't directly connect a defendant to a crime but rather implies a connection exists. (Eyewitness, Witness, Fingerprint)

Physical Evidence or Real Evidence

- It is a material object with a connection to the defendant's potential role in a crime.

Two Types of Physical Evidence:

- Individual Physical Evidence - involves pieces that are unique to a person, such as DNA or fingerprints.

- Class Physical Evidence - Relates to a certain segment of the population, which may help professionals narrow down a list of suspects. Examples of class physical evidence include blood type, tire tread and weapon manufacturers.

<https://www.indeed.com/career-advice/career-development/different-types-of-evidence>

upvoted 2 times

🗳️ 👤 **Eng\_ahmedyoussef** 1 year, 8 months ago

**Selected Answer: C**

C is the correct answer

--> Indirect or circumstantial evidence: extrapolation to a conclusion of fact

upvoted 1 times

🗳️ 👤 **[Removed]** 2 years, 3 months ago

you cant say BEST because you dont see him committing the crime, how do you not know someone did it remotely while he was in there? so indirect would be best.

upvoted 1 times

🗳️ 👤 **[Removed]** 2 years, 4 months ago

Its not best evidence because you do NOT see the suspect commit the crime only walking in there, indirect evidence is what the book is saying, someone could of hacked the data center the same time he walked in.

upvoted 1 times

🗳️ 👤 **anonymous1966** 2 years, 9 months ago

"C" is correct

By the book:

There are three general types of evidence:

--> Best evidence: can be presented in court in the original form (for example, an exact copy of a hard disk drive).

--> Corroborating evidence: tends to support a theory or an assumption deduced by some initial evidence. This corroborating evidence confirms the proposition.



--> Indirect or circumstantial evidence: extrapolation to a conclusion of fact (such as fingerprints, DNA evidence, and so on).

So it could only be "A" or "C".

In this case, it is obvious that the Video is NOT a best evidence.

upvoted 3 times

  **forest111** 3 years, 6 months ago

I think it is D.

Indirect evidence – This is evidence that, in combination with other facts, establishes a hypothesis. This is also known as circumstantial evidence.



For example, evidence that an individual has committed similar crimes can support the assertion that the person committed the crime of which they are accused.

upvoted 1 times

  **forest111** 3 years, 6 months ago

mistake, I thought about C. indirect evidence

upvoted 13 times



  **Mahir7** 3 years, 6 months ago

The correct answer is A: best evidence, is when you have digital copy of the intruder, video, photography or exact copy of the hard disk as evidence.

Indirect evidence, is when you have the DNA or Fingerprints of the person that committed the crime.

Site sources: <https://packitforwarding.com/index.php/2019/08/04/ccna-cyberops-secops-objective-1-6/>

upvoted 1 times

  **bren\_** 3 years, 5 months ago

please check the link you provided again. I think it's C

upvoted 5 times

  **harshi** 2 years, 12 months ago

yes even video recording and digital recording are indirect evidence

upvoted 1 times

## DRAG DROP -

Drag and drop the type of evidence from the left onto the description of that evidence on the right.

Select and Place:

direct evidence	log that shows a command and control check-in from verified malware
corroborative evidence	firewall log showing successful communication and threat intelligence stating an IP is known to host malware
indirect evidence	NetFlow-based spike in DNS traffic

## Suggested Answer:

	direct evidence
	indirect evidence
	corroborative evidence

🗨️ 👤 **Mevijil** Highly Voted 1 year, 10 months ago

I'm pretty sure it should be:

-C2 Log = Best

-Firewall Log = Corroborative

-Netflow = Indirect

The C2 log seems to be direct evidence of a crime, while the firewall log seems to be corroborating that 'something' is happening, while the netflow spike is only circumstantial (could be indicative of something else happening, could not be).

upvoted 15 times

🗨️ 👤 **bn1234** 1 year, 9 months ago

Agreed

upvoted 5 times

🗨️ 👤 **drdecker100** Most Recent 10 months, 2 weeks ago

Overall, the combination of these three pieces of evidence could be used to build a stronger case that there is malware present on the system and that it is communicating with a command and control server. The direct evidence of the malware check-in is supported by the corroborative evidence of the successful communication with a known malware-hosting IP address, while the indirect evidence of the netflow-based spike in DNS traffic provides additional context that further supports the presence of suspicious activity on the network.

upvoted 3 times

🗨️ 👤 **Eng\_ahmedyoussef** 1 year, 2 months ago

Direct - indirect - corroborative

upvoted 3 times

🗨️ 👤 **DLukynsky** 1 year, 9 months ago

corroborative based on next question

upvoted 1 times

Aug 24 2020 09:02:37: %ASA-4-106023: Deny tcp src outside:209.165.200.228/51585 dst inside:192.168.150.77/22 by access-group "OUTSIDE" [0x5063b82f, 0x0]

Refer to the exhibit. An analyst received this alert from the Cisco ASA device, and numerous activity logs were produced. How should this type of evidence be categorized?

- A. indirect
- B. circumstantial
- C. corroborative
- D. best

**Suggested Answer: C**

Community vote distribution

C (82%)

D (18%)

🗳️ **Silexis** 11 months ago

According to the study guide - Best Evidence is one can be presented in court in original form. As a log, it will satisfy this condition, especially that it is a DENY so there is no successful connection and as the question is not presenting what other logs refer to, we cannot elaborate further  
upvoted 1 times

🗳️ **SecurityGuy** 1 year, 4 months ago

**Selected Answer: D**

The question doesn't mentioned an existing evidence, corroborative evidence supports another evidence. The other logs is "probably" same as this log.

The log counts as a single evidence, we might be overthinking this so I'll choose the simplest answer which is D.  
upvoted 1 times

🗳️ **Mack279** 1 year, 7 months ago

Is the analyst trying to prove that .228 attempted ssh to .77? If yes then the answer is D.

But other than that, its C.  
upvoted 1 times

🗳️ **Lenon** 1 year, 8 months ago

A & B auto eliminated since they are same. this leaves only C as correct. It cant be best evidence this one  
upvoted 1 times

🗳️ **StutiKandpal** 1 year, 12 months ago

**Selected Answer: C**

corroborative  
upvoted 2 times

🗳️ **trigger4848** 2 years, 1 month ago

**Selected Answer: C**

not sure how this is best evidence for attribution.. A & B are the same thing indirect = circumstantial so they have to eliminated. That leaves answer C for corroborative.  
upvoted 3 times

🗳️ **cy\_analyst** 2 years, 2 months ago

Best is something that you will go to court with. So here you are far away from that.  
upvoted 4 times

🗳️ **moali012** 2 years, 2 months ago

**Selected Answer: D**

it is direct evidence  
upvoted 1 times

🗨️ 👤 **Eng\_ahmedyoussef** 2 years, 2 months ago

**Selected Answer: C**

C is correct answer

because numerous activity logs were produced.

upvoted 4 times

🗨️ 👤 **Ozair** 2 years, 3 months ago

why not C ?

upvoted 1 times

Category	Started On	Completed On	Duration	Cuckoo Version
FILE	2014-02-23 21:52:16	2014-02-23 21:52:34	18 seconds	1.0

### File Details

<b>File name</b>	Win32.Polip.a.exe
<b>File size</b>	414720 bytes
<b>File type</b>	PE32 executable (GUI) Intel 88386, for MS Windows
<b>CRC32</b>	8848E2EA
<b>MD5</b>	090f906b81776bece10280cc84c0cae8
<b>SHA1</b>	f891d31d3e4a5f07a1f950156322d8ec979b79ba
<b>SHA256</b>	f4855d1b10f7ab1a2e699016437f72c5f98579d69f08b6312cc24400f483177
<b>SHA512</b>	9756e0af8981bc9296a3879fe02d0e102c5557ba99a004230ca4f1dfd03592cf497c123d2a6a05596b07432188aaef42976e0bd9da742c0900275be721db2595
<b>Ssdeep</b>	6144:EuZUY7eiLnfnB7pRi8l+SzLqiZ49XCUGnGyCYUE/1rWDepfYXt+o6YUPL:EuZUY7eandid+SVGCUgM7Ck/1r7EE
<b>PEiD</b>	None matched
<b>Yara</b>	<ul style="list-style-type: none"> <li>• shellcode (Matched shellcode byte patterns)</li> </ul>
<b>VirusTotal</b>	<a href="#">Permalink</a> VirusTotal Scan Date: 2014-01-12 23:43:56 Detection Rate: 26/47 ( <a href="#">collapse</a> )

Refer to the exhibit. Which piece of information is needed to search for additional downloads of this file by other hosts?

- A. file header type
- B. file size
- C. file name
- D. file hash value

**Suggested Answer: D**

Community vote distribution

D (100%)

 **SecurityGuy** 10 months, 3 weeks ago

**Selected Answer: D**

Copying will change a file's system metadata values, including its location, creation data and last accessed date, but as these are all stored outside of the file, the hash shouldn't change.

Therefore, searching for the File Hash Value on other hosts will let you know if the file has been downloaded on other hosts.

upvoted 2 times

 **Eng\_ahmedyoussef** 1 year, 8 months ago

**Selected Answer: D**

D is correct

File Hash value

upvoted 1 times

An organization's security team has detected network spikes coming from the internal network. An investigation has concluded that the spike in traffic was from intensive network scanning. How should the analyst collect the traffic to isolate the suspicious host?

- A. based on the most used applications
- B. by most active source IP
- C. by most used ports
- D. based on the protocols used

**Suggested Answer: B**

*Community vote distribution*

B (100%)

🗨️ 👤 **SecurityGuy** 10 months, 3 weeks ago

**Selected Answer: B**

From an admin point of view, you'll wanna know what sources of the detected anomaly.  
Normally, you'll search for the IP Address or Host.  
upvoted 1 times

🗨️ 👤 **solodoc4l** 1 year, 8 months ago

My daughter got that right just by knowing what an IP address is  
upvoted 1 times

🗨️ 👤 **Eng\_ahmedyoussef** 1 year, 8 months ago

**Selected Answer: B**

By most active source ip  
upvoted 1 times

Which technology on a host is used to isolate a running application from other application?

- A. application allow list
- B. application block list
- C. host-based firewall
- D. sandbox

**Suggested Answer:** D

Reference:

<https://searchsecurity.techtarget.com/definition/sandbox#:~:text=Sandboxes%20can%20be%20used%20to,be%20run%20inside%20a%20sandb>  
ox

Community vote distribution

D (100%)

🗨️ 👤 **AhmedAbdalla** 8 months, 4 weeks ago

Sandbox

A sandbox is a technology used to isolate a running application from other applications and from the host system itself. It provides a controlled environment where the application can run with restricted access to system resources and sensitive data. This isolation helps prevent the application from causing harm to the host system or other applications and serves as a security mechanism to contain potential threats. The other options, such as application allow lists, application block lists, and host-based firewalls, can be part of a broader security strategy but do not inherently provide the same level of isolation as a sandbox.

upvoted 2 times

🗨️ 👤 **Eng\_ahmedyoussef** 1 year, 8 months ago

**Selected Answer: D**

sandbox

upvoted 2 times

```
SELECT * FROM people WHERE username = " OR '1'='1';
```

Refer to the exhibit. Which type of attack is being executed?

- A. cross-site request forgery
- B. command injection
- C. SQL injection
- D. cross-site scripting

**Suggested Answer: C**

Reference:

[https://www.w3schools.com/sql/sql\\_injection.asp](https://www.w3schools.com/sql/sql_injection.asp)

Community vote distribution

C (100%)

🗨️ 👤 **AhmedAbdalla** 8 months, 3 weeks ago

The provided SQL query is an example of a **SQL injection** attack.

In SQL injection attacks, malicious SQL code is injected into input fields or parameters used in SQL queries to manipulate the database query's logic. In this case, the input `" OR '1'='1';` is designed to manipulate the query to always return results because `'1'='1'` is a true statement in SQL. This could potentially allow an attacker to bypass authentication or retrieve sensitive data from the database.

So, the correct answer is **SQL injection**.

upvoted 2 times

🗨️ 👤 **Eng\_ahmedyoussef** 1 year, 8 months ago

**Selected Answer: C**

SQL injection

upvoted 1 times



What is a difference between inline traffic interrogation and traffic mirroring?

- A. Inline inspection acts on the original traffic data flow
- B. Traffic mirroring passes live traffic to a tool for blocking
- C. Traffic mirroring inspects live traffic for analysis and mitigation
- D. Inline traffic copies packets for analysis and security

**Suggested Answer: A**



Community vote distribution

A (100%)

  **olaolaola12345** Highly Voted 3 years, 10 months ago

i think A is correct

upvoted 41 times



  **beowolf** 3 years, 9 months ago

Yes A should be the answer.

Inline traffic interrogation analyzes traffic in real time and has the ability to prevent certain traffic from being forwarded



Traffic mirroring doesn't pass the live traffic instead it copies traffic from one or more source ports and sends the copied traffic to one or more destinations for analysis by a network analyzer or other monitoring device

upvoted 14 times

  **Friendly** 3 years, 10 months ago

It's B

upvoted 2 times

  **CiscoTerminator** Highly Voted 3 years, 3 months ago

Can the Admins not correct the wrong answers for future test-takers?

upvoted 14 times

  **Eholic** 2 years, 9 months ago

On a different website with the same question - the correct answer is A.

upvoted 2 times

  **Eholic** 2 years, 9 months ago

Yesss thank you

upvoted 1 times

  **RoBery** Most Recent 11 months, 3 weeks ago

A is correct.

Mirroring doesn't pass live/real time packets, inline does.

upvoted 1 times

  **Topsecret** 1 year, 5 months ago

Selected Answer: A

The correct answer is A. Inline inspection acts on the original traffic data flow.

Inline traffic interrogation and traffic mirroring are two different approaches used in network security and analysis. The key difference lies in how they handle the traffic data flow.

upvoted 1 times

  **ShammaA** 1 year, 7 months ago

Answer is A

Inline Traffic Int. simply acts on the original traffic flow while traffic mirroring simply "mirrors" live traffic from 1 interface to another hence the name (purpose served is content inspection and threat monitoring).

upvoted 1 times

🗳️ 👤 **drdecker100** 1 year, 10 months ago

**Selected Answer: A**

The difference between inline traffic interrogation and traffic mirroring is:

A. Inline inspection acts on the original traffic data flow - Inline traffic interrogation is a technique in which traffic flows through a device that inspects the traffic and makes decisions about how to handle it. The inspection takes place in real-time and in-line with the traffic flow.

B. Traffic mirroring passes live traffic to a tool for blocking - Traffic mirroring, also known as port mirroring or SPAN (Switched Port Analyzer), is a technique for forwarding a copy of network traffic to a monitoring device. The copy of the traffic is sent to a separate tool for analysis, security or other purposes.

Therefore, the correct answer is A. Inline inspection acts on the original traffic data flow.

upvoted 3 times

🗳️ 👤 **Eng\_ahmedyoussef** 2 years, 2 months ago

**Selected Answer: A**

Sure A. is the correct answer

Inline inspection ==> acts on the original traffic data flow

upvoted 1 times

🗳️ 👤 **Eng\_ahmedyoussef** 2 years, 2 months ago

**Selected Answer: A**

Sure A. is the correct answer

Inline inspection ==> acts on the original traffic data flow Most Voted

upvoted 1 times

🗳️ 👤 **weganos** 2 years, 3 months ago

**Selected Answer: A**

Please change the answer to: A

Traffic mirroring does not pass live traffic to a tool for blocking...

upvoted 1 times

🗳️ 👤 **EmmaDer** 2 years, 5 months ago

**Selected Answer: A**

A should be right as IDS don't block traffic

upvoted 1 times

🗳️ 👤 **adodocletus** 2 years, 6 months ago

Inline traffic interrogation analyzes traffic in real-time and can prevent certain traffic from being forwarded Traffic mirroring doesn't pass the live traffic instead it copies traffic from one or more source ports and sends the copied traffic to one or more destinations for analysis by a network analyzer or other monitoring device, so the answer should be A

upvoted 1 times

🗳️ 👤 **ESTHER\_97** 2 years, 7 months ago

**Selected Answer: A**

A is correct

upvoted 1 times

🗳️ 👤 **DLukynskyy** 2 years, 9 months ago

**Selected Answer: A**

A. Other answers make no sense

upvoted 1 times

🗳️ 👤 **Abdullah00** 2 years, 10 months ago

**Selected Answer: A**

A is correct

upvoted 1 times

🗳️ 👤 **MILOP88** 2 years, 10 months ago

**Selected Answer: A**

Traffic mirroring does not block live traffic, but inline topology traffic inspection, can block suspicious traffic.


upvoted 1 times

🗳️ 👤 **CiscoTerminator** 3 years ago

Selected Answer: A

Traffic mirroring does not block live traffic.

upvoted 2 times

  **GAD90** 3 years, 1 month ago

Answer: A

Explanation:

Inline traffic interrogation analyzes traffic in real time and has the ability to prevent certain traffic from being forwarded Traffic mirroring doesn't pass the live traffic instead it copies traffic from one or more source ports and sends the copied traffic to one or more

destinations for analysis by a network analyzer or other monitoring device

COPY PASTE FROM ANOTHER SOURCE

upvoted 2 times

A system administrator is ensuring that specific registry information is accurate.  
Which type of configuration information does the HKEY\_LOCAL\_MACHINE hive contain?

- A. file extension associations
- B. hardware, software, and security settings for the system
- C. currently logged in users, including folders and control panel settings
- D. all users on the system, including visual settings

**Suggested Answer: B**

Community vote distribution

B (100%)

🗳️ 👤 **Eng\_ahmedyoussef** 8 months, 3 weeks ago

**Selected Answer: B**

B. hardware, software, and security settings for the system  
is the correct answer  
upvoted 2 times

🗳️ 👤 **addpro7** 1 year, 2 months ago

**Selected Answer: B**

B : correct answer

HKEY\_LOCAL\_MACHINE (HKLM): HKLM contains machine hardware-specific information that the operating system runs on. This includes a list of drives mounted on the system and generic configurations of installed hardware and applications. HKLM is a hive that isn't referenced from within another hive.

Cisco CyberOps Associate CBROPS 200-201 Official Cert Guide (Certification Guide) by Omar Santos p597  
upvoted 1 times

🗳️ 👤 **Uzumaki\_Aliyy** 1 year, 6 months ago

B - correct based on this:

<https://docs.microsoft.com/en-us/windows/win32/sysinfo/registry-hives>

[https://ldapwiki.com/wiki/HKEY\\_LOCAL\\_MACHINE#:~:text=HKEY\\_LOCAL\\_MACHINE%20Windows%20registry%20hive%20contains,detected%20hardware%20](https://ldapwiki.com/wiki/HKEY_LOCAL_MACHINE#:~:text=HKEY_LOCAL_MACHINE%20Windows%20registry%20hive%20contains,detected%20hardware%20)  
upvoted 1 times

🗳️ 👤 **anonymous1966** 1 year, 9 months ago

"B" is correct.

See table at

<https://docs.microsoft.com/en-us/troubleshoot/windows-server/performance/windows-registry-advanced-users>  
upvoted 3 times

No.	Time	Source	Destination	Protocol	Length	Info
1878	6.473353	173.37.145.84	10.0.2.15	TCP	62	80-49522 [ACK] Seq=14404 Ack=2987 Win=65535 Len=0
1986	6.736855	173.37.145.84	10.0.2.15	HTTP	245	HTTP/1.1 304 Not Modified
1987	6.736873	10.0.2.15	173.37.145.84	TCP	56	49522->80 [ACK] Seq=2987 Ack=14593 Win=59640 Len=0
2317	7.245088	10.0.2.15	173.37.145.84	TCP	2976	[TCP segment of a reassembled PDU]
2318	7.245192	10.0.2.15	173.37.145.84	HTTP	1020	GET /web/fw/i/ntpametag.gif?js=1&ts=1476292607552.286&tc
2321	7.246633	173.37.145.84	10.0.2.15	TCP	62	80-49522 [ACK] Seq=14593 Ack=4447 Win=65535 Len=0
2322	7.246640	173.37.145.84	10.0.2.15	TCP	62	80-49522 [ACK] Seq=14593 Ack=5907 Win=65535 Len=0
2323	7.246642	173.37.145.84	10.0.2.15	TCP	62	80-49522 [ACK] Seq=14593 Ack=6871 Win=65535 Len=0
2542	7.512750	173.37.145.84	10.0.2.15	HTTP	442	HTTP/1.1 200 OK (GIF89a)
2543	7.512781	10.0.2.15	173.37.145.84	TCP	56	49522->80 [ACK] Seq=6871 Ack=14979 Win=62480 Len=0

Refer to the exhibit. Which packet contains a file that is extractable within Wireshark?

- A. 2317
- B. 1986
- C. 2318
- D. 2542

**Suggested Answer: D**

Community vote distribution

D (100%)

🗳️ 👤 **qz999** Highly Voted 1 year, 10 months ago

Moderator - please strike my previous comment. Packet 2318 is just the request for the file. There is indication of a gif in the 2542 packet.  
upvoted 15 times

🗳️ 👤 **2c44ebe** Most Recent 2 months ago

**Selected Answer: D**

Packet 2542 (HTTP/1.1 200 OK (GIF89a)): This packet is an HTTP response with a 200 OK status code, indicating that the request was successful. The additional information (GIF89a) within this packet strongly suggests that the content of this packet is a GIF image in GIF89a format. Wireshark can reassemble and extract the body of this packet as the GIF file.

upvoted 1 times

🗳️ 👤 **Eng\_ahmedyoussef** 8 months, 3 weeks ago

**Selected Answer: D**

D. Is correct answer

2542 == ""200 OK" status code

upvoted 2 times

🗳️ 👤 **kyle942** 9 months, 1 week ago

**Selected Answer: D**

asking for a file that wireshark can view: it is gif image and wireshark can view it, too easy.

upvoted 2 times

🗳️ 👤 **qz999** 1 year, 10 months ago

Packet 2542 is just an 'ok' status code. Packet 2318 has an actual file indicated at the right end of its line.

upvoted 3 times

🗳️ 👤 **fejec** 1 year, 9 months ago

Try replay by yourself with wireshark accessing a "http" website, then from wireshark go to:

File->Export Objects -> HTTP... and see which are the number packets contains the images from website, all have "200 OK (<format>)", examples image format are GIF89a, PNG, etc.

"D" is correct (2542 packet).

upvoted 8 times




Which regex matches only on all lowercase letters?

- A. `[a-z]'`
- B. `[^a-z]'`
- C. `a-z`
- D. `a*`

**Suggested Answer: A**

Community vote distribution

A (100%)

  **anonymous1966**  1 year, 9 months ago  
"A" is correct

Again in greek for me.

The correct question:

Which regex matches only on all lowercase letters?

