Question #1 *Topic 1*

Thomas, an employee of an organization, is restricted to access specific websites from his office system. He is trying to obtain admin credentials to remove the restrictions. While waiting for an opportunity, he sniffed communication between the administrator and an application server to retrieve the admin credentials. Identify the type of attack performed by Thomas in the above scenario.

A. Vishing

B. Eavesdropping

C. Phishing

D. Dumpster diving

Suggested Answer: *B*

Community vote distribution

B (100%)

Kreno_Maze 11 months, 3 weeks ago

Selected Answer: B

Eavesdropping= Unauthorized

upvoted 1 times

Watchman_Bonda 1 year, 3 months ago

Does any one know what type of Problem based question will be there for CCT

upvoted 1 times

saykre 1 year, 5 months ago

Selected Answer: B

Eavesdropping

upvoted 1 times

RSMCT2011 2 years ago

Selected Answer: B

Eavesdropping Eavesdropping refers to an unauthorized person listening to a conversation or reading others'
messages. It includes the interception of any form of communication, including audio, video, or written, using channels such as telephone lines, email, and instant messaging. An attacker can obtain sensitive information such as passwords, business plans, phone numbers, and addresses

upvoted 1 times

Alvesbtc 2 years, 2 months ago

Eavesdropping

upvoted 2 times

walexo 2 years, 4 months ago

Eavesdropping attack is an attack where the attackers position themselves where they can overhear sensitive information.

upvoted 2 times

Question #2 *Topic 1*

Kayden successfully cracked the final round of interview at an organization. After few days, he received his offer letter through an official company email address. The email stated that the selected candidate should respond within a specified time. Kayden accepted the opportunity and provided e-signature on the offer letter, then replied to the same email address. The company validated the e-signature and added his details to their database. Here, Kayden could not deny company's message, and company could not deny Kayden's signature.
Which of the following information security elements was described in the above scenario?

A. Availability

B. Non-repudiation

C. Integrity

D. Confidentiality

Suggested Answer: *B*

Community vote distribution

B (100%)

⊟ **044f354** 9 months, 2 weeks ago

Selected Answer: B

Certified Cybersecurity Technician Courseware
Module 03 Page 410

Non-repudiation is a way to guarantee that the sender of a message cannot later deny having sent the message and that the recipient cannot deny having received the message. Individuals and organizations use digital signatures to ensure non-repudiation.

upvoted 1 times

⊟ **RSMCT2011** 1 year ago

Selected Answer: B

Explanation:
Non-repudiation is a way to guarantee that the sender of a message cannot later deny having sent the message and that the recipient cannot deny having received the message. Individuals and organizations use digital signatures to ensure non-repudiation.

upvoted 2 times

⊟ **Alvesbtc** 1 year, 2 months ago

Non-Repudiation.
it guarantee that sender of a message cannot later deny having sent the message and that the recipient cannot deny having received the message.

upvoted 1 times

⊟ **walexo** 1 year, 4 months ago

Non-repudiation is simply not being able to deny what you have done because it's on record

upvoted 1 times

Question #3 *Topic 1*

Sam, a software engineer, visited an organization to give a demonstration on a software tool that helps in business development. The administrator at the organization created a least privileged account on a system and allocated that system to Sam for the demonstration. Using this account, Sam can only access the files that are required for the demonstration and cannot open any other file in the system.
Which of the following type of accounts the organization has given to Sam in the above scenario?

A. Service account

B. Guest account

C. User account

D. Administrator account

Suggested Answer: *B*

Community vote distribution

B (100%)

044f354 9 months, 2 weeks ago

Selected Answer: B

Certified Cybersecurity Technician Courseware
Module 04 Page 495

Guest accounts: Guest accounts are least privileged accounts and have no password; they are created to share system resources. These accounts do not have any privileges to modify system files, directories, or settings. Windows automatically configures guest accounts, but they can be enabled or disabled based on preferences. In Linux-based systems, an administrator is required to manually create a guest account after installing the OS. Most web services have default guest accounts that allow users to access web servers without providing credentials.

upvoted 1 times

RSMCT2011 1 year ago

Selected Answer: B

Guest accounts: Guest accounts are least privileged accounts and have no password; they are created to share system resources. These accounts do not have any privileges to modify system files, directories, or settings. Windows automatically configures guest accounts, but they can be enabled or disabled based on preferences. In Linux-based systems, an administrator is required to manually create a guest account after installing the OS. Most web services have default guest accounts that allow users to access web servers without providing credentials.
User accounts: User accounts are the default accounts of operating systems (OSes). User accounts permit individuals to log into the system and access resources. Initially, the system can be accessed by a single account that an administrator creates during the OS installation. These accounts run with the least privileges, with permissions such as running applications/programs and creating and manipulating files that belong to their profile.

upvoted 2 times

Alvesbtc 1 year, 2 months ago

Guest Accounts

upvoted 1 times

bl00d_b0b 1 year, 8 months ago

Selected Answer: B

Guest Accounts
- Least privileged accounts without passwords, created to share system resources
- Do not have any privileges to modify system files, directories, or settings

upvoted 1 times

Question #4 *Topic 1*

Myles, a security professional at an organization, provided laptops for all the employees to carry out the business processes from remote locations. While installing necessary applications required for the business, Myles has also installed antivirus software on each laptop following the company's policy to detect and protect the machines from external malicious events over the Internet.
Identify the PCI-DSS requirement followed by Myles in the above scenario.

A. PCI-DSS requirement no 1.3.2

B. PCI-DSS requirement no 1.3.5

C. PCI-DSS requirement no 5.1

D. PCI-DSS requirement no 1.3.1

Suggested Answer: *C*

Community vote distribution

C (100%)

044f354 9 months, 2 weeks ago

Selected Answer: C

Certified Cybersecurity Technician Courseware
Module 05 Page 511

PCI–DSS requirement no 5.1: “Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).”

upvoted 1 times

Appsec977 1 year, 4 months ago

Such kinda question in CCT ? This ain't CISSP though.

upvoted 1 times

bl00d_b0b 2 years, 8 months ago

Selected Answer: C

PCI–DSS requirement no 5.1: “Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).”

upvoted 4 times

Question #5 *Topic 1*

Ashton is working as a security specialist in SoftEight Tech. He was instructed by the management to strengthen the Internet access policy. For this purpose, he implemented a type of Internet access policy that forbids everything and imposes strict restrictions on all company computers, whether it is system or network usage.
Identify the type of Internet access policy implemented by Ashton in the above scenario.

A. Paranoid policy

B. Prudent policy

C. Permissive policy

D. Promiscuous policy

Suggested Answer: *A*

Community vote distribution

A (100%)

kanchantanwani Highly Voted 👍 1 year, 5 months ago

Promiscuous: No restrictions
Permissive: If something is malicious it's blocked.
Prudent: Restrictive
Paranoid: Highest restrictions

upvoted 6 times

044f354 Most Recent 🕒 9 months, 2 weeks ago

Selected Answer: A

Certified Cybersecurity Technician
Module 05 Page 566

1. Promiscuous Policy: This policy does not impose any restrictions on the usage of system resources.

2. Permissive Policy: This policy is wide open, and only known dangerous services/attacks or behaviors are blocked.

3. Paranoid Policy: A paranoid policy forbids everything. There is a strict restriction on all company computers, whether it is system or network usage. There is either no Internet connection or severely limited Internet usage. Users often try to circumvent such severe restrictions.

4. Prudent Policy: A prudent policy starts with all services blocked. The security professionals enables safe and necessary services individually.

upvoted 1 times

RSMCT2011 1 year ago

Selected Answer: A

Paranoid Policy: A paranoid policy forbids everything. There is a strict restriction on all company computers, whether it is system or network usage. There is either no Internet connection or severely limited Internet usage. Users often try to circumvent such severe restrictions.

upvoted 1 times

Question #6 *Topic 1*

Zion belongs to a category of employees who are responsible for implementing and managing the physical security equipment installed around the facility. He was instructed by the management to check the functionality of equipment related to physical security.
Identify the designation of Zion.

A. Supervisor

B. Chief information security officer

C. Guard

D. Safety officer

Suggested Answer: *D*

Community vote distribution

D (100%)

044f354 9 months, 2 weeks ago

Selected Answer: D

Certified Cybersecurity Technician
Module 06 Page 640

Safety officers: Their responsibilities include implementing and managing safety-related equipment installed around the facility and ensuring the proper functioning of this equipment.

upvoted 1 times

bootleg 1 year, 1 month ago

key word is implementing. It's the Safety Officer.

upvoted 1 times

lamuzu 1 year, 3 months ago

Selected Answer: D

A Safety officer is typically responsible for ensuring the proper functioning of physical security measures, including equipment like cameras, access control systems, and other security devices within a facility.

upvoted 1 times

chiweta 1 year, 11 months ago

The system says Guard

upvoted 1 times

RSMCT2011 2 years ago

Selected Answer: D

Safety officers: Their responsibilities include implementing and managing safety-related equipment installed around the facility and ensuring the proper functioning of this equipment

upvoted 2 times

> **chiweta** 1 year, 11 months ago
>
> i thought its D but in the Quiz its saying Guard
>
> upvoted 1 times

duke_of_kamulu 2 years ago

safety officer is the correct answer on page 640 about security personnel

upvoted 3 times

Ahmed3yad 2 years, 2 months ago

Safety officer.
Module 6 CCT. Page 640

upvoted 3 times

Ahmed3yad 2 years, 2 months ago

Selected Answer: D

because guard cannot manage.

upvoted 1 times

⊟ **AmesCB** 2 years, 2 months ago

Answer is D

upvoted 1 times

Question #7 *Topic 1*

In an organization, all the servers and database systems are guarded in a sealed room with a single entry point. The entrance is protected with a physical lock system that requires typing a sequence of numbers and letters by using a rotating dial that intermingles with several other rotating discs.
Which of the following types of physical locks is used by the organization in the above scenario?

