EXAMTOPICS

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

Custom View Settings

Topic 1 - Single Topic

Question #1 *Topic 1*

Which event is user interaction?

A. gaining root access

B. executing remote code

C. reading and writing file permission

D. opening a malicious file

Question #2 *Topic 1*

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

Question #3 *Topic 1*

How is attacking a vulnerability categorized?

A. action on objectives

B. delivery

C. exploitation

D. installation

Question #4 *Topic 1*

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

Question #5 *Topic 1*

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

Question #6 *Topic 1*

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

Question #7 *Topic 1*

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

Question #8 *Topic 1*

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.

Question #9 *Topic 1*

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

Question #10 *Topic 1*

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

Question #11 *Topic 1*

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

Question #12 *Topic 1*

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

Question #13 *Topic 1*

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

Question #14 *Topic 1*

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

Question #15 *Topic 1*

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

Question #16 *Topic 1*

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

Question #17 *Topic 1*

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

Question #18 *Topic 1*

Which evasion technique is a function of ransomware?

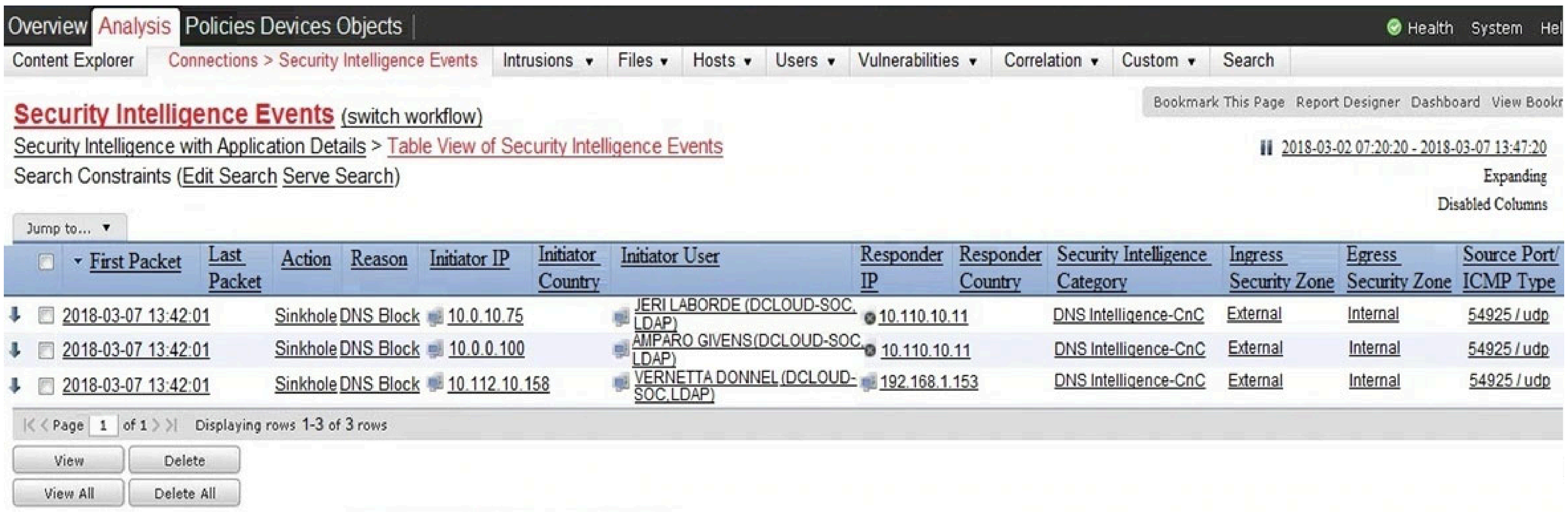
A. extended sleep calls

B. encryption

C. resource exhaustion

D. encoding

Question #19 *Topic 1*


Overview Analysis Policies Devices Objects
Health System Hel
Content Explorer
Connections > Security Intelligence Events
Intrusions ▾
Files ▾
Hosts ▾
Users ▾
Vulnerabilities ▾
Correlation ▾
Custom ▾
Search
Bookmark This Page Report Designer Dashboard View Bookr

Security Intelligence Events (switch workflow)

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

Search Constraints (Edit Search Serve Search)

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

Expanding

Disabled Columns

	□	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		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		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		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

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

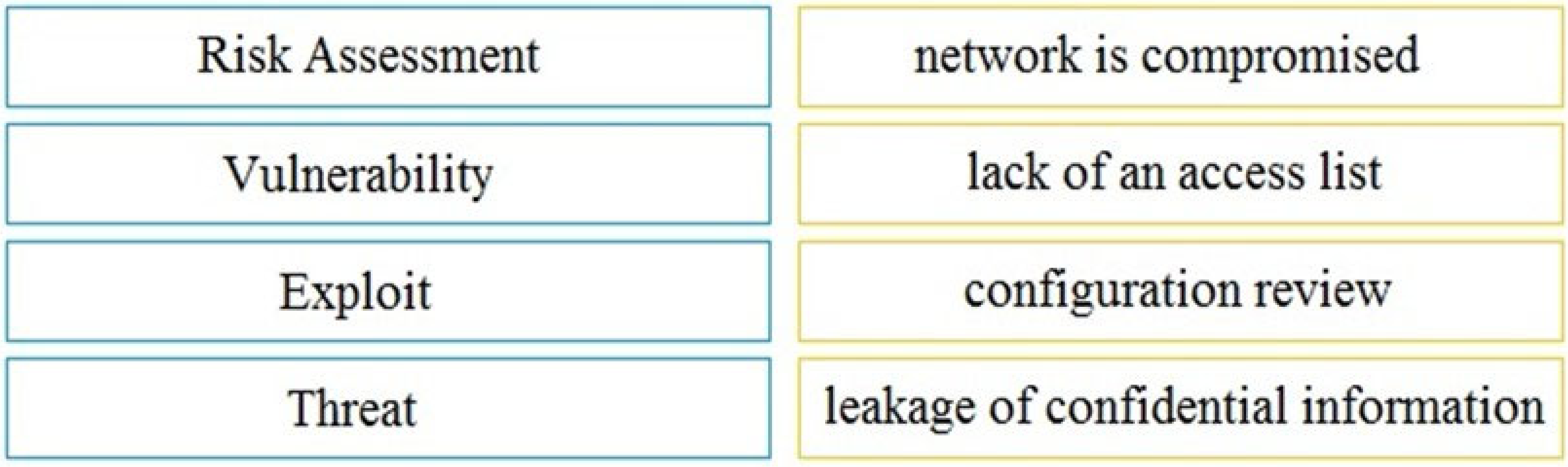
E. Initiator IP

Question #20 *Topic 1*

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

Question #21 *Topic 1*

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

Question #22 *Topic 1*

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.

Question #23 *Topic 1*

Which attack method intercepts traffic on a switched network?

A. denial of service

B. ARP cache poisoning

C. DHCP snooping

D. command and control

Question #24 *Topic 1*

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

Question #25 *Topic 1*

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

Question #26 *Topic 1*

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

Question #27 *Topic 1*

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

Question #28 *Topic 1*

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

Question #29 *Topic 1*

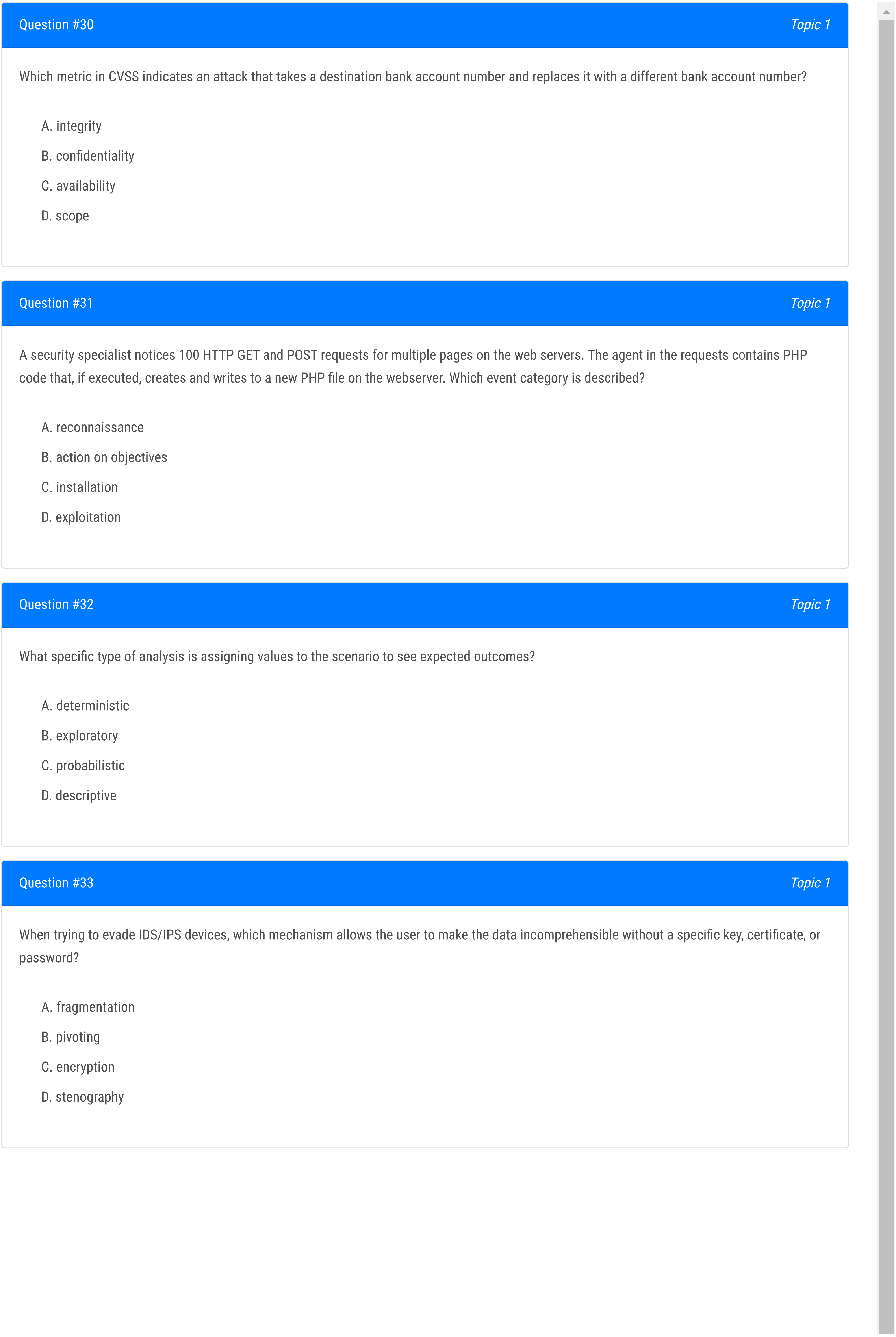
What is the difference between an attack vector and an attack surface?

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.



Question #30

Topic 1

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

Question #31

Topic 1

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

Question #32

Topic 1

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

A. deterministic

B. exploratory

C. probabilistic

D. descriptive

Question #33

Topic 1

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

Question #34 *Topic 1*

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.

Question #35 *Topic 1*

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.

Question #36 *Topic 1*

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

Question #37 *Topic 1*

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

Question #38 *Topic 1*

What is the principle of defense-in-depth?

A. Agentless and agent-based protection for security are used.

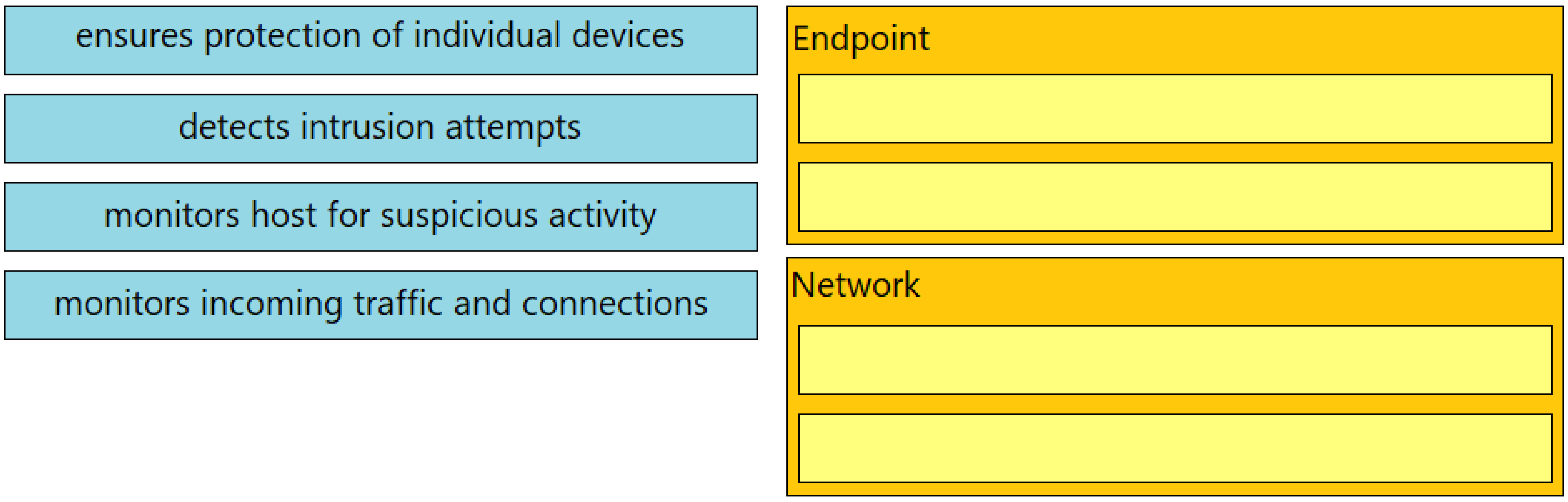
B. Several distinct protective layers are involved.