- A. `[a-z]` <-- a sequence of letters in lower case
- B. `[^a-z]` <-- NOT a sequence of letters in lower case
- C. `a-z` <-- a sequence of "a-z" word
- D. `a*z` <-- exclude "a" finds "z"

upvoted 6 times


  **Eng\_ahmedyoussef**  8 months, 3 weeks ago

**Selected Answer: A**

A is correct answer


`[a-z]`

upvoted 1 times

  **Alannn** 1 year, 9 months ago



A is correct, test here: <https://regex101.com/>

upvoted 4 times

  **Stuple** 2 years, 2 months ago



None of the answers are actually valid

upvoted 2 times

  **harshi** 1 year, 12 months ago

`[az]` is a valid answer ?

upvoted 1 times

  **Dunky** 1 year, 4 months ago

No, that would exclude b-y

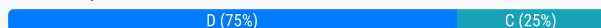
upvoted 1 times

While viewing packet capture data, an analyst sees that one IP is sending and receiving traffic for multiple devices by modifying the IP header. Which technology makes this behavior possible?

- A. encapsulation
- B. TOR
- C. tunneling
- D. NAT

**Suggested Answer: D**

Community vote distribution



**affulinuha** **Highly Voted** 2 years, 10 months ago

the answer is correct, Network address translation (NAT) is a method of mapping an IP address space into another by modifying network address information in the IP header of packets while they are in transit across a traffic routing device.

upvoted 7 times

**Faio** **Most Recent** 11 months, 1 week ago

The answer is C. tunneling.

Tunneling is a technology that allows one network to be encapsulated within another network. This means that all of the traffic from the first network is sent over the second network, as if it were part of the second network.

In the case of the question, the analyst is seeing one IP address sending and receiving traffic for multiple devices. This is possible because the traffic is being tunneled through the one IP address.

upvoted 1 times

**Faio** 11 months, 1 week ago

Sorry, re-reading the question better, I agree that the correct answer is D

upvoted 2 times

**Topsecret** 11 months, 3 weeks ago

**Selected Answer: C**

The correct answer is C. tunneling.

The behavior described, where one IP is sending and receiving traffic for multiple devices by modifying the IP header, is made possible by tunneling technology.

Tunneling involves encapsulating one network protocol within another, allowing the encapsulated protocol to traverse over a network that would not natively support it. In the context of the given scenario, tunneling is used to encapsulate traffic from multiple devices within the IP header of a single IP address.

Option D, "NAT" (Network Address Translation), involves translating IP addresses between different networks. While NAT can be used to enable multiple devices to share a single public IP address, it does not typically involve modifying IP headers to route traffic for multiple devices through a single IP address.

upvoted 1 times

**EverySpanishPersonEver** 10 months, 3 weeks ago

Modifying IP headers is exactly what NAT does... How else are you supposed to route the data? NAT replaces the RFC1989 addresses with the public IP then adds it to a state table allowing a return translation.

Tunneling encapsulates IP headers by adding a new outer IP header for public routing. It's not the same at all.

upvoted 2 times

**Eng\_ahmedyoussef** 1 year, 8 months ago

**Selected Answer: D**

D. is correct answer

NAT (Network Address Translation ) ==> is a method of mapping an IP address space into another by modifying network address information in the IP header of packets while they are in transit across a traffic routing device.

upvoted 3 times



Which action should be taken if the system is overwhelmed with alerts when false positives and false negatives are compared?



- A. Modify the settings of the intrusion detection system.
- B. Design criteria for reviewing alerts.
- C. Redefine signature rules.
- D. Adjust the alerts schedule.

**Suggested Answer: A**

Community vote distribution

B (50%)

A (50%)

  **anonymous1966** Highly Voted 3 years, 9 months ago

"A" is correct

Traditional intrusion detection system (IDS) and intrusion prevention system (IPS) devices need to be tuned to avoid false positives and false negatives. Next-generation IPSs do not need the same level of tuning compared to traditional IPSs. Also, you can obtain much deeper reports and functionality, including advanced malware protection and retrospective analysis to see what happened after an attack took place.

Ref:

Cisco CyberOps Associate CBROPS 200-201 Official Cert Guide

By Omar Santos

upvoted 15 times

  **74cd09c** Most Recent 9 months, 3 weeks ago

C - false positives and false negatives often result from poorly defined or outdated signature rules in intrusion detection systems (IDS). Redefining or tuning these signature rules helps reduce false positives (legitimate actions being flagged) and false negatives (malicious activity going unnoticed), improving the efficiency of the alert system.

upvoted 1 times

  **fisher004** 1 year, 7 months ago

Correct Answer is A

upvoted 2 times

  **Topsecret** 1 year, 11 months ago

Selected Answer: B

The correct answer is B. Design criteria for reviewing alerts.

When a system is overwhelmed with alerts, indicating a high number of both false positives (incorrectly identifying benign events as threats) and false negatives (failing to detect actual threats), it is important to establish criteria for reviewing alerts. This allows for a more efficient and effective handling of the alerts and helps prioritize the investigation of genuine security incidents.

Designing criteria for reviewing alerts involves creating rules or thresholds that filter and prioritize alerts based on their severity, likelihood of being true positives, or other relevant factors. By setting criteria, analysts can focus their efforts on alerts that have a higher probability of being legitimate threats, reducing the time and resources wasted on false positives and irrelevant alerts.

upvoted 1 times

  **Eng\_ahmedyoussef** 2 years, 8 months ago

Selected Answer: A

A. is correct answer

Traditional intrusion detection system (IDS) and intrusion prevention system (IPS) devices need to be tuned to avoid false positives and false negatives.

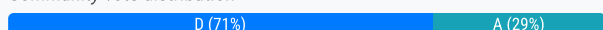
upvoted 1 times

What is the impact of false positive alerts on business compared to true positive?

- A. True positives affect security as no alarm is raised when an attack has taken place, while false positives are alerts raised appropriately to detect and further mitigate them.
- B. True-positive alerts are blocked by mistake as potential attacks, while False-positives are actual attacks identified as harmless.
- C. False positives alerts are manually ignored signatures to avoid warnings that are already acknowledged, while true positives are warnings that are not yet acknowledged.
- D. False-positive alerts are detected by confusion as potential attacks, while true positives are attack attempts identified appropriately.

**Suggested Answer: D**

Community vote distribution



🗳️ 👤 **AhmedAbdalla** 8 months, 3 weeks ago

False-positive alerts are detected by confusion as potential attacks, while true positives are attack attempts identified appropriately.

In the context of security alerts and detection systems, a "false positive" occurs when an alert is triggered for something that is not actually a security threat, potentially leading to confusion and wasted resources. On the other hand, a "true positive" is when the system correctly identifies a genuine security threat or attack attempt.

upvoted 2 times

🗳️ 👤 **Faio** 11 months, 1 week ago

The answer is D

upvoted 2 times

🗳️ 👤 **Topsecret** 11 months, 3 weeks ago

Options B, C, and D are incorrect as they do not accurately describe the impact of false positive and true positive alerts on businesses.

upvoted 1 times

🗳️ 👤 **Topsecret** 11 months, 3 weeks ago

**Selected Answer: A**

The correct answer is A. True positives affect security as no alarm is raised when an attack has taken place, while false positives are alerts raised appropriately to detect and further mitigate them.

False positive alerts occur when an alert is generated indicating a threat or security incident, but upon investigation, it is determined to be a benign event or a result of a misconfiguration. On the other hand, true positive alerts are generated when an actual security incident or attack has occurred, and the alert accurately identifies it.

upvoted 2 times

🗳️ 👤 **drdecker100** 1 year, 4 months ago

**Selected Answer: D**

A false positive occurs when an alert or warning is triggered when no threat is present. For example, an antivirus program detecting a harmless file as malicious.

A false negative occurs when an alert or warning is not triggered when a threat is present. For example, a virus infecting a system without being detected by antivirus software.

A true positive occurs when an alert or warning is triggered correctly when a threat is present. For example, an intrusion detection system detecting a hacking attempt.

A true negative occurs when an alert or warning is not triggered correctly when no threat is present. For example, an intrusion detection system not detecting any malicious activity on a network that is in fact safe.

upvoted 4 times

🗳️ 👤 **Eng\_ahmedyoussef** 1 year, 8 months ago

**Selected Answer: D**

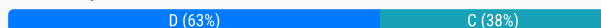
D. False-positive alerts are detected by confusion as potential attacks, while true positives are attack attempts identified appropriately.  
upvoted 3 times

An engineer needs to fetch logs from a proxy server and generate actual events according to the data received. Which technology should the engineer use to accomplish this task?

- A. Firepower
- B. Email Security Appliance
- C. Web Security Appliance
- D. Stealthwatch

**Suggested Answer: D**

Community vote distribution



🗳️ 👤 **Faio** 11 months, 1 week ago

The correct answer is D. Stealthwatch.  
upvoted 2 times

🗳️ 👤 **slippery31** 1 year, 1 month ago

Correct ANS= C  
upvoted 1 times

🗳️ 👤 **Stevens0103** 1 year, 1 month ago

Stealthwatch is a network traffic monitoring and analysis tool that provides visibility into network behavior and detects anomalies and threats. It can collect and analyze data from a variety of sources, including network devices, servers, and applications, and generate alerts and reports based on predefined rules and machine learning algorithms.

In this case, the engineer can configure Stealthwatch to collect logs from the proxy server and analyze the data to identify any suspicious or malicious activity. Stealthwatch can also correlate the logs with other network data to provide a more comprehensive view of the network and detect advanced threats that may be hiding in the noise.

Firepower, Email Security Appliance, and Web Security Appliance are security technologies that can provide additional layers of protection for specific types of traffic, but they are not designed for network monitoring and analysis like Stealthwatch.

upvoted 4 times

🗳️ 👤 **alhamry** 1 year, 2 months ago

The best answer is C. The Web Security Appliance (WSA) is designed to filter web traffic and enforce corporate security policies. It can also generate logs and alerts based on the traffic it filters, allowing for event correlation and analysis. Firepower is a network security platform that provides intrusion prevention, advanced malware protection, and URL filtering. The Email Security Appliance (ESA) is designed to protect against email-based threats, including spam, viruses, and phishing attacks. Stealthwatch is a network traffic analysis platform that provides visibility into network behavior and detects anomalous activity. While all of these technologies can generate logs, the WSA is the best choice for generating events based on proxy server traffic.

upvoted 2 times

🗳️ 👤 **mozaki** 1 year, 3 months ago

**Selected Answer: C**

the answer is C WSA: fetches logs related to web traffic such as URLs, web requests, and responses. It also collects information about user activity, web applications, and malware threats. WSA is designed to monitor and control web traffic, fetch logs related to web traffic, and generate alerts and events based on certain conditions or criteria.

Stealthwatch: fetches logs related to network traffic such as flow data, NetFlow, and other telemetry data. It also collects information about user and device behavior, network connections, and threat intelligence.

upvoted 1 times

🗳️ 👤 **mozaki** 1 year, 3 months ago

**Selected Answer: D**

The answer is

WSA: fetches logs related to web traffic such as URLs, web requests, and responses. It also collects information about user activity, web applications,

and malware threats.

Stealthwatch: fetches logs related to network traffic such as flow data, NetFlow, and other telemetry data. It also collects information about user and device behavior, network connections, and threat intelligence.

WSA is enough

upvoted 1 times

🗨️ 👤 **mozaki** 1 year, 3 months ago

The answer is C WSA

upvoted 1 times

🗨️ 👤 **drdecker100** 1 year, 4 months ago

**Selected Answer: D**

The technology that the engineer should use to accomplish this task is D. Stealthwatch. Stealthwatch is a network traffic analysis (NTA) tool that provides real-time visibility into network traffic and helps to detect and respond to threats. It can also be used to fetch logs from various network devices and generate actual security events according to the data received. Firepower, Email Security Appliance, and Web Security Appliance are different security technologies that provide various security features such as firewall, intrusion prevention, email security, and web security.

upvoted 1 times

🗨️ 👤 **Eng\_ahmedyoussef** 1 year, 8 months ago

**Selected Answer: D**

D. is correct

Stealthwatch collects telemetry from every part of the network and applies advanced security analytics to the data. It creates a baseline of normal web and network activity for a network host, and applies context-aware analysis to automatically detect anomalous behaviors.

upvoted 1 times

🗨️ 👤 **aplicacion101** 1 year, 12 months ago

**Selected Answer: D**

D is correct

upvoted 2 times

🗨️ 👤 **aplicacion101** 2 years ago

Wsa as proxy can export logs to Stealwatch to analysis and correlation.

upvoted 2 times

🗨️ 👤 **JayPEI** 2 years ago

**Selected Answer: C**

should be WSA

upvoted 2 times

```
Mar 07 2020 16:16:48: %ASA-4-106023: Deny tcp src
outside:10.22.219.221/54602 dst outside:10.22.250.212/504
by access-group "outside" [0x0, 0x0]
```

Refer to the exhibit. Which technology generates this log?

- A. NetFlow
- B. IDS
- C. web proxy
- D. firewall

**Suggested Answer: D**


Community vote distribution

D (80%)

B (20%)

 **tsabee** Highly Voted 2 years, 2 months ago

This picture was in the exam, but in another aspect: wich type of evidence is this picture: Best, Corroboration, Circumstance or Indirect.  
upvoted 7 times

 **Nikolas** 1 year, 10 months ago

Indirect

upvoted 1 times

 **Pantela\_26** 1 year, 10 months ago

Should be corroborative, since it's an ACL hit

upvoted 3 times

 **dponce** Most Recent 9 months, 3 weeks ago

correct is D (Firewall)

see logs in my FW ASA

```
Mar 10 2023 23:07:03: %ASA-4-106023: Deny tcp src INSIDE:10.98.55.13/61588 dst InternetGSuite:35.235.210.68/445 by access-group "inside" [0x0, 0x0]
```

```
Mar 10 2023 23:07:03: %ASA-4-106023: Deny tcp src InternetGSuite:106.0.48.146/55356 dst INSIDE:10.98.36.2/3306 by access-group "GSUITE" [0x0, 0x0]
```

```
Mar 10 2023 23:07:04: %ASA-2-106001: Inbound TCP connection denied from 10.100.52.2/3001 to 10.23.4.102/60430 flags SYN ACK on interface INSIDE
```

```
Mar 10 2023 23:07:04: %ASA-3-713061: Group = 200.29.67.26, IP = 200.29.67.26, Rejecting IPSec tunnel: no matching crypto map entry for remote proxy 172.19.1.51/255.255.255.255/0/0 local proxy 172.29.218.5/255.255.255.255/0/0 on interface InternetGSuite
```


upvoted 2 times

 **Eng\_ahmedyoussef** 1 year, 2 months ago

Selected Answer: D

D is correct (Firewall)

upvoted 1 times

 **cy\_analyst** 1 year, 2 months ago

Selected Answer: D

ASA is a firewall

upvoted 2 times

 **RSA001** 1 year, 8 months ago

Selected Answer: D

Should be correct



upvoted 1 times

  **JohnMangley** 1 year, 9 months ago

**Selected Answer: B**



An IDS should generate this log

upvoted 1 times

  **RSA001** 1 year, 8 months ago

Why? Adaptive Security Appliance (ASA) is a firewall product. The given answer should be correct

upvoted 3 times

  **MartinRB** 10 months, 2 weeks ago

IDS wouldnt deny the connection

upvoted 2 times

Which filter allows an engineer to filter traffic in Wireshark to further analyze the PCAP file by only showing the traffic for LAN 10.11.x.x, between workstations and servers without the Internet?

- A. src=10.11.0.0/16 and dst=10.11.0.0/16
- B. ip.src==10.11.0.0/16 and ip.dst==10.11.0.0/16
- C. ip.src=10.11.0.0/16 and ip.dst=10.11.0.0/16
- D. src==10.11.0.0/16 and dst==10.11.0.0/16

**Suggested Answer: B**

Community vote distribution

B (100%)

  **[Removed]**  11 months ago

B is correct. New exam quistion - filtering by port in this case by FTP port (21) in wireshark the correct answer is "tcp.port==21".  
upvoted 6 times

  **Eng\_ahmedyoussef**  8 months, 3 weeks ago

**Selected Answer: B**

B is correct

ip.src==10.11.0.0/16 and ip.dst==10.11.0.0/16

upvoted 2 times



Which tool provides a full packet capture from network traffic?

- A. Nagios
- B. CAINE
- C. Hydra
- D. Wireshark

**Suggested Answer:** D

*Community vote distribution*

D (100%)

🗨️ 👤 **Mack279** 6 months, 3 weeks ago

**Selected Answer: D**

The answer is obviously D.

Quick google on the items below for reference:

Nagios - A network, server and log monitoring software.

CAINE - Computer Aided Investigative Environment is an open-source platform that is used in forensics.

Hydra - used for fast network login hacking. It uses both dictionary and brute-force attacks to attack login pages.

upvoted 1 times

🗨️ 👤 **Eng\_ahmedyoussef** 1 year, 2 months ago

**Selected Answer: D**

D is correct

full packet capture ==> Wireshark

upvoted 2 times

A company is using several network applications that require high availability and responsiveness, such that milliseconds of latency on network traffic is not acceptable. An engineer needs to analyze the network and identify ways to improve traffic movement to minimize delays. Which information must the engineer obtain for this analysis?

- A. total throughput on the interface of the router and NetFlow records
- B. output of routing protocol authentication failures and ports used
- C. running processes on the applications and their total network usage
- D. deep packet captures of each application flow and duration

**Suggested Answer: A**

Community vote distribution



**anonymous1966** Highly Voted 2 years, 9 months ago

"D" is correct

DPI can be made by AVC that can setup QoS to tune traffic.

Cisco AVC uses existing Cisco Network-Based Application Recognition Version 2 (NBAR2) to provide deep packet inspection (DPI) technology to identify a wide variety of applications within the network traffic flow, using Layer 3 to Layer 7 data. NBAR works with quality of services (QoS) features to help ensure that the network bandwidth is best used to fulfill its main primary objectives. The benefits of combining these features include the ability to guarantee bandwidth to critical applications, limit bandwidth to other applications, drop selective packets to avoid congestion, and mark packets appropriately so that the network and the service provider's network can provide QoS from end to end.

Cisco CyberOps Associate CBROPS 200-201 Official Cert Guide

By Omar Santos

upvoted 11 times

**mozaki** 1 year, 3 months ago

The information the engineer needs to obtain for this analysis is A. total throughput on the interface of the router and NetFlow records.

To minimize delays and improve network performance for applications that require high availability and responsiveness, it's important to identify any network bottlenecks or congestion points that may be causing latency. The total throughput on the interface of the router provides an indication of the amount of data being transmitted across the network, while NetFlow records provide detailed information on the network traffic patterns and the source and destination of each packet

upvoted 2 times

**itousattud** 1 year, 3 months ago

ChatGPT

upvoted 1 times

**Faio** Most Recent 8 months, 3 weeks ago

The correct answer is A. total throughput on the interface of the router and NetFlow records.

upvoted 1 times

**SecurityGuy** 10 months, 3 weeks ago

**Selected Answer: A**

Throughput - tells you how much data was transferred from a source at any given time

Bandwidth - tells you how much data could theoretically be transferred from a source at any given time.

<https://www.dnsstuff.com/network-throughput-bandwidth>

We're talking about "high availability and responsiveness" which is inclined on the networking side.

From a Network Engineer's perspective, you'll "need to check first" how much throughput you have to determine if an interface have enough bandwidth to handle the throughput?

upvoted 1 times

**Topsecret** 11 months, 3 weeks ago

**Selected Answer: A**

The correct answer is A. total throughput on the interface of the router and NetFlow records.

To analyze the network and identify ways to improve traffic movement to minimize delays, the engineer must obtain information related to the total throughput on the interface of the router and NetFlow records.

upvoted 1 times

🗨️ **slippery31** 1 year, 1 month ago

Correct ANS = C

upvoted 1 times

🗨️ **drdecker100** 1 year, 4 months ago

**Selected Answer: A**

i think "A".

The engineer needs to obtain the total throughput on the interface of the router and NetFlow records to analyze the network and identify ways to improve traffic movement to minimize delays. This information will allow the engineer to identify the current network traffic patterns and use this information to optimize network traffic movement, ensuring high availability and responsiveness of the network applications.

upvoted 2 times

🗨️ **MaliDong** 1 year, 8 months ago

**Selected Answer: D**

Answer C does not help investigating into "latency". D is correct.

upvoted 1 times

🗨️ **Eng\_ahmedyoussef** 1 year, 8 months ago

**Selected Answer: C**

C is the correct answer ==> running processes on the applications and their total network usage

upvoted 3 times

🗨️ **ivlis\_27** 2 years, 7 months ago

i think c, because latency is affected by running processes

upvoted 1 times

🗨️ **halamah** 2 years, 7 months ago

a is correct

upvoted 3 times

🗨️ **mage81** 2 years, 7 months ago

are u sure?

upvoted 2 times

🗨️ **[Removed]** 2 years, 9 months ago

I think that correct answer is:

A. total throughput on the interface of the router and NetFlow records

upvoted 3 times

🗨️ **JohnBB** 3 years ago

The correct answer is C: running processes on the applications and their total network usage

D is not correct. Deep packet inspection slowdown your network.

upvoted 2 times

🗨️ **beowolf** 3 years, 1 month ago

Deep packet inspection offers immediate insight into network slowdowns

Resolve end-user slowdowns

Narrow down the issue to determine whether slowness is caused by the network or an application.

Analyze applications

Calculate response times for all relevant applications and determine the impact on user experience.

Classify network traffic

Classify and restrict network traffic as needed and identify associated risk levels.

upvoted 4 times

  **Barney\_Stinson** 3 years, 1 month ago

I think the important part of this question is:

"identify ways to improve traffic movement to minimize delays"

Why is deep packet inspection needed to improve traffic movement?

Shouldn't be the answer something like "packet flow information for every application"?

upvoted 2 times

```
root@:~# cat access-logs/access_130603.txt | grep '192.168.1.91' | cut -d "\"" -f 2 |
uniq -c
  1 GET /portal.php?mode=addevent&date=2018-05-01 HTTP/1.1
  1 GET /blog/?attachment_id=2910 HTTP/1.1
  1 GET /blog/?attachment_id=2998&feed=rss2 HTTP/1.1
  1 GET /blog/?attachment_id=3156 HTTP/1.1
```

Refer to the exhibit. What is depicted in the exhibit?

- A. Windows Event logs
- B. Apache logs
- C. IIS logs
- D. UNIX-based syslog

**Suggested Answer: B**

*Community vote distribution*

B (100%)

🗳️ 👤 **RoBery** 11 months, 3 weeks ago

(root) means unix based logs as Apache, however it is not syslog.  
upvoted 2 times

🗳️ 👤 **SecurityGuy** 1 year, 4 months ago

**Selected Answer: B**

[https://www.w3schools.com/tags/ref\\_httpmethods.asp](https://www.w3schools.com/tags/ref_httpmethods.asp)

"GET" is an HTTP Method which more inclined to web technologies such as Apache or IIS.