A. Digital locks

B. Combination locks

C. Mechanical locks

D. Electromagnetic locks

Suggested Answer: *B*

Community vote distribution

B (100%)

044f354 9 months, 2 weeks ago

Selected Answer: B

Certified Cybersecurity Technician
Module 06 Page 643

Combination locks: These require the user to provide a combination of numbers and letters to unlock. Users may enter the combination sequence either through a keypad or by using a rotating dial that intermingles with several other rotating discs. Combination locks do not use keys for functioning.

upvoted 1 times

RSMCT2011 1 year ago

Selected Answer: B

Combination locks: These require the user to provide a combination of numbers and letters to unlock. Users may enter the combination sequence either through a keypad or by using a rotating dial that intermingles with several other rotating discs. Combination locks do not use keys for functioning.

upvoted 1 times

Question #8 *Topic 1*

Lorenzo, a security professional in an MNC, was instructed to establish centralized authentication, authorization, and accounting for remote-access servers. For this purpose, he implemented a protocol that is based on the client-server model and works at the transport layer of the OSI model.

Identify the remote authentication protocol employed by Lorenzo in the above scenario.

A. SNMPv3

B. RADIUS

C. POP3S

D. IMAPS

Suggested Answer: *B*

Community vote distribution

B (100%)

044f354 9 months, 2 weeks ago

Selected Answer: B

Certified Cybersecurity Technician

Module 07 Page 682

RADIUS: The RADIUS protocol provides centralized authentication, authorization, and accounting (AAA) for remote-access servers to communicate with a central server.

upvoted 1 times

Kreno_Maze 11 months, 3 weeks ago

Selected Answer: B

RADIUS (Remote Authentication Dial-In User Service)

upvoted 1 times

RSMCT2011 1 year ago

Selected Answer: B

RADIUS: The RADIUS protocol provides centralized authentication, authorization, and accounting (AAA) for remote-access servers to communicate with a central server.

upvoted 1 times

MERMER1 1 year, 3 months ago

Remote Authentication Dial-In User Service is a networking protocol that provides centralized authentication, authorization, and accounting management for users who connect and use a network service.

upvoted 1 times

Question #9 *Topic 1*

Malachi, a security professional, implemented a firewall in his organization to trace incoming and outgoing traffic. He deployed a firewall that works at the session layer of the OSI model and monitors the TCP handshake between hosts to determine whether a requested session is legitimate.
Identify the firewall technology implemented by Malachi in the above scenario.

A. Next generation firewall (NGFW)

B. Circuit-level gateways

C. Network address translation (NAT)

D. Packet filtering

Suggested Answer: *B*

Community vote distribution

B (100%)

044f354 9 months, 2 weeks ago

Selected Answer: B

Certified Cybersecurity Technician
Module 07 Page 773

Circuit level gateways work at the session layer of the OSI model, or the TCP layer of TCP/IP. They monitor the TCP handshake between packets to determine whether a requested session is legitimate or not. Information passed to a remote computer through a circuit-level gateway appears to have originated from the gateway.

upvoted 1 times

RSMCT2011 1 year ago

Selected Answer: B

Circuit level gateways work at the session layer of the OSI model, or the TCP layer of TCP/IP. They monitor the TCP handshake between packets to determine whether a requested session is legitimate or not. Information passed to a remote computer through a circuit-level gateway appears to have originated from the gateway.

upvoted 2 times

Question #10 *Topic 1*

Rhett, a security professional at an organization, was instructed to deploy an IDS solution on their corporate network to defend against evolving threats. For this purpose, Rhett selected an IDS solution that first creates models for possible intrusions and then compares these models with incoming events to make detection decisions.
Identify the detection method employed by the IDS solution in the above scenario.

A. Not-use detection

B. Protocol anomaly detection

C. Anomaly detection

D. Signature recognition

Suggested Answer: *C*

Community vote distribution

C (67%) D (33%)

044f354 9 months, 2 weeks ago

Selected Answer: C

Certified Cybersecurity Technician
Module 07 Page 811

Anomaly-based IDS: An anomaly-based IDS uses statistical techniques to compare the monitored traffic with the normal traffic.

upvoted 1 times

Raypapi 10 months ago

Selected Answer: C

The correct answer is C. Anomaly detection.

Rhett's description of the IDS solution, which creates models for possible intrusions and compares them with incoming events to make detection decisions, matches the concept of anomaly detection. This method involves identifying patterns or behavior that deviate from normal activity on the network, indicating potential intrusions or malicious activity.

upvoted 1 times

ChR0m15 10 months, 2 weeks ago

Selected Answer: C

Signature recognition – Signature-based detection relies on matching incoming events with known attack patterns or signatures. The scenario describes an IDS that creates models for normal behavior rather than matching with predefined signatures, so this is not the correct choice.

upvoted 1 times

ChR0m15 10 months, 2 weeks ago

Selected Answer: C

In Anomaly detection, the IDS (Intrusion Detection System) first creates baseline models for what is considered normal behavior within the network. It then compares incoming events or traffic against these models to detect deviations or anomalies, which could indicate potential intrusions or attacks. This method helps detect previously unknown or evolving threats, as it doesn't rely on pre-defined attack signatures, but rather identifies unusual patterns that differ from the baseline.

upvoted 1 times

lucy11111 1 year, 2 months ago

The use of "evolving threats" makes all the difference. It's Anomaly Detection since signature detection are used for currently known intrusion unlike anomaly which is used for not known or evolving threat.

upvoted 1 times

NetworkH 1 year, 2 months ago

It is signature based. On page 814 in the EC Council Study guide it says this verbatim

upvoted 1 times

sfsc91 1 year, 7 months ago

Selected Answer: C

Signature recognition involves comparing network traffic or system activity against a database of known attack patterns or signatures. While effective at detecting known threats, signature recognition is not suitable for identifying new or evolving threats that do not match any existing signatures. Therefore, in this case, since the threat is evolving, Anomaly detection is the correct answer because the IDS is looking for deviations from normal behavior rather than specific known signatures of attacks.

upvoted 1 times

MPA3333 1 year, 8 months ago

Page 814 : it's signature-based recognition D

upvoted 1 times

bracokey 1 year, 11 months ago

From the EC CCT book, signature recongition '... This technique involves first creating models of possible intrusions and then comparing these models with incoming events to make a detection decision. ..'

upvoted 1 times

duke_of_kamulu 2 years ago

KEY WORD "defend against evolving threats" that is when anomaly comes in otherwise it could be signature based but that puts the difference

upvoted 2 times

RSMCT2011 2 years ago

Selected Answer: D

Signature Recognition

Signature recognition, also known as misuse detection, tries to identify events that indicate an abuse of a system or network. This technique involves first creating models of possible intrusions and then comparing these models with incoming events to make a detection decision. The signatures for IDS were created under the assumption that the model must detect an attack without disturbing normal system traffic. Only attacks should match the model; otherwise, false alarms could occur.

upvoted 2 times

kikkie 2 years, 1 month ago

Signature based.

Signature-based detection is typically best used for identifying known threats. It operates by using a pre-programmed list of known threats and their indicators of compromise (IOCs) while anomaly-based intrusion detection systems can alert you to suspicious behavior that is unknown.

upvoted 1 times

KnifeRing 2 years, 1 month ago

Answer Signature recognition

This technique involves first creating models of possible intrusions and then comparing these models with incoming events to make a detection decision. The signatures for IDS were created under the assumption that the model must detect an attack without disturbing normal system traffic.

upvoted 2 times

AmesCB 2 years, 2 months ago

Answer is definitely signature recognition

upvoted 2 times

Munyasa 2 years, 4 months ago

This looks like signature recognition

upvoted 1 times

kanchantanwani 2 years, 4 months ago

Selected Answer: C

Anomaly-based detection is correct: The anomaly-based detection process depends on observing and comparing the observed events with the normal behavior and then detecting any deviation from it.

upvoted 1 times

kanchantanwani 2 years, 5 months ago

I think it's Signature Detection too

upvoted 2 times

Question #11 *Topic 1*

Richards, a security specialist at an organization, was monitoring an IDS system. While monitoring, he suddenly received an alert of an ongoing intrusion attempt on the organization's network. He immediately averted the malicious actions by implementing the necessary measures.
Identify the type of alert generated by the IDS system in the above scenario.

A. True positive

B. True negative

C. False negative

D. False positive

Suggested Answer: *A*

Community vote distribution

A (100%)

kikkie Highly Voted 1 year, 1 month ago

True Positive -There is an attack and alert.

upvoted 5 times

Sego87 Most Recent 9 months ago

Selected Answer: A

True positive:there is an attack that triggered an alarm

upvoted 1 times

044f354 9 months, 2 weeks ago

Selected Answer: A

Certified Cybersecurity Technician
Module 07 Page 859

True Positive (Attack - Alert): A true positive is a condition that occurs when an event triggers an alarm and causes the IDS to react as if a real attack is in progress.

False Positive (No attack - Alert): A false positive occurs if an event triggers an alarm when no actual attack is in progress.

False Negative (Attack - No Alert): A false negative is a condition that occurs when an IDS fails to react to an actual attack event.

True Negative (No attack - No Alert): A true negative is a condition that occurs when an IDS identifies an activity as acceptable behavior, and the activity is acceptable.

upvoted 1 times

Raypapi 10 months ago

Selected Answer: A

The correct answer is A. True positive.

A true positive occurs when an IDS correctly identifies a genuine threat or intrusion attempt, as described in Richards' scenario. The IDS system detected the ongoing intrusion attempt and alerted Richards to take necessary measures to mitigate the threat, indicating a high degree of accuracy and effectiveness.

upvoted 1 times

Narasimha559 11 months, 2 weeks ago

Selected Answer: A

Since the attack and alert are ture it is True Positive

upvoted 1 times

Question #12 *Topic 1*

Karter, a security professional, deployed a honeypot on the organization's network for luring attackers who attempt to breach the network. For this purpose, he configured a type of honeypot that simulates a real OS as well as applications and services of a target network. Furthermore, the honeypot deployed by Karter only responds to preconfigured commands.
Identify the type of Honeypot deployed by Karter in the above scenario.