C. Access control models are involved.

D. Authentication, authorization, and accounting mechanisms are used.

Question #39 *Topic 1*

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
detects intrusion attempts
monitors host for suspicious activity
monitors incoming traffic and connections
Endpoint
Network

Question #40 *Topic 1*

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.

Question #41 *Topic 1*

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

Question #42 *Topic 1*

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.

Question #43 *Topic 1*

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

A. statistical data

B. session data

C. alert data

D. connectivity data

Question #44 *Topic 1*

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

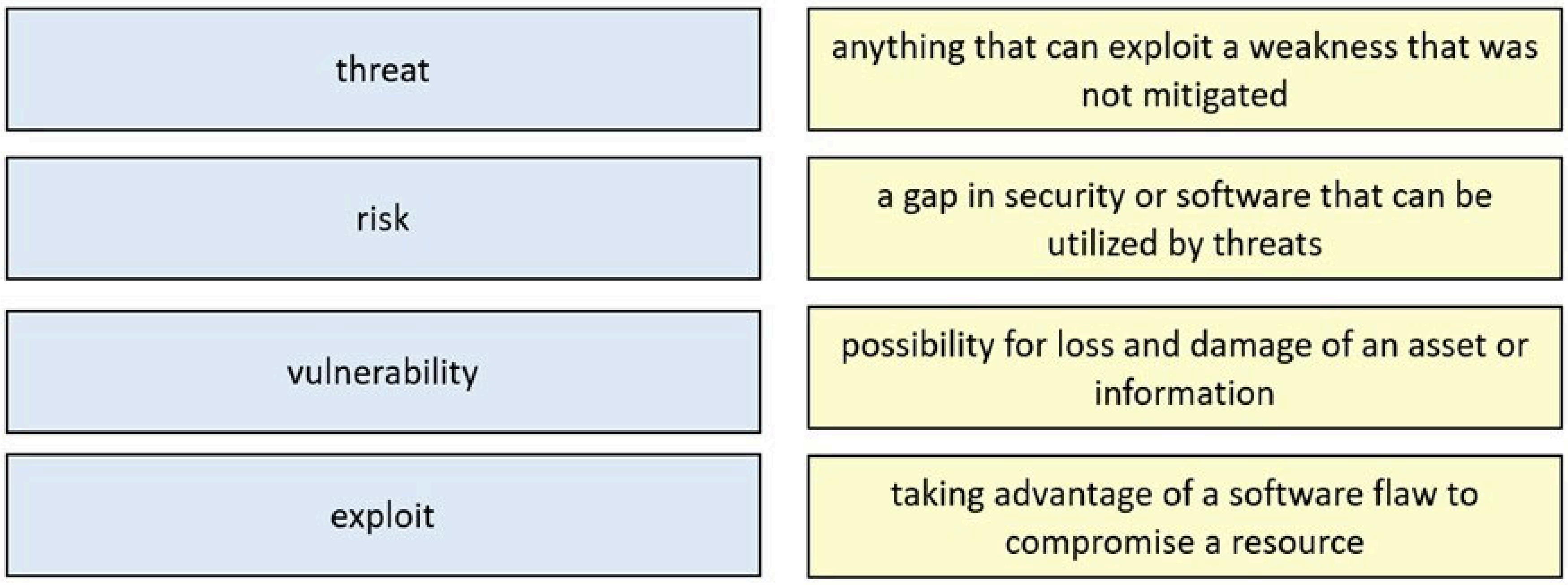
D. setting up a rogue access point near a public hotspot

Question #45 *Topic 1*

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

Question #46 *Topic 1*

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.

Question #47 *Topic 1*

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.

Question #48 *Topic 1*

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.

Question #49 *Topic 1*

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

Question #50 *Topic 1*

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

Question #51 *Topic 1*

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

Question #52 *Topic 1*

Which list identifies the information that the client sends to the server in the negotiation phase of the TLS handshake?

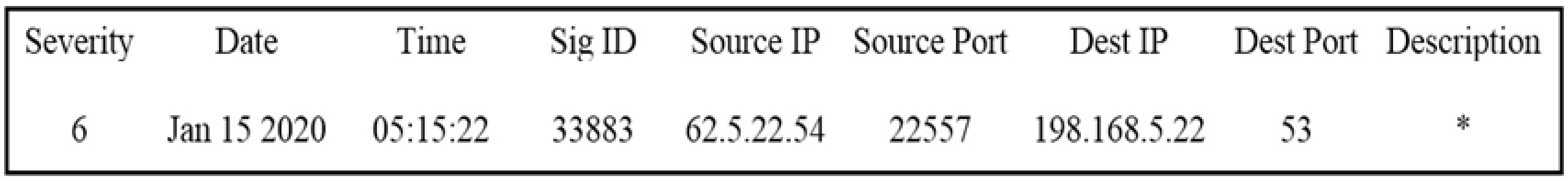
A. ClientStart, ClientKeyExchange, cipher-suites it supports, and suggested compression methods

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

Question #53 *Topic 1*



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?

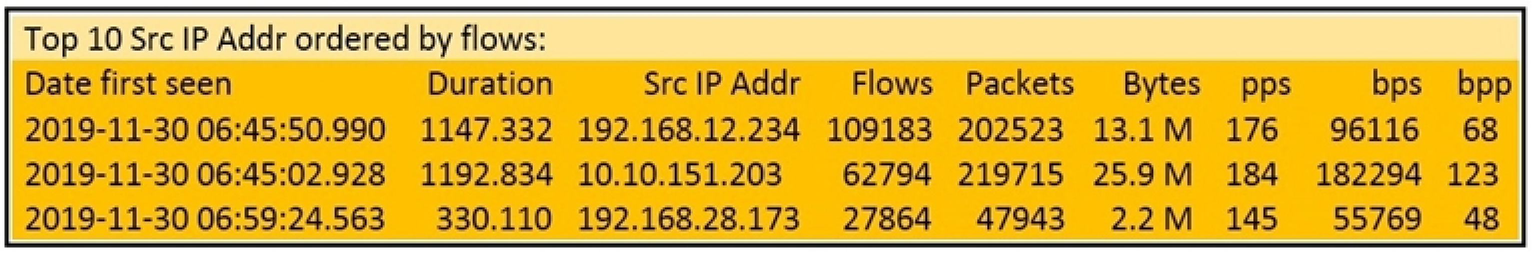
A. IDS

B. proxy

C. NetFlow

D. sys

Question #54 — *Topic 1*



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

Question #55 — *Topic 1*

What is the difference between the ACK flag and the RST flag in the NetFlow log session?

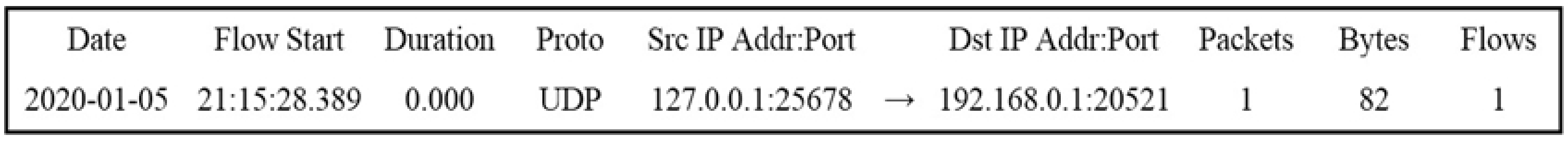
A. The RST flag confirms the beginning of the TCP connection, and the ACK flag responds when the data for the payload is complete

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

Question #56 — *Topic 1*



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

Question #57 — *Topic 1*

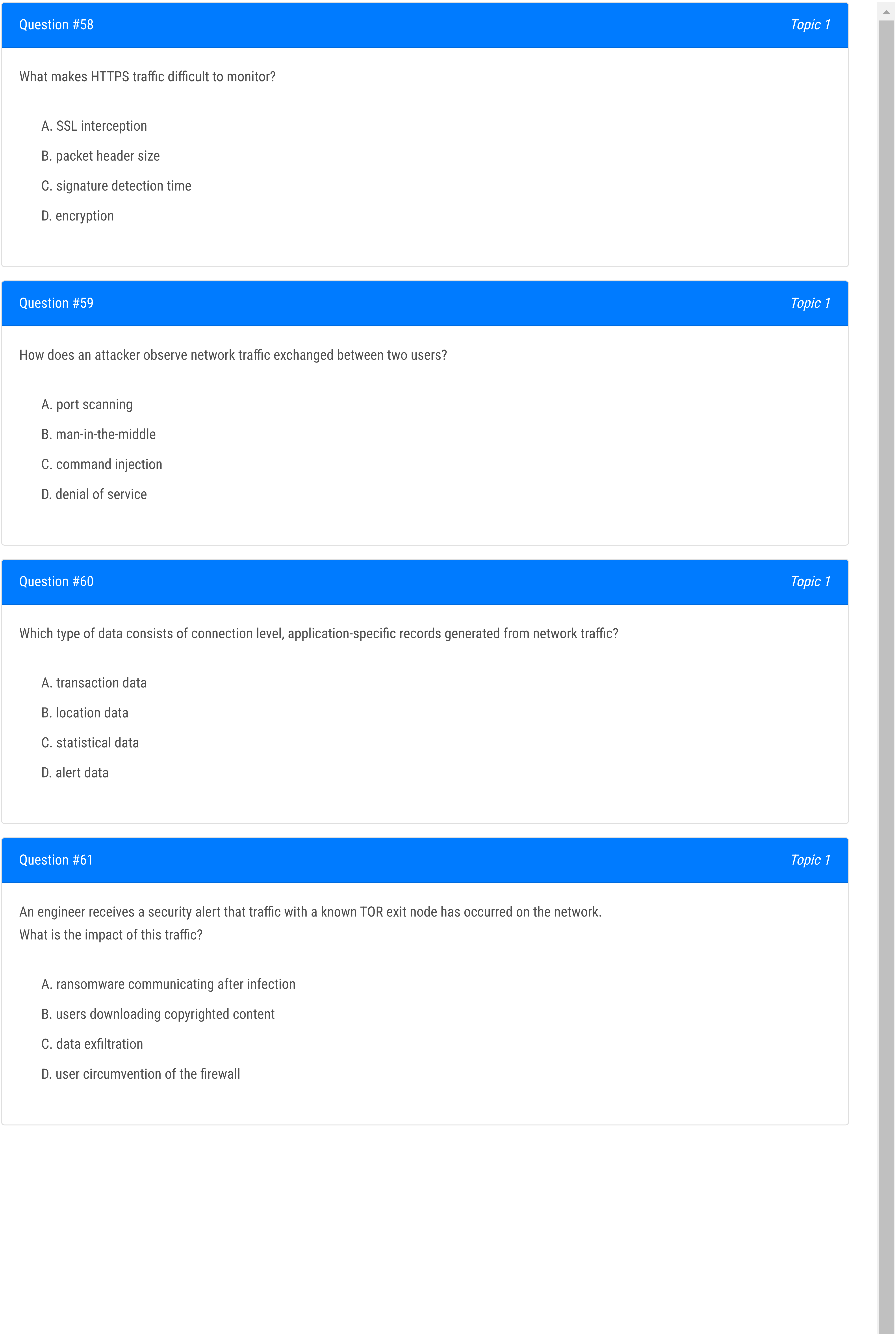
How is NetFlow different from traffic mirroring?

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.



Question #58 *Topic 1*

What makes HTTPS traffic difficult to monitor?