HTTP Methods:

- GET
- POST
- PUT
- HEAD
- DELETE
- PATCH
- OPTIONS
- CONNECT
- TRACE

IIS Logs Format:

[https://learn.microsoft.com/en-us/previous-versions/iis/6.0-sdk/ms525807\(v=vs.90\)](https://learn.microsoft.com/en-us/previous-versions/iis/6.0-sdk/ms525807(v=vs.90))

upvoted 3 times

🗳️ 👤 **Eng\_ahmedyoussef** 2 years, 2 months ago

**Selected Answer: B**

B is correct answer  
upvoted 1 times



🗳️ 👤 **Tobds234** 2 years, 8 months ago

**Selected Answer: B**

B is correct  
upvoted 2 times

🗳️ 👤 **omita** 3 years ago

Is correct answer is not "D"? Any idea please share..  
upvoted 1 times

  **Bubu3k** 2 years, 7 months ago

syslog has a different format

upvoted 1 times

Which technology should be used to implement a solution that makes routing decisions based on HTTP header, uniform resource identifier, and SSL session ID attributes?

- A. AWS
- B. IIS
- C. Load balancer
- D. Proxy server

**Suggested Answer: C**

Community vote distribution

C (100%)

  **beowolf**  3 years, 8 months ago

Load Balancing: HTTP(S) load balancing is one of the oldest forms of load balancing. This form of load balancing relies on layer 7, which means it operates in the application layer. This allows routing decisions based on attributes like HTTP header, uniform resource identifier, SSL session ID, and HTML form data.

upvoted 21 times

  **drdecker100**  1 year, 10 months ago

**Selected Answer: C**

A proxy server can be used for routing and forwarding requests, but it may not be designed to handle the high traffic load and make efficient routing decisions based on HTTP header, URI, and SSL session ID attributes. Therefore, a load balancer is the best choice for this scenario.


upvoted 5 times

  **rukmi**  8 months, 1 week ago

D. Proxy server

A proxy server can be configured to intercept and inspect HTTP headers, uniform resource identifiers (URIs), and SSL session IDs to make routing decisions. By analyzing these attributes, the proxy server can determine the appropriate destination for incoming requests, such as forwarding them to different backend servers based on predefined rules or policies. This allows for flexible and granular control over traffic routing, making it an appropriate technology for implementing solutions that require routing decisions based on specific attributes of HTTP requests

upvoted 1 times

  **Faio** 1 year, 4 months ago


A load balancer

upvoted 1 times

  **slippery31** 1 year, 7 months ago

Correct ANS= C

upvoted 1 times

  **JOSH20** 1 year, 10 months ago

c is correct



upvoted 2 times

  **Eng\_ahmedyoussef** 2 years, 2 months ago

**Selected Answer: C**

Load Balancer is correct answer

upvoted 2 times

  **Nhendy** 2 years, 5 months ago

**Selected Answer: C**

agree with C

upvoted 1 times

  **[Removed]** 2 years, 9 months ago

load balancing is more for redundancy i believe, and proxy is what gets you out to your destination using HTTP, URI and SSL i think proxy

upvoted 1 times

🗨️ 👤 **DLukynskyy** 2 years, 9 months ago

**Selected Answer: C**

Proxy does not route.

upvoted 3 times

🗨️ 👤 **sandiagodecuba** 2 years, 9 months ago

**Selected Answer: C**

Load Balancing

upvoted 1 times

🗨️ 👤 **saakovv** 2 years, 11 months ago

- C!

Load balancing applies to layers 4-7 in the seven-layer Open System Interconnection (OSI) model. Its capabilities are:

L4. Directing traffic based on network data and transport layer protocols, e.g., IP address and TCP port.

L7. Adds content switching to load balancing, allowing routing decisions depending on characteristics such as HTTP header, uniform resource identifier, SSL session ID, and HTML form data.

GSLB. Global Server Load Balancing expands L4 and L7 capabilities to servers in different sites

upvoted 1 times

🗨️ 👤 **halamah** 3 years, 1 month ago

c is correct

upvoted 2 times

🗨️ 👤 **HarryPotter69** 3 years, 3 months ago

I read this as being part of "Setting up custom HTTP header-based routing"

I would answer C - load balancer

upvoted 2 times

🗨️ 👤 **anonymous1966** 3 years, 3 months ago

"C" is correct.

Layer 7 load balancer, like AWS ELB.

The keyword is "routing"

upvoted 3 times

🗨️ 👤 **JohnBB** 3 years, 6 months ago

Accroding to some other dumps the answer is B. IIS. Makes sense.

upvoted 1 times

🗨️ 👤 **Vetterous** 3 years, 5 months ago

IIS isn't going to handle the routing part of the question. I agree with the answer of Load Balancing.

upvoted 1 times



Which regular expression matches "color" and "colour"?

- A. colo?ur
- B. col[08'^λ]+our
- C. colou?r
- D. col[09'^λ]+our

**Suggested Answer:** C

Community vote distribution

C (100%)

🗳️ **anonymous1966** Highly Voted 3 years, 9 months ago  
"C" is correct

For me there are some codification error in the page that greek chars are shown.

The correct question is:

Which regular expression matches "color" and "colour"?

- A . colo?ur
  - B . col[08]+our
  - C . colou?r
  - D . col[09]+our
- upvoted 9 times

🗳️ **2a814b3** Most Recent 8 months, 2 weeks ago  
The answer is C. If you plot the characters in regex101.com it is expressed correctly on the right under explanation.  
upvoted 1 times

🗳️ **Faio** 1 year, 10 months ago  
The answer is C. colou?r.  
upvoted 1 times

🗳️ **Topsecret** 1 year, 11 months ago  
The correct answer is A. colo?ur.

The regular expression "colo?ur" matches both "color" and "colour." Here's the breakdown of the regular expression:

"col" matches the characters "col" literally.

"o?" makes the "o" character optional. It matches zero or one occurrence of the preceding character, which in this case is "o."

"ur" matches the characters "ur" literally.

upvoted 1 times

🗳️ **Eng\_ahmedyoussef** 2 years, 8 months ago  
Selected Answer: C  
C. colou?r  
upvoted 2 times

🗳️ **bn1234** 3 years, 3 months ago  
Selected Answer: C  
C is correct, try for yourself at regex101.com  
upvoted 1 times

Which artifact is used to uniquely identify a detected file?

- A. file timestamp
- B. file extension
- C. file size
- D. file hash

**Suggested Answer:** D

*Community vote distribution*

D (100%)

🗨️ **SecurityGuy** 10 months, 3 weeks ago

**Selected Answer: D**

A file hash is a unique signature for data that helps to identify it in a verifiable way.

<https://codesigningstore.com/what-is-a-file-hash-definition>

upvoted 2 times

🗨️ **Eng\_ahmedyoussef** 1 year, 8 months ago

**Selected Answer: D**

D. is correct

File Hash ==> used to uniquely identify a detected file.

upvoted 1 times

🗨️ **EnjoiTech** 2 years, 2 months ago

Correct answer is D

upvoted 1 times

A security engineer deploys an enterprise-wide host/endpoint technology for all of the company's corporate PCs. Management requests the engineer to block a selected set of applications on all PCs. Which technology should be used to accomplish this task?

- A. application whitelisting/blacklisting
- B. network NGFW
- C. host-based IDS
- D. antivirus/antispyware software

**Suggested Answer: A**

*Community vote distribution*

A (100%)

🗲️ 👤 **SecurityGuy** 10 months, 3 weeks ago

**Selected Answer: A**

Key Phrase: "block a selected set of applications on all PCs."

upvoted 1 times

🗲️ 👤 **Eng\_ahmedyoussef** 1 year, 8 months ago

**Selected Answer: A**

Application Blacklisting ==> block a selected set of applications on all PCs

upvoted 3 times

🗲️ 👤 **EnjoiTech** 2 years, 2 months ago

Correct answer A

upvoted 1 times

Which utility blocks a host portscan?

- A. HIDS
- B. sandboxing
- C. host-based firewall
- D. antimalware

**Suggested Answer:** C

Community vote distribution

C (100%)

  **beowolf**  3 years, 3 months ago

Look at the wording "Blocks" HIDS doesn't block anything. Answer is correct  
upvoted 14 times

  **SecurityGuy**  10 months, 3 weeks ago



**Selected Answer: C**

HIDS (Host-based Intrusion Detection System) - Doesn't block threats.  
Sanboxing - Technology used to isolate an application from other applications.  
Antimalware - Blocks malware.  
Firewall - Blocks and unblocks traffic. e.g. from / to specific IP or Por.  
upvoted 1 times

  **Eng\_ahmedyoussef** 1 year, 8 months ago

**Selected Answer: C**

C. is correct Answer  
Host based Firewall ==> blocks a host port scan.  
upvoted 1 times

  **JoeDinsmore** 3 years, 3 months ago

HIDS (unlike HIPS) does not take any further actions (other than reporting) when detecting an Emerging Threats on local system.  
That's why I think Host-based Firewall is the right answer.  
upvoted 4 times

  **toucansam** 3 years, 5 months ago

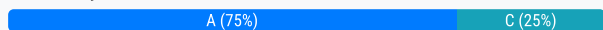
I think this could be the host based firewall or a HIDS that drops it, and not only detects.  
upvoted 2 times

Which evasion technique is indicated when an intrusion detection system begins receiving an abnormally high volume of scanning from numerous sources?

- A. resource exhaustion
- B. tunneling
- C. traffic fragmentation
- D. timing attack

**Suggested Answer: A**

Community vote distribution



🗲️ 👤 **anonymous1966** Highly Voted 2 years, 9 months ago

"A" is correct

Resource exhaustion is a type of denial-of-service attack; however, it can also be used to evade detection by security defenses. A simple definition of resource exhaustion is "consuming the resources necessary to perform an action."

Cisco CyberOps Associate CBROPS 200-201 Official Cert Guide

By Omar Santos

upvoted 7 times

🗲️ 👤 **sheyshey** Most Recent 7 months ago

Selected Answer: A

Can also be called ddos.. A for me

upvoted 2 times

🗲️ 👤 **SecurityGuy** 10 months, 3 weeks ago

Selected Answer: A

Key Phrase: "receiving an abnormally high volume of scanning from numerous sources"

I'd agree with A. Resource Exhaustion

upvoted 1 times

🗲️ 👤 **Topsecret** 11 months, 3 weeks ago

Selected Answer: C

The correct answer is C. traffic fragmentation.

When an intrusion detection system (IDS) starts receiving an abnormally high volume of scanning from numerous sources, the indicated evasion technique is traffic fragmentation.

Option A, resource exhaustion, refers to attacks that aim to deplete system resources such as CPU, memory, or network bandwidth. It is not directly related to the scenario described.

upvoted 1 times

🗲️ 👤 **Eng\_ahmedyoussef** 1 year, 8 months ago

Selected Answer: A

A. is correct

Resource exhaustion is a type of denial-of-service attack;

upvoted 2 times

DRAG DROP -

Drag and drop the technology on the left onto the data type the technology provides on the right.

Select and Place:

tcpdump	session data
web content filtering	full packet capture
traditional stateful firewall	transaction data
NetFlow	connection event

Suggested Answer:	tcpdump	web content filtering
	web content filtering	tcpdump
	traditional stateful firewall	NetFlow
	NetFlow	traditional stateful firewall

 **VegasBF** Highly Voted 2 years, 11 months ago

Netflow=Session data for sure!

My answer Netflow-->TCPdump-->Web content filter-->Stateful F/W

upvoted 38 times

 **anonymous1966** 2 years, 9 months ago

Agreed

upvoted 5 times

 **Nerdx1** Most Recent 8 months ago

tcpdump -- full packet capture

web content filtering -- transaction data

stateful firewall - connection event

Netflow -- session data

upvoted 2 times

 **Faio** 8 months, 3 weeks ago

Netflow

tcpdump

web content filtering

stateful firewall

upvoted 3 times

 **drdecker100** 1 year, 4 months ago

tcpdump: full packet capture - tcpdump is a tool for capturing and analyzing packets, allowing for detailed analysis of network traffic.

web content filtering: transaction data - web content filtering is a technology that inspects and filters web traffic, looking for specific types of content or behavior.

traditional stateful firewall: connection event - a stateful firewall monitors connections between devices and tracks their state, allowing it to make informed decisions about whether to allow or block traffic.

Netflow: session data - Netflow is a protocol used to collect and analyze network traffic data, providing information about the volume and flow of traffic in a given network.

upvoted 3 times

 **manu427** 1 year, 5 months ago

It is easier to store large amounts of NetFlow data because it is only a transactional record.

upvoted 1 times

🗨️ 👤 **Eng\_ahmedyoussef** 1 year, 9 months ago

Netflow

tcpdump

web content filtering

stateful firewall

upvoted 2 times

🗨️ 👤 **akustic** 2 years, 7 months ago

Wrong answer. Corect is as VegasBF writes. But in Question #158 they put correct answer :)

upvoted 2 times

🗨️ 👤 **affulinuha** 2 years, 10 months ago

it should NTWS and it would like this for sure!

upvoted 1 times

🗨️ 👤 **MiKeDee** 2 years, 11 months ago

I agree with VegasBF

upvoted 1 times

🗨️ 👤 **xoe123** 3 years ago

It is easier to store large amounts of

NetFlow data because it is only a transactional record.

upvoted 2 times

🗨️ 👤 **Barney\_Stinson** 3 years, 1 month ago

Netflow is session data, not transaction data..

upvoted 4 times

🗨️ 👤 **CiscoTerminator** 2 years, 9 months ago

@Barney\_Stinson its the other way around. Netflow is Transaction data : <https://insights.sei.cmu.edu/blog/why-netflow-data-still-matters/>

upvoted 4 times

🗨️ 👤 **RSA001** 2 years, 3 months ago

Session data refers to communication establishing between two end hosts, whereas transaction data refers to what is inside of the session ongoing (requests, responses, file downloading etc)

upvoted 1 times

No.	Time	Source	Destination	Protocol	Length	Info
18	0.011918	10.0.2.15	192.124.249.9	TCP	78	50588→443 [SYN] Seq=1
19	0.022656	192.124.249.9	10.0.2.15	TCP	62	443→50588 [SYN, ACK]
20	0.022702	10.0.2.15	192.124.249.9	TCP	56	50588→443 [ACK] Seq=1
21	0.022988	192.124.249.9	10.0.2.15	TCP	62	443→50586 [SYN, ACK]
22	0.022996	10.0.2.15	192.124.249.9	TCP	56	50586→443 [ACK] Seq=1
23	0.023212	10.0.2.15	192.124.249.9	TCP	261	50588→443 [PSH, ACK]
24	0.023373	10.0.2.15	192.124.249.9	TCP	261	50586→443 [PSH, ACK]
25	0.023445	192.124.249.9	10.0.2.15	TCP	62	443→50588 [ACK] Seq=1
26	0.023617	192.124.249.9	10.0.2.15	TCP	62	443→50586 [ACK] Seq=1
27	0.037413	192.124.249.9	10.0.2.15	TCP	2792	443→50586 [PSH, ACK]
28	0.037426	10.0.2.15	192.124.249.9	TCP	56	50586→443 [ACK] Seq=2

> Frame 24: 261 bytes on wire (2088 bits), 261 bytes captured (2088 bits)

> Linux cooked capture

> Internet Protocol Version 4, Src: 10.0.2.15 (10.0.2.15), Dst: 192.124.249.9 (192.124.249.9)

> Transmission Control Protocol, Src Port: 50586 (50586), Dst Port: 443 (443), Seq: 1, A

> Data [205 bytes]

Data: 16030100c8010000c403030e06ead078d17676c13ab46ebf...

[Length: 205]

0000	00 04 00 01 00 06 08 00	27 7a 3c 93 00 00 08 00	..... *z<.....
0010	45 00 00 f5 48 7b 40 00	40 06 2b f3 0a 00 02 0f	E...H{@. @.+.....
0020	c0 7c f9 09 c5 9a 01 bb	0e 1f dc b4 00 b4 aa 02	. . ....
0030	50 18 72 10 c6 7c 00 00	16 03 01 00 c8 01 00 00	P.r.. . ....
0040	c4 03 03 0e 06 ea d0 78	d1 76 76 c1 3a b4 6e bf	.....x.vv.:.n..
0050	e6 b8 b8 b2 ba 08 d6 6d	0d 38 fb 91 45 de fc ee	.....m .8.E...
0060	8b 6e f8 00 00 1e c0 2b	c0 2f cc a9 cc a8 c0 2c	.n.....+ ./.....
0070	c0 30 c0 0a c0 09 c0 13	c0 14 00 33 00 39 00 2f	.0..... ..3.9./
0080	00 35 00 0a 01 00 00 7d	00 00 00 16 00 14 00 00	.5.....} .....
0090	11 77 77 77 2e 6c 69 6e	75 78 6d 69 6e 74 2e 63	.wwwlin uxmint.c
00a0	6f 6d 00 17 00 00 ff 01	00 01 00 00 0a 00 08 00	om.....
00b0	06 00 17 00 18 00 19 00	0b 00 02 01 00 00 23 00	.....#.
00c0	00 33 74 00 00 00 10 00	17 00 15 02 68 32 08 73	.3t..... ..h2.s
00d0	70 64 79 2f 33 2e 31 08	68 74 74 70 2f 31 2e 31	pdY/3.1. http/1.1
00e0	00 05 00 05 01 00 00 00	00 00 0d 00 18 00 16 04	.....
00f0	01 05 01 06 01 02 01 04	03 05 03 06 03 02 03 05	.....
0100	02 04 02 02 02		.....

Refer to the exhibit. Which application protocol is in this PCAP file?

- A. SSH
- B. TCP
- C. TLS
- D. HTTP

**Suggested Answer: C**

Community vote distribution

C (67%)

D (33%)

**skysoft** Highly Voted 4 years ago

Correct answer should be "D".

TCP is not a application layer protocol. Http is and the used port is 443 (https).

upvoted 27 times

**tsabee** 3 years, 2 months ago

It's a very tricky or wrong question

Partially agree with you, but the correct answer actually should be "B", because the wireshark identify and recognise automatically the TLS as a protocol (Make sure in the next #112 question - TLSv1.2) and also HTTP.

On the one hand in this captured packet there isn't TLS header/layer. Although the port is TCP443, but it doesn't mean that is a HTTPS traffic! It's only a traffic that use TCP443: for extreme idiot example this traffic would be a telnet traffic with modified port number.

On the other hand the HTTP also wrong answer: firstly the wireshark recognise the HTTP also, secondly in this case the bulk data/body is showed in the captured packet as "Hypertext Transfer Protocol" not as simple "Data [205 byte]"

I know there is a "www" data in the body, but it isn't mean that is a real HTTP packet. And I know the TCP isn't an application protocol, so may be the question also wrong.

But I think the key here is the port/TCP not an upper layer protocol.



upvoted 3 times

🗨️ **maxson69** 3 years ago

Http is port 80 but TLS is 443

upvoted 3 times

🗨️ **maxson69** 3 years ago

So it's TLS over HTTP

upvoted 1 times

🗨️ **maxson69** 3 years ago

Answer should be C

upvoted 3 times

🗨️ **bren\_** 3 years, 12 months ago

or maybe the error is within the question. It should be: "Which protocol.."

In that case, TCP is the correct answer

upvoted 1 times

🗨️ **anonymous1966** **Highly Voted** 🍌 2 years, 5 months ago

**Selected Answer: C**

A. SSH - port 22

B. TCP - not application protocol (it is a transport protocol)

\*C. TLS - port 443

D. HTTP - port 80

The aim of the question is to evaluate if you know the TCP ports and ISO/OSI layers.

upvoted 6 times

🗨️ **SecurityGuy** 1 year, 4 months ago

I'd agree with this.

upvoted 1 times

🗨️ **stickerbombmaster** 9 months, 1 week ago

But TLS is not application protocol neither mate, question is just dumb

upvoted 1 times

🗨️ **RoBery** **Most Recent** 🕒 11 months, 3 weeks ago

D- HTTP is the correct answer.

When using HTTP over TLS (HTTPS) on port 443, the application protocol is still HTTP. However, it is secured using Transport Layer Security (TLS) to encrypt the communication between the client and the server. The combination of HTTP and TLS results in HTTPS, which is the secure version of HTTP. The application layer protocol remains HTTP, but it operates over a secure TLS-encrypted connection, providing confidentiality and integrity for the data exchanged between the client and server.

upvoted 1 times

🗨️ **Stevens0103** 1 year, 7 months ago

**Selected Answer: D**

The destination port number 443 indicates that the application protocol in this PCAP file is HTTPS (HTTP over TLS/SSL). Port 443 is the well-known port for secure HTTP communication, commonly known as HTTPS. In the PCAP file, you can see the TCP SYN and SYN-ACK packets exchanged between the source and destination, followed by TLS handshake packets (PSH, ACK) indicating the establishment of a secure connection. The data in the PCAP file shows the encrypted TLS/SSL payload. Therefore, the application protocol in this PCAP file is HTTPS.

upvoted 1 times

🗨️ **alhamry** 1 year, 8 months ago

Answer C: The captured frame contains TLS (Transport Layer Security) protocol.

The frame in the PCAP capture shows that the packet is using Transmission Control Protocol (TCP) as the transport layer protocol. However, the data payload in the packet is encrypted and cannot be determined without further analysis.

The presence of port 443 as the destination port in the TCP header suggests that this is a secure web session using HTTPS. HTTPS uses Transport Layer Security (TLS) to provide encryption for the communication. Therefore, the correct answer is C - TLS.

HTTP is not the correct answer because HTTP does not provide encryption for the communication. It is possible that the encrypted data in the packet is related to HTTP traffic, but this cannot be determined from the given information.

SSH is not the correct answer because SSH uses a different port number (usually port 22) and a different protocol for secure shell access.

upvoted 1 times

🗳️ 👤 **alhamry** 1 year, 8 months ago

TLS (Transport Layer Security) is a protocol that is usually implemented at the transport layer of the OSI model. While it is not strictly an application-layer protocol like HTTP or SMTP, it is often used to secure application-layer protocols such as HTTP, SMTP, and FTP. So, depending on the context in which the term "application protocol" is used, TLS may be considered an application protocol or a lower-level protocol. In the context of the given question, where the options were SSH, TCP, TLS, and HTTP, TLS is the most appropriate answer.

upvoted 1 times

🗳️ 👤 **Brickit** 1 year, 10 months ago

Correct answer is TLS (not V1.3).

With TLS, the first part of the URL (<https://www.example.com/>) is still visible as it builds the connection.

upvoted 1 times

🗳️ 👤 **Eng\_ahmedyoussef** 2 years, 2 months ago

**Selected Answer: C**

I Think it is TLS

upvoted 2 times

🗳️ 👤 **Entivo** 2 years, 4 months ago

Whoever wrote this question has confused everyone by asking which "application layer" protocol is in use, and there is only one application layer protocol in this list (HTTP). The actual protocol being displayed by Wireshark is SSL/TLS but that is a presentation layer protocol. So the question is a mess and needs clearing up.

upvoted 4 times

🗳️ 👤 **Heil\_Hitler** 2 years, 5 months ago

**Selected Answer: D**

The answer is D. Because if you look carefully, you will see that the coded part below has the text "http/1.1."

upvoted 2 times

🗳️ 👤 **aplicacion101** 2 years, 5 months ago

Correct answer should be D-> HTTP. Show the capture in the PCAP indicate : "www.linuxnint.....http1/1...". Besides that is inside Data ( 205 bytes) .