A. Low-interaction honeypot

B. Pure honeypot

C. Medium-interaction honeypot

D. High-interaction honeypot

Suggested Answer: *C*

Community vote distribution

C (94%) 6%

⊟ **Sego87** 9 months ago

Selected Answer: C

Certified Cybersecurity Technician Courseware
Module 07 Page 871-872

upvoted 1 times

⊟ **044f354** 9 months, 2 weeks ago

Selected Answer: C

Certified Cybersecurity Technician Courseware
Module 07 Page 871-872

Low-interaction Honeypots
Low-interaction honeypots emulate only a limited number of services and applications of a target system or network.

Medium-interaction Honeypots
Medium-interaction honeypots simulate a real OS as well as applications and services of a target network.

High-Interaction Honeypots
Unlike their low-and medium-interaction counterparts, high-interaction honeypots do not emulate anything; they run actual vulnerable services or software on production systems with real OS and applications.

Pure Honeypots
Pure honeypots emulate the real production network of a target organization.

upvoted 1 times

⊟ **Raypapi** 10 months ago

Selected Answer: D

The correct answer is D. High-Interaction Honeypot.

Karter's deployment of a honeypot that simulates a real OS, applications, and services of the target network suggests a high level of interaction between the honeypot and potential attackers. This type of honeypot aims to provide a realistic environment for attackers to interact with, making it more likely that they will reveal their intentions and methods.

upvoted 1 times

⊟ **duke_of_kamulu** 1 year ago

Selected Answer: C

Medium-interaction honeypots simulate a real OS as well as applications and services of a target network. They provide greater misconception of an OS than low-interaction honeypots. Therefore, it is possible to log and analyze more complex attacks. These honeypots capture more useful data than low-interaction honeypots. They can only respond to preconfigured commands; therefore, the risk of intrusion increases.

upvoted 2 times

aman_baik 1 year, 1 month ago

Selected Answer: C

Module 07 Page 871 Types of Honeypots

Medium-interaction honeypots simulate a real OS as well as applications and services of a target network. They can only respond to preconfigured commands; therefore, the risk of intrusion increases.

upvoted 2 times

KnifeRing 1 year, 1 month ago

Medium Interaction: simulate a real OS as well as applications and services of a target network. They provide greater misconception of an OS than low-interaction honeypots. Therefore, it is possible to log and analyze more complex attacks. These honeypots capture more useful data than low-interaction honeypots. They can only respond to preconfigured commands;

upvoted 2 times

duke_of_kamulu 1 year, 3 months ago

medium is correct answer

upvoted 1 times

kanchantanwani 1 year, 5 months ago

Selected Answer: C

Low-interaction: These simulate only a limited # of services & applications of a target system or network

Medium-interation: These honeypots simulate a real operating system, applications, and services of a target network

High-interaction: these honeypots simulate all services and applications of a target network

Pure honeypots: these honeypots emulate the real production network of a target organization

upvoted 4 times

bivixa2510 1 year, 5 months ago

Selected Answer: C

Medium-interaction Honeypots: These honeypots simulate a real operating system, applications, and services of a target network

Correct Answer: C

upvoted 1 times

keloki2020 1 year, 6 months ago

This is actually a Medium Interaction Honeypot.

upvoted 2 times

jRoger14 1 year, 10 months ago

Selected Answer: C

Focus on question phrase: "simulates a real OS ". About official documentation, only Medium-interaction honeypot simulates real Operating System.

upvoted 4 times

Question #13 *Topic 1*

An MNC hired Brandon, a network defender, to establish secured VPN communication between the company's remote offices. For this purpose, Brandon employed a VPN topology where all the remote offices communicate with the corporate office but communication between the remote offices is denied.
Identify the VPN topology employed by Brandon in the above scenario.

A. Point-to-Point VPN topology

B. Star topology

C. Hub-and-Spoke VPN topology

D. Full-mesh VPN topology

Suggested Answer: *B*

Community vote distribution

B (67%) C (33%)

044f354 9 months, 2 weeks ago

Selected Answer: B

EC Council Certified Cybersecurity Technician Courseware
Module 07 Page 940-948

Hub-and-Spoke VPN Topology In hub-and-spoke technology, the main organization is considered the hub, and its remote offices are considered the spokes. The spokes access the VPN through the hub.

Point-to-Point VPN Topology In a point-to-point topology, any two end points are considered as peer devices that can communicate with each other. Any of the devices can be used to initiate the connection.

Full Mesh VPN Topology In a fully meshed VPN network, all peers can communicate with each other, making it a complex network. This topology is suitable for complicated networks where all peers communicate with one another.

[CORRECT] Star Topology
This is the most commonly used topology in organizations. In this topology, all the remote offices communicate with the corporate office, but communication between the remote offices is denied.

upvoted 1 times

ChR0m15 10 months, 2 weeks ago

Selected Answer: C

In a Hub-and-Spoke VPN topology, all remote offices (spokes) connect to a central corporate office (hub), but communication between the remote offices (spokes) is typically not allowed. This setup is commonly used for organizations where all remote offices need to access centralized resources at the corporate office, but direct communication between remote offices is unnecessary or undesirable for security or operational reasons.

upvoted 1 times

iitc_duo 1 year, 5 months ago

B. Star Topology (CCTv1 book Page No: 947)

upvoted 2 times

Markwest100 1 year, 5 months ago

Selected Answer: C

C. Hub-and-Spoke VPN topology

Here's why:

Point-to-Point VPN: This connects two individual points, not ideal for multiple remote offices.
Full-mesh VPN: This creates a complex network where all offices connect directly with each other, unnecessary in this scenario.
Star topology: In a star topology, all remote offices connect to a central hub, which could be the corporate office. However, it doesn't explicitly restrict communication between remote offices.

Hub-and-Spoke VPN: This topology perfectly fits the scenario. It creates a central hub (corporate office) where all remote offices connect (spokes). This allows communication between remote offices and the central office but restricts communication directly between remote offices.

upvoted 1 times

BurntCanary 1 year, 8 months ago

Star Topology. This topology allows the branches to communicate with the headquarters, however, Interconnection between branches is not allowed.

upvoted 1 times

bracokey 1 year, 11 months ago

From the CCT book, Star topology ...'This is the most commonly used topology in organizations. In this topology, all the remote offices communicate with the corporate office, but communication between the remote offices is denied. '...

upvoted 2 times

aovshine 1 year, 11 months ago

The Hub-and-Spoke and star topology look the same in terms of communications but the question is asking for VPN topology, I think C is the answer as Star topology does not have VPN in the answer.

upvoted 1 times

RSMCT2011 2 years ago

Selected Answer: C

Explanation:

Hub-and-Spoke VPN Topology In hub-and-spoke technology, the main organization is considered the hub, and its remote offices are considered the spokes. The spokes access the VPN through the hub. This topology is mainly used in banking and international organizations. The hub controls the following two types of communication:

 Communication between a spoke and hub

 Communication between spokes

upvoted 2 times

RSMCT2011 2 years ago

Sorry, correction<BR>

More correct Answer is B.

Star Topology

This is the most commonly used topology in organizations. In this topology, all the remote offices communicate with the corporate office, <B>but communication between the remote offices is denied<B>. Each device on the network is connected to a central hub that manages the traffic through the network.

upvoted 2 times

kikkie 2 years, 1 month ago

Star Topology

upvoted 1 times

aman_baik 2 years, 1 month ago

Selected Answer: B

Star Topology

This is the most commonly used topology in organizations.

upvoted 3 times

AmesCB 2 years, 2 months ago

Answer Start topology

upvoted 1 times

duke_of_kamulu 2 years, 3 months ago

it is star topology

upvoted 2 times

kanchantanwani 2 years, 5 months ago

Selected Answer: B

Star Topology: Interconnection between branches is not allowed

upvoted 1 times

bivixa2510 2 years, 5 months ago

Star Topology. From courseware: Interconnection between branches is not allowed

upvoted 1 times

⊟ **keloki2020** 2 years, 6 months ago

Star Topology. From courseware: Interconnection between branches is not allowed

upvoted 2 times

⊟ **LPD** 2 years, 11 months ago

Selected Answer: B

Not hub and spoke.

upvoted 3 times

Question #14 Topic 1

Mark, a security analyst, was tasked with performing threat hunting to detect imminent threats in an organization's network. He generated a hypothesis based on the observations in the initial step and started the threat hunting process using existing data collected from DNS and proxy logs.
Identify the type of threat hunting method employed by Mark in the above scenario.

A. Entity-driven hunting

B. TTP-driven hunting

C. Data-driven hunting

D. Hybrid hunting

Suggested Answer: *C*

Community vote distribution

C (100%)

044f354 9 months, 2 weeks ago

Selected Answer: C

Certified Cybersecurity Technician Courseware
Module 08 Page 1017

Data-driven Hunting: Generating a hypothesis from observations is the initial step in hunting activities. It is a simple process of searching for what analysts can hunt from existing data. Organizations check DNS data and proxy logs for hunting.

upvoted 1 times

kikkie 1 year, 1 month ago

Data -driven hunting
CCT
Module 8 ,page 1017 -Types of threat hunting Methods

upvoted 3 times

Question #15 *Topic 1*

An organization hired a network operations center (NOC) team to protect its IT infrastructure from external attacks. The organization utilized a type of threat intelligence to protect its resources from evolving threats. The threat intelligence helped the NOC team understand how attackers are expected to perform an attack on the organization, identify the information leakage, and determine the attack goals as well as attack vectors.
Identify the type of threat intelligence consumed by the organization in the above scenario.