A. SSL interception

B. packet header size

C. signature detection time

D. encryption

Question #59 *Topic 1*

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

Question #60 *Topic 1*

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

Question #61 *Topic 1*

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

Question #62

Topic 1

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

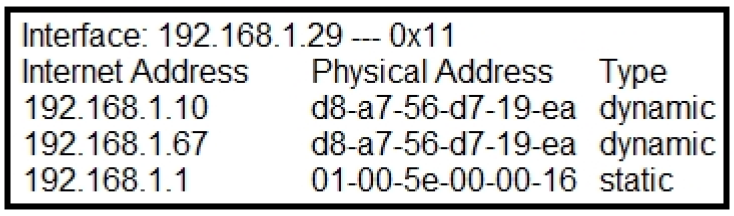
B. receiving an email from human resources requesting a visit to their secure website to update contact information

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

Question #63

Topic 1



```
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

Question #64

Topic 1

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

Question #65

Topic 1

Which action prevents buffer overflow attacks?

A. variable randomization

B. using web based applications

C. input validation

D. using a Linux operating system

Question #66 *Topic 1*

Which type of attack occurs when an attacker is successful in eavesdropping on a conversation between two IP phones?

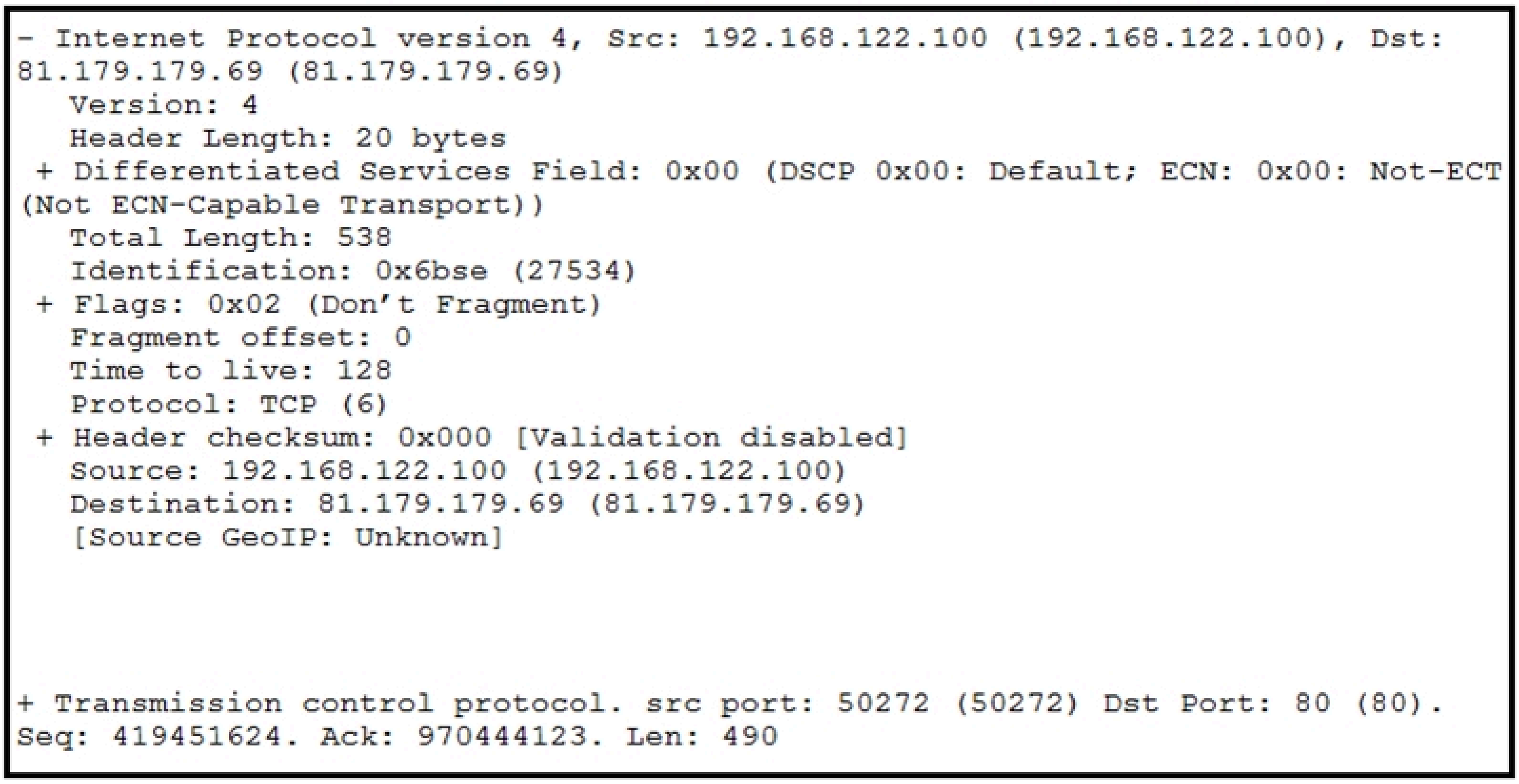
A. known-plaintext

B. replay

C. dictionary

D. man-in-the-middle

Question #67 *Topic 1*



```
- 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.

Question #68 *Topic 1*

What are the two characteristics of the full packet captures? (Choose two.)

A. Identifying network loops and collision domains.

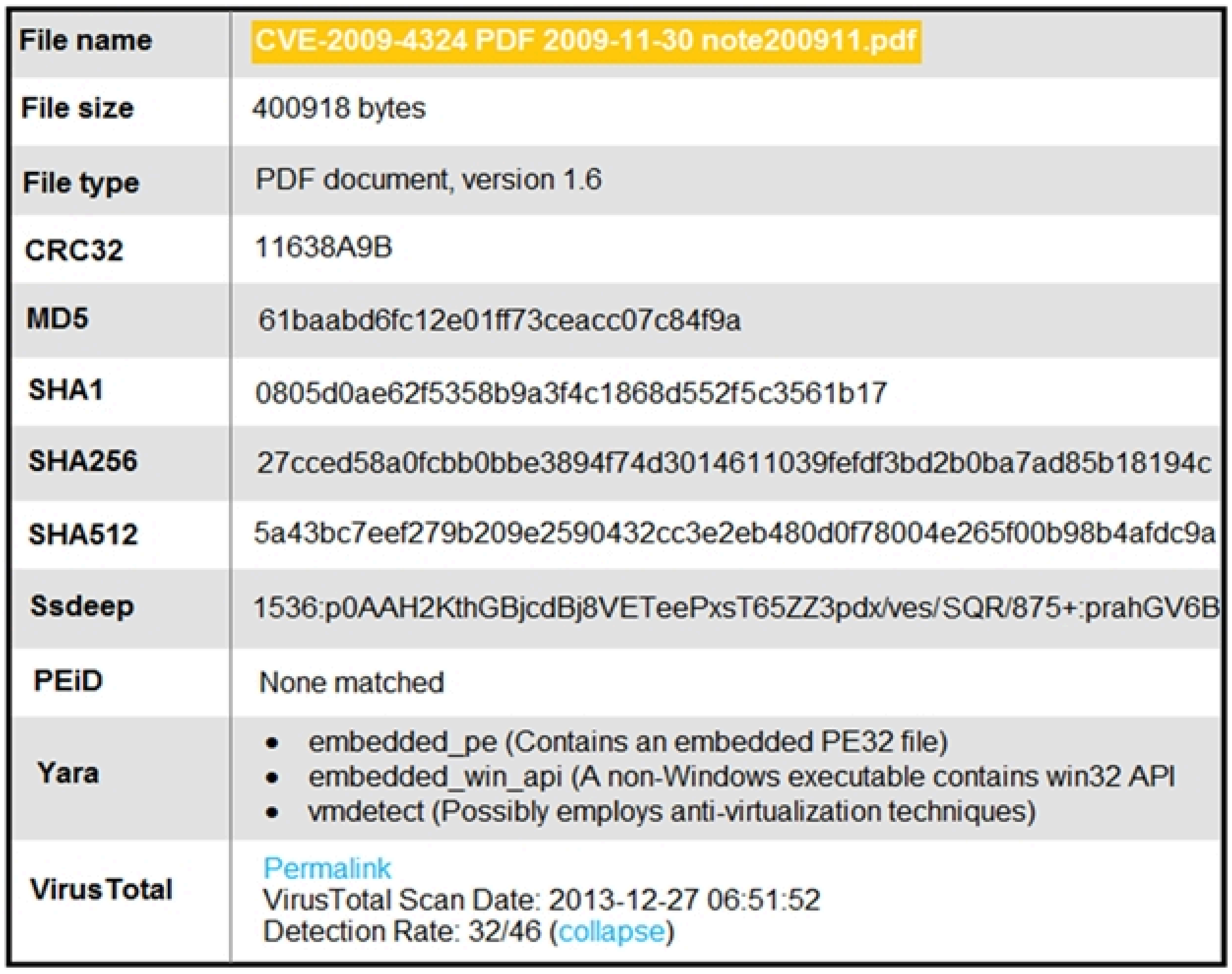
B. Troubleshooting the cause of security and performance issues.

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.

Question #69 Topic 1



File name	CVE-2009-4324 PDF 2009-11-30 note200911.pdf
File size	400918 bytes
File type	PDF document, version 1.6
CRC32	11638A9B
MD5	61baabd6fc12e01ff73ceacc07c84f9a
SHA1	0805d0ae62f5358b9a3f4c1868d552f5c3561b17
SHA256	27cced58a0fcbb0bbe3894f74d3014611039fefdf3bd2b0ba7ad85b18194c
SHA512	5a43bc7eef279b209e2590432cc3e2eb480d0f78004e265f00b98b4afdc9a
Ssdeep	1536:p0AAH2KthGBjcdBj8VETeePxsT65ZZ3pdx/ves/SQR/875+:prahGV6B
PEiD	None matched
Yara	• embedded_pe (Contains an embedded PE32 file) • embedded_win_api (A non-Windows executable contains win32 API • vmdetect (Possibly employs anti-virtualization techniques)
VirusTotal	Permalink VirusTotal Scan Date: 2013-12-27 06:51:52 Detection Rate: 32/46 (collapse)

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.

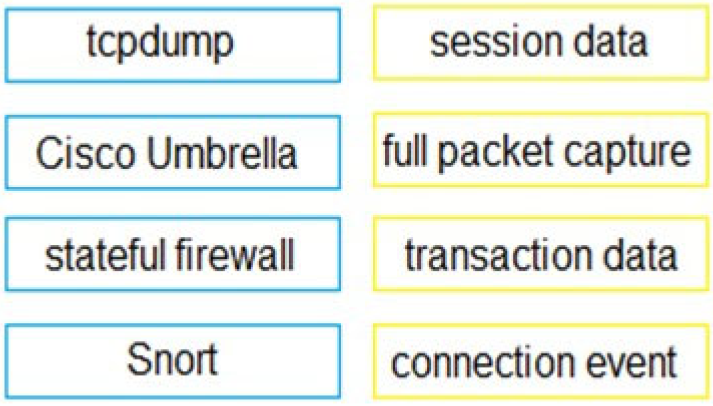
D. The file was matched by PEiD threat signatures but no suspicious features are identified since the signature list is up to date.

Question #70 Topic 1

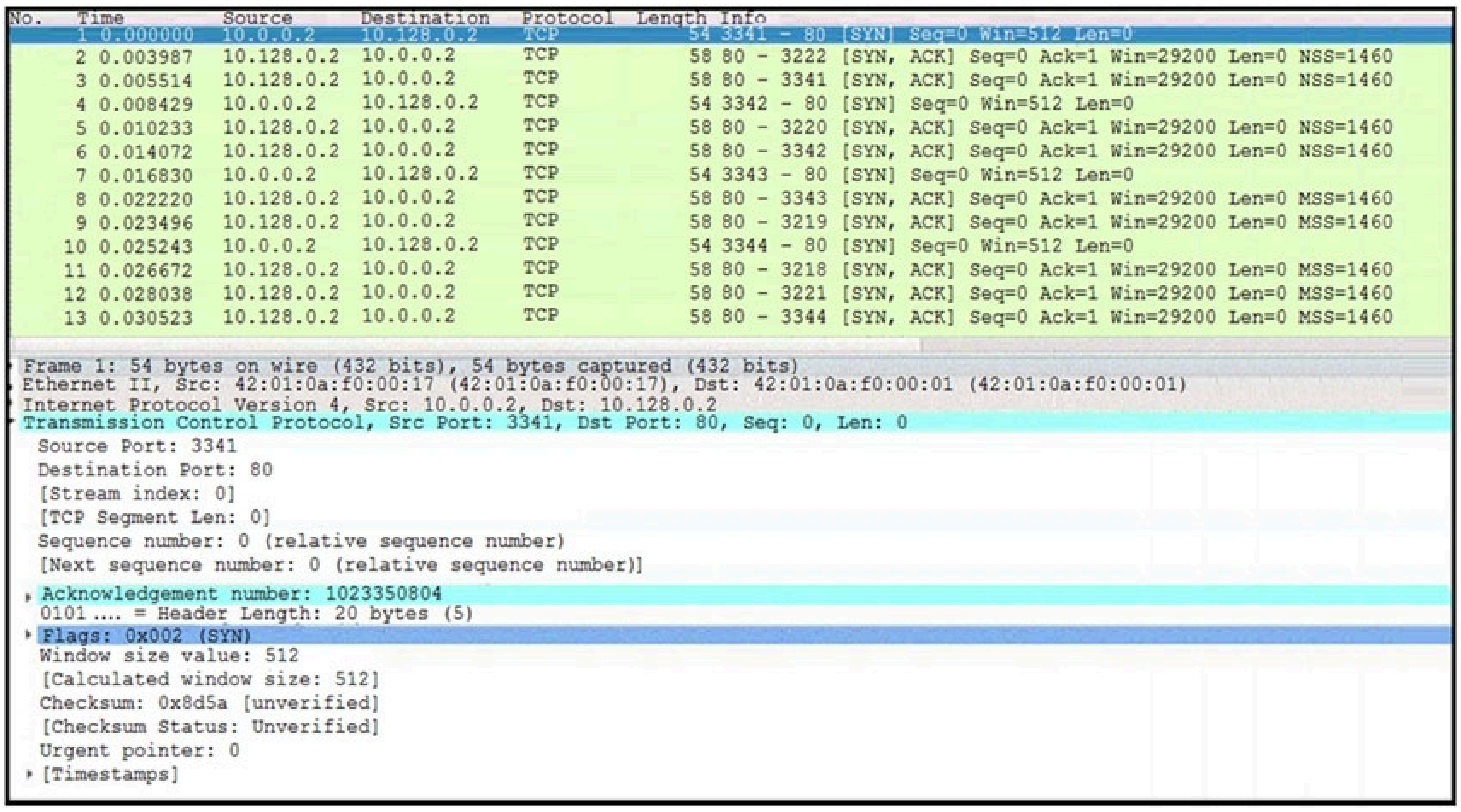
DRAG DROP -

Drag and drop the technology on the left onto the data type the technology provides on the right.