Image why is the complete capture showing all secrets?

upvoted 1 times

🗳️ 👤 **surforlife** 2 years, 5 months ago

A TLS session operates over a TCP connection. TLS is responsible for the encryption and the authentication of the SDUs exchanged by the application layer protocol while TCP provides the reliable delivery of this encrypted and authenticated bytestream. TLS is used by many different application layer protocols. The most frequent ones are HTTP (HTTP over TLS is called HTTPS 443).

TCP is layer 4 protocol not layer 7.

upvoted 1 times

🗳️ 👤 **omita** 2 years, 11 months ago

TLS is an Application Protocol, So answer is TLS

upvoted 2 times

🗳️ 👤 **omita** 2 years, 11 months ago

Wikipedia: TLS belongs to the Application layer in terms of the TCP/IP model.

upvoted 2 times

🗳️ 👤 **anonymous1966** 3 years, 3 months ago

The correct is TLS over HTTP

I believe "C" is correct.

upvoted 6 times

🗳️ 👤 **HarryPotter69** 3 years, 3 months ago

SSH = port 22 (standard port number)

TCP = a transport protocol (They ask for a application protocol) so this one is ruled out.



TLS = depending what its used for can be other ports, but in this case i assume they talk about port 443

HTTP = 80 (standard port number)

Now in the packet capture frame 24 the Dst Port shows 443.

I believe TLS is the correct answer here.

upvoted 5 times

  **Worlak** 3 years, 4 months ago

Vote for C because the next question 112 states that TLS is an application level protocol

upvoted 4 times

  **DPRamone** 3 years, 4 months ago

This is an ambiguous question since the answer depends on which model you're referencing. Under the OSI model, TLS is a presentation layer protocol, under the TCP/IP model it's an applicatiion protocol. So under the former, the correct answer is HTTP, while under the latter it can be both HTTP and TLS . But since Question 112 explicitly mentions "application protocol", the safe bet here is probably to go with TLS.

upvoted 2 times

  **VegasBF** 3 years, 5 months ago

TCP is an APPLICATION protocol, LMAO.

Refer to the destination port and the encrypted content. The APPLICATION protocol is TLS for sure.

upvoted 4 times

DRAG DROP -

No.	Time	Source	Destination	Protocol	Length	Info
17	0.011641	10.0.2.15	192.124.249.9	TCP	76	50586-443 [SYN] Seq=0 Win=
18	0.011918	10.0.2.15	192.124.249.9	TCP	76	50588-443 [SYN] Seq=0 Win=
19	0.022656	192.124.249.9	10.0.2.15	TCP	62	443-50588 [SYN, ACK] Seq=0
20	0.022702	10.0.2.15	192.124.249.9	TCP	56	50588-443 [ACK] Seq=1 Ack=
21	0.022988	192.124.249.9	10.0.2.15	TCP	62	443-50586 [SYN, ACK] Seq=0
22	0.022996	10.0.2.15	192.124.249.9	TCP	56	50586-443 [ACK] Seq=1 Ack=
23	0.023212	10.0.2.15	192.124.249.9	TLSv1.2	261	Client Hello
24	0.023373	10.0.2.15	192.124.249.9	TLSv1.2	261	Client Hello
25	0.023445	192.124.249.9	10.0.2.15	TCP	62	443-50588 [ACK] Seq=1 Ack=
26	0.023617	192.124.249.9	10.0.2.15	TCP	62	443-50586 [ACK] Seq=1 Ack=
27	0.037413	192.124.249.9	10.0.2.15	TLSv1.2	2792	Server Hello
28	0.037426	10.0.2.15	192.124.249.9	TCP	56	50586-443 [ACK] Seq=206 Ac

> Frame 23: 261 bytes on wire (2088 bits), 261 bytes captured (2088 bits)  
 > Linux cooked capture  
 > Internet Protocol Version 4, Src: 10.0.2.15 (10.0.2.15), Dst: 192.124.249.9 (192.124.249.9)  
 > Transmission Control Protocol, Src Port: 50588 (50588), Dst Port: 443 (443), Seq: 1, Ack:1,  
 > Secure Sockets Layer

```

0000  00 04 00 01 00 06 08 00 27 7a 3c 93 00 00 08 00 ..... *z<....
0010  45 00 00 f5 eb 3e 40 00 40 06 89 2f 0a 00 02 0f E....>@. @../...
0020  c0 7c f9 09 c5 9c 01 bb 4d db 7f f7 00 b3 b0 02 .|..... M.....
0030  50 18 72 10 c6 7c 00 00 16 03 01 00 c8 01 00 00 P.r..|.. ....
0040  c4 03 03 d1 08 45 78 b7 2c 90 04 ee 51 16 f1 82 ....Ex. ,...0...
0050  16 43 ec d4 89 60 34 4a 7b 80 a6 d1 72 d5 11 87 .C...`4J {...r...
0060  10 57 cc 00 00 1e c0 2b c0 2f cc a9 cc a8 c0 2c .W.....+ ./.....
0070  c0 30 c0 0a c0 09 c0 13 c0 14 00 33 00 39 00 2f .0..... ..3.9./
0080  00 35 00 0a 01 00 00 7d 00 00 00 16 00 14 00 00 .5.....} .....
0090  11 77 77 77 2e 6c 69 6e 75 78 6d 69 6e 74 2e 63 .www.lin uxmint.c
00a0  6f 6d 00 17 00 00 ff 01 00 01 00 00 0a 00 08 00 om..... ....
00b0  06 00 17 00 18 00 19 00 0b 00 02 01 00 00 23 00 ..... ..#.....
00c0  00 33 74 00 00 00 10 00 17 00 15 02 68 32 08 73 .3t..... ..h2.s
00d0  70 64 79 2f 33 2e 31 08 68 74 74 70 2f 31 2e 31 pdy/3.1. http/1.1
00e0  00 05 00 05 01 00 00 00 00 00 0d 00 18 00 16 04 ..... ....
00f0  01 05 01 06 01 02 01 04 03 05 03 06 03 02 03 05 ..... ....
0100  02 04 02 02 02 .....

```

Refer to the exhibit. Drag and drop the element name from the left onto the appropriate piece of the PCAP file on the right.

Select and Place:

source address	10.0.2.15
destination address	50588
source port	443
destination port	192.124.249.9
Network Protocol	Transmission Control Protocol
Transport Protocol	Internet Protocol v4
Application Protocol	Transport Layer Security v1.2

Suggested Answer:

source address	source address
destination address	source port
source port	destination port
destination port	destination address
Network Protocol	Transport Protocol
Transport Protocol	Network Protocol
Application Protocol	Application Protocol




  **qz999**  1 year, 10 months ago

Solution is just showing the same thing in both columns. My answer:

sip .15; dip .9; sppt 50588; dprt 443; net proto ipv4; transport proto tcp; and app tls.

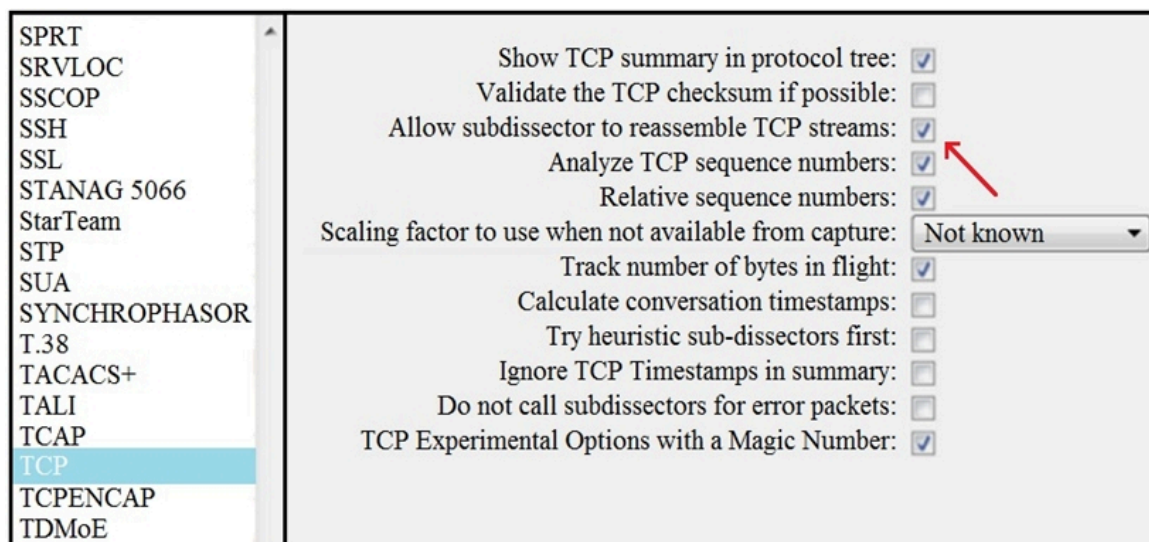
Though TLS is actually a session layer protocol that provides services to the presentation and transport layers in OSI. Since TCP/IP model combines top three OSI layers, one could interpret TLS as an application protocol within that context.

upvoted 8 times

  **Eng\_ahmedyoussef**  8 months, 3 weeks ago

the answer is correct

upvoted 1 times

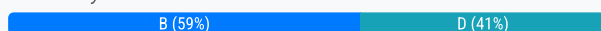


Refer to the exhibit. What is the expected result when the "Allow subdissector to reassemble TCP streams" feature is enabled?

- A. insert TCP subdissectors
- B. extract a file from a packet capture
- C. disable TCP streams
- D. unfragment TCP

**Suggested Answer: B**

Community vote distribution



**Fringe** Highly Voted 2 years, 11 months ago

**Selected Answer: B**

B is correct

upvoted 10 times

**Cnoteone** Highly Voted 2 years, 6 months ago

Answer must be D?

The TCP protocol preference "Allow subdissector to reassemble TCP streams" (enabled by default) makes it possible for Wireshark to collect a contiguous sequence of TCP segments and hand them over to the higher-level protocol (for example, to reconstruct a full HTTP message).

7.8. Packet Reassembly - Wireshark <https://www.wireshark.org> ›

upvoted 9 times

**Scipions** Most Recent 9 months, 1 week ago

**Selected Answer: B**

B is correct

upvoted 1 times

**Faio** 1 year, 4 months ago

The answer is D. unfragment TCP.

The Option B, "extract a file from a packet capture", would allow you to save a file from a packet capture. This would not affect the TCP streams in the capture file

upvoted 5 times

**mduck2** 1 year, 5 months ago

Its B. Protocols such as HTTP or TLS are likely to span multiple TCP segments. The TCP protocol preference "Allow subdissector to reassemble TCP streams" (enabled by default) makes it possible for Wireshark to collect a contiguous sequence of TCP segments and hand them over to the higher-

level protocol (for example, to reconstruct a full HTTP message). All but the final segment will be marked with "[TCP segment of a reassembled PDU]" in the packet list

upvoted 1 times

🗨️ 👤 **alhamry** 1 year, 8 months ago

The expected result when the "Allow subdissector to reassemble TCP streams" feature is enabled is that it allows TCP subdissectors to reassemble TCP streams. Therefore, the correct answer is A.

The "Allow subdissector to reassemble TCP streams" feature in packet capture software enables TCP subdissectors to reassemble TCP streams, which allows the user to see the entire conversation between two endpoints. This feature does not relate to file extraction or unfragmenting TCP, so options B and D are incorrect.

upvoted 3 times

🗨️ 👤 **Brickit** 1 year, 10 months ago

The detail is in the question 'what is the expected result' = D

Yes you can extract a file that is unfragmented, but this is an example of what could be done..

upvoted 1 times

🗨️ 👤 **Eng\_ahmedyoussef** 2 years, 2 months ago

**Selected Answer: D**

i agreed with answer D. but not sure

unfragmented TCP ==> Allow subdissector to reassemble TCP streams.

upvoted 3 times

🗨️ 👤 **[Removed]** 2 years, 3 months ago

**Selected Answer: D**

D agreed

upvoted 4 times

🗨️ 👤 **surforlife** 2 years, 5 months ago

During a TCP transmission of datagrams between two devices, each packet is tagged with a sequence number by the sender. This sequence number is used to reassemble the packets back into data. During the transmission of packets, each packet may take a different path to the destination. So best answer is D, deals with reassembling!

upvoted 4 times

Which type of data collection requires the largest amount of storage space?

- A. alert data
- B. transaction data
- C. session data
- D. full packet capture

**Suggested Answer:** D

*Community vote distribution*

D (100%)

🗳️ 👤 **Eng\_ahmedyoussef** 9 months, 1 week ago

**Selected Answer: D**

D Correct

upvoted 1 times

🗳️ 👤 **Uzumaki\_Aliyy** 1 year, 6 months ago

D - correct

check: Cisco CyberOps Associate CBROPS 200-201 Official Cert Guide by Omar Santos

upvoted 1 times

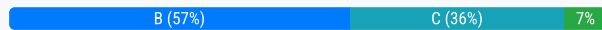


An analyst discovers that a legitimate security alert has been dismissed.  
Which signature caused this impact on network traffic?

- A. true negative
- B. false negative
- C. false positive
- D. true positive

**Suggested Answer: B**

Community vote distribution



🗳️ 👤 **HarryPotter69** Highly Voted 3 years, 9 months ago

A false negative occurs when the security system (usually a WAF) fails to identify a threat.  
It produces a "negative" outcome (meaning that no threat has been observed), even though a threat exists.

This is the opposite of a false positive alarm,  
where a system mistakenly identifies legitimate traffic as being hostile.

I would answer - false negative  
upvoted 25 times

🗳️ 👤 **JayPEI** 3 years ago  
identifie nothing means false positive  
upvoted 1 times

🗳️ 👤 **MartinRB** 2 years, 4 months ago  
false positive means, alert raised by mistake, no threat is there, example a SPAM vs malicious email, SPAM is a false positive.  
upvoted 1 times

🗳️ 👤 **Hellome123** Most Recent 6 months ago

Selected Answer: B

False Positive - Incorrectly classified as positive  
True Positive - Correctly classified as positive  
False Negative - Incorrectly classified as Negative  
True Negative - Correctly classified as Negative  
upvoted 1 times

🗳️ 👤 **d503c75** 9 months, 3 weeks ago

True = Attack  
False = No Attack  
Positive = Alert  
Negative = No Alert

Sooo the answer is A -> There's an attack, but no alert.  
upvoted 1 times

🗳️ 👤 **d503c75** 9 months, 2 weeks ago

Sorry, correcting:

FP -> - Alert -- NoAttack  
FN -> - NoAlert -- Attack

TP -> Attack - Alert  
TN -> NoAttack - NoAlert

The answer is FN. Option B

upvoted 1 times

🗨️ 👤 **sheyshey** 1 year, 6 months ago

**Selected Answer: B**

should be B

upvoted 2 times

🗨️ 👤 **Faio** 1 year, 10 months ago

The answer is B. false negative.

upvoted 1 times

🗨️ 👤 **SecurityGuy** 1 year, 10 months ago

**Selected Answer: B**

False Positive - Incorrectly classified as positive

True Positive - Correctly classified as positive

False Negative - Incorrectly classified as Negative

True Negative - Correctly classified as Negative

In this case, the legitimate alert was "incorrectly classified as negative".

upvoted 1 times

🗨️ 👤 **slippery31** 1 year, 11 months ago

False Negative

upvoted 1 times

🗨️ 👤 **Topsecret** 1 year, 11 months ago

**Selected Answer: C**

The correct answer is C. false positive.

When an analyst discovers that a legitimate security alert has been dismissed, it indicates a false positive.

A false positive occurs when a security system or tool generates an alert or indicates a security incident that is not actually malicious or threatening. In this case, the dismissed alert was mistakenly considered as a non-threatening event, leading to the legitimate security alert being ignored or overlooked.

upvoted 1 times

🗨️ 👤 **ethhacker** 1 year, 10 months ago

Wrong. Answer is false negative. Attack not detected by system. End of discussion

upvoted 2 times

🗨️ 👤 **Swordfishtaco** 2 years ago

false negative =no alarm with a true attack.

upvoted 1 times

🗨️ 👤 **Isuckatexams** 2 years ago

**Selected Answer: D**

A True Positive generated the Alert. The alert was dismissed

upvoted 1 times

🗨️ 👤 **CrazyD1337** 2 years ago

a false negative occurs when a system fails to identify a threat producing a negative outcome even though a threat exists... the system didn't fail to identify a threat.

a false positive occurs when a system mistakenly identifies legitimate traffic as being hostile... the system didn't mistakenly identify legitimate traffic as being hostile, it's a legitimate security alert.

a true negative security alert refers to a situation where an alert has not been generated when a specific activity has occurred (i.e. a threat)... the system didn't fail to generate an alert. it was dismissed.

a true positive security alert refers to a legitimate attack that triggers an alarm.. a legitimate alert was generated... and the only 'thing' (signature) that could cause this, would be a true positive.

an analyst discovers that a LEGITIMATE security alert (true positive) has been dismissed... someone dismissed a legitimate alert... imo, A, B and C are incorrect. I'm going with D.

upvoted 1 times

🗨️ 👤 **Mack279** 2 years, 1 month ago

Put the question this way, there is a legit attack/threat but the system did not see it as a threat. Answer is B, false negative.

upvoted 1 times

🗨️ 👤 **alhamry** 2 years, 1 month ago

negative means: there is no alert.

false negative means: the "no alert" is false > a legitimate security alert has been dismissed

therefore the correct answer is B

upvoted 1 times

🗨️ 👤 **alhamry** 2 years, 1 month ago

to understand it, think like that:

- positive: there is alert triggered:

1- true positive: true alert > there is a threat

2- false positive: false alert > no actual threat

- negative: there is no alert triggered:

1- true negative: true "no alert" > there is no threat

2- false negative: false "no alert" > there is a threat

upvoted 3 times

🗨️ 👤 **drdecker100** 2 years, 4 months ago

**Selected Answer: B**

The correct answer is B.

A false negative occurs when a security alert is missed or dismissed, allowing malicious traffic to go unnoticed. In this case, the analyst discovered that a legitimate security alert was dismissed, indicating that a threat was present but was not detected by the system. Therefore, the impact on network traffic was a false negative.

upvoted 3 times

🗨️ 👤 **apebrz** 2 years, 8 months ago

I think it D:

An analyst discovers that a legitimate security alert (True Positive) has been dismissed (whatever the reason, human fail for example)

upvoted 3 times

🗨️ 👤 **weganos** 2 years, 9 months ago

**Selected Answer: B**

I agree it's B

upvoted 2 times

🗨️ 👤 **surforlife** 2 years, 12 months ago

Real true then is the opposite negative. Not true is then negative! Answer is B False Negative.

upvoted 1 times

Which signature impacts network traffic by causing legitimate traffic to be blocked?

- A. false negative
- B. true positive
- C. true negative
- D. false positive

**Suggested Answer:** D

Community vote distribution

D (100%)

🗳️ 👤 **SecurityGuy** 10 months, 3 weeks ago

**Selected Answer: D**

False Positive - Incorrectly classified as positive

True Positive - Correctly classified as positive

False Negative - Incorrectly classified as Negative

True Negative - Correctly classified as Negative

In this case, the legitimate traffic was "incorrectly classified as positive".

upvoted 1 times

🗳️ 👤 **Eng\_ahmedyoussef** 1 year, 8 months ago

**Selected Answer: D**

False Positive

upvoted 1 times

🗳️ 👤 **Tobds234** 2 years, 2 months ago

**Selected Answer: D**

False positive: Happens when the system raises an event against legitimate traffic that is not malicious. The IPS or IDS administrator's goal is to minimize false positive events because these types of the events can cause unneeded investigation.

upvoted 1 times

🗳️ 👤 **Tobds234** 2 years, 2 months ago

A is the correct answer

upvoted 1 times

🗳️ 👤 **Tobds234** 2 years, 2 months ago

D IS the correct answer

upvoted 1 times

🗳️ 👤 **HarryPotter69** 2 years, 9 months ago

A false negative occurs when the security system (usually a WAF) fails to identify a threat.

It produces a "negative" outcome (meaning that no threat has been observed), even though a threat exists.

This is the opposite of a false positive alarm, where a system mistakenly identifies legitimate traffic as being hostile.

I would answer - false positive

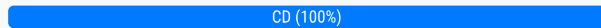
upvoted 4 times

Which two pieces of information are collected from the IPv4 protocol header? (Choose two.)

- A. UDP port to which the traffic is destined
- B. TCP port from which the traffic was sourced
- C. source IP address of the packet
- D. destination IP address of the packet
- E. UDP port from which the traffic is sourced

**Suggested Answer:** *CD*

*Community vote distribution*



 **Eng\_ahmedyoussef** 9 months, 1 week ago

**Selected Answer:** CD

source IP and Destination IP

upvoted 4 times

Which HTTP header field is used in forensics to identify the type of browser used?

- A. referrer
- B. host
- C. user-agent
- D. accept-language

**Suggested Answer: C**

*Community vote distribution*

C (100%)

Eng\_ahmedyoussef 8 months, 3 weeks ago

**Selected Answer: C**

C is correct

User Agent

[https://en.wikipedia.org/wiki/User\\_agent#User\\_agent\\_identification](https://en.wikipedia.org/wiki/User_agent#User_agent_identification)

upvoted 2 times

anonymous1966 1 year, 9 months ago

"C" is correct.

Example:

User-Agent: Mozilla/5.0 (X11; Linux x86\_64; rv:12.0) Gecko/20100101 Firefox/12.0

In computing, a user agent is any software, acting on behalf of a user, which "retrieves, renders and facilitates end-user interaction with Web content".

[1] A user agent is therefore a special kind of software agent.

[https://en.wikipedia.org/wiki/User\\_agent#User\\_agent\\_identification](https://en.wikipedia.org/wiki/User_agent#User_agent_identification)

upvoted 3 times

Pwned 1 year, 8 months ago

"C" is Correct

A user agent is a computer program representing a person, for example, a browser in a Web context.

[https://developer.mozilla.org/en-US/docs/Glossary/User\\_agent](https://developer.mozilla.org/en-US/docs/Glossary/User_agent)

upvoted 1 times

Which event artifact is used to identify HTTP GET requests for a specific file?

- A. destination IP address
- B. TCP ACK
- C. HTTP status code
- D. URI

**Suggested Answer:** D

*Community vote distribution*

D (100%)

🗲️ 👤 **omita** Highly Voted 👍 1 year, 5 months ago

Answer D: A Uniform Resource Identifier (URI) is a unique sequence of characters that identifies a logical or physical resource used by web technologies. URIs may be used to identify anything, including real-world objects, such as people and places, concepts, or information resources such as web pages and books

upvoted 5 times

🗲️ 👤 **Eng\_ahmedyoussef** Most Recent ⌚ 9 months, 1 week ago

**Selected Answer: D**

D - URI

upvoted 1 times

🗲️ 👤 **DaveEly** 1 year, 5 months ago

**Selected Answer: D**

[https://en.wikipedia.org/wiki/Uniform\\_Resource\\_Identifier](https://en.wikipedia.org/wiki/Uniform_Resource_Identifier)

upvoted 2 times

🗲️ 👤 **Luas** 1 year, 7 months ago

D) URI => [https://pl.wikipedia.org/wiki/Uniform\\_Resource\\_Identifier](https://pl.wikipedia.org/wiki/Uniform_Resource_Identifier)

upvoted 1 times

What should a security analyst consider when comparing inline traffic interrogation with traffic tapping to determine which approach to use in the network?