A. Operational threat intelligence

B. Strategic threat intelligence

C. Technical threat intelligence

D. Tactical threat intelligence

Suggested Answer: *D*

Community vote distribution

D (71%) A (29%)

⊟ **bkob** Highly Voted 2 years, 4 months ago

It is Tactical Threat Intelligence

upvoted 8 times

⊟ **044f354** Most Recent 9 months, 2 weeks ago

Selected Answer: D

Certified Cybersecurity Technician Courseware
Module 08 Page 1029

Tactical Threat Intelligence Tactical threat intelligence plays a major role in protecting the resources of the organization. It provides information related to TTPs used by threat actors (attackers) to perform attacks. Tactical threat intelligence is consumed by cyber security professionals such as IT service managers, security operations managers, network operations center (NOC) staff, administrators, and architects. It helps the cyber security professionals understand how the adversaries are expected to perform the attack on the organization, identify the information leakage from the organization, and the technical capabilities and goals of the attackers along with the attack vectors.

upvoted 1 times

⊟ **kikkie** 1 year, 3 months ago

Tactical threat intelligence-Module 8 CCT -page 1029

upvoted 1 times

⊟ **a613c45** 1 year, 6 months ago

Technical threat intelligence focuses on particular indicators or proof of an attack and serves as a foundation for analyzing such incidents. An analyst from Threat Intelligence looks for indicators of compromise (IOCs) and command and control channels, tools, etc., including reported IP addresses, phishing email content, malware samples, and bogus URLs. Because IOCs like rogue IPs or fraudulent URLs become outdated in a matter of days, communicating technical intelligence at the right time is crucial.

upvoted 2 times

⊟ **KnifeRing** 1 year, 7 months ago

Tactical is the answer:
It helps the cyber security professionals understand how the adversaries are expected to perform the attack on the organization, identify the information leakage from the organization, and the technical capabilities and goals of the attackers along with the attack vectors. Using tactical threat intelligence security personnel develop detection and mitigation strategies beforehand by updating security products with identified indicators, patching vulnerable systems,

upvoted 3 times

⊟ **pepcyber** 1 year, 8 months ago

This is Tactical

upvoted 1 times

⊟ **AmesCB** 1 year, 8 months ago

Definitely Tactical Threat intelligence

upvoted 2 times

duke_of_kamulu 1 year, 9 months ago

tactical intelligence

upvoted 2 times

kanchantanwani 1 year, 10 months ago

Tactical Threat Intelligence: Tactical threat intelligence plays a major role in protecting the resources of the organization. It provides information related to TTPs used by threat actors (attackers) to perform attacks. Tactical threat intelligence is consumed by cyber security professionals such as IT service managers, security operations managers, network operations center (NOC) staff, administrators, and architects. It helps the cyber security professionals understand how the adversaries are expected to perform the attack on the organization, identify the information leakage from the organization, and the technical capabilities and goals of the attackers along with the attack vectors. Using tactical threat intelligence security personnel develop detection and mitigation strategies beforehand by updating security products with identified indicators, patching vulnerable systems, etc. The collection sources for tactical threat intelligence include campaign reports, malware, incident reports, attack group reports, human intelligence, etc.

upvoted 4 times

bivixa2510 1 year, 11 months ago

Selected Answer: D

Tactical (Low Level)

Information on attacker's tactics, techniques, and procedures (TIPS)

Consumed by IT Service and Managers, Administrators

upvoted 4 times

LPD 2 years, 5 months ago

Selected Answer: A

This is operational threat.

upvoted 2 times

Question #16 *Topic 1*

Tristan, a professional penetration tester, was recruited by an organization to test its network infrastructure. The organization wanted to understand its current security posture and its strength in defending against external threats. For this purpose, the organization did not provide any information about their IT infrastructure to Tristan. Thus, Tristan initiated zero-knowledge attacks, with no information or assistance from the organization.
Which of the following types of penetration testing has Tristan initiated in the above scenario?

A. Black-box testing

B. White-box testing

C. Gray-box testing

D. Translucent-box testing

Suggested Answer: *A*

Community vote distribution

A (100%)

044f354 9 months, 2 weeks ago

Selected Answer: A

EC-Council Official Curricula
Certified Cybersecurity Technician v1
https://online.vitalsource.com/reader/books/9781635679533/

Module 08 Page 1109

Black-box testing
To simulate real-world attacks and minimize false positives, penetration testers can choose to undertake black-box testing (or zero-knowledge attack, with no information or assistance from the client) and map the network while enumerating services, shared file systems, and operating systems (OSes) discreetly.

upvoted 1 times

> **044f354** 9 months, 2 weeks ago
>
> CORRECTION TO PAGE NUMBER:
>
> Module 09 Page 1152
>
> upvoted 1 times
>
> > **044f354** 9 months, 2 weeks ago
> >
> > Nevermind. The first page number (1109) is accurate.
> > I just confused myself, sorry all.
> >
> > upvoted 1 times

c9abb92 1 year, 1 month ago

Its A, Black-box testing

upvoted 1 times

RSMCT2011 2 years ago

Selected Answer: A

Black-box testing To simulate real-world attacks and minimize false positives, penetration testers can choose to undertake black-box testing (or zero-knowledge attack, with no information or assistance from the client) and map the network while enumerating services, shared file systems, and operating systems (OSes) discreetly.

upvoted 1 times

Question #17 *Topic 1*

Miguel, a professional hacker, targeted an organization to gain illegitimate access to its critical information. He identified a flaw in the end-point communication that can disclose the target application's data.
Which of the following secure application design principles was not met by the application in the above scenario?

A. Secure the weakest link

B. Do not trust user input

C. Exception handling

D. Fault tolerance

Suggested Answer: *A*

Community vote distribution

A (100%)

kanchantanwani Highly Voted 1 year, 11 months ago

Selected Answer: A

The correct answer is A: Secure the weakest link
Attackers target a system that is easy to penetrate. For example, to gain access to the encrypted data on the network, attackers will not intercept the data and crack encryption; instead they will go after the end points of communication to find a flaw that discloses the data. Identify and strengthen the areas at risk until levels of risk are satisfactory.
Source: EC Council - C|CT: Courseware Module 9 - Understand Secure Application Design & Architecture - Define Secure Design Principles

upvoted 5 times

044f354 Most Recent 9 months, 2 weeks ago

Selected Answer: A

EC-Council Official Curricula
Certified Cybersecurity Technician v1
https://online.vitalsource.com/reader/books/9781635679533/

Module 09 Page 1152

Secure the weakest link
Attackers target a system that is easy to penetrate. For example, to gain access to the encrypted data on the network, attackers will not intercept the data and crack encryption; instead they will go after the end points of communication to find a flaw that discloses the data. Identify and strengthen the areas at risk until levels of risk are satisfactory.

upvoted 1 times

jamiekji 1 year, 2 months ago

Selected Answer: A

Secure the weakest link

upvoted 1 times

aman_baik 1 year, 7 months ago

Selected Answer: A

Secure the weakest link. Module 09 Page 1152.

upvoted 4 times

AmesCB 1 year, 8 months ago

Secure the weakest link

upvoted 2 times

pepcyber 1 year, 8 months ago

Secure the weakest Link A

upvoted 3 times

Question #18 *Topic 1*

A software company is developing a new software product by following the best practices for secure application development. Dawson, a software analyst, is checking the performance of the application on the client's network to determine whether end users are facing any issues in accessing the application.
Which of the following tiers of a secure application development lifecycle involves checking the performance of the application?

A. Development

B. Testing

C. Quality assurance (QA)

D. Staging

Suggested Answer: *C*

Community vote distribution

C (100%)

bivixa2510 Highly Voted 👍 1 year, 5 months ago

Selected Answer: C

Quality Assurance (QA): Testers perform quality checks on the deployed software to check whether end users face any issue in accessing the application

Correct Answer: C

upvoted 5 times

044f354 Most Recent 🕘 9 months, 2 weeks ago

Selected Answer: C

EC-Council Official Curricula
Certified Cybersecurity Technician v1
https://online.vitalsource.com/reader/books/9781635679533/

Module 09 Page 1183

Quality Assurance (QA): In this phase, the application's performance is monitored, and its quality is evaluated in the end users' network. Testers perform quality checks on the deployed software to determine whether end users face any issue in accessing the application.

upvoted 1 times

AmesCB 1 year, 2 months ago

Quality Assurance is the answer

upvoted 1 times

pepcyber 1 year, 2 months ago

Quality Assurance is correct, because we have passed the development stages

upvoted 3 times

duke_of_kamulu 1 year, 3 months ago

it should be Quality assurance cct module 9 page 1182/83

upvoted 2 times

bkob 1 year, 10 months ago

Selected Answer: C

It Quality check, because testing is done indevelopment & staging

upvoted 2 times

Question #19 *Topic 1*

Nicolas, a computer science student, decided to create a guest OS on his laptop for different lab operations. He adopted a virtualization approach in which the guest OS will not be aware that it is running in a virtualized environment. The virtual machine manager (VMM) will directly interact with the computer hardware, translate commands to binary instructions, and forward them to the host OS.
Which of the following virtualization approaches has Nicolas adopted in the above scenario?