Select and Place:



Question #71 *Topic 1*



```
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.

Question #72 *Topic 1*

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

Question #73 *Topic 1*

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

Question #74 *Topic 1*

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

Question #75 *Topic 1*

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

Question #76 *Topic 1*

Which security monitoring data type requires the largest storage space?

A. transaction data

B. statistical data

C. session data

D. full packet capture

Question #77 *Topic 1*

What are two denial of service attacks? (Choose two.)

A. MITM

B. TCP connections

C. ping of death

D. UDP flooding

E. code red

Question #78 *Topic 1*

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 ג€"sP 192.168.1.0/24

C. nmap -sL 192.168.1.0/24

D. nmap -sV 192.168.1.0/24

Question #79 *Topic 1*

Which open-sourced packet capture tool uses Linux and Mac OS X operating systems?

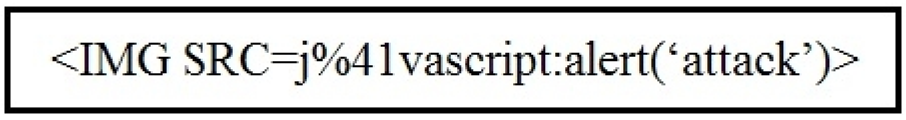
A. NetScout

B. tcpdump

C. SolarWinds

D. netsh

Question #80 *Topic 1*



```
<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

Question #81 *Topic 1*

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

Question #82 *Topic 1*

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

Question #83 *Topic 1*

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 fink 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

Question #84 *Topic 1*

What are two social engineering techniques? (Choose two.)

A. privilege escalation

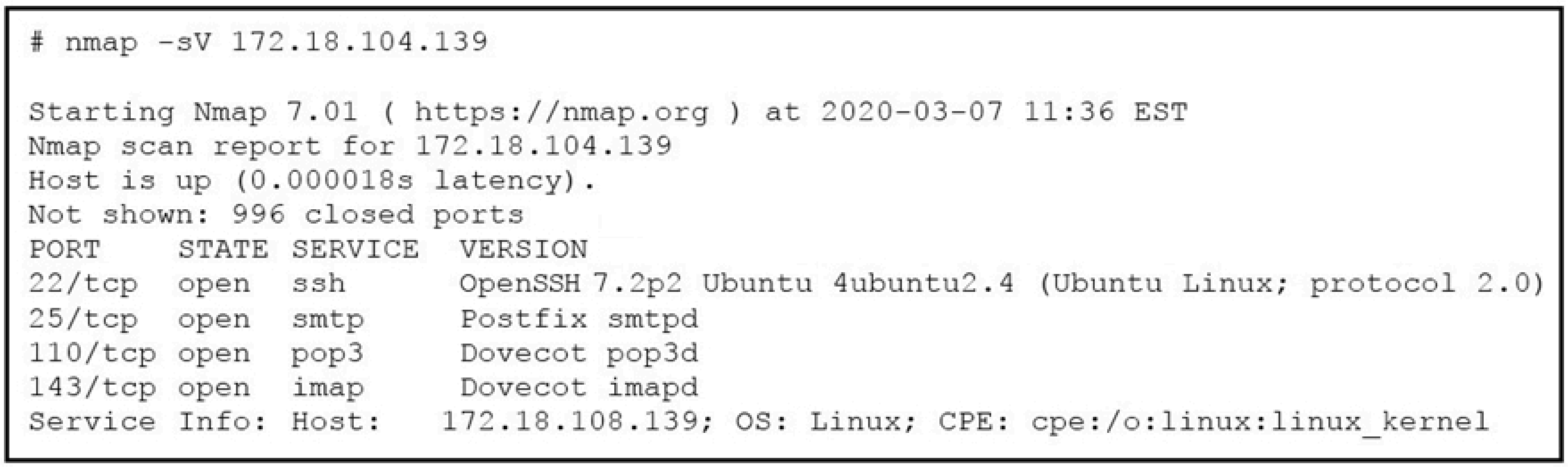
B. DDoS attack

C. phishing

D. man-in-the-middle

E. pharming

Question #85 *Topic 1*



```
# 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

Question #86 *Topic 1*

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.

Question #87 *Topic 1*

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

Question #88 *Topic 1*

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

Question #89 *Topic 1*

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

Question #90 *Topic 1*

Which attack represents the evasion technique of resource exhaustion?

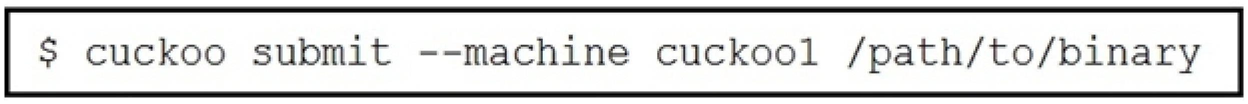
A. SQL injection

B. bluesnarfing

C. denial-of-service

D. man-in-the-middle

Question #91 *Topic 1*



```
$ 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.

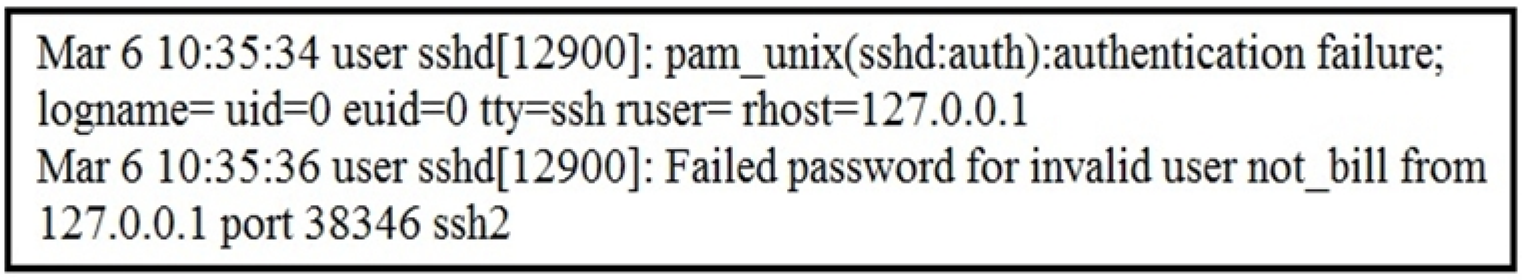
B. A binary is being submitted to run on VM cuckoo1

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

Question #92

Topic 1



```
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

Question #93

Topic 1

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

Question #94

Topic 1

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

Question #95

Topic 1

What causes events on a Windows system to show Event Code 4625 in the log messages?

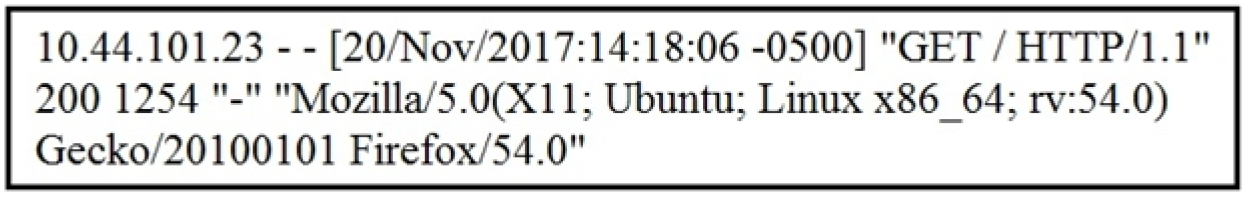
A. The system detected an XSS attack

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

Question #96 *Topic 1*



```
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?

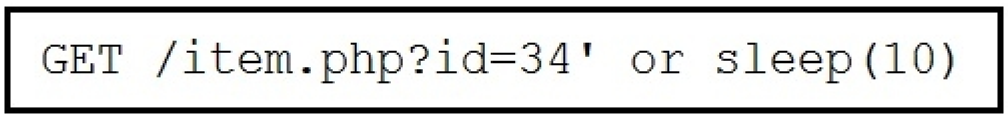
A. an access attempt was made from the Mosaic web browser

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

Question #97 *Topic 1*



```
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

Question #98 *Topic 1*

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

Question #99 *Topic 1*

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

Question #100 *Topic 1*

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

Question #101 *Topic 1*

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?

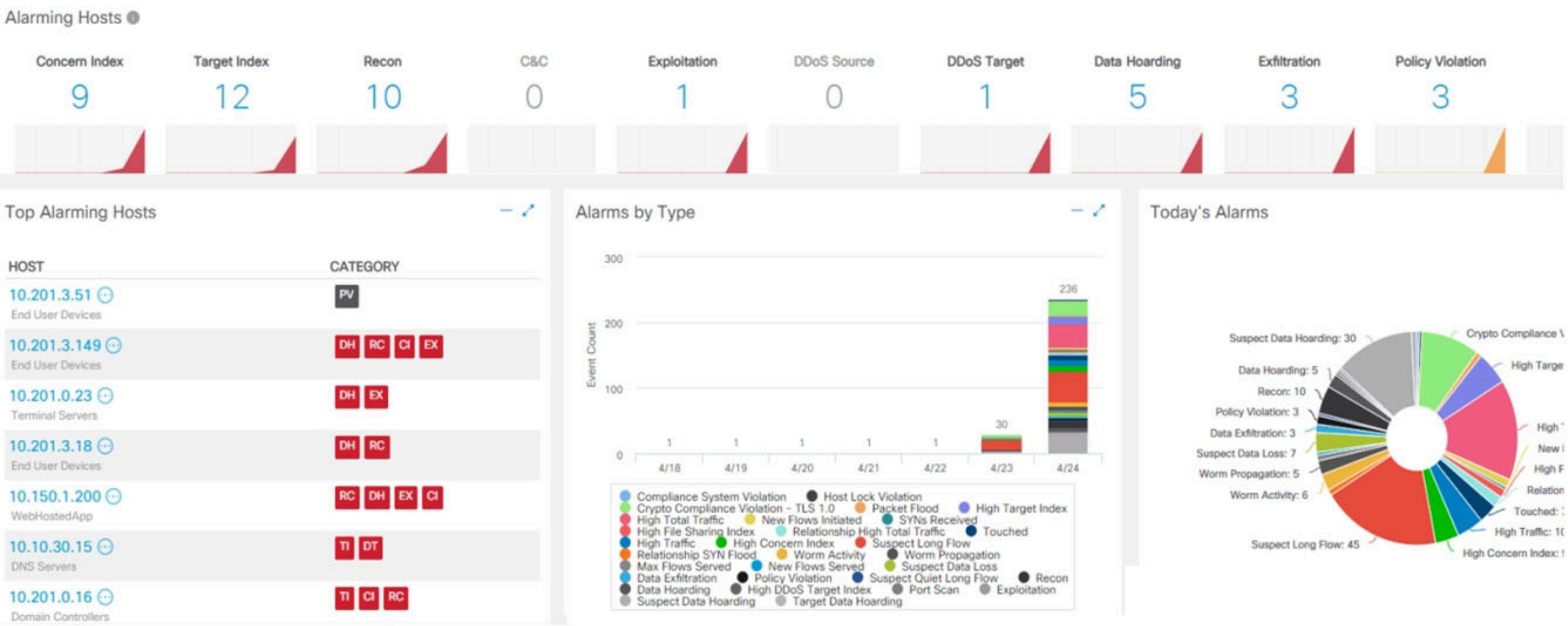
A. The computer has a HIPS installed on it.

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.

Question #102 *Topic 1*



Alarming Hosts

Concern Index	Target Index	Recon	C&C	Exploitation	DDoS Source	DDoS Target	Data Hoarding	Exfiltration	Policy Violation
9	12	10	0	1	0	1	5	3	3

Top Alarming Hosts

HOST	CATEGORY
10.201.3.51 End User Devices	PV
10.201.3.149 End User Devices	DH RC CI EX
10.201.0.23 Terminal Servers	DH EX
10.201.3.18 End User Devices	DH RC
10.150.1.200 WebHostedApp	RC DH EX CI
10.10.30.15 DNS Servers	TI DT
10.201.0.16 Domain Controllers	TI CI RC

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.

Question #103 *Topic 1*

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.

Question #104 *Topic 1*

What is a sandbox interprocess communication service?

A. A collection of rules within the sandbox that prevent the communication between sandboxes.

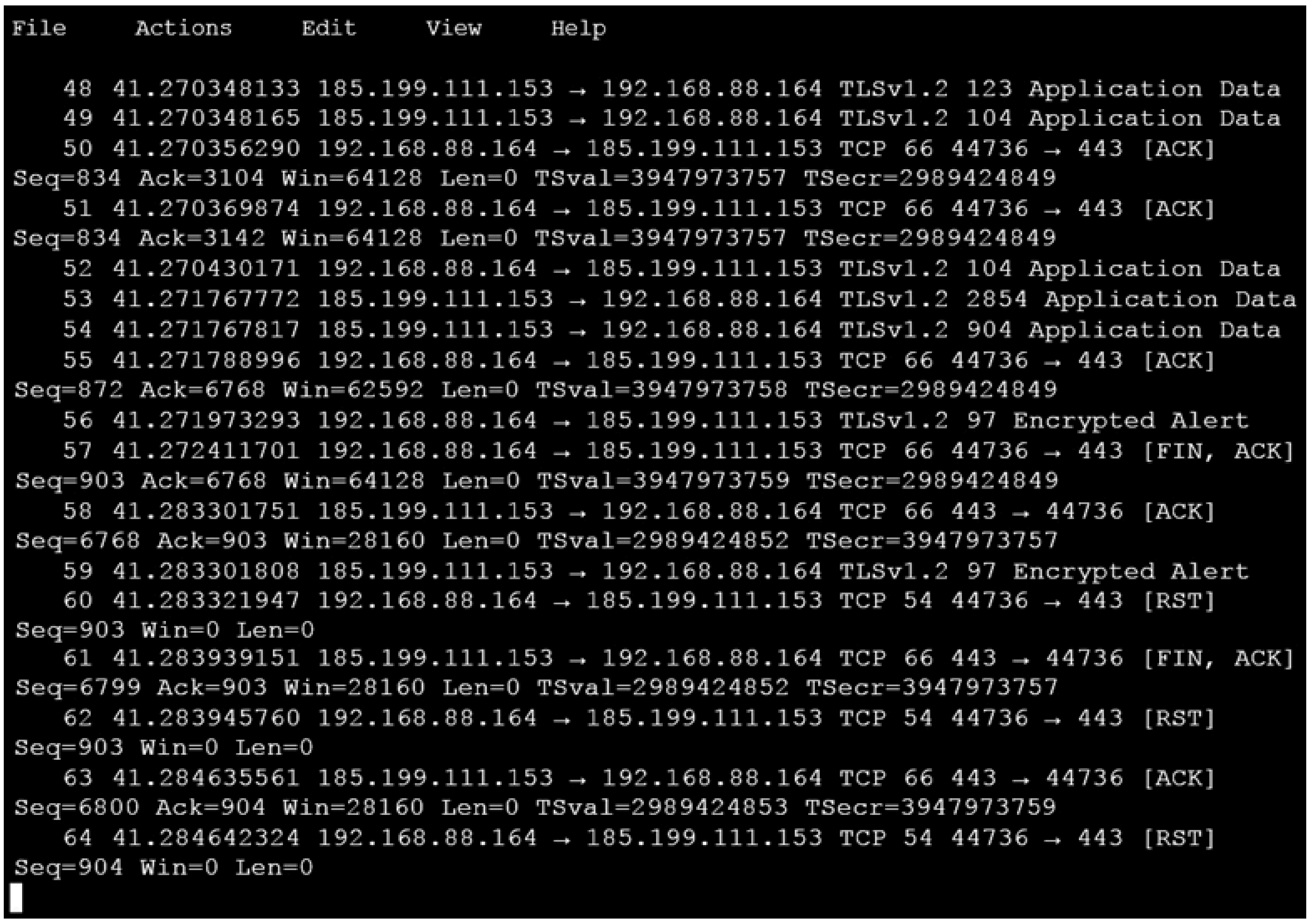
B. A collection of network services that are activated on an interface, allowing for inter-port communication.

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.

Question #105

Topic 1