- A. Tapping interrogation replicates signals to a separate port for analyzing traffic
- B. Tapping interrogations detect and block malicious traffic
- C. Inline interrogation enables viewing a copy of traffic to ensure traffic is in compliance with security policies
- D. Inline interrogation detects malicious traffic but does not block the traffic

**Suggested Answer: A**

Community vote distribution

A (100%)

Eng\_ahmedyoussef 9 months, 1 week ago

**Selected Answer: A**

A is the best answer

upvoted 2 times

anonymous1966 11 months, 3 weeks ago

**Selected Answer: A**

Reading the colleagues arguments, I changed my opinion. Correct = A

upvoted 4 times

halamah 1 year, 7 months ago

a is correct

upvoted 3 times

Pwned 1 year, 8 months ago

"A" is correct

A network TAP is a simple device that connects directly to the cabling infrastructure to split or copy packets for use in analysis, security, or general network management

Cisco CyberOps Associate CBROPS 200-201 Official Cert Guide by Omar Santos

upvoted 3 times

alocin 1 year, 8 months ago

i agree with "A" = SPAN (not TAP).

for me the C would be correct if it were only "Inline interrogation enables viewing a copy of traffic"

upvoted 1 times

anonymous1966 1 year, 9 months ago

In my oppinion Correct is "C"

"A" = SPAN (not TAP)

According to the book:

The following are some key benefits of using a physical inline tap:

It will create a full copy of the network traffic and send it to the security monitoring device.

It does not drop any traffic.

A physical inline tap does not require any sort of configuration.

It is simple to implement on a network.

Most inline taps do not require power for the device to operate.


It does not create any contention on the network.

upvoted 2 times

Pwned 1 year, 8 months ago



"C" can't be the answer because Inline interrogation process the live traffic before it is forwarded, its doesnt process a copy of the traffic. and options B and D are wrong :v  
upvoted 1 times

  **RSA001** 1 year, 2 months ago

Seems i can prove why A is correct

A. Tapping interrogation replicates SIGNALS to a separate port for analyzing traffic

SPAN does not replicate signals, but packets

upvoted 2 times

At which layer is deep packet inspection investigated on a firewall?

- A. internet
- B. transport
- C. application
- D. data link

**Suggested Answer:** C

Community vote distribution

C (86%)

14%

Eng\_ahmedyoussef 8 months, 3 weeks ago

**Selected Answer: C**

Application layer

Deep packet inspection ==> evaluates the contents of a packet that is going through a checkpoint.

upvoted 1 times

anonymous1966 11 months, 3 weeks ago

**Selected Answer: C**

Deep packet = Application.

With deep packet inspection (DPI), firewalls can look at specific Layer 7 payloads to protect against security threats. You can also configure these devices to deny specific FTP commands, HTTP content types, and other application protocols.

Ref: Cisco CyberOps Associate CBROPS 200-201 Official Cert Guide

Omar Santos

upvoted 4 times

addpro7 1 year, 2 months ago

**Selected Answer: C**

Deep Packet => Layer 7 => application

so the correct answer = C

upvoted 1 times

DLukynskyy 1 year, 3 months ago

**Selected Answer: A**

"deep" is the keyword

upvoted 1 times

AVT 1 year, 7 months ago

C is the correct answer.

Deep packet inspection is a form of packet filtering usually carried out as a function of your firewall. It is applied at the Open Systems Interconnection's application layer. Deep packet inspection evaluates the contents of a packet that is going through a checkpoint.

upvoted 4 times

akustic 1 year, 7 months ago

But traditional firewall doesn't understand what application is. So we can only analyze up to transport layer. If we want to see smth more, what is in app layer we should use Wireshark or smth else... Answer B is correct in my opinion.

upvoted 3 times

WillBui 1 year, 3 months ago

nextgen fw like palo alto understand lay 7 protocol

upvoted 3 times

## DRAG DROP -

Drag and drop the access control models from the left onto its corresponding descriptions on the right.

Select and Place:

MAC	object owner determines permissions
ABAC	OS determines permissions
RBAC	role of the subject determines permissions
DAC	attributes of the subject determines permissions

## Suggested Answer:

MAC	DAC
ABAC	MAC
RBAC	RBAC
DAC	ABAC

**[Removed]** Highly Voted 2 years, 9 months ago

DAC -> object owner determines permissions

MAC -> OS determines permissions

RBAC -> role of the subject determines permissions

ABAC -> attributes of the subject determines permissions

upvoted 14 times

**tsabee** 2 years, 8 months ago

Agree with you!

Most important to see: "the object owner determines the permissions" is the exact definition of DAC

There are lot reference, f.e.:

<https://www.ekransystem.com/en/blog/mac-vs-dac>

Mandatory access control (MAC) is a model of access control where the operating system provides users with access based on data confidentiality and user clearance levels. In this model, access is granted on a need to know basis: users have to prove a need for information before gaining access.

Discretionary access control (DAC) is an identity-based access control model that provides users a certain amount of control over their data. Data owners (or any users authorized to control data) can define access permissions for specific users or groups of users.

upvoted 4 times

**macxwhale** Most Recent 12 months ago

The first letter of some two options gives the answer! A-attribute based and R-role based! D-is object owner... Then balance is obvious!

upvoted 1 times

**Eng\_ahmedyoussef** 1 year, 8 months ago

Answer is correct

DAC ==> object owner determines permissions and provides users a certain amount of control over their data , it is a least restrictive model.

MAC ==> OS determines permissions, it provides users with access based on data confidentiality and user clearance levels, it is most restrictive model.

RBAC ==> role of the subject determines permissions.

ABAC ==> attributes of the subject determines permissions.

upvoted 2 times

**anonymous1966** 2 years, 9 months ago

Answer is correct.

M = Mandatory

D = Discretionary

R = Role

A = Attribute

upvoted 1 times

## DRAG DROP -

Drag and drop the event term from the left onto the description on the right.

Select and Place:

true negative	malicious traffic is identified and an alert is generated
false negative	benign traffic incorrectly generates an alert
true positive	benign traffic does not generate an alert
false positive	malicious traffic does not generate an alert

## Suggested Answer:

	true positive
	false positive
	true negative
	false negative

## Reference:

<https://www.cisco.com/c/en/us/support/docs/security/ips-4200-series-sensors/13876-f-pos.html>

 **Mack279** 7 months ago

true positive - there is a threat and triggers an alert.  
 true negative - there is no threat and no alert triggers.  
 false positive - there is no threat but triggers an alert.  
 false negative - there is a threat but no alert triggers.

Answer is correct.

upvoted 3 times

 **youvi** 7 months ago

correct answer

- positive: there is alert triggered:  
 1- true positive: true alert > there is a threat  
 2- false positive: false alert > no actual threat  
 - negative: there is no alert triggered:  
 1- true negative: true "no alert" > there is no threat  
 2- false negative: false "no alert" > there is a threat  
 upvoted 2 times

 **cy\_analyst** 1 year, 2 months ago



true negative --> third

false negative --> fourth

true positive --> first

false positive --> second

upvoted 1 times

  **omita** 1 year, 11 months ago

Bengin traffic: Harmless or well intentioned, the opposite of malicious.

upvoted 1 times

```
192.168.10.10 - - [01/Dec/2020:11:12:22 -0200] "GET/icons/powered_by_rh.png HTTP/1.1" 200 1213 "http://192.168.0.102/" "Mozilla/5.0 (X11; U; Linux x86_64; en-US; rv:1.9.0.12) Gecko/2009070812 Ubuntu/8.04 (hardy) Firefox/3.0.12"
192.168.10.10 - - [01/Dec/2020:11:13:15 -0200] "GET/favicon.ico HTTP/1.1" 404 288 "-" "Mozilla/5.0 (X11; U; Linux x86_64; en-US; rv:1.9.0.12) Gecko/2009070812 Ubuntu/8.04 (hardy) Firefox/3.0.12"
192.168.10.10 - - [01/Dec/2020:11:14:22 -0200] "GET /%27%27;!--%22%3CXSS%3E=&{()} HTTP/1.1" 404 310 "-" "Mozilla/5.0 (X11; U; Linux x86_64; en-US; rv:1.9.0.12) Gecko/2009070812 Ubuntu/8.04 (hardy) Firefox/3.0.12"
```


Refer to the exhibit. What is occurring?

- A. insecure deserialization
- B. cross-site scripting attack
- C. XML External Entities attack
- D. regular GET requests

**Suggested Answer: B**

Community vote distribution

B (100%)

 **fjcsanchez** Highly Voted 2 years, 3 months ago

Correct is B

<https://security.tcnj.edu/resources-tips/resources-for-server-administrators-and-developers/detecting-cross-site-scripting-attacks/>

"GET /%27%27;!--%22%3CXSS%3E=&{()"

} HTTP/1.1"

upvoted 7 times

 **cy\_analyst** 2 years, 2 months ago

Thanks for sharing the part to look for is --> GET /%27%27 and some more variants of that.

upvoted 3 times

 **RoBery** Most Recent 11 months, 3 weeks ago

B

/ followed by URL-encoded characters: %27 represents a single quote ('), %22 represents a double quote ("), and %3C and %3E represent the less-than (<) and greater-than (>) symbols, respectively. These characters are being URL-encoded.

;!--: This might be an attempt to include a comment in the payload.

%22%3CXSS%3E=: This part might be trying to inject an XSS payload.

&{()}: This could be part of the payload, potentially attempting to inject additional characters or execute certain actions.

upvoted 1 times

 **CCNPTT** 1 year, 1 month ago

Selected Answer: B

Special Characters:

%27: '

%22: "

%3C: <

%3E: >

Is an XSS attack, it's trying to get something like

/" ;!--<XSS>=&{() }

upvoted 3 times

 **MartinRB** 1 year, 10 months ago

Selected Answer: B

Here is one sample web access log entry that is a sign of an XSS attack.

```
192.168.0.252 -- [05/Aug/2009:15:16:42 -0400] "GET /%27%27;!-%22%3CXSS%3E=&{()  
} HTTP/1.1" 404 310 "-" "Mozilla/5.0 (X11; U; Linux x86_64; en-US; rv:1.9.0.12)  
Gecko/2009070812 Ubuntu/8.04 (hardy) Firefox/3.0.12"
```

The part to look for is the GET /%27%27 command (there are several variants).

upvoted 3 times

  **cy\_analyst** 2 years, 2 months ago

**Selected Answer: B**

B because of --> GET /%27%27

upvoted 1 times

  **Eng\_ahmedyoussef** 2 years, 2 months ago

i think that it is

C. XML External Entities attack

upvoted 1 times



What is a difference between data obtained from Tap and SPAN ports?

- A. SPAN passively splits traffic between a network device and the network without altering it, while Tap alters response times.
- B. Tap mirrors existing traffic from specified ports, while SPAN presents more structured data for deeper analysis.
- C. SPAN improves the detection of media errors, while Tap provides direct access to traffic with lowered data visibility.
- D. Tap sends traffic from physical layers to the monitoring device, while SPAN provides a copy of network traffic from switch to destination.

**Suggested Answer:** D

Reference:

<https://www.gigamon.com/resources/resource-library/white-paper/to-tap-or-to-span.html>

*Community vote distribution*

D (100%)

🗨️ 👤 **Eng\_ahmedyoussef** 8 months, 3 weeks ago

**Selected Answer: D**

Yes D is the correct answer

- TAP sends traffic from physical layers to the monitoring device
  - SPAN provides a copy of network traffic from switch to destination.
- upvoted 2 times

🗨️ 👤 **omita** 1 year, 5 months ago

<https://www.gigamon.com/resources/resource-library/white-paper/to-tap-or-to-span.html>

upvoted 3 times

## DRAG DROP -

Drag and drop the data source from the left onto the data type on the right.

Select and Place:

Wireshark	session data
NetFlow	alert data
server log	full packet capture
IPS	transaction data

**Suggested Answer:**

	NetFlow
	IPS
	Wireshark
	server log

 **addpro7** Highly Voted 2 years, 2 months ago

the correct answer :

Wireshark => Full Packet Capture

Netflow => Session Data

Server log => Transaction

IPS = > Alert Data

the confusion is between session data & transaction data,

so,

NetFlow provides information about network session data, and NetFlow records take less space than a full packet capture.

P957\_ Cisco CyberOps Associate CBROPS 200-201 Official Cert Guide (Certification Guide) by Omar Santos

upvoted 9 times

 **wienio** Highly Voted 2 years, 4 months ago

transaction data = netflow

upvoted 7 times

 **CCNPTT** Most Recent 7 months, 2 weeks ago

Answer provided is correct.

upvoted 3 times

 **Eng\_ahmedyoussef** 1 year, 8 months ago

Answer Is Correct

Netflow ==> Session Data

IPS ==> Alert Data

Wireshark ==> Full Packet Capture

Server log == Transaction Data.

upvoted 3 times

A threat actor penetrated an organization's network. Using the 5-tuple approach, which data points should the analyst use to isolate the compromised host in a grouped set of logs?

- A. event name, log source, time, source IP, and username
- B. event name, log source, time, source IP, and host name
- C. protocol, log source, source IP, destination IP, and host name
- D. protocol, source IP, source port destination IP, and destination port

**Suggested Answer:** D

Reference:

<https://blogs.cisco.com/security/the-dreaded-5-tuple>

*Community vote distribution*

D (100%)

🗨️ 👤 **seyfo** 11 months, 2 weeks ago

**Selected Answer: D**

D is correct

upvoted 1 times

🗨️ 👤 **Eng\_ahmedyoussef** 1 year, 2 months ago

**Selected Answer: D**

D is Correct

5-Touple ==> protocol, source IP, source port destination IP, and destination port

upvoted 1 times

What is a difference between an inline and a tap mode traffic monitoring?

- A. Tap mode monitors packets and their content with the highest speed, while the inline mode draws a packet path for analysis.
- B. Inline monitors traffic without examining other devices, while a tap mode tags traffic and examines the data from monitoring devices.
- C. Inline mode monitors traffic path, examining any traffic at a wire speed, while a tap mode monitors traffic as it crosses the network.
- D. Tap mode monitors traffic direction, while inline mode keeps packet data as it passes through the monitoring devices.

**Suggested Answer:** C

Community vote distribution

C (100%)

🗳️ 👤 **RoBery** 11 months, 3 weeks ago

C:

In inline mode, the monitoring device is placed directly in the traffic path and actively participates in the flow of packets. It examines and potentially takes action on the traffic at wire speed.

In tap mode, a network tap is used to passively capture a copy of the traffic as it traverses the network. The tap is typically placed on a network link, and the monitoring device receives a duplicate copy of the traffic.

So, the key difference is that inline mode actively participates in the traffic path, while tap mode is a passive monitoring method that captures a copy of the traffic.

upvoted 1 times

🗳️ 👤 **drdecker100** 1 year, 10 months ago

**Selected Answer: C**

Inline mode and tap mode are two different methods of network traffic monitoring.

Inline mode involves inserting a monitoring device, such as an Intrusion Prevention System (IPS), directly into the network traffic path. The monitoring device actively inspects all traffic passing through it, typically at wire speed, and can take action to block or allow specific traffic based on security policies.

In contrast, tap mode involves using a network tap, which is a device that is inserted into the network without disrupting the normal flow of traffic. The tap makes a copy of the traffic and sends it to a monitoring device for analysis. This means that tap mode can capture traffic as it crosses the network, but at a potentially lower speed than inline mode.

Therefore, the correct answer is C, as inline mode monitors traffic path, examining any traffic at a wire speed, while a tap mode monitors traffic as it crosses the network.

upvoted 3 times

🗳️ 👤 **ItsBananass** 2 years, 5 months ago

I think the answer should be "D"

upvoted 1 times

An engineer is addressing a connectivity issue between two servers where the remote server is unable to establish a successful session. Initial checks show that the remote server is not receiving a SYN-ACK while establishing a session by sending the first SYN. What is causing this issue?

- A. incorrect TCP handshake
- B. incorrect UDP handshake
- C. incorrect OSI configuration
- D. incorrect snaplen configuration

**Suggested Answer: A**

Reference:

<https://www.sciencedirect.com/topics/computer-science/three-way-handshake#:~:text=The%20TCP%20handshake,as%20shown%20in%20Figure%203.8>

Community vote distribution

A (100%)

🗨️ 👤 **AhmedAbdalla** 8 months, 3 weeks ago

incorrect TCP handshake

In a typical TCP handshake, the process involves three steps:

SYN: The client sends a SYN (synchronize) packet to the server to initiate the connection.

SYN-ACK: The server responds with a SYN-ACK (synchronize-acknowledgment) packet to acknowledge the client's request and indicate readiness to establish the connection.

ACK: Finally, the client sends an ACK (acknowledgment) packet back to the server to confirm the connection.

If the remote server is not receiving the expected SYN-ACK response after sending the first SYN, it indicates a problem in the TCP handshake, which could be due to network issues, firewall rules, or other misconfigurations.

upvoted 1 times

🗨️ 👤 **Eng\_ahmedyoussef** 1 year, 8 months ago

**Selected Answer: A**

A. incorrect TCP handshake

upvoted 2 times

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	6.131.174.187	106.153.244.155	TCP	62	wfremoterm > http [SYN] Seq=8 Win=6
2	1.000000	106.153.244.155	6.131.174.187	TCP	58	http > wfremoterm [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
3	2.000000	6.131.174.187	106.153.244.155	TCP	60	wfremoterm > http [ACK] Seq=1 Ack=1 Win=64240 Len=0
4	3.000000	6.131.174.187	106.153.244.155	HTTP	151	GET /png.php?D347B0e086125BA1FCC75FA73B89FE9C377E066692F812728F1C1C8BBF26E67FA44A41C1E388854073FA2DD9B435FE97B1C337A1113FEDB781F0D68876BE326AF5DEC11AC0FF255A49
5	4.000000	106.153.244.155	6.131.174.187	TCP	54	http > wfremoterm [ACK] Seq=1 Ack=648 Win=65535 Len=0
6	5.000000	106.153.244.155	6.131.174.187	HTTP	482	HTTP/1.1 200 OK (text/html)
7	6.000000	6.131.174.187	106.153.244.155	TCP	60	wfremoterm > http [ACK] Seq=648 Ack=429 Win=63812 Len=0
8	7.000000	106.153.244.155	6.131.174.187	TCP	54	http > wfremoterm [FIN, ACK] Seq=429 Ack=648 Win=65535 Len=0
9	8.000000	6.131.174.187	106.153.244.155	TCP	60	wfremoterm > http [ACK] Seq=648 Ack=430 Win=63812 Len=0

[Window size scaling factor: -2 (no window scaling used)]  
 Checksum: 0xe318 (validation disabled)  
 [SEQ/ACK analysis]

**Hypertext Transfer Protocol**

[truncated] GET /png.php?D347B0e086125BA1FCC75FA73B89FE9C377E066692F812728F1C1C8BBF26E67FA44A41C1E388854073FA2DD9B435FE97B1C337A1113FEDB781F0D68876BE326AF5DEC11AC0FF255A49  
 Expert Info (Chat/Sequence): [truncated] GET /png.php?D347B0e086125BA1FCC75FA73B89FE9C377E066692F812728F1C1C8BBF26E67FA2DD9B435FE97B1C337A1113FEDB781F0D68876BE326AF5DEC11  
 Request Method: GET  
 Request URI: [truncated] /png.php?D347B0e086125BA1FCC75FA73B89FE9C377E066692F812728F1C1C8BBF26E67FA44A41C1E388854073FA2DD9B435FE97B1C337A1113FEDB781F0D68876BE326AF5DEC11  
 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; .NET CLR 2.0.50727; .NET CLR 3.0.4586.2152; .NET CLR 3.5.  
 Host: fdsalre367hs64a.ase4wrfdsfg9.com/r/n  
 Connection: Keep-Alive\r/n  
 \r/n  
 [full request URI [truncated]: http://fdsalre367hs64a.ase4wrfdsfg9.com/png.php?D347B0e086125BA1FCC75FA73B89FE9C377E066692F812728F1C1C8BBF26E67FA44A41C1E388854073FA2DD9B435F

0070 17 37 32 30 46 31 45 31 45 30 42 42 45 46 32 30 272B7F1C1 C8BBF26E67FA44A41C1E388854073FA2DD9B435FE97B1C337A1113FEDB781F0D68876BE326AF5DEC11AC0FF255A49  
 0080 45 36 37 46 41 34 34 41 34 31 43 31 45 33 38 30 B67FA44A 41C1E1B6  
 0090 39 35 34 30 37 35 46 41 32 44 44 39 42 34 33 35 B54675BA 2DD9B435  
 00a0 46 45 39 37 42 31 41 33 33 37 41 31 31 31 33 46 FE97B1C3 37A1113F  
 00b0 45 44 42 37 38 31 46 30 44 36 36 38 37 36 42 45 FDB781F0 D66876BE  
 00c0 33 32 16 41 46 35 44 45 41 31 31 41 43 38 46 46 326AF5DE C11ACBFF  
 00d0 31 32 15 41 34 39 36 32 38 36 45 33 41 41 41 31 255A4962 B6E2AAC1  
 00e0 45 39 11 39 38 26 27 41 34 36 35 33 34 37 32 33 B619667C 48534723  
 00f0 36 35 30 39 36 46 35 33 31 44 33 43 43 34 37 33 65696F33 103CC472  
 0100 12 32 32 41 16 43 11 11 46 11 45 28 36 41 41 44 222ABC21 F1CBBAED  
 0110 13 32 32 31 19 44 46 37 31 31 34 36 14 43 33 38 122190F7 1146DC3B  
 0120 14 38 41 35 38 44 30 41 39 14 30 41 41 35 35 44 13A5BDCC 248B666D  
 0130 36 43 43 43 45 43 43 46 45 43 37 45 36 33 36 43 6C8C8C0F E77F83BC  
 0140 31 31 34 34 41 44 41 31 36 39 35 39 14 39 36 18 1144CDA1 69394960  
 0150 46 41 46 37 36 41 17 41 17 44 39 38 45 41 36 37 FB76A7B 2D98ECB7

Refer to the exhibit. What is shown in this PCAP file?

- A. The User-Agent is Mozilla/5.0.
- B. Timestamps are indicated with error.
- C. The HTTP GET is encoded.
- D. The protocol is TCP.

**Suggested Answer: C**

Community vote distribution

C (100%)

**d503c75** 9 months, 1 week ago

The answer is D. See the print line protocol

There's no encoded "code"...so, can't be C.

upvoted 1 times

**Eng\_ahmedyoussef** 2 years, 8 months ago

**Selected Answer: C**

C. The HTTP GET is encoded.

upvoted 1 times

**anonymous1966** 2 years, 11 months ago

**Selected Answer: C**

Remember it is a CyberOps exam.

Encoding URI is an attack type.