A. Hardware-assisted virtualization

B. Full virtualization

C. Hybrid virtualization

D. OS-assisted virtualization

Suggested Answer: *B*

Community vote distribution

B (60%) D (40%)

kikkie Highly Voted 1 year, 7 months ago

CCT MODULE 10 PG1244 Full Virtualization: In this type of virtualization, the guest OS is not aware that it is running in a virtualized environment.
OS assisted-The guest OS is aware its running on a virtual machine
Hybrid Virtualization: In this type of virtualization, the guest OS adopts the functionality of para virtualization

upvoted 5 times

044f354 Most Recent 9 months, 2 weeks ago

Selected Answer: B

EC-Council Official Curricula
Certified Cybersecurity Technician v1
https://online.vitalsource.com/reader/books/9781635679533/

Module 10 Page 1244

Full Virtualization: In this type of virtualization, the guest OS is not aware that it is running in a virtualized environment. It sends commands to the virtual machine manager (VMM) to interact with the computer hardware. The VMM then translates the commands to binary instructions and forwards them to the host OS. The resources are allocated to the guest OS through the VMM.

upvoted 1 times

laolu 1 year, 2 months ago

Selected Answer: B
Full Virtualization: In this type of virtualization, the guest OS is not aware that it is running in a virtualized environment. It sends commands to the virtual machine manager (VMM) to interact with the computer hardware. The VMM then translates the commands to binary instructions and forwards them to the host OS. The resources are allocated to the guest OS through the VMM.

upvoted 3 times

inull0 1 year, 4 months ago

Selected Answer: B

Full Virt

upvoted 2 times

RSMCT2011 1 year, 6 months ago

Selected Answer: D

Explanation:
Full Virtualization: In this type of virtualization, the guest OS is not aware that it is running in a virtualized environment. It sends commands to the virtual machine manager (VMM) to interact with the computer hardware. The VMM then translates the commands to binary instructions and forwards them to the host OS. The resources are allocated to the guest OS through the VMM.

upvoted 2 times

044f354 9 months, 2 weeks ago

You voted for incorrect answer D (OS assisted).

Your explanation is for correct answer B (Full).

upvoted 1 times

Question #20 *Topic 1*

Walker, a security team member at an organization, was instructed to check if a deployed cloud service is working as expected. He performed an independent examination of cloud service controls to verify adherence to standards through a review of objective evidence. Further, Walker evaluated the services provided by the CSP regarding security controls, privacy impact, and performance.
Identify the role played by Walker in the above scenario.

A. Cloud auditor

B. Cloud provider

C. Cloud carrier

D. Cloud consumer

Suggested Answer: *A*

Community vote distribution

A (100%)

044f354 9 months, 2 weeks ago

Selected Answer: A

EC-Council Official Curricula
Certified Cybersecurity Technician v1
https://online.vitalsource.com/reader/books/9781635679533/

Module 10 Page 1324

Cloud Auditor
A cloud auditor is a party that performs an independent examination of cloud service controls to express an opinion thereon. Audits verify adherence to standards through a review of the objective evidence. A cloud auditor can evaluate the services provided by a CSP regarding security controls (management, operational, and technical safeguards intended to protect the confidentiality, integrity, and availability of the system and its information), privacy impact (compliance with applicable privacy laws and regulations governing an individual's privacy), performance, etc.

upvoted 1 times

044f354 9 months, 2 weeks ago

Selected Answer: A

Certified Cybersecurity Technician Courseware
Module 10 Page 1324

Cloud Auditor
A cloud auditor is a party that performs an independent examination of cloud service controls to express an opinion thereon. Audits verify adherence to standards through a review of the objective evidence. A cloud auditor can evaluate the services provided by a CSP regarding security controls (management, operational, and technical safeguards intended to protect the confidentiality, integrity, and availability of the system and its information), privacy impact (compliance with applicable privacy laws and regulations governing an individual's privacy), performance, etc.

upvoted 1 times

KnifeRing 1 year, 1 month ago

A is correct, A party for making independent assessments of cloud service controls and taking an opinion thereon

upvoted 3 times

Question #21 *Topic 1*

A software company has implemented a wireless technology to track the employees' attendance by recording their in and out timings. Each employee in the company will have an entry card that is embedded with a tag. Whenever an employee enters the office premises, he/she is required to swipe the card at the entrance. The wireless technology uses radio-frequency electromagnetic waves to transfer data for automatic identification and for tracking tags attached to objects.
Which of the following technologies has the software company implemented in the above scenario?

A. WiMAX

B. RFID

C. Bluetooth

D. Wi-Fi

Suggested Answer: *B*

Community vote distribution

B (100%)

044f354 9 months, 2 weeks ago

Selected Answer: B

EC-Council Official Curricula
Certified Cybersecurity Technician v1
https://online.vitalsource.com/reader/books/9781635679533/

Module 11 Page 1407

RFID The radio-frequency identification (RFID) technology uses radio frequency (RF)
electromagnetic waves to transfer data for automatic identification and for tracking tags attached to objects. RFID devices work within a small range of up to 20 ft.

upvoted 1 times

kikkie 1 year ago

CCT MODULE 11 PAGE 1407
RFID
The radio-frequency identification (RFID) technology uses radio frequency (RF)
electromagnetic waves to transfer data for automatic identification and for tracking tags attached to objects. RFID devices work within a small range of up to 20 ft.

upvoted 4 times

Question #22 *Topic 1*

Matias, a network security administrator at an organization, was tasked with the implementation of secure wireless network encryption for their network. For this purpose, Matias employed a security solution that uses 256-bit Galois/Counter Mode Protocol (GCMP-256) to maintain the authenticity and confidentiality of data.
Identify the type of wireless encryption used by the security solution employed by Matias in the above scenario.

A. WPA2 encryption

B. WPA3 encryption

C. WEP encryption

D. WPA encryption

Suggested Answer: *B*

Community vote distribution

B (100%)

044f354 9 months, 2 weeks ago

Selected Answer: B

EC-Council Official Curricula
Certified Cybersecurity Technician v1
https://online.vitalsource.com/reader/books/9781635679533/

Module 11 Page 1429

WPA3: It is a third-generation Wi-Fi security protocol that provides new features for personal and enterprise usage. It uses Galois/Counter Mode-256 (GCMP-256) for encryption and the 384-bit hash message authentication code with the Secure Hash Algorithm (HMAC-SHA-384) for authentication.

upvoted 1 times

RSMCT2011 1 year ago

Selected Answer: B

WPA3: It is a third-generation Wi-Fi security protocol that provides new features for personal and enterprise usage. It uses Galois/Counter Mode-256 (GCMP-256) for encryption and the 384-bit hash message authentication code with the Secure Hash Algorithm (HMAC-SHA-384) for authentication

upvoted 2 times

Question #23 *Topic 1*

Rickson, a security professional at an organization, was instructed to establish short-range communication between devices within a range of 10 cm. For this purpose, he used a mobile connection method that employs electromagnetic induction to enable communication between devices.
The mobile connection method selected by Rickson can also read RFID tags and establish Bluetooth connections with nearby devices to exchange information such as images and contact lists.
Which of the following mobile connection methods has Rickson used in above scenario?

A. NFC

B. Satcom

C. Cellular communication

D. ANT

Suggested Answer: *A*

Community vote distribution

A (100%)

kikkie Highly Voted 1 year ago

CCT MODULE 12 PAGE 1483
Near-field Communication (NFC) It employs electromagnetic induction to enable communication between the devices connected within a range of 10 cm

upvoted 5 times

044f354 Most Recent 9 months, 2 weeks ago

Selected Answer: A

EC-Council Official Curricula
Certified Cybersecurity Technician v1
https://online.vitalsource.com/reader/books/9781635679533/

Module 13 Page 1562

Near-Field Communication (NFC): NFC is a type of short-range communication that uses magnetic field induction to enable communication between two electronic devices. It is primarily used in contactless mobile payment, social networking, and the identification of documents or other products.

upvoted 1 times

044f354 9 months, 2 weeks ago

ALSO:
Glossary Page 2415

Near-field Communication (NFC): NFC covers very short distances. It employs electromagnetic induction to enable communication between devices connected within 10 cm.

upvoted 1 times

RSMCT2011 1 year ago

Selected Answer: A

Explanation:
Near-field communication (NFC): NFC covers very short distances using RFID technology. It employs electromagnetic induction to enable communication between devices connected within a range of 10 cm. The NFC chip embedded within a mobile device can read RFID tags and also be used to establish Bluetooth connections with nearby devices to exchange information such as images and contact lists. Although it allows a very narrow communication range, an attacker with a specialized antenna can intercept and capture the data by jamming the traffic. This security issue may result from the improper configuration of NFC and non-encrypted data transmission. An attacker may craft and send malicious RFID tags, forcing the mobile user to visit a fake website in the browser. Furthermore, an attacker may perform a DoS attack by creating enormous RF signals to corrupt the NFC data being transmitted in that area.

upvoted 3 times

Question #24 *Topic 1*

Stephen, a security professional at an organization, was instructed to implement security measures that prevent corporate data leakage on employees' mobile devices. For this purpose, he employed a technique using which all personal and corporate data are isolated on an employee's mobile device. Using this technique, corporate applications do not have any control of or communication with the private applications or data of the employees.
Which of the following techniques has Stephen implemented in the above scenario?

A. Full device encryption

B. Geofencing

C. Containerization

D. OTA updates

Suggested Answer: *C*

Community vote distribution

C (100%)

044f354 9 months, 2 weeks ago

Selected Answer: C

EC-Council Official Curricula
Certified Cybersecurity Technician v1
https://online.vitalsource.com/reader/books/9781635679533/

Module 12 Page 1495

Module 12 Page 1495

upvoted 1 times

RSMCT2011 1 year ago

Selected Answer: C

Containerization Containerization is a technique in which all personal and organizational data are segregated on an employee's mobile device. With the increasing adoption of BYOD policies, using this technique substantially helps in improving the security of organizational data. It also improves productivity and enables the easy use of company resources and applications. These applications do not have any control of or communication with the private applications or data of the employees as they exist outside the container.

upvoted 3 times

Question #25 *Topic 1*

Leo has walked to the nearest supermarket to purchase grocery. At the billing section, the billing executive scanned each product's machine-readable tag against a readable machine that automatically reads the product details, displays the prices of the individual product on the computer, and calculates the sum of those scanned items. Upon completion of scanning all the products, Leo has to pay the bill.
Identify the type of short-range wireless communication technology that the billing executive has used in the above scenario.