```
   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

Question #106

Topic 1

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

Question #107 *Topic 1*

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

Question #108 *Topic 1*

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

Question #109 *Topic 1*

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

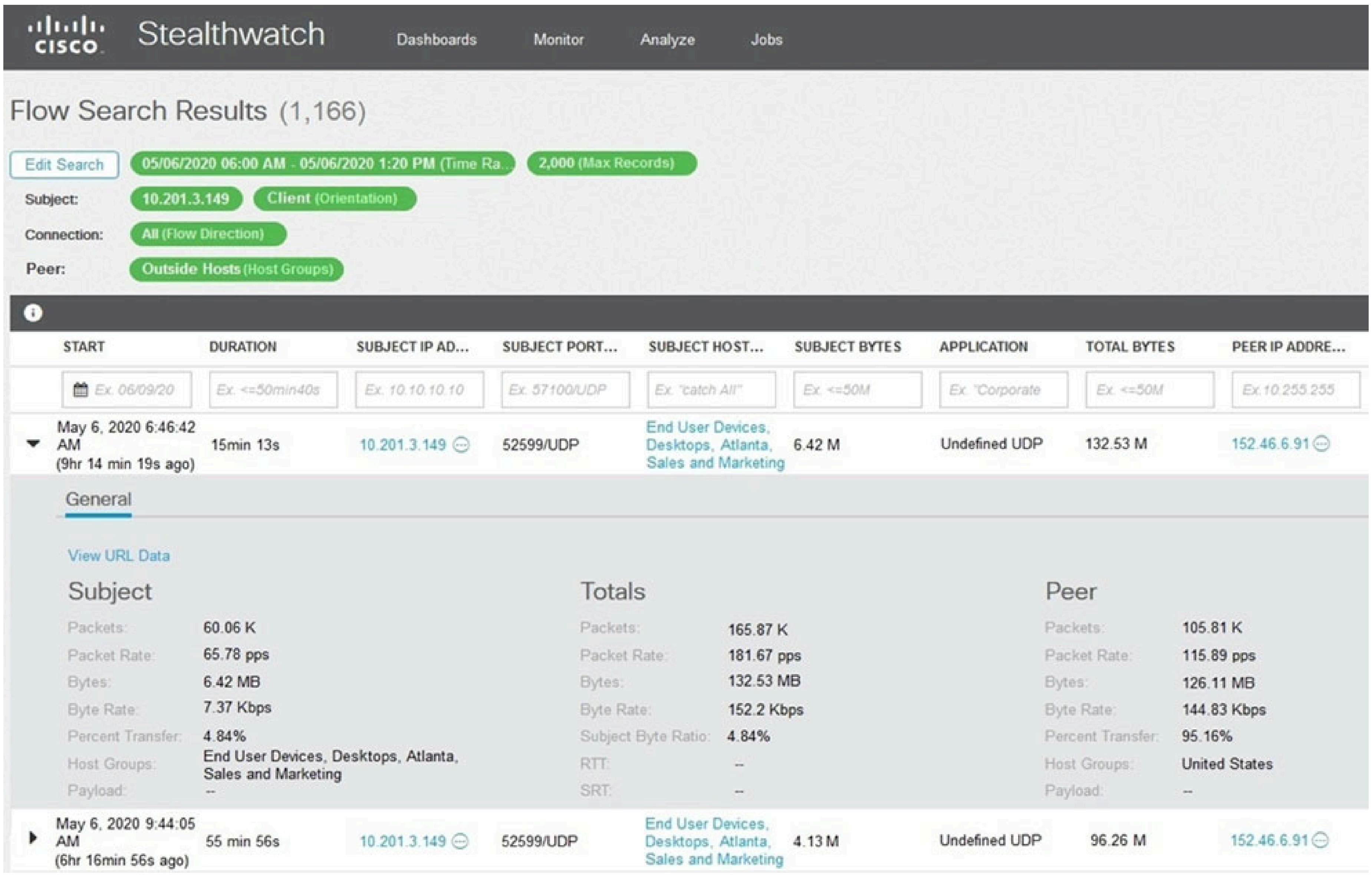
B. file size

C. file name

D. file hash value

Question #110

Topic 1



Flow Search Results (1,166)

Edit Search | 05/06/2020 06:00 AM - 05/06/2020 1:20 PM (Time Ra... | 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 ADDRE...
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:	--

START	DURATION	SUBJECT IP AD...	SUBJECT PORT...	SUBJECT HOST...	SUBJECT BYTES	APPLICATION	TOTAL BYTES	PEER IP ADDRE...
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.

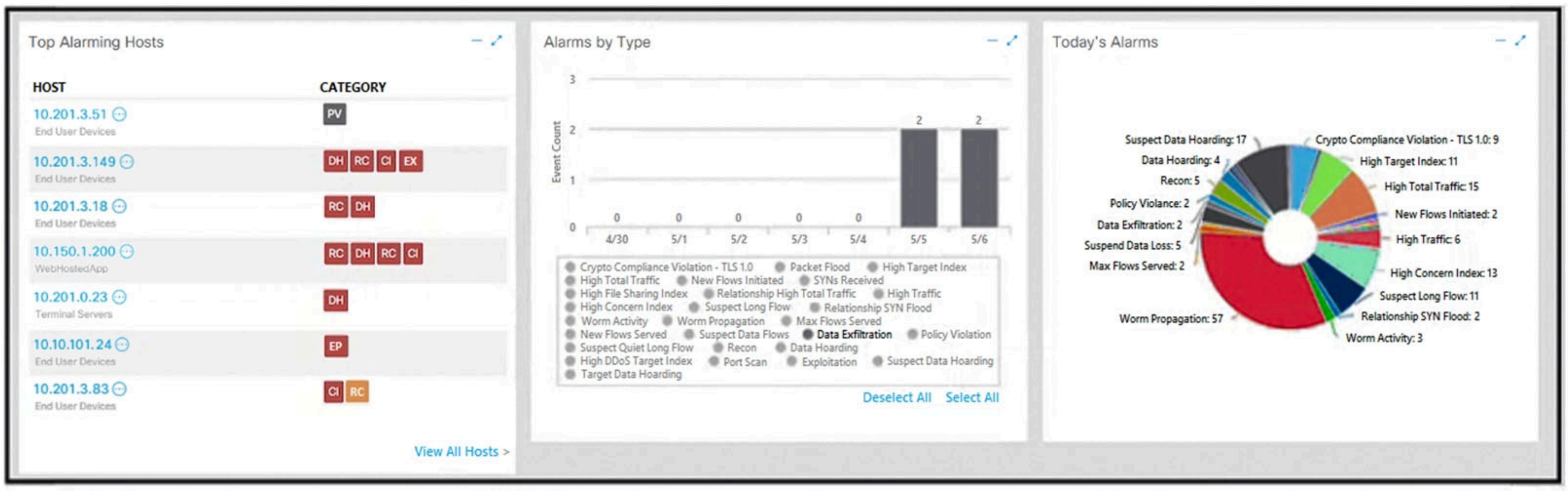
B. Host 152.46.6.91 is being identified as a watchlist country for data transfer.

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.

Question #111

Topic 1



Top Alarming Hosts

HOST	CATEGORY
10.201.3.51 End User Devices	PV
10.201.3.149 End User Devices	DH RC CI EX
10.201.3.18 End User Devices	RC DH
10.150.1.200 WebHostedApp	RC DH RC CI
10.201.0.23 Terminal Servers	DH
10.10.101.24 End User Devices	EP
10.201.3.83 End User Devices	CI RC

View All Hosts >

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.