[https://owasp.org/www-community/Double\\_Encoding#](https://owasp.org/www-community/Double_Encoding#)

upvoted 2 times

**halamah** 3 years, 7 months ago

d is correct

upvoted 2 times

**Pwned** 3 years, 7 months ago

"C" cant be the answer... URL encoding serves the purpose of replacing these non-conforming characters with a % symbol followed by two hexadecimal digits that represent the ASCII code of the character



Ex. <http://www.thedesignshop.com/%23somequotes%23.html>

this URL is using %23 to encode "#" character

[https://launchschool.com/books/http/read/what\\_is\\_a\\_url](https://launchschool.com/books/http/read/what_is_a_url)

maybe the answer is D

upvoted 1 times

  **Pwned** 3 years, 7 months ago

My bad... "C" is correct.... but it is using Base64 image encoding, and it says the file is a .png

upvoted 2 times



Which regular expression is needed to capture the IP address 192.168.20.232?

- A. `^(?:[0-9]{1,3}\.){3}[0-9]{1,3}`
- B. `^(?:[0-9]{1,3}\.)*`
- C. `^(?:[0-9]{1,3}\.){1,4}`
- D. `^([0-9]{3})`

**Suggested Answer: A**

Community vote distribution

A (100%)

 **Pwned**  3 years, 1 month ago

A is correct... but this is the correct form `^(?:[0-9]{1,3}\.){3}[0-9]{1,3}`  
upvoted 12 times

 **anonymous1966**  2 years, 5 months ago

**Selected Answer: A**

Correct options are:

- A) `^(?:[0-9]{1,3}\.){3}[0-9]{1,3}`
- B) `^(?:[0-9]{1,3}\.){1,4}`
- C) `^(?:[0-9]{1,3}\.){1,4}`
- D) `^([0-9]{3})`

Test and verify the correct option A at <https://regex101.com/>

upvoted 8 times

 **RoBery**  11 months, 3 weeks ago

A. `^(?:[0-9]{1,3}\.){3}[0-9]{1,3}`

Explanation:

`^`: Asserts the start of the string.

`(?:[0-9]{1,3}\.){3}`: This non-capturing group matches three occurrences of digits 1 to 3 in length followed by a dot (.), representing the first three octets.

`[0-9]{1,3}`: Matches the fourth octet, consisting of digits 1 to 3 in length.

`$`: Asserts the end of the string.

This regular expression is designed to match the pattern of an IPv4 address and captures the IP address 192.168.20.232.

upvoted 1 times

 **Eng\_ahmedyoussef** 2 years, 2 months ago

**Selected Answer: A**

A. `^(?:[0-9]{1,3}\.){3}[0-9]{1,3}`

upvoted 2 times

An engineer received an alert affecting the degraded performance of a critical server. Analysis showed a heavy CPU and memory load. What is the next step the engineer should take to investigate this resource usage?

- A. Run `ps -u` to find out who executed additional processes that caused a high load on a server
- B. Run `ps -ef` to understand which processes are taking a high amount of resources
- C. Run `ps -d` to decrease the priority state of high load processes to avoid resource exhaustion
- D. Run `ps -m` to capture the existing state of daemons and map required processes to find the gap

**Suggested Answer: B**

Community vote distribution

B (100%)

 **anonymous1966** Highly Voted 2 years, 5 months ago

**Selected Answer: B**

B is correct.

The options appears encoded to me.

The options are:

- a) Run `"ps -u"` to find out who executed additional processes that caused a high load on a server.
- b) Run `"ps -ef"` to understand which processes are taking a high amount of resources.
- c) Run `"ps -d"` to decrease the priority state of high load processes to avoid resource exhaustion.
- d) Run `"ps -m"` to capture the existing state of daemons and map required processes to find the gap.

`ps -u` --> Filter processes according to the user

`ps -ef` --> To see every process on the system using standard syntax

`ps -d` --> View all the processes except session leaders

`ps -m` --> display the scheduling policies of a thread

In fact `ps -ef` should be better

<https://www.journaldev.com/24613/linux-ps-command>

<https://www.geeksforgeeks.org/ps-command-in-linux-with-examples/>

<https://www.ibm.com/docs/en/aix/7.2?topic=p-ps-command>

upvoted 5 times

 **RoBery** Most Recent 11 months, 3 weeks ago

B

The command `"ps -ef"` provides a detailed list of all processes running on the system along with their resource utilization.

Analyzing the output of `"ps -ef"` will help the engineer identify which processes are consuming high CPU and memory resources, helping to pinpoint the cause of the degraded performance.

This information is crucial for understanding the current state of the system and determining the processes that may be contributing to the resource load.

upvoted 1 times

 **Eng\_ahmedyoussef** 2 years, 2 months ago

**Selected Answer: B**

B is the best answer

`ps -ef` ==> understand which processes are taking a high amount of resources.

upvoted 1 times

 **AVT** 3 years, 1 month ago

The correct answer is B.

`ps -ef` command

upvoted 2 times

# HKEY\_LOCAL\_MACHINE

Refer to the exhibit. Which component is identifiable in this exhibit?

- A. Windows Registry hive
- B. Trusted Root Certificate store on the local machine
- C. Windows PowerShell verb
- D. local service in the Windows Services Manager

**Suggested Answer: A**

Reference:

<https://docs.microsoft.com/en-us/windows/win32/sysinfo/registry-hives>

Community vote distribution

A (100%)

🗨️ 👤 **AhmedAbdalla** 8 months, 3 weeks ago

Windows Registry hive

The text "HKEY\_LOCAL\_MACHINE" refers to a specific Windows Registry hive. The Windows Registry is a hierarchical database that stores configuration settings and options on Microsoft Windows operating systems. "HKEY\_LOCAL\_MACHINE" is one of the root keys in the Windows Registry and contains configuration data related to the local machine or computer.

upvoted 1 times

🗨️ 👤 **SecurityGuy** 10 months, 2 weeks ago

**Selected Answer: A**

A hive is a logical group of keys, subkeys, and values in the registry that has a set of supporting files loaded into memory when the operating system is started or a user logs in.

<https://learn.microsoft.com/en-us/windows/win32/sysinfo/registry-hives>

upvoted 1 times

🗨️ 👤 **Eng\_ahmedyoussef** 1 year, 8 months ago

**Selected Answer: A**

HKEY\_LOCAL\_MACHINE == > Windows Registry hive

So A. is the correct answer

upvoted 1 times

🗨️ 👤 **Uzumaki\_Aliyy** 2 years, 6 months ago

A is correct:

<https://docs.microsoft.com/en-us/windows/win32/sysinfo/registry-hives>

[https://ldapwiki.com/wiki/HKEY\\_LOCAL\\_MACHINE#:~:text=HKEY\\_LOCAL\\_MACHINE%20Windows%20registry%20hive%20contains,detected%20hardware%20](https://ldapwiki.com/wiki/HKEY_LOCAL_MACHINE#:~:text=HKEY_LOCAL_MACHINE%20Windows%20registry%20hive%20contains,detected%20hardware%20)

upvoted 1 times

An organization has recently adjusted its security stance in response to online threats made by a known hacktivist group. What is the initial event called in the NIST SP800-61?

- A. online assault
- B. precursor
- C. trigger
- D. instigator

**Suggested Answer: B**

Community vote distribution

B (100%)

Eng\_ahmedyoussef 8 months, 3 weeks ago

**Selected Answer: B**

B is Correct

A precursor ==> is a sign that a cyber-attack is about to occur on a system or network.

upvoted 2 times

eggheadsv 1 year, 7 months ago

A precursor is a sign that a cyber-attack is about to occur on a system or network. An indicator is the actual alerts that are generated as an attack is happening. Therefore, as a security professional, it's important to know where you can find both precursor and indicator sources of information.

The following are common sources of precursor and indicator information:

Security Information and Event Management (SIEM)

Anti-virus and anti-spam software

File integrity checking applications/software

Logs from various sources (operating systems, devices, and applications)

People who report a security incident

upvoted 2 times

anonymous1966 1 year, 9 months ago

"B" is correct.

Precursors is the way the document name the method/event. The document do not have the other words in the alternatives.

3.2.3 Sources of Precursors and Indicators

Precursors and indicators are identified using many different sources, with the most common being computer security software alerts, logs, publicly available information, and people

upvoted 4 times

anonymous1966 1 year, 9 months ago

<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf>

upvoted 1 times

Which NIST IR category stakeholder is responsible for coordinating incident response among various business units, minimizing damage, and reporting to regulatory agencies?

- A. CSIRT
- B. PSIRT
- C. public affairs
- D. management

**Suggested Answer:** D

🗨️ 👤 **Vetterous** Highly Voted 🍌 1 year, 11 months ago

<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf>

Management. Management establishes incident response policy, budget, and staffing. Ultimately, management is held responsible for coordinating incident response among various stakeholders, minimizing damage, and reporting to Congress, OMB, the General Accounting Office (GAO), and other parties.

upvoted 8 times

🗨️ 👤 **fjcsanchez** Most Recent 🔔 9 months, 2 weeks ago

Point 2.4.4., page 17

<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf>

upvoted 1 times

🗨️ 👤 **COLCRISS** 1 year ago

Management. Management establishes incident response policy, budget, and staffing. Ultimately, management is held responsible for coordinating incident response among various stakeholders, minimizing damage, and reporting to Congress, OMB, the General Accounting Office (GAO), and other parties

<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf>

upvoted 1 times

🗨️ 👤 **Nikolas** 1 year, 5 months ago

dont agree, i think it is CSIRT - answer A

upvoted 3 times

Which incidence response step includes identifying all hosts affected by an attack?



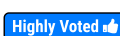
- A. detection and analysis
- B. post-incident activity
- C. preparation
- D. containment, eradication, and recovery

**Suggested Answer: A**

Community vote distribution

A (71%)

D (29%)


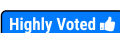
  **seriously5000**  3 years, 1 month ago

D. Eradication

From NIST SP 800-61r2, Section 3.3.4

"During eradication, it is important to identify all affected hosts within the organization so that they can be remediated."

upvoted 12 times

  **anonymous1966**  3 years, 3 months ago



"D" is correct

3.3.3 Identifying the Attacking Hosts

During incident handling, system owners and others sometimes want to or need to identify the attacking host or hosts. Although this information can be important, incident handlers should generally stay focused on containment, eradication, and recovery.

<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf>

upvoted 8 times

  **RSA001** 2 years, 8 months ago

Not really... the question is asking about attacked host, not attacking host. Below explanation from examcol is correct:

The correct answer is A. detection and analysis.

Based on <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf>

3.2 Detection and Analysis > 3.2.4 Incident Analysis

"When the team believes that an incident has occurred, the team should rapidly perform an initial analysis to determine the incident's scope, such as which networks, systems, or applications are affected..."


upvoted 12 times

  **RoBery**  11 months, 3 weeks ago

A. detection and analysis

In the incident response process, the step that includes identifying all hosts affected by an attack is typically part of the "detection and analysis" phase. During this phase, security teams analyze the detected incident, assess the scope of the attack, and work to identify all systems and hosts that may have been affected. This step is crucial for understanding the extent of the incident and planning the appropriate response actions.

upvoted 1 times

  **CCNP TT** 1 year, 1 month ago

**Selected Answer: D**

As seriously5000 mentioned, this question is literally taken from the NIST document:

"During eradication, it is important to identify all affected hosts within the organization so that they can be remediated"

upvoted 2 times

  **Faio** 1 year, 3 months ago

The answer is A. detection and analysis.

upvoted 1 times

  **SecurityGuy** 1 year, 4 months ago

Selected Answer: A

Detection and Analysis

- An incident response analyst is responsible for collecting and analyzing data to find any clues to help identify the source of an attack.
- In this step, analysts identify the nature of the attack and its impact on systems.
- The business and the security professionals it works with utilize the tools and indicators of compromise (IOCs) that have been developed to track the attacked systems.

<https://eccouncil.org/cybersecurity-exchange/incident-handling/what-is-incident-response-life-cycle/>

From a SOC Analyst's POV, when IOCs are detected, you'll naturally want to know how many endpoints are affected and "what are the affected endpoints or hosts".

upvoted 1 times

🗲️ 👤 **Isuckatexams** 1 year, 6 months ago

Selected Answer: A

Incident handling is the process of detecting and analyzing incidents and limiting the incident's effect. For example, if an attacker breaks into a system through the Internet, the incident handling process should detect the security breach. Incident handlers will then analyze the data and determine how serious the attack is. The incident will be prioritized, and the incident handlers will take action to ensure that the progress of the incident is halted and that the affected systems return to normal operation as soon as possible.

upvoted 1 times

🗲️ 👤 **drdecker100** 1 year, 10 months ago

Selected Answer: A

The correct answer is A, detection and analysis.

The detection and analysis phase of an incident response process involves identifying and confirming the presence of a security incident. This includes identifying all hosts that may have been affected by the attack.

During this phase, incident responders collect and analyze information about the incident, such as network traffic, system logs, and other data, to determine the nature and scope of the incident. This information is used to develop an initial understanding of the incident, including which hosts have been affected.

upvoted 2 times

🗲️ 👤 **sman22** 1 year, 10 months ago

D. containment, eradication, and recovery is correct.

Module 28.4.7 After containment, the first step to eradication is identifying all of the hosts that need remediation. All of the effects of the security incident must be eliminated.

upvoted 1 times

🗲️ 👤 **sami43** 1 year, 10 months ago

Selected Answer: A

A. detection and analysis

identifying all hosts affected (not affecting)

upvoted 1 times

🗲️ 👤 **COLCRISS** 2 years, 6 months ago

Its A. Detection and analysis --> and have in mind this is before CONTAINMENT you have to analyze first what happend before even know how to contain ....

Analysis: The incident response team should work quickly to analyze and validate each incident, following a predefined process and documenting each step that is taken. When the team believes that an incident has occurred, the team should rapidly perform an initial analysis to determine the scope of the incident.

The initial analysis may include:

Which networks, systems, or applications are affected?

Who or what originated the incident?

Which tools or attack methods are being used?

Which vulnerabilities are being exploited?

upvoted 1 times

🗨️ 👤 **AVT** 3 years, 1 month ago

The correct answer is D

The response phase, or containment, of incident response, is the point at which the incident response team begins interacting with affected systems and attempts to keep further damage from occurring as a result of the incident.

upvoted 1 times

🗨️ 👤 **halamah** 3 years, 1 month ago

a is correct

upvoted 1 times

🗨️ 👤 **[Removed]** 3 years, 3 months ago

The correct answer is A. detection and analysis.

Based on <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf>

3.2 Detection and Analysis > 3.2.4 Incident Analysis

"When the team believes that an incident has occurred, the team should rapidly perform an initial analysis to determine the incident's scope, such as which networks, systems, or applications are affected..."

upvoted 5 times

🗨️ 👤 **tsabee** 3 years, 2 months ago

I think the "D" is correct, because the Detection and Analsys step deal with identify the threat/malicious activity (who, how, what), the Containment step should define the scope of the incident.

And actually the question was "identifying ALL hosts affected by an attack"

upvoted 3 times

🗨️ 👤 **tsabee** 3 years, 2 months ago

but... actually it's true for only the containment phase, not the others... so I don't know :).

upvoted 1 times

🗨️ 👤 **tsabee** 3 years, 2 months ago

Correct myself: "A" - because of the examcol answer.

upvoted 4 times




Which two elements are used for profiling a network? (Choose two.)

- A. session duration
- B. total throughput
- C. running processes
- D. listening ports
- E. OS fingerprint

**Suggested Answer:** AB

Community vote distribution

AB (100%)

  **forest111** Highly Voted 4 years, 6 months ago

AB. Explanation: A network profile should include some important elements, such as the following:

Total throughput – the amount of data passing from a given source to a given destination in a given period of time

Session duration – the time between the establishment of a data flow and its termination

Ports used – a list of TCP or UDP processes that are available to accept data


Critical asset address space – the IP addresses or the logical location of essential systems or data

upvoted 23 times

  **slimer** 8 months, 1 week ago

agree on this that the answer is A & B due the question is pertaining to network.

upvoted 1 times

  **bren\_** 4 years, 5 months ago

if you're planning to attack, wouldn't you check which ports are open?

imho C is a very legit answer.

upvoted 1 times

  **bren\_** 4 years, 5 months ago



sorry, typo. I meant D

upvoted 2 times

  **bren\_** 4 years, 5 months ago

also, to know which OS is in front of me (if I'm playing the attacker) would help me look for known vulnerabilities

upvoted 2 times

  **Friendly** 4 years, 4 months ago

It's not about attacking now, the question is obvious about network profiling, I guess.

upvoted 2 times

  **Dunky** Highly Voted 4 years, 1 month ago


Network Profiling - Total throughput, session duration, ports used, critical address space. As forest says its AB. Taken from cybersecurity course by IT Pro.tv

upvoted 8 times

  **beowolf** 4 years, 1 month ago

Correct A & B

upvoted 2 times

  **fejec** 3 years, 9 months ago

I Agree. Also from cert guide by Omar S. Chapter 10 : Network Profiling

"These are methods used to capture network-based data that can reveal how systems are functioning on the network. The areas of focus for this section are determining throughput, ports used, session duration, and address space."

upvoted 2 times

  **Faio** Most Recent 1 year, 9 months ago

A-D: The two elements used to profile a network are total throughput and listening ports.

Total throughput is the amount of data sent or received over a network in a given period of time. This can be used to identify unusual traffic patterns, such as a sudden increase in traffic to a particular server.

Listening ports are the ports on a device that are open and listening for incoming connections. It can be used to identify the applications running on a device and the services available.

upvoted 1 times

🗳️ 👤 **slippery31** 2 years, 1 month ago

Correct ANS= A,B

upvoted 2 times

🗳️ 👤 **MaliDong** 2 years, 7 months ago

**Selected Answer: AB**

Agree with A, and B.

upvoted 1 times

🗳️ 👤 **Eng\_ahmedyoussef** 2 years, 8 months ago

**Selected Answer: AB**

A & B is the correct answer

profiling a network

A. session duration

B. total throughput

upvoted 1 times

🗳️ 👤 **cy\_analyst** 2 years, 8 months ago

**Selected Answer: AB**

Network Profiling =

1)Session duration: This is the time between the establishment of a data flow and its termination.

2)Total throughput: This is the amount of data passing from a given source to a given destination in a given period of time.

3)Ports used: This is a list of TCP or UDP processes that are available to accept data.

4)Critical asset address space: These are the IP addresses or the logical location of essential systems or data.

From the book CCNA Cybersecurity Operations Companion Guide

upvoted 2 times

🗳️ 👤 **studyelprof** 2 years, 9 months ago

Answer is A B, Total Throughput and Session duration are one of the 4 elements for network profiling, according to Cisco Cyber Ops Exam blueprint

upvoted 1 times

🗳️ 👤 **addpro7** 3 years, 2 months ago

**Selected Answer: AB**

A & B are correct,

based on page 688, section NETWORK PROFILING of: Cisco CyberOps Associate CBROPS 200-201 Official Cert Guide by Omar Santos

#### NETWORK PROFILING

This section focuses on network profiling concepts.

These are methods used to capture network-based data that can reveal how systems are functioning on the network. The areas of focus for this section are determining throughput, ports used, session duration, and address space.

upvoted 1 times

🗳️ 👤 **RolandoFiee** 3 years, 4 months ago

Respuesta A y B, Network Profiling - Total throughput, session duration, ports used, critical address space

upvoted 1 times

🗳️ 👤 **Uzumaki\_Aliyy** 3 years, 6 months ago

Correct A and B

based on page 689 of: Cisco CyberOps Associate CBROPS 200-201 Official Cert Guide by Omar Santos

upvoted 2 times

🗳️ 👤 **halamah** 3 years, 7 months ago

a and b

upvoted 2 times

🗳️ 👤 **halamah** 3 years, 7 months ago

a and b

upvoted 1 times

🗨️ 👤 **[Removed]** 3 years, 9 months ago

The correct answers are A, B.

Profiling data are data that system has gathered, these data helps for incident response and to detect incident

Network profiling = throughput, sessions duration, port used, Critical Asset Address Space

Host profiling = Listening ports, logged in accounts, running processes, running tasks, applications

upvoted 1 times

🗨️ 👤 **anonymous1966** 3 years, 9 months ago

A and B = correct

Network : A. session duration ; B. total throughput

Host: C. running processes ; D. listening ports ; E. OS fingerprint

upvoted 5 times

🗨️ 👤 **anonymous1966** 3 years, 9 months ago

A and B are correct.

The other alternatives is related to hosts. Even disconnected from network.

upvoted 2 times

🗨️ 👤 **anonymous1966** 3 years, 9 months ago

A and B are correct.

The other alternatives is related to hosts. Even disconnected from network.

upvoted 2 times

Which category relates to improper use or disclosure of PII data?

- A. legal
- B. compliance
- C. regulated
- D. contractual

**Suggested Answer: C**

Community vote distribution

C (70%)


B (30%)

 **addpro7** Highly Voted 1 year, 8 months ago

**Selected Answer: C**

Many regulations as well as the United States government require organizations to identify personally identifiable information (PII) and protected health information (PHI) and handle them in a secure manner. Unauthorized release or loss of such data could result in severe fines and penalties for the organization. Given the importance of PII and PHI, regulators and the government want to oversee the usage more efficiently. This section explains what PII and PHI are.

based on page 158, section PERSONALLY IDENTIFIABLE INFORMATION AND PROTECTED HEALTH INFORMATION of: Cisco CyberOps Associate CBROPS 200-201 Official Cert Guide by Omar Santos  
upvoted 5 times

 **drdecker100** Most Recent 10 months, 2 weeks ago

**Selected Answer: B**

The category that relates to improper use or disclosure of personally identifiable information (PII) data is the compliance category. Compliance refers to adhering to legal and regulatory requirements, as well as internal policies and procedures, to protect sensitive data and ensure the confidentiality, integrity, and availability of information. Compliance requirements often include data protection regulations that mandate how PII data should be collected, stored, and processed, and require organizations to take measures to prevent unauthorized access or disclosure of PII.  
upvoted 3 times


 **Interrogantis** 10 months, 3 weeks ago

**Selected Answer: C**

The improper use or disclosure of Personally Identifiable Information (PII) data is a regulated issue. NIST SP 800-53 and SP 800-171 provide specific guidelines for protecting PII data, including security requirements for non-federal information systems and organizations that process, store, or transmit Controlled Unclassified Information (CUI), which includes PII data. These guidelines address areas such as access control, incident response, and media protection, and aim to ensure the confidentiality, integrity, and availability of PII data. Organizations are expected to comply with these regulations and guidelines, and failure to do so may result in legal consequences.  
upvoted 2 times

 **CiscoTerminator** 2 years ago

What are question: I would flag this in a Cisco exam.  
Key word here is "improper" and still PII data is "regulated" if you dont "comply" then "legal" ramifications will follow the organisation.  
upvoted 3 times

 **Alannn** 2 years, 3 months ago

I think legal is the correct answer aswell: An organization that is subject to any obligations to protect PII should consider such obligations when determining the PII confidentiality impact level. Many organizations are subject to laws, regulations, or other mandates<sup>36</sup> governing the obligation to protect personal information,<sup>37</sup> such as the Privacy Act of 1974, OMB memoranda, and the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Additionally, some Federal agencies, such as the Census Bureau and the Internal Revenue Service (IRS), are subject to additional specific legal obligations to protect certain types of PII.  
upvoted 1 times

 **anonymous1966** 2 years, 3 months ago

"A" should be correct.  
With GDPR (General Data Protection Regulation) I believe is Legal.