A. Radio-frequency identification (RFID)

B. Near-field communication (NFC)

C. QUIC

D. QR codes and barcodes

Suggested Answer: *D*

Community vote distribution

D (100%)

044f354 9 months, 2 weeks ago

Selected Answer: D

IGNORE ANYONE WHO DOES NOT CITE THE OFFICIAL CURRICULA

Vendor Certifications exams are based on the vendor's official training material, not internet forum troll opinion consensus. The wording below is from the book, and matches the wording in the question.

EC-Council Official Curricula
Certified Cybersecurity Technician v1
https://online.vitalsource.com/reader/books/9781635679533/

Module 13 Page 1562

QR Codes and Barcodes: These codes are machine-readable tags that contain information about the product or item to which they are attached. A quick response code, or QR code, is a two-dimensional code that stores product information and can be scanned using smartphones, whereas a barcode comes in both one-dimensional (1D) and two-dimensional (2D) forms of code.

upvoted 1 times

iitc_duo 1 year, 5 months ago

Wireless doesn't mean to be readio frequency alone, it can be optical bar code reader too. So As per CCT book machine radable tag most of the time QR codes or 2D bar code. Thus, correct answer is D.

upvoted 2 times

Ligeti15 1 year, 5 months ago

Selected Answer: D

QR Codes and barcodes are listed under short-range wireless communication (page 1562), and the description matches the question perfectly. There are no tags used in NFC (maybe RFID, but not NFC), NFC communication is done between two devices to "exchange" information, RFID is for identification... IMHO

upvoted 2 times

RSMCT2011 2 years ago

Selected Answer: D

Explanation:
QR Codes and Barcodes: These codes are machine-readable tags that contain information about the product or item to which they are attached. A quick response code, or QR code, is a two-dimensional code that stores product information and can be scanned using smartphones, whereas a barcode comes in both one-dimensional (1D) and two-dimensional (2D) forms of code

upvoted 2 times

Markwest100 1 year, 5 months ago

QR codes and barcodes are not short-range wireless communication technologies. They are considered optical scanning technologies.

upvoted 1 times

⊟ **Markwest100** 1 year, 5 months ago

B. NFC is the correct answer

upvoted 1 times

⊟ **chuck4real** 2 years, 2 months ago

The correct answer is C, a short-range wireless communication.

upvoted 1 times

⊟ **chuck4real** 2 years, 2 months ago

My bad, I meant B (NFC).

upvoted 1 times

⊟ **044f354** 9 months, 2 weeks ago

Still incorrect.

Correct answer is D: QR Codes and Barcodes

EC-Council Official Curricula
Certified Cybersecurity Technician v1
https://online.vitalsource.com/reader/books/9781635679533/

Module 13 Page 1562

QR Codes and Barcodes: These codes are machine-readable tags that contain information about the product or item to which they are attached.

upvoted 1 times

Question #26 *Topic 1*

Hayes, a security professional, was tasked with the implementation of security controls for an industrial network at the Purdue level 3.5 (IDMZ). Hayes verified all the possible attack vectors on the IDMZ level and deployed a security control that fortifies the IDMZ against cyber-attacks. Identify the security control implemented by Hayes in the above scenario.

A. Point-to-point communication

B. MAC authentication

C. Anti-DoS solution

D. Use of authorized RTU and PLC commands

Suggested Answer: *C*

Community vote distribution

C (100%)

kanchantanwani Highly Voted 👍 2 years, 4 months ago

Selected Answer: C

Answer is C:

Zone: Industrial DMZ 3.5 (IDMZ)

Attack Vector: DoS attacks

Risks: Malware injections, Network infections

Security Controls: Anti-DoS solutions, IPS, Antibot, Application control

Purdue Level 2 & 1 (Manufacturing): Use of authorized RTU and PLC commands

Source (https://online.vitalsource.com/reader/books/9781635679533/pageid/1637)

upvoted 6 times

Ahmed3yad Most Recent 🕓 2 years, 2 months ago

Selected Answer: C

Anti-Dos.

CCT Module 13 IOT and OT Security. page 1623

upvoted 3 times

Question #27 *Topic 1*

Paul, a computer user, has shared information with his colleague using an online application. The online application used by Paul has been incorporated with the latest encryption mechanism. This mechanism encrypts data by using a sequence of photons that have a spinning trait while traveling from one end to another, and these photons keep changing their shapes during their course through filters: vertical, horizontal, forward slash, and backslash.
Identify the encryption mechanism demonstrated in the above scenario.

A. Quantum cryptography

B. Homomorphic encryption

C. Rivest Shamir Adleman encryption

D. Elliptic curve cryptography

Suggested Answer: *A*

KURT324 1 year ago

definitely a great one

upvoted 1 times

Question #28 *Topic 1*

Riley sent a secret message to Louis. Before sending the message, Riley digitally signed the message using his private key. Louis received the message, verified the digital signature using the corresponding key to ensure that the message was not tampered during transit.
Which of the following keys did Louis use to verify the digital signature in the above scenario?

A. Riley's public key

B. Louis's public key

C. Riley's private key

D. Louis's private key

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #29 *Topic 1*

Grace, an online shopping freak, has purchased a smart TV using her debit card. During online payment, Grace's browser redirected her from ecommerce website to a third-party payment gateway, where she provided her debit card details and OTP received on her registered mobile phone. After completing the transaction, Grace navigated to her online bank account and verified the current balance in her savings account.
Identify the state of data when it is being processed between the ecommerce website and the payment gateway in the above scenario.

A. Data at rest

B. Data in inactive

C. Data in transit

D. Data in use

Suggested Answer: *C*

Community vote distribution

C (100%)

⊟ **044f354** 9 months, 2 weeks ago

Selected Answer: C

EC-Council Official Curricula
Certified Cybersecurity Technician v1
https://online.vitalsource.com/reader/books/9781635679533/

Module 15 Page 1752

Table 15.1: Data at rest vs Data in use vs Data in transit

Data in Transit

Description: Data traversing using some means of communication
Examples: An email being sent
Security Controls: SSL and TLS, Email encryption tools such as PGP or S/MIME, Firewall controls
upvoted 1 times

Question #30 *Topic 1*

Andre, a security professional, was tasked with segregating the employees' names, phone numbers, and credit card numbers before sharing the database with clients. For this purpose, he implemented a deidentification technique that can replace the critical information in database fields with special characters such as asterisks (*) and hashes (#).
Which of the following techniques was employed by Andre in the above scenario?

A. Tokenization

B. Masking

C. Hashing

D. Bucketing

Suggested Answer: *B*

Community vote distribution

B (100%)

044f354 9 months, 2 weeks ago

Selected Answer: B

EC-Council Official Curricula
Certified Cybersecurity Technician v1
https://online.vitalsource.com/reader/books/9781635679533/

Module 15 Page 1759

Data Masking
Protecting information by obscuring specific areas of data with random characters or codes. Data masking protects sensitive data such as personally identifiable information, protected health information, payment card information, intellectual property, etc. Apart from this, data masking also protects against an insider threat. Implementing data masking will bolster the security strategies of an organization.

upvoted 1 times

Question #31

Topic 1

Ryleigh, a system administrator, was instructed to perform a full back up of organizational data on a regular basis. For this purpose, she used a backup technique on a fixed date when the employees are not accessing the system i.e., when a service-level down time is allowed a full backup is taken.

Identify the backup technique utilized by Ryleigh in the above scenario.

A. Nearline backup

B. Cold backup

C. Hot backup

D. Warm backup

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #32 *Topic 1*

Jaden, a network administrator at an organization, used the ping command to check the status of a system connected to the organization's network. He received an ICMP error message stating that the IP header field contains invalid information. Jaden examined the ICMP packet and identified that it is an IP parameter problem.
Identify the type of ICMP error message received by Jaden in the above scenario.

A. Type =12

B. Type = 8

C. Type = 5

D. Type = 3

Suggested Answer: *A*

Community vote distribution

A (100%)

kanchantanwani Highly Voted 2 years, 4 months ago

Selected Answer: A

Answer is A: Type 12
Basic Network Issues: IP Parameter Problem
Devices that process datagrams may not be able to forward a datagram owing to some type of error in the header. This error does not relate to the state of the destination host or network but still prevents the datagram from being processed and delivered. An ICMP type-12 parameter problem message is sent to the source of the datagram.

upvoted 5 times

luna21318 Most Recent 1 year, 4 months ago

Selected Answer: A

parameter problem not redirect

upvoted 2 times

a613c45 2 years ago

Selected Answer: A

CCT v1 Module 16 Page 1938/939

upvoted 3 times

Ahmed3yad 2 years, 2 months ago

Selected Answer: A

Answer is A. Type =12
CCT v1 Module 16 Page 1938/939
https://online.vitalsource.com/reader/books/9781635679533/pageid/1952

upvoted 3 times

elwo_111 2 years, 5 months ago

Selected Answer: A

I think the answer is A) Type 12 known as "Parameter Problem". Type 5 is "Redirect", which sounds wrong in this scenario.

upvoted 2 times

Question #33 *Topic 1*

Steve, a network engineer, was tasked with troubleshooting a network issue that is causing unexpected packet drops. For this purpose, he employed a network troubleshooting utility to capture the ICMP echo request packets sent to the server. He identified that certain packets are dropped at the gateway due to poor network connection.
Identify the network troubleshooting utility employed by Steve in the above scenario.

A. dnsenurn

B. arp

C. traceroute

D. ipconfig

Suggested Answer: *C*

Community vote distribution

C (100%)

044f354 9 months, 2 weeks ago

Selected Answer: C

EC-Council Official Curricula
Certified Cybersecurity Technician v1
https://online.vitalsource.com/reader/books/9781635679533/

Module 16 Page 1980-1981

traceroute/tracert
The multi-OS-compatible command-line tool trace route (tracert)/traceroute is used to trace packets across a network and to understand connections to a server. It allows the user to understand Internet connection problems, including packet loss and high latency.