Question #112 *Topic 1*

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

Question #113 *Topic 1*

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

Question #114 *Topic 1*

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 arid fail logs

Question #115 *Topic 1*

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

Question #116 *Topic 1*

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

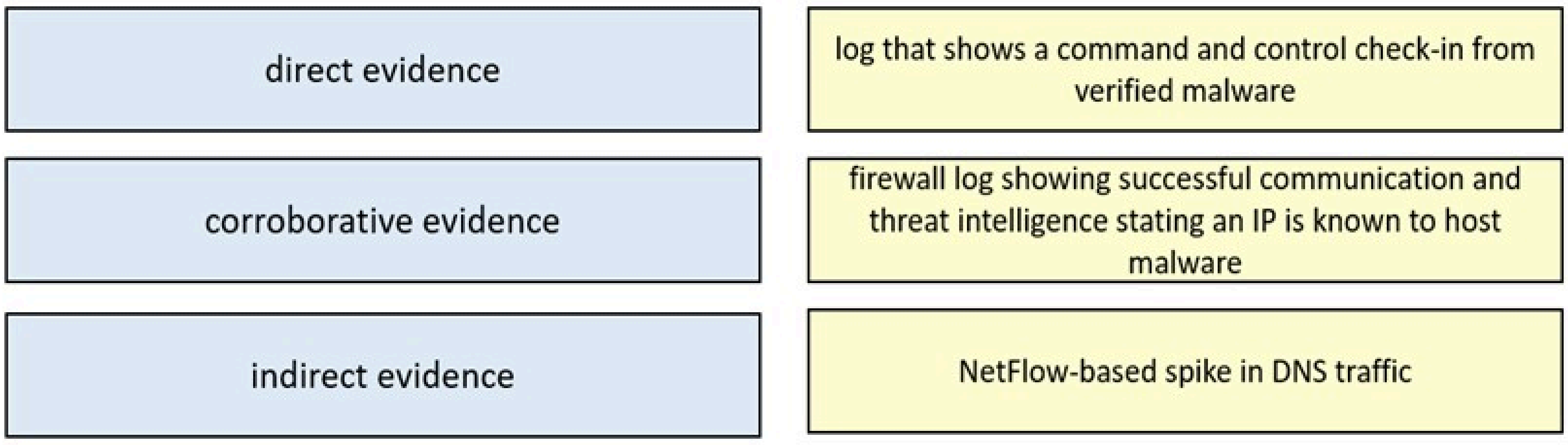
B. prima facie evidence

C. indirect evidence

D. physical evidence

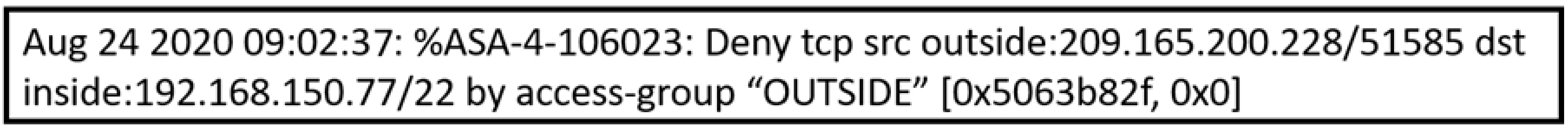
Question #117 *Topic 1*

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

Question #118 *Topic 1*



```
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?

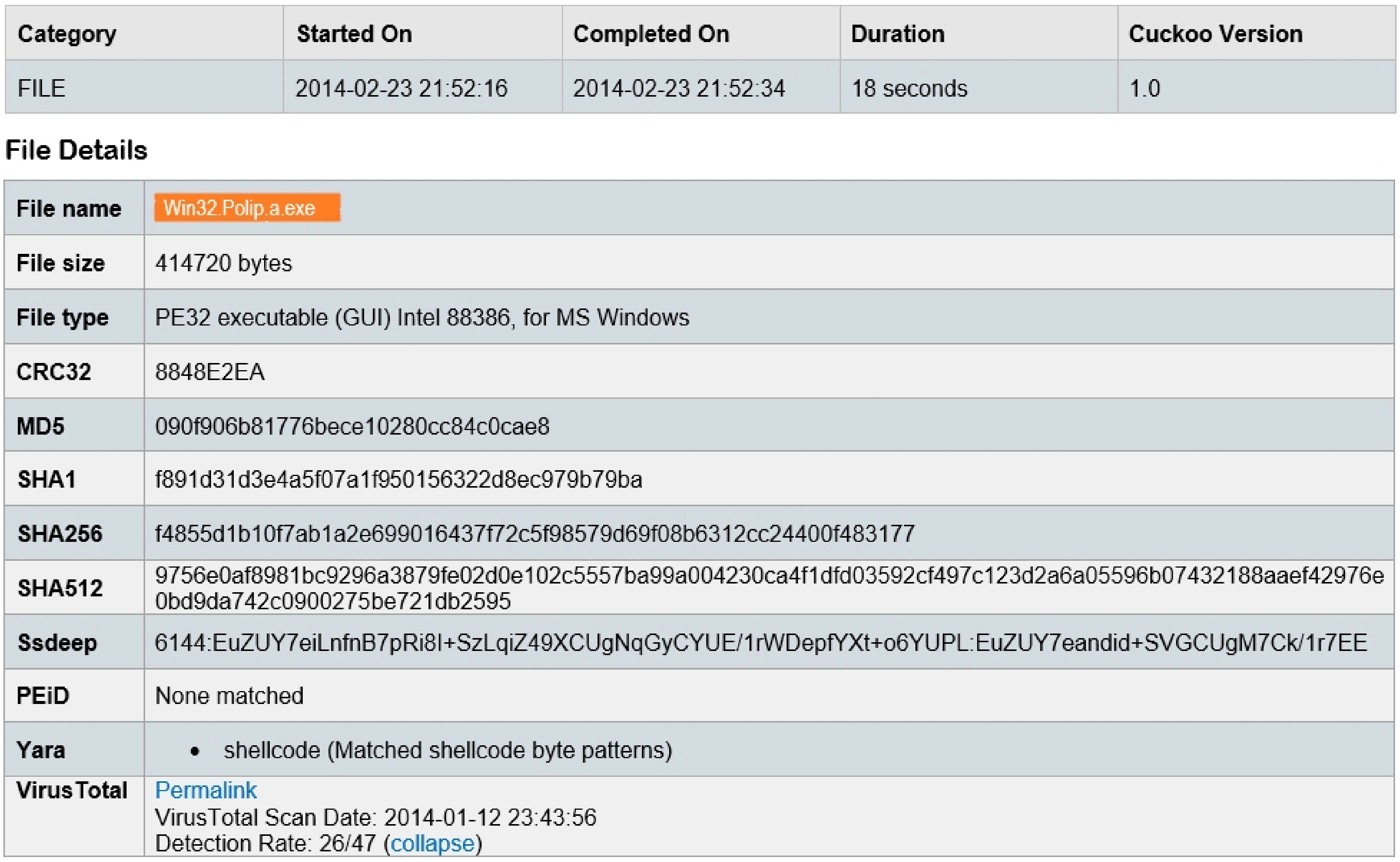
A. indirect

B. circumstantial

C. corroborative

D. best

Question #119 *Topic 1*



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

File name	Win32.Polip.a.exe
File size	414720 bytes
File type	PE32 executable (GUI) Intel 88386, for MS Windows
CRC32	8848E2EA
MD5	090f906b81776bece10280cc84c0cae8
SHA1	f891d31d3e4a5f07a1f950156322d8ec979b79ba
SHA256	f4855d1b10f7ab1a2e699016437f72c5f98579d69f08b6312cc24400f483177
SHA512	9756e0af8981bc9296a3879fe02d0e102c5557ba99a004230ca4f1dfd03592cf497c123d2a6a05596b07432188aaef42976e0bd9da742c0900275be721db2595
Ssdeep	6144:EuZUY7eiLnfnB7pRi8l+SzLqiZ49XCUgNqGyCYUE/1rWDepfYXt+o6YUPL:EuZUY7eandid+SVGCUgM7Ck/1r7EE
PEiD	None matched
Yara	• shellcode (Matched shellcode byte patterns)
VirusTotal	Permalink VirusTotal Scan Date: 2014-01-12 23:43:56 Detection Rate: 26/47 (collapse)

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

Question #120 *Topic 1*

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

Question #121 *Topic 1*

Which technology on a host is used to isolate a running application from other application?

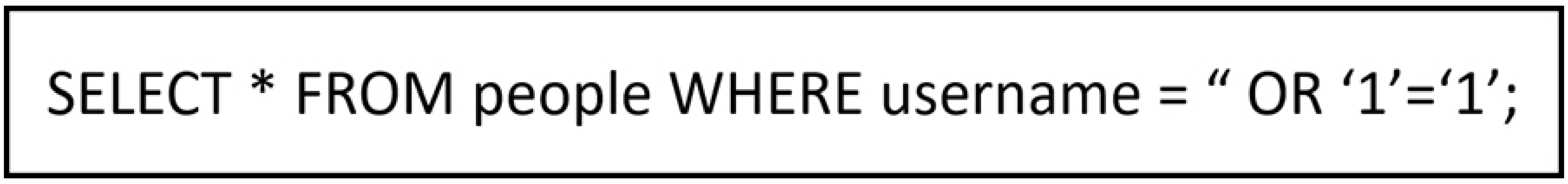
A. application allow list

B. application block list

C. host-based firewall

D. sandbox

Question #122 *Topic 1*



```
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

Question #123 *Topic 1*

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

Question #124 *Topic 1*

A system administrator is ensuring that specific registry information is accurate.
Which type of configuration information does the HKEY_LOCAL_MACHINE hive contain?

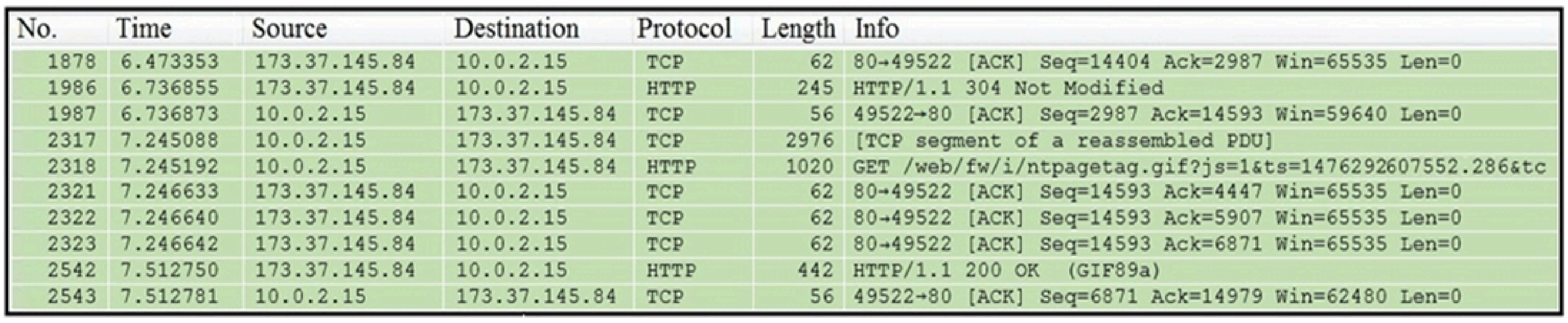
A. file extension associations

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

Question #125 *Topic 1*



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/ntpagetag.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

Question #126 *Topic 1*

Which regex matches only on all lowercase letters?

A. [aλˆ’z]+

B. [^aλˆ’z]+

C. aλˆ’z+

D. a*z+

Question #127 *Topic 1*

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

Question #128 *Topic 1*

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.

Question #129 *Topic 1*

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.

Question #130 *Topic 1*

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?

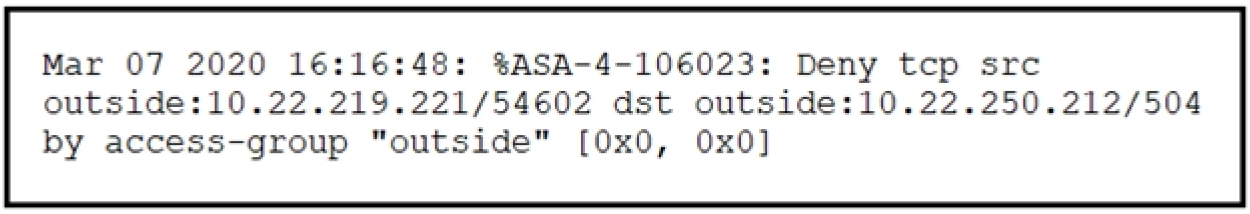
A. Firepower

B. Email Security Appliance

C. Web Security Appliance

D. Stealthwatch

Question #131 *Topic 1*



```
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

Question #132 *Topic 1*

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

Question #133 *Topic 1*

Which tool provides a full packet capture from network traffic?

A. Nagios

B. CAINE

C. Hydra

D. Wireshark

Question #134 *Topic 1*

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?

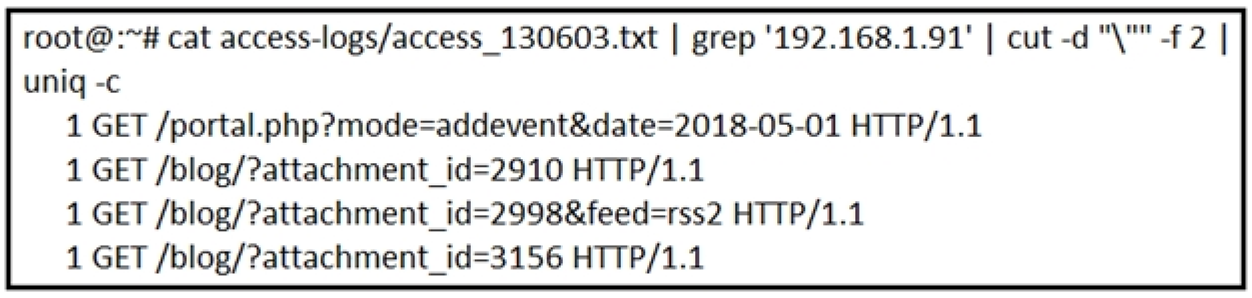
A. total throughput on the interface of the router and NetFlow records

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

Question #135 *Topic 1*



```
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

Question #136 *Topic 1*

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

Question #137 *Topic 1*

Which regular expression matches "color" and "colour"?

A. colo?ur

B. col[08’ˆג]+our

C. colou?r

D. col[09’ˆג]+our

Question #138 *Topic 1*

Which artifact is used to uniquely identify a detected file?

A. file timestamp

B. file extension

C. file size

D. file hash

Question #139 *Topic 1*

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

Question #140 *Topic 1*

Which utility blocks a host portscan?