The other alternative are mere consequences.

But...



For certification exam, I believe "C" is the right alternative, because inside the companies this information is Regulated.

upvoted 4 times

  **qz999** 2 years, 4 months ago

Seems to me that the correct answer is 'compliance', as compliance must be maintained for all applicable laws, regulations, and contracts.



upvoted 3 times

  **beowolf** 2 years, 9 months ago

PII is related to compliance requirement. This question is not clear.

When it comes to PII, its about collection minimization and storing the collected data securely such as encryption or use tokenization therefore this is a compliance requirement.

upvoted 3 times

  **beowolf** 2 years, 7 months ago

I am not sure about the correct answer, improper use of PII is perhaps related to law or regulated.

upvoted 4 times

Which type of evidence supports a theory or an assumption that results from initial evidence?

- A. probabilistic
- B. indirect
- C. best
- D. corroborative

**Suggested Answer:** D

Community vote distribution

D (100%)

 **anonymous1966** Highly Voted 1 year, 9 months ago

"D" is correct

Corroborating evidence (or corroboration) is evidence that tends to support a theory or an assumption deduced by some initial evidence. This corroborating evidence confirms the proposition.

Cisco CyberOps Associate CBROPS 200-201 Official Cert Guide

By Omar Santos

upvoted 7 times

 **Eng\_ahmedyoussef** Most Recent 8 months, 3 weeks ago

Selected Answer: D

D. is correct

corroborative evidence ==> evidence that supports a theory or an assumption that results from initial evidence.

upvoted 1 times

Which two elements are assets in the role of attribution in an investigation? (Choose two.)

- A. context
- B. session
- C. laptop
- D. firewall logs
- E. threat actor

**Suggested Answer:** CD

Community vote distribution



**mozaki** Highly Voted 1 year, 9 months ago

**Selected Answer:** AE

NIST, defines the assets used in the role of attribution in a cybersecurity investigation as elements that can help identify the threat actor and understand the background circumstances of the incident. According to NIST, these assets include:

Context: This refers to the background information surrounding the incident, such as the time and date of the attack, the type of target, the method of attack, and any other relevant details that can provide insight into the identity of the attacker.

Threat actor: This refers to the individual or group responsible for carrying out the attack. Identifying the threat actor is an essential part of attribution and can help determine the motive behind the attack and the level of sophistication of the attacker.

upvoted 8 times

**halamah** Highly Voted 3 years, 1 month ago

c and d

upvoted 7 times

**036e554** Most Recent 3 weeks, 5 days ago

**Selected Answer:** AE

NIST, defines the assets used in the role of attribution in a cybersecurity investigation as elements that can help identify the threat actor and understand the background circumstances of the incident. According to NIST, these assets include: Context: This refers to the background information surrounding the incident, such as the time and date of the attack, the type of target, the method of attack, and any other relevant details that can provide insight into the identity of the attacker. Threat actor: This refers to the individual or group responsible for carrying out the attack. Identifying the threat actor is an essential part of attribution and can help determine the motive behind the attack and the level of sophistication of the attacker.

upvoted 1 times

**mgo28404** 5 months, 2 weeks ago

**Selected Answer:** DE

Correct Answers: D and E

D. Firewall Logs

Firewall logs contain valuable data about traffic patterns, IP addresses, ports, and protocols used. These logs can help trace malicious activity back to its origin, making them an essential asset in attribution.

E. Threat Actor

Understanding the threat actor—their tactics, techniques, and procedures (TTPs)—is key to attributing an attack to a specific group or individual. This element connects evidence to known attacker profiles, aiding in attribution

upvoted 1 times

**f2354fb** 9 months, 1 week ago

**Selected Answer:** CD

1.8 Describe the role of attribution ("action of bestowing or assigning") in an investigation. (Cyber attribution is the process of tracking, identifying and laying blame on the perpetrator of a cyberattack or other hacking exploit). This a nice read on the problem of attribution.

a. Assets: In information security, computer security and network security, an asset is any data, device, or other component of the environment that supports information-related activities.

b. Threat actor: Responsible for the cyberattack.

<https://vwannabe.com/2018/01/02/ccna-cyber-ops-secops-1-0/>

upvoted 1 times

🗳️ 👤 **RoBery** 11 months, 3 weeks ago

A and E

upvoted 2 times

🗳️ 👤 **sheyshey** 1 year ago

**Selected Answer: CD**

keyword.... assets CD

upvoted 2 times

🗳️ 👤 **ethhacker** 1 year, 4 months ago

I would answer AE, as the question asks for methods to identify the attacker. You would need the context of the attack, methods used, motivation and so on to get a clue if the attacker is motivated by money, political background or other etc... And Threat actor as this helps narrow down the surface of possible attackers

upvoted 4 times

🗳️ 👤 **Max\_DeJaV** 1 year, 3 months ago

I agree with this answer, the word "asset" could lead to a wrong assumptions

upvoted 2 times

🗳️ 👤 **NoorJay** 1 year, 6 months ago

The correct answer is CD.

Role of Attribution in an investigation: Assets, Threat Actor, IOC, Indicator of Attack and Chain of Custody.

upvoted 3 times

🗳️ 👤 **slippery31** 1 year, 7 months ago

Correct ANS= C, D

upvoted 2 times

🗳️ 👤 **itmonkey1** 1 year, 8 months ago

This is from Google:

Assets used in the role of attribution in a cybersecurity investigation as elements that can help identify the threat actor and understand the background circumstances of the incident.

which makes me think that A and E are correct.

upvoted 2 times

🗳️ 👤 **Eng\_ahmedyoussef** 2 years, 2 months ago

**Selected Answer: CD**

C & D are the correct answers.

asset ==> is anything that has value to an organization.

laptop and firewall logs consider an assets in an organization.

upvoted 5 times

🗳️ 👤 **studyelprof** 2 years, 3 months ago

C and D

upvoted 2 times

🗳️ 👤 **studyelprof** 2 years, 3 months ago

Sorry for the above, the correct answer is D and E Threat actor and Firewall log

upvoted 1 times

🗳️ 👤 **addpro7** 2 years, 8 months ago

**Selected Answer: CE**

correct answer : C & E

upvoted 5 times



🗨️ 👤 **Alannn** 3 years, 3 months ago

I think C,D should be correct: An asset is any data, device or other component of an organisation's systems that is valuable – often because it contains sensitive data or can be used to access such information.

For example, an employee's desktop computer, laptop or company phone would be considered an asset, as would applications on those devices. Likewise, critical infrastructure, such as servers and support systems, are assets.

An organisation's most common assets are information assets. These are things such as databases and physical files – i.e. the sensitive data that you store.

upvoted 6 times

🗨️ 👤 **anonymous1966** 3 years, 3 months ago

I believe that only C may be correct.

I understand that the question asks for the definition of "Asset" in the context of attribution in an investigation.

The following are some factors that are used during attribution in an investigation:

Assets, Threat actor, Indicators of Compromise (IoCs), Indicators of Attack (IoAs), Chain of custody

Asset: This factor identifies which assets were compromised by a threat actor or hacker. An example of an asset can be an organization's domain controller (DC) that runs Active Directory Domain Services (AD DS). AD is a service that allows an administrator to manage user accounts, user groups, and policies across a Microsoft Windows environment. Keep in mind that an asset is anything that has value to an organization; it can be something physical, digital, or even people.

Cisco Certified CyberOps Associate 200-201 Certification Guide

By Glen D. Singh

upvoted 2 times

What is personally identifiable information that must be safeguarded from unauthorized access?

- A. date of birth
- B. driver's license number
- C. gender
- D. zip code

**Suggested Answer: B**

🗨️ **weganos** 1 year ago

Personally identifiable information (PII) can be sensitive or non-sensitive.

Sensitive personal information includes legal statistics such as:

Full name

Social Security Number (SSN)

Driver's license

Mailing address

Credit card information

Passport information

Financial information

Medical records

Non-Sensitive PII

Zip code

Race

Gender

Date of birth

Place of birth

Religion

source: <https://www.investopedia.com/terms/p/personally-identifiable-information-pii.asp>

upvoted 2 times

🗨️ **tsabee** 2 years, 2 months ago

On the exam was only one option. So the driver license is the correct answer.

upvoted 2 times

🗨️ **Dunky** 2 years, 7 months ago

Although credit card is not on the list if it was given to the credit card company they could identify you from that 1 piece of information alone as no one else will have that same credit card number. Correct answer Driving License.

upvoted 1 times

🗨️ **Barney\_Stinson** 2 years, 8 months ago

I guess Date of birth and driver license number are both correct...

From 200-201 Training Resources:

Examples of PII data include the following:

Name, such as full name, maiden name, mother's maiden name

Telephone numbers, including home, and mobile numbers

!!!Date and place of birth!!!

Passport number, social security number, !!!driver license number!!!

Personal characteristics, including photographic image [...]

upvoted 4 times



🗨️ **tsabee** 2 years, 2 months ago

I agree with you, there are two reliable sources of answer. And the exam strongly deals with PII.

The National Institute of Standards and Technology (NIST) SP 800-122(4) defines personally identifiable information (PII) as "any information about an individual that is maintained by an agency, including any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information."

- Understanding Cisco Cybersecurity Operations Fundamentals Official Course

upvoted 1 times

  **tsabee** 2 years, 2 months ago



Other:

According to the Executive Office of the President, Office of Management and Budget (OMB), and the U.S. Department of Commerce, Office of the Chief Information Officer, PII refers to "information which can be used to distinguish or trace an individual's identity."

The following are a few examples:



- An individual's name
- Social security number
- Biological or personal characteristics, such as an image of distinguishing features, fingerprints, Xrays, voice signature, retina scan, and the geometry of the face
- Date and place of birth
- Mother's maiden name
- Credit card numbers
- Bank account numbers
- Driver license number
- Address information, such as email addresses or street addresses, and telephone numbers for businesses or personal use
- Cisco CyberOps Associate CBROPS 200-201 Official Cert Guide Omar Santos

upvoted 1 times

  **tsabee** 2 years, 2 months ago



So the right answer is "AB".

upvoted 1 times

  **beowolf** 2 years, 7 months ago

something is not considered as PII unless it is linked to a name. without a name a DOB or credit card number etc is not a PII. Given answer is correct.

upvoted 1 times

  **Dunky** 2 years, 7 months ago

They are all attributes that can be used together to possibly identify you but only the drivers licence on its own from the given list can uniquely identify you as no one else has the same drivers number whereas being male, having a zip code and even your date of birth are not unique to you.

upvoted 2 times

In a SOC environment, what is a vulnerability management metric?

- A. code signing enforcement
- B. full assets scan
- C. internet exposed devices
- D. single factor authentication

**Suggested Answer: C**

Community vote distribution

C (75%)

B (25%)

 **qz999** Highly Voted 2 years, 10 months ago

I agree with C as this is a 'metric', so we're looking for some sort of count rather than a specific vulnerability.  
upvoted 8 times

 **mgo28404** Most Recent 5 months, 2 weeks ago

**Selected Answer: B**

The correct answer is B

Full Assets Scan

Explanation

A vulnerability management metric is a measurable indicator used to evaluate and track the effectiveness of a vulnerability management program. It provides insights into how well an organization identifies, assesses, and mitigates vulnerabilities across its systems.

Why B. Full Assets Scan is Correct:

Conducting a full assets scan is a critical component of vulnerability management. It helps ensure that all assets in the organization are checked for known vulnerabilities, misconfigurations, and compliance issues.

Metrics derived from these scans, such as the number of detected vulnerabilities or the time to remediate them, are key for assessing the state of the organization's security posture.

upvoted 1 times

 **SecurityGuy** 10 months, 2 weeks ago

**Selected Answer: C**

<https://purplesec.us/learn/vulnerability-management-metrics/>

6. Internal Vs External Exposure

Your external internet facing applications inherently are at highest exposure to outside threats compared to internal. An organization should have separate scanners for each environment.

Although an external scan has high priority, internal scans should be prioritized as well due to the potential of a threat actor entering your network and exploiting a threat is always probable.

upvoted 3 times

 **drdecker100** 1 year, 4 months ago

**Selected Answer: B**

A vulnerability management metric is a measure of the effectiveness of an organization's vulnerability management program. Full asset scan is a metric used to evaluate the coverage and accuracy of a vulnerability management program. It measures the percentage of an organization's assets that have been scanned for vulnerabilities.

upvoted 1 times

 **[Removed]** 2 years, 4 months ago



from reading the book i would say B because it talks about scanning all your devices for vulnerabilities not just internet pointing devices. then running a report analysis.

upvoted 2 times

 **halamah** 2 years, 7 months ago

b is correct

upvoted 2 times

  **sakjifs** 3 years, 3 months ago



It's D

upvoted 2 times

  **Dion\_Weby** 2 years, 7 months ago

Well you must study more

upvoted 3 times

  **sakjifs** 3 years, 3 months ago

Sorry, C seems to be the best answer

upvoted 2 times

  **Sun2sun** 2 years ago

You really need to think before posting

upvoted 4 times

A security expert is working on a copy of the evidence, an ISO file that is saved in CDFS format. Which type of evidence is this file?

- A. CD data copy prepared in Windows
- B. CD data copy prepared in Mac-based system
- C. CD data copy prepared in Linux system
- D. CD data copy prepared in Android-based system

**Suggested Answer: C**

Community vote distribution


C (100%)

  **samismayilov** Highly Voted 3 years, 9 months ago



C. CD data copy prepared in Linux system  
upvoted 24 times

  **ckampi** Highly Voted 3 years, 7 months ago

This question is the same than 87, and the answer on that one was C  
upvoted 8 times

  **89ac226** Most Recent 3 weeks, 2 days ago

**Selected Answer: A**  
El formato CDFS (Compact Disc File System) es un sistema de archivos estándar utilizado para discos ópticos como CD-ROMs  
upvoted 1 times

  **phryde** 1 month, 1 week ago

**Selected Answer: A**  
An ISO file that is saved in CDFS format is a CD data copy prepared in Windows.  
Here's why:  
CDFS (Compact Disc File System) is largely synonymous with ISO 9660, which is the international standard for organizing data on CD-ROMs. However, "CDFS" specifically often refers to the Microsoft implementation of ISO 9660, which includes extensions like Joliet (for longer filenames and a wider character set) that are commonly used when burning CDs in Windows.  
While other operating systems (Linux, macOS) can also read and create ISO 9660 images, the term "CDFS format" in this context often specifically points to the way Windows handles CD file systems. DVDs typically use UDF (Universal Disk Format), not CDFS.  
upvoted 1 times

  **mgo28404** 5 months, 2 weeks ago

**Selected Answer: A**  
A. CD data copy prepared in Windows

Explanation:

CDFS (Compact Disc File System) is widely used for managing CD-ROM data, and it is most commonly associated with Windows systems, where it is natively supported for reading ISO 9660 file systems.

While Linux and macOS can also read and write CDFS/ISO 9660 file systems, the question points to the most common use case, which is in a Windows environment.

Why the Other Options Are Incorrect:

B. CD data copy prepared in Mac-based system

Mac systems often use HFS+ or APFS for disk management and do not natively default to CDFS/ISO 9660 unless specifically formatted for compatibility.

C. CD data copy prepared in Linux system (Most Voted)

Linux systems can read and write ISO 9660, but CDFS is not specific to Linux and is less commonly prepared on Linux compared to Windows.

D. CD data copy prepared in Android-based system

Android systems are not typically used to prepare CD data. They lack direct support for handling CDFS/ISO 9660 files natively.  
upvoted 2 times

🗨️ 👤 **Silexis** 11 months ago

This question is an - any selection will match - because the CDFS standard was developed independent of any OS.  
upvoted 1 times

🗨️ 👤 **RoBery** 11 months, 3 weeks ago

A

CDFS (Compact Disc File System) is a file system specifically designed for optical discs like CDs. It is commonly associated with Windows operating systems and may not be the default file system used in Linux.

Linux systems often use the ISO 9660 file system for CD-ROMs and DVDs. ISO 9660 is a standard file system for optical disc media, and it is widely supported across different operating systems, including Linux.

Therefore, if you encounter an ISO file that is saved in CDFS format, it's more likely to be associated with a Windows-based system. For Linux-based systems, ISO 9660 is a more common file system for optical discs.

upvoted 2 times

🗨️ 👤 **AhmedAbdalla** 1 year, 2 months ago

CD data copy prepared in a Linux system

An ISO file saved in CDFS format typically indicates that it was created in a Linux-based system. CDFS stands for "Compact Disc File System," and Linux often uses this format for CD/DVD images. So, the evidence in this case is likely a CD data copy prepared in a Linux system.

upvoted 1 times

🗨️ 👤 **SecurityGuy** 1 year, 4 months ago

**Selected Answer: C**

CDFS - Compact Disc File System

CDFS

- It is a virtual file system for Unix-like operating systems; it provides access to data and audio tracks on Compact Discs.
- When the CDFS driver mounts a Compact Disc, it represents each track as a file.
- This is consistent with the Unix convention "everything is a file".

upvoted 1 times

🗨️ 👤 **slippery31** 1 year, 7 months ago

Correct ANS=C

upvoted 1 times

🗨️ 👤 **GiorTal** 1 year, 10 months ago

**Selected Answer: C**

Linux system

upvoted 1 times

🗨️ 👤 **Eng\_ahmedyoussef** 2 years, 3 months ago

**Selected Answer: C**

CDFS ==> Linux

upvoted 1 times

🗨️ 👤 **DLukynskyy** 2 years, 9 months ago

**Selected Answer: C**

CDFS = Linux

upvoted 2 times

🗨️ 👤 **BobbyYarush** 2 years, 9 months ago

CDFS is not specific to a single Operating System, it means that a disc burned on Macintosh using CDFS can be read on a Windows or Linux based computer. Any input??

upvoted 1 times

🗨️ 👤 **IslamSa** 2 years, 12 months ago

Please ignore my last message, pls clarify answers for ques 113 and 175 , supposed not to be same answer Linux?

upvoted 1 times

🗨️ 👤 **Arrmanas** 1 year, 6 months ago

please think carefully before you post and regret your statement.

upvoted 1 times

🗨️ 👤 **IslamSa** 2 years, 12 months ago

Answer for ques 113 is C but ques 175 is A, please clarify

upvoted 1 times

  **anonymous1966** 3 years, 3 months ago

For certification one should mark "C".

But, of course, any desktop SO can prepare CDFS CD's.

upvoted 6 times



Which two elements of the incident response process are stated in NIST Special Publication 800-61 r2? (Choose two.)

- A. detection and analysis
- B. post-incident activity
- C. vulnerability management
- D. risk assessment
- E. vulnerability scoring

**Suggested Answer:** AB

Community vote distribution

AB (100%)

Eng\_ahmedyoussef 8 months, 3 weeks ago

Selected Answer: AB

A & B is the correct answers

The NIST Incident Response Process contains four steps:

1. Preparation
2. Detection and Analysis
3. Containment, Eradication, and Recovery
4. Post-Incident Activity

upvoted 2 times

Eng\_ahmedyoussef 8 months, 3 weeks ago

Selected Answer: AB

A. detection and analysis

B. post-incident activity

upvoted 1 times

## DRAG DROP -

Drag and drop the definition from the left onto the phase on the right to classify intrusion events according to the Cyber Kill Chain model.

Select and Place:

The threat actor takes actions to violate data integrity and availability.	Exploitation
The targeted environment is taken advantage of triggering the threat actor's code.	Installation
Backdoor is placed on the victim system allowing the threat actor to maintain the persistence.	Command and Control
An outbound connection is established to an Internet-based controller server.	Actions and Objectives

## Suggested Answer:

The threat actor takes actions to violate data integrity and availability.	The targeted environment is taken advantage of triggering the threat actor's code.
The targeted environment is taken advantage of triggering the threat actor's code.	An outbound connection is established to an Internet-based controller server.
Backdoor is placed on the victim system allowing the threat actor to maintain the persistence.	Backdoor is placed on the victim system allowing the threat actor to maintain the persistence.
An outbound connection is established to an Internet-based controller server.	The threat actor takes actions to violate data integrity and availability.

**HarryPotter69** Highly Voted 3 years, 3 months ago

Google Figure 2: Original Lockheed Martin Cyber (Intrusion) Kill Chain - has a very nice image

Based on that I would say

Exploitation - The targeted Environment is taken advantage of triggering the threat actor's code

Installation - Backdoor is placed on the victim system allowing the threat actor to maintain the persistence.

Command and Control - An outbound connection is established to an Internet-based controller server.

Actions and Objectives - The threat actor takes actions to violate data integrity and availability

upvoted 42 times

**Silexis** 11 months ago

At a second thought, I think that the provided solution is correct and you - as well as me - might be wrong.

Backdoors are used for C2C and the initial malware installation - which is not a backdoor - has "called home" signaling the accomplish of its mission - system compromise.

After that, a backdoor was deployed in order to assure persistence and C2C functionality for the attackers

upvoted 1 times

**ethhacker** 1 year, 4 months ago

Agreed.

upvoted 1 times

**[Removed]** Highly Voted 3 years, 3 months ago

I agree with HarryPotter69.

Correct answer is: 2,3,4,1

Exploitation - The targeted Environment is taken advantage of triggering the threat actor's code

Installation - Backdoor is placed on the victim system allowing the threat actor to maintain the persistence.

Command and Control - An outbound connection is established to an Internet-based controller server.

Actions and Objectives - The threat actor takes actions to violate data integrity and availability

upvoted 10 times

🗨️ 👤 **alhamry** Most Recent 1 year, 8 months ago

Exploitation: The targeted environment is taken advantage of triggering the threat actor's code. (key words: ..taken advantage..).

Installation: Backdoor is placed on the victim system allowing the threat actor to maintain the persistence. (key words: ..is placed on..).

Command an Control: An outbound connection is established on an Internet-based controller server. (key words: ..controller server..).

Actions an Objectives: The threat actor takes actions to violate data integrity and availability. (key words: ..takes actions to violate..).

upvoted 3 times

🗨️ 👤 **Eng\_ahmedyoussef** 2 years, 2 months ago

Lockheed Martin Cyber Kill Chain.

1. reconnaissance, 2.weaponization, 3.delivery, 4.exploitation, 5.installation, 6.command and control (C2), 7. actions on objectives

Exploitation ==> The targeted Environment is taken advantage of triggering the threat actor's code.

Installation ==> Backdoor is placed on the victim system allowing the threat actor to maintain the persistence.

Command and Control ==> An outbound connection is established to an Internet-based controller server.