Tracert (for Windows) uses ICMP. It sends ICMP echo request messages to the specified destination. If the destination is active, it sends ICMP echo reply messages as a response, confirming that the connection is active. Otherwise, the destination may not be active, or it could be a connectivity issue of the source.

upvoted 1 times

kanchantanwani 1 year, 4 months ago

Selected Answer: C

Traceroute is correct: The traceroute utility is used to trace packets across a network and to understand connections to a serve

upvoted 2 times

Question #34 *Topic 1*

Anderson, a security engineer, was Instructed to monitor all incoming and outgoing traffic on the organization's network to identify any suspicious traffic. For this purpose, he employed an analysis technique using which he analyzed packet header fields such as IP options, IP protocols, IP fragmentation flags, offset, and identification to check whether any fields are altered in transit.
Identify the type of attack signature analysis performed by Anderson in the above scenario.

A. Context-based signature analysis

B. Atomic-signature-based analysis

C. Composite-signature-based analysis

D. Content-based signature analysis

Suggested Answer: *A*

Community vote distribution

A (100%)

kanchantanwani Highly Voted 👍 1 year, 4 months ago

Selected Answer: A

Answer is A: Context-based Signature Analysis : Attack signatures are contained in packet headers
Inspect packets for unusual/suspicious header information such as the following: Source and destination IP addresses IP options, protocols, and checksums Source and destination port numbers IP fragmentation flags, offset, or identification

upvoted 5 times

044f354 Most Recent 🕓 9 months, 2 weeks ago

Selected Answer: A

EC-Council Official Curricula
Certified Cybersecurity Technician v1
https://online.vitalsource.com/reader/books/9781635679533/

Module 17 Page 2037

Context-based signature analysis: Packets are usually altered using the header information. Suspicious signatures in the header can include malicious data that can affect the following:

o Source and destination IP addresses
o Source and destination port numbers
o IP options
o IP protocols
o IP, TCP, and UDP checksums
o IP fragmentation flags, offset, or identification

upvoted 1 times

Ahmed3yad 1 year, 2 months ago

Selected Answer: A

Context-based signature analysis
CCT Module 17. page 2037

upvoted 2 times

AmesCB 1 year, 2 months ago

answer A

upvoted 2 times

Ahmed3yad 1 year, 2 months ago

Answer is A. Context-based signature analysis
CCT v1 Module 17 Page 2037/939
https://online.vitalsource.com/reader/books/9781635679533/pageid/2051

upvoted 2 times

Question #35 *Topic 1*

Leilani, a network specialist at an organization, employed Wireshark for observing network traffic. Leilani navigated to the Wireshark menu icon that contains items to manipulate, display and apply filters, enable, or disable the dissection of protocols, and configure user-specified decodes. Identify the Wireshark menu Leilani has navigated in the above scenario.

A. Statistics

B. Capture

C. Main toolbar

D. Analyze

Suggested Answer: *D*

Community vote distribution

D (100%)

Ahmed3yad 1 year, 2 months ago

Selected Answer: D

Analyze

CCT Module 17. page 2044

upvoted 2 times

AmesCB 1 year, 2 months ago

Analyse

upvoted 1 times

kanchantanwani 1 year, 5 months ago

Selected Answer: D

Source: https://www.wireshark.org/docs/wsug_html_chunked/ChUseMenuSection.html

Analyze

This menu contains items to manipulate display filters, enable or disable the dissection of protocols, configure user specified decodes and follow a TCP stream.

upvoted 4 times

elwo_111 1 year, 5 months ago

Seconded D

upvoted 1 times

Question #36 *Topic 1*

Tenda, a network specialist at an organization, was examining logged data using Windows Event Viewer to identify attempted or successful unauthorized activities. The logs analyzed by Tenda include events related to Windows security; specifically, log-on/log-off activities, resource access, and also information based on Windows system's audit policies.
Identify the type of event logs analyzed by Tenda in the above scenario.

A. Application event log

B. Setup event log

C. Security event log

D. System event log

Suggested Answer: *C*

Community vote distribution

C (100%)

044f354 9 months, 2 weeks ago

Selected Answer: C

EC-Council Official Curricula
Certified Cybersecurity Technician v1
https://online.vitalsource.com/reader/books/9781635679533/

Module 18 Page 2080

Security event log:
This includes events related to Windows security; specifically, log-on/log-off activities, resource access, and also information based on Windows system's audit policies. It is analyzed by security professionals to identify attempted and/or successful unauthorized activities. For example, if the system attempts to verify account credentials when an end-user tries to log-on to a machine.

upvoted 1 times

Ocipala 1 year, 3 months ago

C. Security event log

upvoted 1 times

Question #37 *Topic 1*

Nancy, a security specialist, was instructed to identify issues related to unexpected shutdown and restarts on a Linux machine. To identify the incident cause, Nancy navigated to a directory on the Linux system and accessed a log file to troubleshoot problems related to improper shutdowns and unplanned restarts.
Identify the Linux log file accessed by Nancy in the above scenario.

A. /var/log/secure

B. /var/log/kern.log

C. /var/log/boot.log

D. /var/log/lighttpd/

Suggested Answer: *C*

Community vote distribution

C (100%)

044f354 9 months, 2 weeks ago

Selected Answer: C

EC-Council Official Curricula
Certified Cybersecurity Technician v1
https://online.vitalsource.com/reader/books/9781635679533/

Module 18 Page 2096

/var/log/boot.log: This file stores all information related to system booting.

The booting messages are sent by system initialization script, /etc/init.d/bootmisc.sh, to this log file. This file is helpful when trying to troubleshoot problems related to improper shutdowns, booting failures, or unplanned reboots. By checking this file, the time span of system downtime that occurred due to an unexpected shutdown can be determined.

upvoted 1 times

kanchantanwani 1 year, 4 months ago

Selected Answer: C

C is correct: /var/log/boot.log: This file stores all information related to system booting. The booting messages are sent by system initialization script, /etc/init.d/bootmisc.sh, to this log file. This file is helpful when trying to troubleshoot problems related to improper shutdowns, booting failures, or unplanned reboots. By checking this file, the time span of system downtime that occurred due to an unexpected shutdown can be determined.

upvoted 3 times

Question #38 *Topic 1*

Warren, a member of IH&R team at an organization, was tasked with handling a malware attack launched on one of servers connected to the organization's network. He immediately implemented appropriate measures to stop the infection from spreading to other organizational assets and to prevent further damage to the organization.
Identify the IH&R step performed by Warren in the above scenario.

A. Containment

B. Recovery

C. Eradication

D. Incident triage

Suggested Answer: *A*

Ocipala 1 year, 3 months ago

A. Containment

upvoted 1 times

Question #39 *Topic 1*

The IH&R team in an organization was handling a recent malware attack on one of the hosts connected to the organization's network. Edwin, a member of the IH&R team, was involved in reinstating lost data from the backup media. Before performing this step, Edwin ensured that the backup does not have any traces of malware.
Identify the IH&R step performed by Edwin in the above scenario.

A. Eradication

B. Incident containment

C. Notification

D. Recovery

Suggested Answer: *D*

Ocipala 1 year, 3 months ago

D. Recovery

upvoted 1 times

Question #40 *Topic 1*

Kason, a forensic officer, was appointed to investigate a case where a threat actor has bullied certain children online. Before proceeding legally with the case, Kason has documented all the supporting documents, including source of the evidence and its relevance to the case, before presenting it in front of the jury.
Which of the following rules of evidence was discussed in the above scenario?

A. Authentic

B. Understandable

C. Reliable

D. Admissible

Suggested Answer: *A*

Community vote distribution

A (100%)

MPA3333 1 year, 2 months ago

D. :Investigators need to present evidence in an admissible manner, which means that it should be relevant to the case...

upvoted 1 times

a613c45 1 year, 6 months ago

D: Admissible: ... "and its relevance to the case"

upvoted 2 times

Ahmed3yad 1 year, 8 months ago

Selected Answer: A

Module 20 page 2186 (Authentic)

upvoted 2 times

AmesCB 1 year, 8 months ago

Selected Answer: A

Authentic

upvoted 1 times

kanchantanwani 1 year, 10 months ago

Selected Answer: A

Answer is A: Authentic

Authentic: Given that digital evidence can be easily manipulated, its ownership needs to be clarified. Therefore, investigators must provide supporting documents regarding the authenticity of the evidence with details such as the source of the evidence and its relevance to the case. If necessary, they must also furnish details such as the author of the evidence or path of transmission.

Source: Module 20 Page 2186 Certified Cybersecurity Technician EC COUNCIL

upvoted 3 times

Question #41 *Topic 1*

Arabella, a forensic officer, documented all the evidence related to the case in a standard forensic investigation report template. She filled different sections of the report covering all the details of the crime along with the daily progress of the investigation process.
In which of the following sections of the forensic investigation report did Arabella record the "nature of the claim and information provided to the officers"?

A. Investigation process

B. Investigation objectives

C. Evidence information

D. Evaluation and analysis process

Suggested Answer: *C*

Community vote distribution

A (100%)

dewayuhei Highly Voted 1 year, 9 months ago

this answer is A.

upvoted 6 times

mameid Most Recent 9 months, 3 weeks ago

Selected Answer: A

Not evidence information

upvoted 2 times

MPA3333 1 year, 2 months ago

Definitely A.

upvoted 3 times

inull0 1 year, 4 months ago

A.

Page 2224.

Investigation Process - Nature of the claim and information provided to the investigators.

upvoted 4 times

Question #42 *Topic 1*

Shawn, a forensic officer, was appointed to investigate a crime scene that had occurred at a coffee shop. As a part of investigation, Shawn collected the mobile device from the victim, which may contain potential evidence to identify the culprits.
Which of the following points must Shawn follow while preserving the digital evidence? (Choose three.)