A. HIDS

B. sandboxing

C. host-based firewall

D. antimalware

Question #141 Topic 1

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

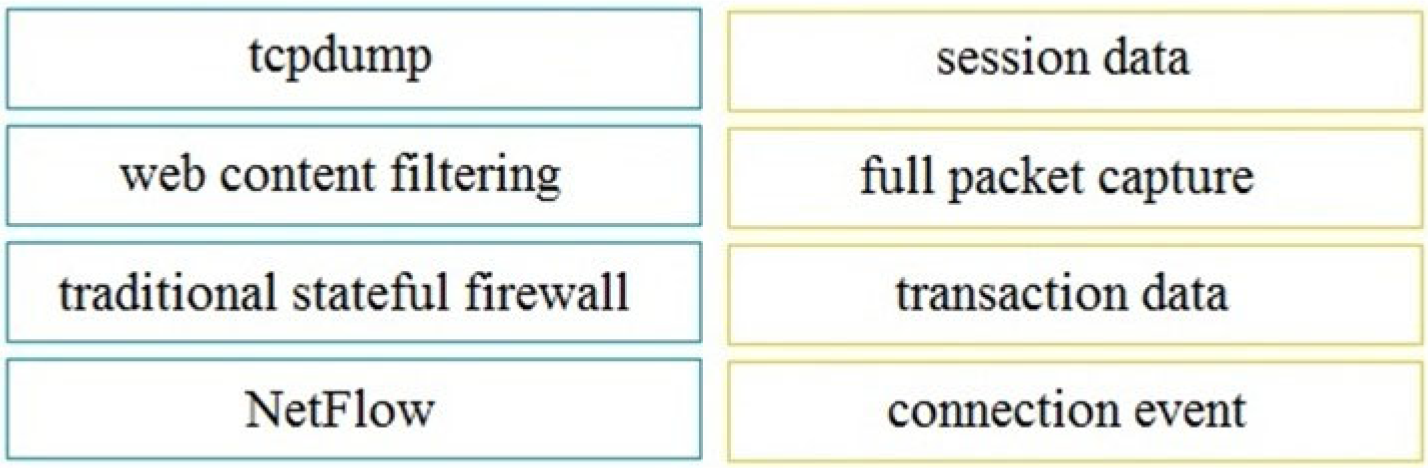
D. timing attack

Question #142 Topic 1

DRAG DROP -

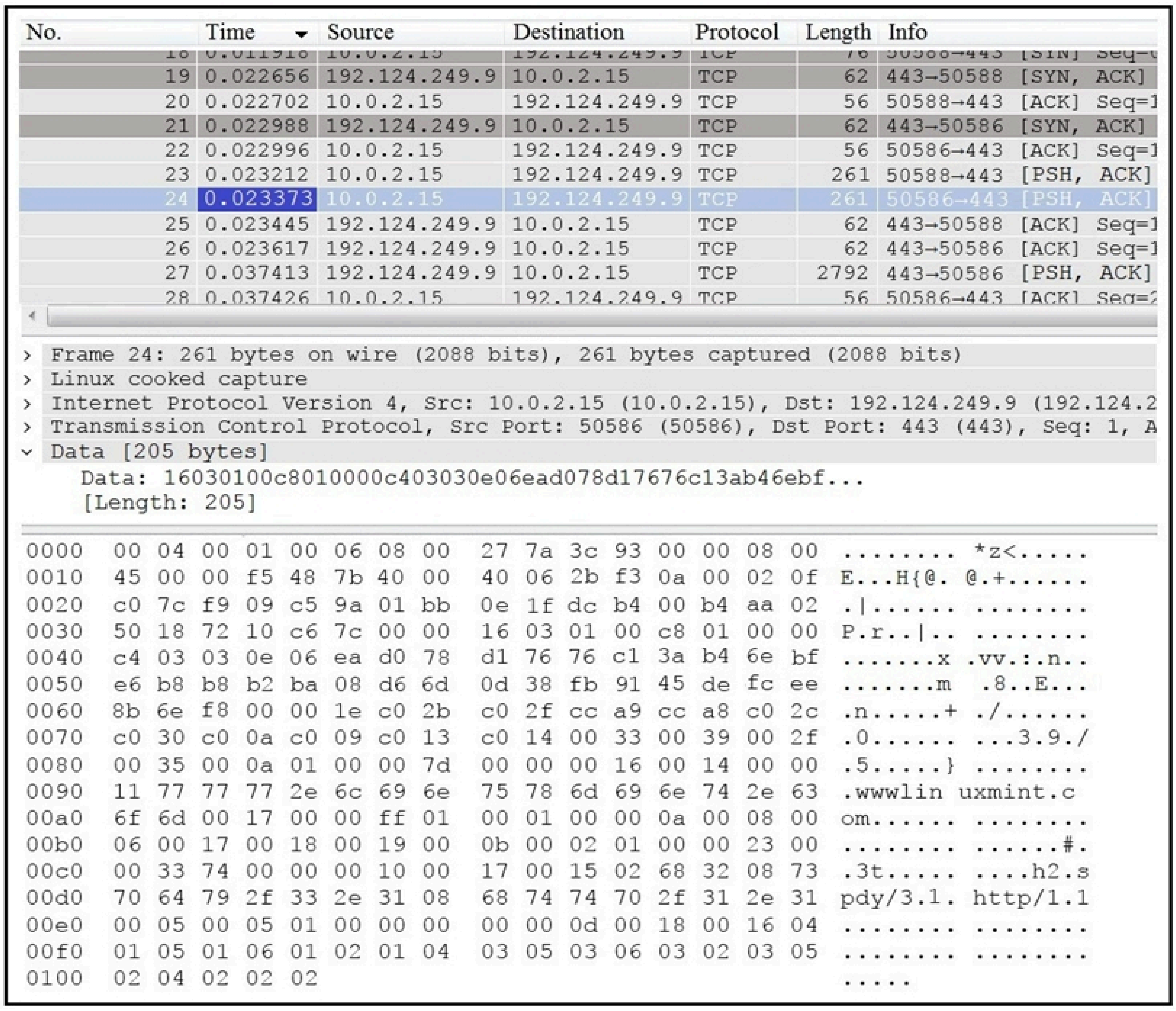
Drag and drop the technology on the left onto the data type the technology provides on the right.

Select and Place:



tcpdump	session data
web content filtering	full packet capture
traditional stateful firewall	transaction data
NetFlow	connection event

Question #143 *Topic 1*



No.	Time	Source	Destination	Protocol	Length	Info
18	0.011918	10.0.2.15	192.124.249.9	TCP	76	50588→443 [SYN] Seq=0
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 (192.124.2
> Transmission Control Protocol, Src Port: 50586 (50586), Dst Port: 443 (443), Seq: 1, A
v 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