Actions and Objectives ==> The threat actor takes actions to violate data integrity and availability

upvoted 3 times

🗨️ 👤 **COLCRISS** 2 years, 6 months ago

Agrre with mr Harry Potter

upvoted 1 times

🗨️ 👤 **omita** 3 years ago

I agree with harryPotter69.

upvoted 1 times

🗨️ 👤 **CiscoTerminator** 3 years, 2 months ago

2,3,41 is the correct answer

upvoted 3 times

🗨️ 👤 **anonymous1966** 3 years, 3 months ago

For me, the right order is: 4,1,2,3

upvoted 3 times

🗨️ 👤 **qz999** 3 years, 4 months ago

Agree with Barney\_Stinson entry. Backdoor placement is installation and victim outbound connection would be to the CnC server. Middle two items are reversed in the answer given.

upvoted 4 times

🗨️ 👤 **Barney\_Stinson** 3 years, 8 months ago

The answer is shuffled.

e.g. the outbound connection is definitely CnC, not installation

upvoted 5 times

```

PS C:\Program Files (x86)\Nmap> nmap --top-ports 5 172.31.45.240
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-22 22:05 Coordinated Universal Time
'map scan report for ip-172-31-45-240.us-west-2.compute.internal (172.31.45.240)
Host is up (0.00s latency).

PORT      STATE  SERVICE
21/tcp    closed ftp
22/Lt_p   Clusal "It
23/tcp    closed telnet
80/tcp    closed http
443/tcp    closed https

'map done: 1. IP address (1 host up) scanned in 0.19 seconds
Ps C:\Program Files (x86)\Nmap> nmap --top-ports 10 172.31.45.240
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-22 22:05 Coordinated Universal Time
'map scan report for ip-172-31-45-240.us-west-2.compute.internal (172.31.45.240)
Host is up (0.00s latency).

PORT      STATE  SERVICE
21/tcp    closed ftp
22/tcp    closed ssh
23/tcp    closed telnet
25/tcp    closed smtp
80/tcp    closed http
110/tcp   closed pop3

139/tcp   open  netbios-ssn|
443/tcp   closed https
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server

'map done: 1 IP address (1 host up) scanned in 0.19 seconds PS
C:\Program Files (x86)\Nmap>

```

Refer to the exhibit. What does this output indicate?

- A. HTTPS ports are open on the server.
- B. SMB ports are closed on the server.
- C. FTP ports are open on the server.
- D. Email ports are closed on the server.

**Suggested Answer: D**

Community vote distribution

D (80%)

B (20%)

 **SecurityGuy** 10 months, 2 weeks ago

**Selected Answer: D**

What Are Ports 139 And 445?

SMB has always been a network file sharing protocol. As such, SMB requires network ports on a computer or server to enable communication to other systems. SMB uses either IP port 139 or 445.

Port 139 - SMB originally ran on top of NetBIOS using port 139. NetBIOS is an older transport layer that allows Windows computers to talk to each other on the same network.

Port 445 - Later versions of SMB (after Windows 2000) began to use port 445 on top of a TCP stack. Using TCP allows SMB to work over the internet.

<https://www.varonis.com/blog/smb-port>

SMB Ports 139 and 445 are open

Email Ports 25 and 110 are closed

Therefore "D. Email Ports are closed on the Server."

upvoted 3 times

 **GOG097654** 1 year, 4 months ago

**Selected Answer: B**

SMTP and POP3 are closed

upvoted 1 times

🗨️ 👤 **Eng\_ahmedyoussef** 1 year, 8 months ago

**Selected Answer: D**

SMTP and POP3 are closed

upvoted 1 times

🗨️ 👤 **surforlife** 1 year, 12 months ago

B SMB Ports are open!

upvoted 1 times

🗨️ 👤 **Nhendy** 1 year, 11 months ago

B says SMB are closed, they are not closed..

Answer is correct >> D

upvoted 2 times

🗨️ 👤 **Nhendy** 1 year, 11 months ago

SMB ports are 445 and 139 , both open

upvoted 1 times

## DRAG DROP -

Drag and drop the elements from the left into the order for incident handling on the right.

Select and Place:

preparation	create communication guidelines for effective incident handling
containment, eradication, and recovery	gather indicators of compromise and restore the system
post-incident analysis	document information to mitigate similar occurrences
detection and analysis	collect data from systems for further investigation


**Suggested Answer:**

preparation	preparation
containment, eradication, and recovery	containment, eradication, and recovery
post-incident analysis	post-incident analysis
detection and analysis	detection and analysis

  **stickerbombmaster** 9 months, 1 week ago

correct

upvoted 3 times

  **sheyshey** 1 year ago

given answer is correct.

upvoted 2 times

Which metric should be used when evaluating the effectiveness and scope of a Security Operations Center?

- A. The average time the SOC takes to register and assign the incident.
- B. The total incident escalations per week.
- C. The average time the SOC takes to detect and resolve the incident.
- D. The total incident escalations per month.

**Suggested Answer:** C

*Community vote distribution*

C (100%)

🗉 👤 **RoBery** 11 months, 3 weeks ago

C - MTTD: mean time to detect

upvoted 1 times

🗉 👤 **Eng\_ahmedyoussef** 2 years, 2 months ago

**Selected Answer: C**

KPI of SOC ==> The average time the SOC takes to detect and resolve the incident.

upvoted 2 times

🗉 👤 **Eng\_ahmedyoussef** 2 years, 3 months ago

**Selected Answer: C**

correct answer

upvoted 1 times

A developer is working on a project using a Linux tool that enables writing processes to obtain these required results:

- ⇒ If the process is unsuccessful, a negative value is returned.
- ⇒ If the process is successful, 0 value is returned to the child process, and the process ID is sent to the parent process.

Which component results from this operation?

- A. parent directory name of a file pathname
- B. process spawn scheduled
- C. macros for managing CPU sets
- D. new process created by parent process

**Suggested Answer: D**

Community vote distribution

D (100%)

🗳️ 👤 **JohnBB** Highly Voted 👍 3 years ago

Probalby the correct answer is D: D. new process created by parent process  
upvoted 15 times

🗳️ 👤 **drdecker100** Highly Voted 👍 1 year, 4 months ago

**Selected Answer: D**

The Linux tool described in the question is most likely the `fork()` system call, which creates a new process by duplicating the calling process. When `fork()` is called, it returns a process ID (PID) to the parent process and a value of 0 to the child process. If an error occurs during the `fork()` call, a negative value is returned.

Therefore, the operation described in the question results in a new process being created by the parent process, and the process ID being sent to the parent process. This is what the `fork()` system call does in Linux.

upvoted 6 times

🗳️ 👤 **Faio** Most Recent 🕒 9 months ago

The answer is: D. new process created by parent process  
upvoted 1 times

🗳️ 👤 **slippery31** 1 year, 1 month ago

Correct ANS=D  
upvoted 1 times

🗳️ 👤 **Eng\_ahmedyoussef** 1 year, 8 months ago

**Selected Answer: D**

i think that D is the correct answer.  
==> new process created by parent process  
upvoted 1 times

🗳️ 👤 **surforlife** 1 year, 11 months ago

"D"

Does a child process return 0?

Zero: Returned to the newly created child process. Positive value: Returned to parent or caller. The value contains process ID of newly created child process!

upvoted 1 times

🗳️ 👤 **omita** 2 years, 6 months ago

Each unix process has two ID numbers assigned to it: The Process ID (pid) and the Parent process ID (ppid). Each user process in the system has a parent process.

Most of the commands that you run have the shell as their parent. Check the `ps -f` example where this command listed both the process ID and the parent process ID.

upvoted 1 times



🗨️ 👤 **omita** 2 years, 5 months ago

Answer D

upvoted 1 times

🗨️ 👤 **halamah** 2 years, 7 months ago

d is correcxt

upvoted 2 times

🗨️ 👤 **alocin** 2 years, 8 months ago

The spawn(8) daemon provides the Postfix equivalent of inetd. It listens on a port as specified in the Postfix master.cf file and spawns an external command whenever a connection is established. The connection can be made over local IPC (such as UNIX-domain sockets) or over non-local IPC (such as TCP sockets). The command's standard input, output and error streams are connected directly to the communication endpoint

upvoted 1 times

🗨️ 👤 **alocin** 2 years, 8 months ago

There are two tasks with specially distinguished process IDs: swapper or sched has process ID 0 and is responsible for paging, and is actually part of the kernel rather than a normal user-mode process. Process ID 1 is usually the init process primarily responsible for starting and shutting down the system. Originally, process ID 1 was not specifically reserved for init by any technical measures: it simply had this ID as a natural consequence of being the first process invoked by the kernel. More recent Unix systems typically have additional kernel components visible as 'processes', in which case PID 1 is actively reserved for the init process to maintain consistency with older systems

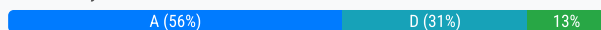
upvoted 1 times

An engineer discovered a breach, identified the threat's entry point, and removed access. The engineer was able to identify the host, the IP address of the threat actor, and the application the threat actor targeted. What is the next step the engineer should take according to the NIST SP 800-61 Incident handling guide?

- A. Recover from the threat.
- B. Analyze the threat.
- C. Identify lessons learned from the threat.
- D. Reduce the probability of similar threats.

**Suggested Answer: A**

Community vote distribution



**Vetterous** Highly Voted 2 years, 11 months ago

Per: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf>

3.3.3 Identifying the Attacking Hosts

3.3.4 Eradication and Recovery

If it were me, I would select A

upvoted 17 times

**tsabee** 2 years, 8 months ago

A is correct.

According to Official Understanding Cisco Cybersecurity Operations Fundamentals Course It has to get answer below question in those state:

Analysis -every question was answered.:

Which networks, systems, or applications are affected? -OK

Who or what originated the incident? -OK

Which tools or attack methods are being used? -OK

Which vulnerabilities are being exploited? -OK

Containment -some questions were answered, and actually it was made a containment action by removed access:

("Decision points for containment may include:")

What is the scope of the incident? -partially OK

What is the type of device? -OK

What is the network reachability of the device that has been affected by the incident?

How quickly can the incident response team get containment in place? - Irrelevant in this situation

How quickly is containment needed? - Irrelevant in this situation

upvoted 3 times

**JayPEI** 2 years ago

discovered a breach, identified the threat's entry point, and !!!removed access!!! means done detection and analysis phase,so should start:

containment, eradication, and recovery phase:

Gathering and handling evidence

Identifying the attacking hosts

Choosing a containment strategy to effectively contain and eradicate the attack, successfully recover from it

upvoted 1 times

**sheyshey** Most Recent 6 months, 4 weeks ago

**Selected Answer: A**

Should b A

upvoted 3 times

**Faio** 9 months, 4 weeks ago

C \*\* Containment:\*\*

According to the NIST SP 800-61 Incident Handling Guide, the incident response process consists of the following phases:

**\*\* Preparation:\*\*** This phase involves establishing incident response policies and procedures, training personnel, and developing communication plans.

**\*\* Identification:\*\*** This phase involves detecting and acknowledging an incident.

**\*\* Containment:\*\*** This phase involves limiting the spread of the incident and preventing further damage.

**\*\* Eradication:\*\*** This phase involves removing the threat actor from the system and restoring the system to normal operations.

**\*\* Recovery:\*\*** This phase involves restoring data and applications that were lost or damaged during the incident.

**\*\* Lessons learned:\*\*** This phase involves identifying what went wrong and how to prevent similar incidents from happening in the future.

upvoted 1 times

🗳️ 👤 **Faio** 9 months, 2 weeks ago

CORRECT ANS= A

upvoted 1 times

🗳️ 👤 **slippery31** 1 year, 1 month ago

CORRECT ANS= A

upvoted 1 times

🗳️ 👤 **alhamry** 1 year, 2 months ago

Option A, "Recover from the threat," refers to the containment, eradication, and recovery phase of incident response, which is already completed in the given scenario since the engineer was able to identify the threat's entry point and remove access. Option D, "Reduce the probability of similar threats," is a proactive measure that should be taken before an incident occurs, rather than a step in the incident handling process.

The next step according to the NIST SP 800-61 Incident handling guide is to analyze the threat, which involves gathering and analyzing information about the incident to determine the cause, scope, and extent of the damage. So the best answer is B.

upvoted 2 times

🗳️ 👤 **MaliDong** 1 year, 7 months ago

Selected Answer: A

the engineer 'identify the .... application the threat actor targeted', means that the 'application' has not been 'fixed/repaired'. Engineer should get that application recovered.

upvoted 3 times

🗳️ 👤 **Eng\_ahmedyoussef** 1 year, 8 months ago

Selected Answer: D

i think D is the correct answer

- the Engineer identified the threat's entry point ==> so he Analyze the threat.

- the engineer removed access ==> so he Recover from the threat.

the next step is to =====>

\*\*\*\* D. Reduce the probability of similar threats. \*\*\*\*

upvoted 4 times

🗳️ 👤 **studylprof** 1 year, 9 months ago

According to NIST 800-61 incident handling life cycle----> After an incident has been contained, eradication may be necessary to eliminate components of the

incident, : Correct answer is A (Eradication and Recovery)

upvoted 1 times

🗳️ 👤 **Entivo** 1 year, 10 months ago

Selected Answer: A

A. Recover from the threat.

B. Analyze the threat.

C. Identify lessons learned from the threat.

D. Reduce the probability of similar threats.

I have just read 800-61r2 and in my opinion the detection and analysis phase is over because the breach has been detected and the threat actor and vector identified. Also, the containment is complete because the engineer removed access, however in the same phase we have "recovery" which has not yet been completed. C & D are both done in the "Post Incident Activity" phase, but as we have not yet recovered from the breach, these cannot be the correct answer. Just my opinion.

upvoted 3 times

🗳️ 👤 **anonymous1966** 1 year, 11 months ago

Selected Answer: C

3. Handling an Incident:

3.1. Preparation (2 items)

3.2. Detection and Analysis (7 items)

3.2.4 Incident Analysis

3.3 Containment, Eradication, and Recovery (4 items)

3.3.4 Eradication and Recovery

3.4 Post-Incident Activity

3.4.1 Lessons Learned <----

3.4.2 Using Collected Incident Data

3.4.3 Evidence Retention

To answer the question you must know in which phase of the Handling an Incident the case is.

The engineer did 3.1, 3.2 and 3.3, so it is now time to 3.4.

So the correct answer is "C"

Ref: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf>

upvoted 2 times

  **adodocletus** 2 years ago

"A" is correct

upvoted 1 times

  **DLukynskyy** 2 years, 3 months ago

**Selected Answer: D**

Check for similar breaches right away

upvoted 1 times

  **[Removed]** 2 years, 4 months ago

so in the question they stated they removed access so that's 1st part, now I'm assuming you should prevent this from happening again. ?? so is answer D or A ? I have test next week.

upvoted 2 times

  **Franky4** 2 years, 6 months ago

D - Reduce the probability of similar threats, could possibly be categorised under 'Eradication'

800.61r2 states the following for Eradication:

"During eradication, it is important to identify all affected hosts within the organization so that they can be remediated."

And in the checklist under the Eradication section



- Identify and mitigate all vulnerabilities that were exploited

- If more affected hosts are discovered (e.g., new malware infections), repeat the Detection and Analysis steps (1.1, 1.2) to identify all other affected hosts, then contain (5) and eradicate (6) the incident for them

Assuming the Detection and Analysis phase has been conducted, and none of the answers fall into the Containment category... Answer (D) might be warranted.



The 'similar' wording in the question makes it difficult to confirm if the aforementioned threats pertain to the impacted network or 'just in general'

upvoted 2 times

  **Jaboori** 2 years, 7 months ago

I think the correct answer is D.

upvoted 1 times

  **Jaboori** 2 years, 7 months ago

Sorry, the correct answer for me is A

according to NIST "In recovery, administrators restore systems to normal operation, confirm that the systems are functioning normally, and (if applicable) remediate vulnerabilities to prevent similar incidents."

So reducing the probability of similar threats is under Recovery.

upvoted 1 times

  **halamah** 2 years, 7 months ago

b is correct

upvoted 1 times

  **shibli\_zahir** 2 years, 7 months ago

so what is the correct answer. please stop confusing me

upvoted 4 times

## DRAG DROP -

Drag and drop the definition from the left onto the phase on the right to classify intrusion events according to the Cyber Kill Chain model.  
Select and Place:

The threat actor engages in identification and selection of targets

reconnaissance

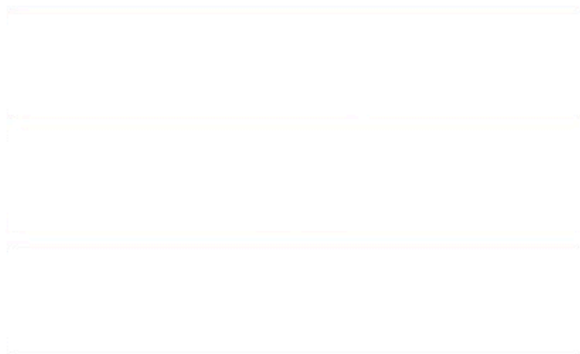
An exploit is coupled with a remote access trojan

weaponization

The weapon is transferred to the target environment

delivery

## Suggested Answer:



The threat actor engages in identification and selection of targets

An exploit is coupled with a remote access trojan

The weapon is transferred to the target environment

 **d503c75** 9 months, 2 weeks ago

The answer is correct.

upvoted 3 times

A user received an email attachment named `Hr402-report3662-empl621.exe` but did not run it. Which category of the cyber kill chain should be assigned to this type of event?

- A. delivery
- B. reconnaissance
- C. weaponization
- D. installation

**Suggested Answer: A**

Reference:

<https://packitforwarding.com/index.php/2019/08/29/ccna-cyberops-secops-objective-5-1-cyber-kill-chain/>

🗨️ 👤 **[Removed]** 1 year, 11 months ago

they stated they did NOT run it, so it cant be installation. I would have to be delivery.  
upvoted 2 times

🗨️ 👤 **ivlis\_27** 2 years, 1 month ago

i think the question is a bit ambiguous?  
which category of the cyber kill chain 'SHOULD BE ASSIGNED' to this type of event?  
if it SHOULD BE ASSIGNED, shouldn't it be installation?  
if it ask which category of the cyber kill chain is perpetrating/ if it ask which step it is, i would answer delivery  
it's my guess  
upvoted 1 times

🗨️ 👤 **ivlis\_27** 2 years, 1 month ago

dont mind my rant, if i look at the step, the next step would be exploitation, then installation. Since exploitation isn't on the option, wouldn't it be installation?  
upvoted 1 times

🗨️ 👤 **MartinRB** 10 months, 2 weeks ago

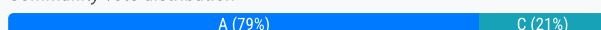
..but did not ran it. So it is delivered but not yet installed.  
upvoted 2 times

An analyst received a ticket regarding a degraded processing capability for one of the HR department's servers. On the same day an engineer noticed a disabled antivirus software and was not able to determine when or why it occurred. According to the NIST Incident Handling Guide, what is the next phase of this investigation?

- A. Analysis
- B. Eradication
- C. Detection
- D. Recovery

**Suggested Answer: A**

Community vote distribution



🗳️ 👤 **CiscoTerminator** Highly Voted 🍌 3 years, 7 months ago

**Selected Answer: A**

This has already been detected - next step is to analyse the incident.

upvoted 8 times

🗳️ 👤 **d503c75** Most Recent ⌚ 9 months, 2 weeks ago

C is the correct answer.

After that, we can move to analysis...

When the team believes that an incident has occurred, the team should rapidly perform an initial analysis to determine the incident's scope, such as which networks, systems, or applications are affected; who or what originated the incident; and how the incident is occurring (e.g., what tools or attack methods are being used, what vulnerabilities are being exploited).

The initial analysis should provide enough information for the team to prioritize subsequent activities, such as containment of the incident and deeper analysis of the effects of the incident.

Source: <https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf>

upvoted 1 times

🗳️ 👤 **JT33333** 1 year, 7 months ago

**Selected Answer: A**

The next phase of the investigation is Analysis according to the NIST Incident Handling Guide .

upvoted 1 times

🗳️ 👤 **Faio** 1 year, 9 months ago

The next phase of the investigation according to the NIST Incident Handling Guide is Analysis.

upvoted 2 times

🗳️ 👤 **blackmetal** 2 years, 1 month ago

**Selected Answer: A**

In the analysis phase, the incident responders would gather and analyze the available information to understand the scope, impact, and cause of the incident. This would involve examining logs, system configurations, and other relevant data to determine the root cause of the degraded processing capability and the reason for the disabled antivirus software.

upvoted 1 times

🗳️ 👤 **Eng\_ahmedyoussef** 2 years, 8 months ago

**Selected Answer: C**

i think correct answer i C. Detection

because the engineer is only has noticed that the antivirus is disabled .. so the next step engineer needs to go to Detection Step.

upvoted 3 times

🗳️ 👤 **Entivo** 2 years, 10 months ago

**Selected Answer: A**

Detection has occurred but detection and analysis are the same phase. As yet no analysis has taken place so I would answer A to this.



upvoted 1 times

🗨️ **surforlife** 2 years, 11 months ago

Both are correct because they go together. Detection and Analysis is the correct answer.

Since degradation was detected, we recommend "A".

upvoted 2 times

🗨️ **ivlis\_27** 3 years, 7 months ago

Incident detection and analysis would be easy if every precursor or indicator were guaranteed to be accurate; unfortunately, this is not the case. For example, user-provided indicators such as a complaint of a server being unavailable are often incorrect. Intrusion detection systems may produce false positives—incorrect indicators. These examples demonstrate what makes incident detection and analysis so difficult: each indicator ideally should be evaluated to determine if it is legitimate. Making matters worse, the total number of indicators may be thousands or millions a day. Finding the real security incidents that occurred out of all the indicators can be a daunting task.

from guide it says this and then,

there's the sentence:

==On the same day an engineer noticed a disabled antivirus software and was not able to determine when or why it occurred. ==

for me it's A because it's already detected.

upvoted 2 times

🗨️ **ivlis\_27** 3 years, 7 months ago

An analyst received a ticket regarding a degraded processing capability for one of the HR department's servers. On the same day an engineer noticed a disabled antivirus software and was not able to determine when or why it occurred. According to the NIST Incident Handling Guide, what is the next phase of this investigation?

supported by the question, i think it's already happened and it's already detected. So the next step is analysis.

because detection is done, if the first sentence isn't part of the question, i would say DETECTION because the engineer only noticed a disabled antivirus, but there's already a proof from the first sentence of "a degraded processing capability" so the next step to be done is not detection again but began documenting the incident which is analysis

upvoted 2 times

🗨️ **halamah** 3 years, 7 months ago

a is correct

upvoted 1 times

🗨️ **AVT** 3 years, 7 months ago

The correct answer is C.

Detection and Analysis>> Create communication guidelines for effective incident handling.

upvoted 2 times

🗨️ **halamah** 3 years, 7 months ago

a is coreect

upvoted 3 times

🗨️ **seriously5000** 3 years, 7 months ago

A. Analysis

The ticket and admin's observation are both forms of Detection of an incident. The next step after an incident is detected is Analysis. Thoughts?

upvoted 2 times