A. Never record the screen display of the device

B. Turn the device ON if it is OFF

C. Do not leave the device as it is if it is ON

D. Make sure that the device is charged

Suggested Answer: *BCD*

kanchantanwani Highly Voted 2 years, 4 months ago

The answers don't make sense to the question asked. There IS only one correct answer here, 3 of them are the wrong ones:
For handheld devices such as cell phones, tablets, and digital cameras:
 Do not turn the device ON if it is OFF
 Leave the device as it is if it is ON
 Photograph the screen display of the device
 Label and collect all cables and transport them along with the device
 Make sure that the device is charged

upvoted 5 times

iitc_duo Most Recent 1 year, 5 months ago

Page No: 2247

upvoted 1 times

kanchantanwani 2 years, 4 months ago

Therefore the only correct answer is to make sure the device is charged.

upvoted 3 times

Question #43 *Topic 1*

Ruben, a crime investigator, wants to retrieve all the deleted files and folders in the suspected media without affecting the original files. For this purpose, he uses a method that involves the creation of a cloned copy of the entire media and prevents the contamination of the original media. Identify the method utilized by Ruben in the above scenario.

A. Sparse acquisition

B. Bit-stream imaging

C. Drive decryption

D. Logical acquisition

Suggested Answer: *B*

Ocipala 1 year, 3 months ago

B. Bit-stream imaging

upvoted 2 times

Question #44 *Topic 1*

Kasen, a cybersecurity specialist at an organization, was working with the business continuity and disaster recovery team. The team initiated various business continuity and discovery activities in the organization. In this process, Kasen established a program to restore both the disaster site and the damaged materials to the pre-disaster levels during an incident.
Which of the following business continuity and disaster recovery activities did Kasen perform in the above scenario?

A. Prevention

B. Resumption

C. Response

D. Recovery

Suggested Answer: *D*

Ocipala 1 year, 3 months ago

D. Recovery

upvoted 1 times

Question #45 *Topic 1*

Cassius, a security professional, works for the risk management team in an organization. The team is responsible for performing various activities involved in the risk management process. In this process, Cassius was instructed to select and implement appropriate controls on the identified risks in order to address the risks based on their severity level.
Which of the following risk management phases was Cassius instructed to perform in the above scenario?

A. Risk analysis

B. Risk treatment

C. Risk prioritization

D. Risk identification

Suggested Answer: *B*

Community vote distribution

B (67%) C (33%)

mameid 9 months, 3 weeks ago

Selected Answer: B

Prioritizing its about to severity and impact of business its just ranking.

upvoted 2 times

iitc_duo 1 year, 5 months ago

Correct Answer is : B (As per CCT book Page No: 2357)

upvoted 2 times

ge0c0de 1 year, 7 months ago

B) risk treatment p. 2357

upvoted 2 times

Erthco 1 year, 8 months ago

Selected Answer: C

Risk Prioritization

upvoted 1 times

Question #46 *Topic 1*

RAT has been setup in one of the machines connected to the network to steal the important Sensitive corporate docs located on Desktop of the server, further investigation revealed the IP address of the server 20.20.10.26. Initiate a remote connection using thief client and determine the number of files present in the folder.
Hint: Thief folder is located at: Z:\CCT-Tools\CCT Module 01 Information Security Threats and Vulnerabilities\Remote Access Trojans (RAT)\Thief of Attacker Machine-1.

A. 2

B. 4

C. 3

D. 5

Suggested Answer: *C*

⊟ **Ocipala** 1 year, 3 months ago

C. 3 files

upvoted 1 times

Question #47 *Topic 1*

An FTP server has been hosted in one of the machines in the network. Using Cain and Abel the attacker was able to poison the machine and fetch the FTP credentials used by the admin. You're given a task to validate the credentials that were stolen using Cain and Abel and read the file flag.txt

A. white@hat

B. red@hat

C. hat@red

D. blue@hat

Suggested Answer: *C*

Ocipala 1 year, 3 months ago

C. hat@red

upvoted 1 times

Question #48 *Topic 1*

An attacker with malicious intent used SYN flooding technique to disrupt the network and gain advantage over the network to bypass the Firewall. You are working with a security architect to design security standards and plan for your organization. The network traffic was captured by the SOC team and was provided to you to perform a detailed analysis. Study the Synflood.pcapng file and determine the source IP address.
Note: Synflood.pcapng file is present in the Documents folder of Attacker-1 machine.

A. 20.20.10.180

B. 20.20.10.19

C. 20.20.10.60

D. 20.20.10.59

Suggested Answer: *B*

Ocipala 1 year, 3 months ago

B. 20.20.10.19

upvoted 1 times

Question #49 *Topic 1*

A web application www.movieabc.com was found to be prone to SQL injection attack. You are given a task to exploit the web application and fetch the user credentials. Select the UID which is mapped to user john in the database table.

Note:

Username: sam -

Pass: test

A. 5

B. 3

C. 2

D. 4

Suggested Answer: *D*

Ocipala 1 year, 3 months ago

D. 4 database table

upvoted 1 times

Question #50 *Topic 1*

A pfSense firewall has been configured to block a web application www.abchacker.com. Perform an analysis on the rules set by the admin and select the protocol which has been used to apply the rule.
Hint: Firewall login credentials are given below:

Username: admin -
Password: admin@l23

A. POP3

B. TCP/UDP

C. FTP

D. ARP

Suggested Answer: *B*

Ocipala 1 year, 3 months ago
B. TCP/UDP
upvoted 1 times

Question #51 *Topic 1*

You are Harris working for a web development company. You have been assigned to perform a task for vulnerability assessment on the given IP address 20.20.10.26. Select the vulnerability that may affect the website according to the severity factor.
Hint: Greenbone web credentials: admin/password

A. TCP timestamps

B. Anonymous FTP Login Reporting

C. FTP Unencrypted Cleartext Login

D. UDP timestamps

Suggested Answer: *C*

Ocipala 1 year, 3 months ago
C. FTP Unencrypted Cleartext Login
upvoted 1 times

Question #52 *Topic 1*

A threat intelligence feed data file has been acquired and stored in the Documents folder of Attacker Machine-1 (File Name: Threatfeed.txt). You are a cybersecurity technician working for an ABC organization. Your organization has assigned you a task to analyze the data and submit a report on the threat landscape. Select the IP address linked with http://securityabc.s21sec.com.

A. 5.9.200.200

B. 5.9.200.150

C. 5.9.110.120

D. 5.9.188.148

Suggested Answer: *D*

Ocipala 1 year, 3 months ago

D. 5.9.188.148

upvoted 1 times

Question #53 *Topic 1*

An IoT device that has been placed in a hospital for safety measures, it has sent an alert command to the server. The network traffic has been captured and stored in the Documents folder of the Attacker Machine-1. Analyze the IoTdeviceTraffic.pcapng file and select the appropriate command that was sent by the IoT device over the network.

A. Tempe_Low

B. Low_Tempe

C. Temp_High

D. High_Tempe

Suggested Answer: *C*

Ocipala 1 year, 3 months ago

C. Temp_High

upvoted 1 times

Question #54 *Topic 1*

A text file containing sensitive information about the organization has been leaked and modified to bring down the reputation of the organization. As a safety measure, the organization did contain the MD5 hash of the original file. The file which has been leaked is retained for examining the integrity. A file named "Sensitiveinfo.txt" along with OriginalFileHash.txt has been stored in a folder named Hash in Documents of Attacker Machine-1. Compare the hash value of the original file with the leaked file and state whether the file has been modified or not by selecting yes or no.

A. No

B. Yes

Suggested Answer: *B*

Ocipala 1 year, 3 months ago

B. Yes

upvoted 1 times

Question #55 *Topic 1*

Initiate an SSH Connection to a machine that has SSH enabled in the network. After connecting to the machine find the file flag.txt and choose the content hidden in the file. Credentials for SSH login are provided below:
Hint:

Username: sam -
Password: admin@l23

A. sam@bob

B. bob2@sam

C. bob@sam

D. sam2@bob

Suggested Answer: *C* -

Ocipala 1 year, 3 months ago

C. bob@sam

upvoted 1 times

Question #56 *Topic 1*

You are assigned to perform a nmap scan on the target subnet 10.30.50.0/24 and determine the IP address of the host machine with port 514 in an open state. (Practical Question)

A. 10.30.50.58

B. 10.30.50.56

C. 10.30.50.55

D. 10.30.50.57

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #57 *Topic 1*

As a Virtualization Software Engineer/Analyst, you are employed on a Project with Alpha Inc. Company, the OS Virtualization is used for isolation of Physical/Base OS with the Hypervisor OS. What is the security benefit of OS virtualization in terms of isolation?

A. Virtual machines can freely access the resources of other VMs on the same host.

B. OS virtualization offers no security benefits in isolation.

C. A compromised virtual machine can easily infect the physical host and other VMs.

D. Virtual machines are isolated from each other, preventing a security breach in one from impacting others.

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #58 *Topic 1*

DigitalVault Corp., a premier financial institution, has recently seen a significant rise in advanced persistent threats (APTs) targeting its mainframe systems. Considering the sensitivity of the data stored, it wants to employ a strategy that deceives attackers into revealing their techniques. As part of its defense strategy, the cybersecurity team is deliberating over-deploying a honeypot system. Given the bank's requirements, the team are evaluating different types of honeypots. DigitalVault's primary goal is to gather extensive information about the attackers' methods without putting its actual systems at risk. Which of the following honeypots would BEST serve DigitalVault's intent?

A. Low-interaction honeypots, designed to log basic information such as IP addresses and attack vectors.

B. Research honeypots, aimed at understanding threats to a specific industry and sharing insights with the broader community.

C. High-interaction honeypots, offering a real system's replica for attackers, and observing their every move.

D. Production honeypots, which are part of the organization's active network and collect information about daily attacks.

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!