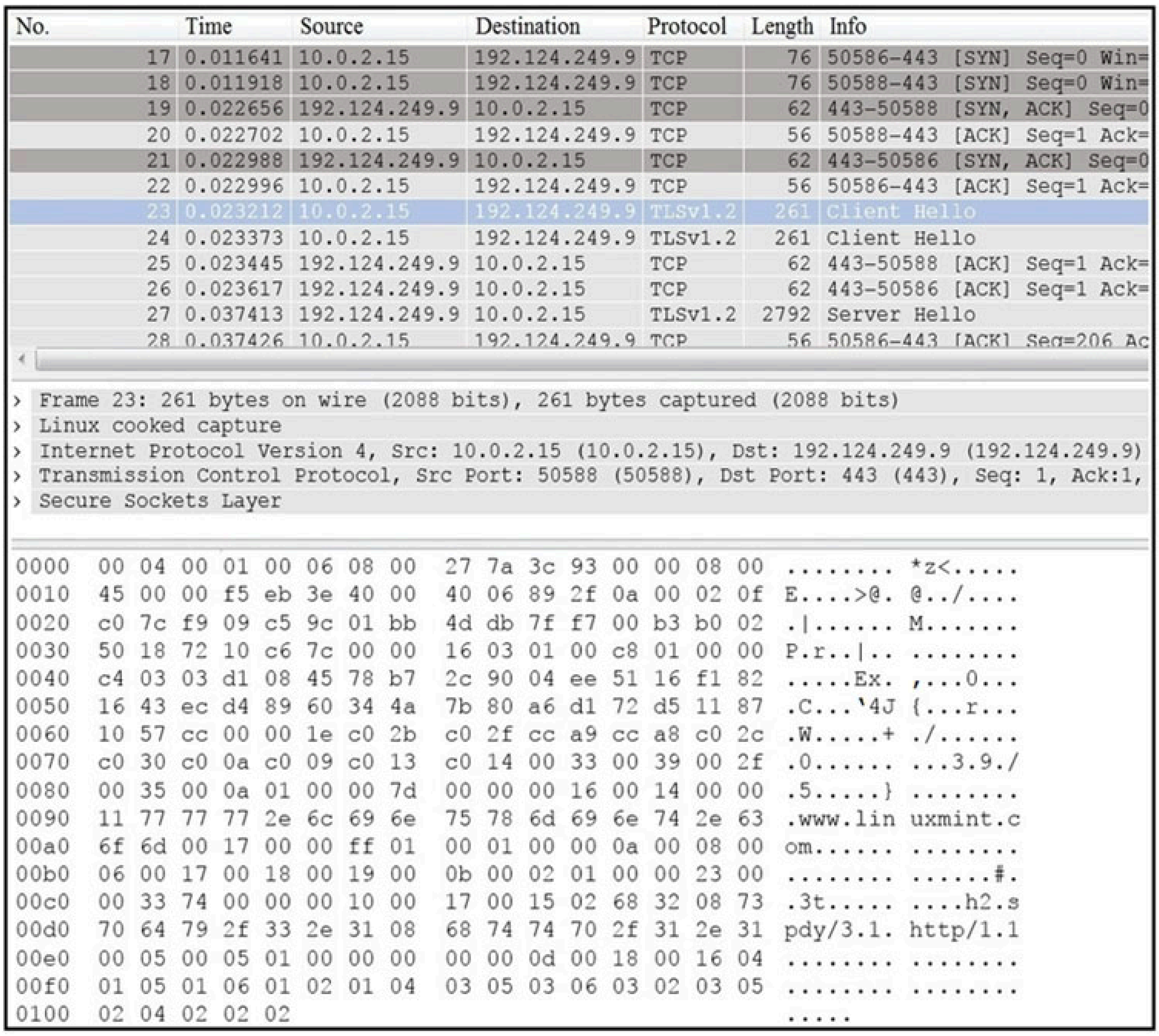
B. TCP

C. TLS

D. HTTP

Question #144 *Topic 1*

DRAG DROP -



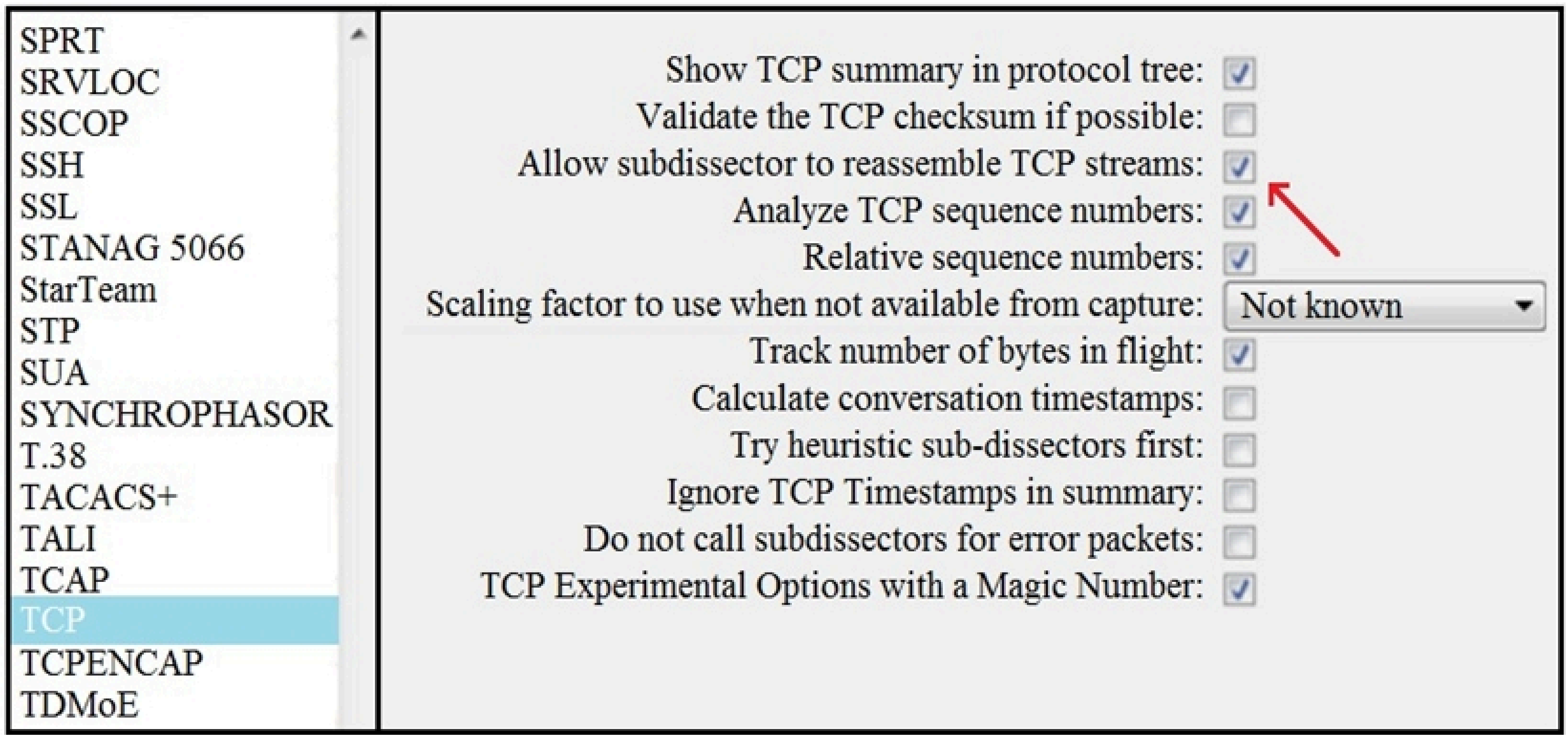
```
No.        Time     Source          Destination     Protocol Length Info
        17 0.011641 10.0.2.15       192.124.249.9   TCP          76 50586-443 [SYN] Seq=0 Win=
        18 0.011918 10.0.2.15       192.124.249.9   TCP          76 50588-443 [SYN] Seq=0 Win=
        19 0.022656 192.124.249.9   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

Question #145 *Topic 1*



Show TCP summary in protocol tree: ☑
Validate the TCP checksum if possible: □
Allow subdissector to reassemble TCP streams: ☑
Analyze TCP sequence numbers: ☑
Relative sequence numbers: ☑
Scaling factor to use when not available from capture: Not known
Track number of bytes in flight: ☑
Calculate conversation timestamps: □
Try heuristic sub-dissectors first: □
Ignore TCP Timestamps in summary: □
Do not call subdissectors for error packets: □
TCP Experimental Options with a Magic Number: ☑

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

Question #146 *Topic 1*

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

Question #147 *Topic 1*

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

Question #148 *Topic 1*

Which signature impacts network traffic by causing legitimate traffic to be blocked?

A. false negative

B. true positive

C. true negative

D. false positive

Question #149 *Topic 1*

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

Question #150 *Topic 1*

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

Question #151 *Topic 1*

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

Question #152 *Topic 1*

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

Question #153 *Topic 1*

At which layer is deep packet inspection investigated on a firewall?

A. internet

B. transport

C. application

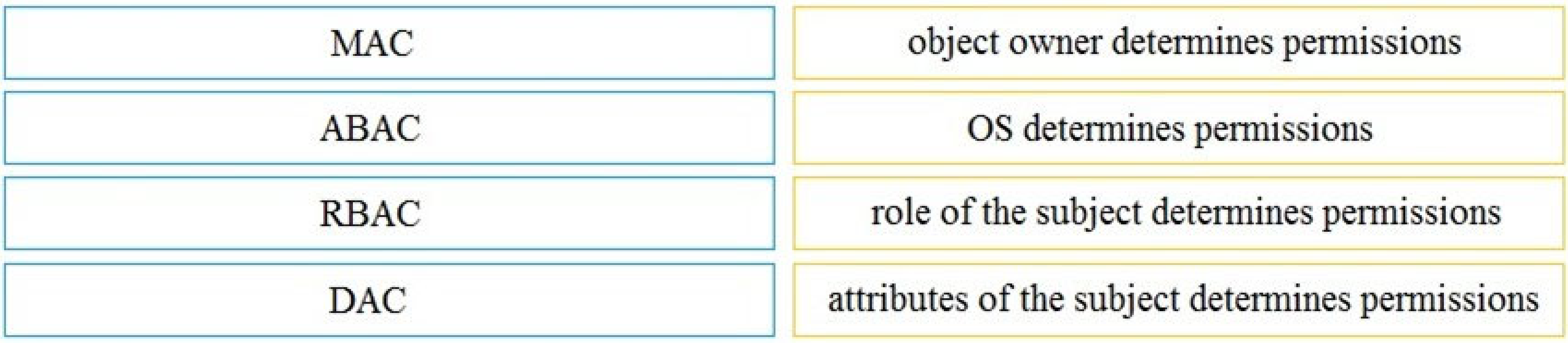
D. data link

Question #154 *Topic 1*

DRAG DROP -

Drag and drop the access control models from the left onto its corresponding descriptions on the right.

Select and Place:



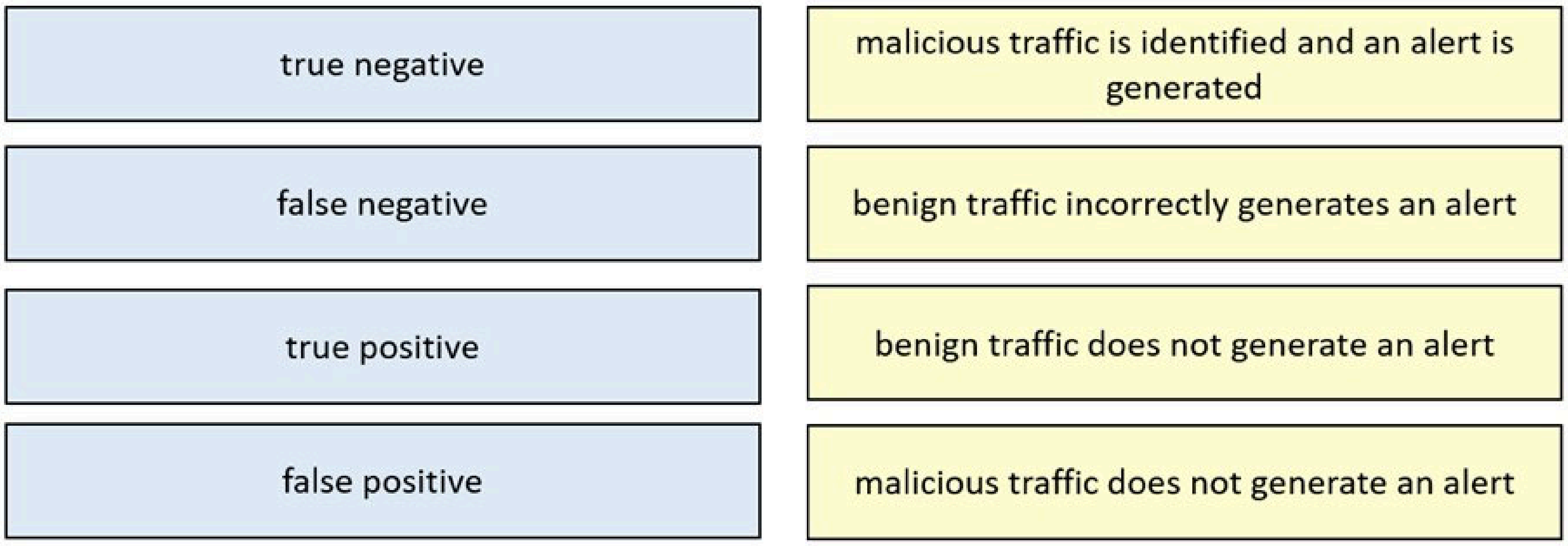
MAC	object owner determines permissions
ABAC	OS determines permissions
RBAC	role of the subject determines permissions
DAC	attributes of the subject determines permissions

Question #155 *Topic 1*

DRAG DROP -

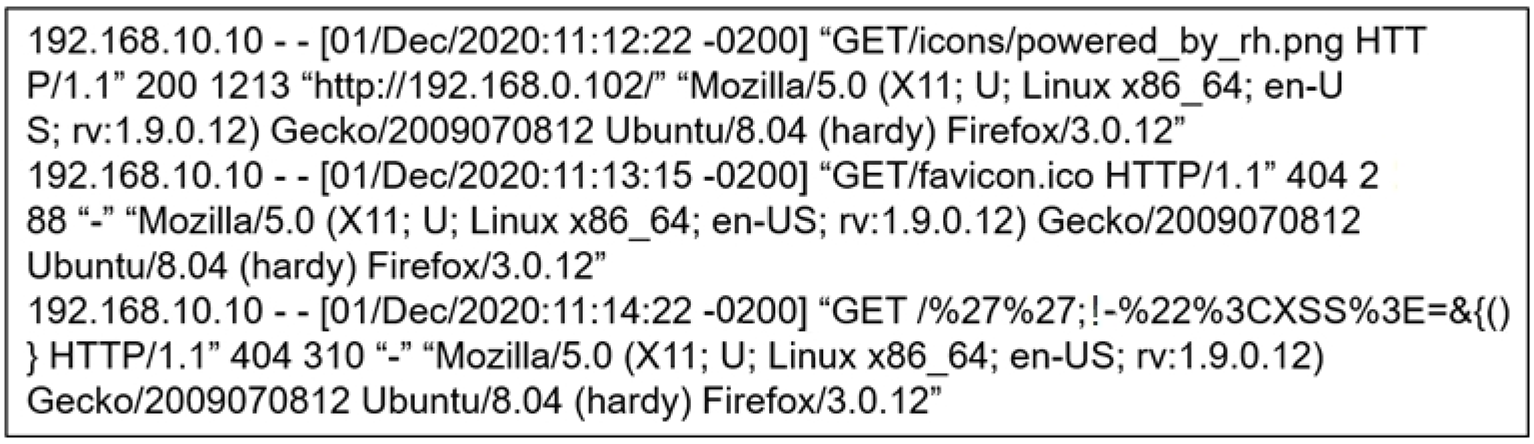
Drag and drop the event term from the left onto the description on the right.

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

Question #156 *Topic 1*



```
192.168.10.10 - - [01/Dec/2020:11:12:22 -0200] “GET/icons/powered_by_rh.png HTT
P/1.1” 200 1213 “http://192.168.0.102/” “Mozilla/5.0 (X11; U; Linux x86_64; en-U
S; 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 2
88 “-” “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

Question #157 *Topic 1*

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.

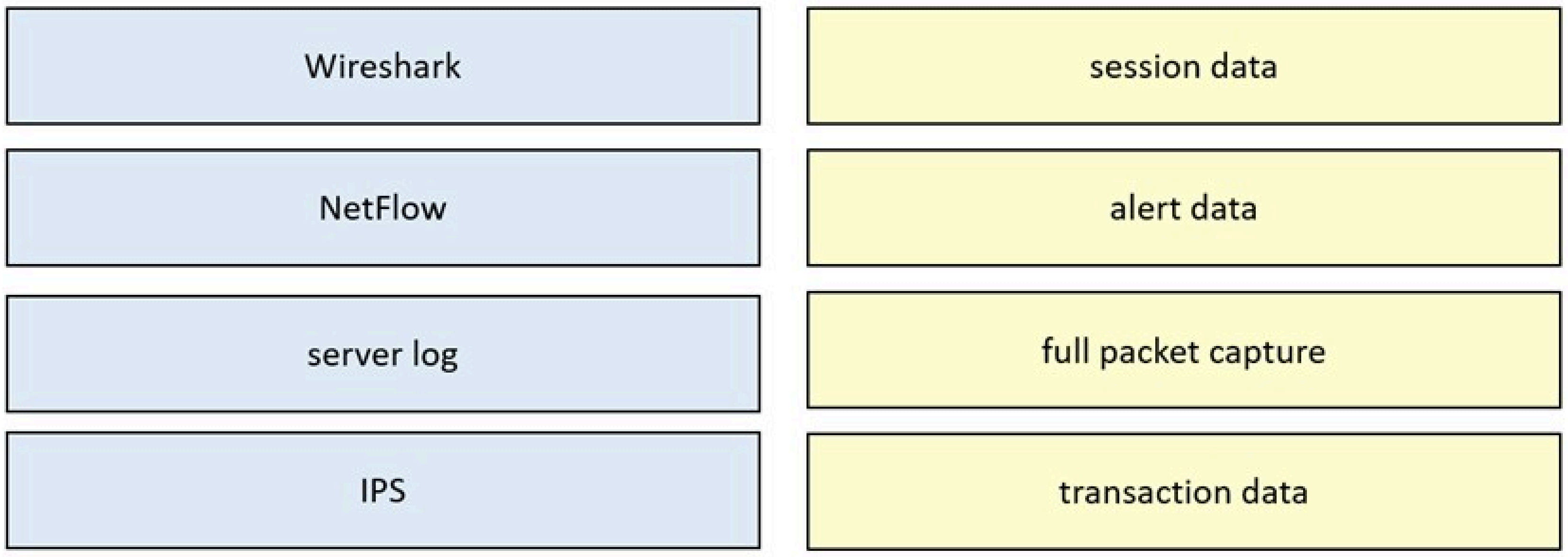
D. Tap sends traffic from physical layers to the monitoring device, while SPAN provides a copy of network traffic from switch to destination.

Question #158 *Topic 1*

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

Question #159 *Topic 1*

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

Question #160 *Topic 1*

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.

Question #161 *Topic 1*

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?

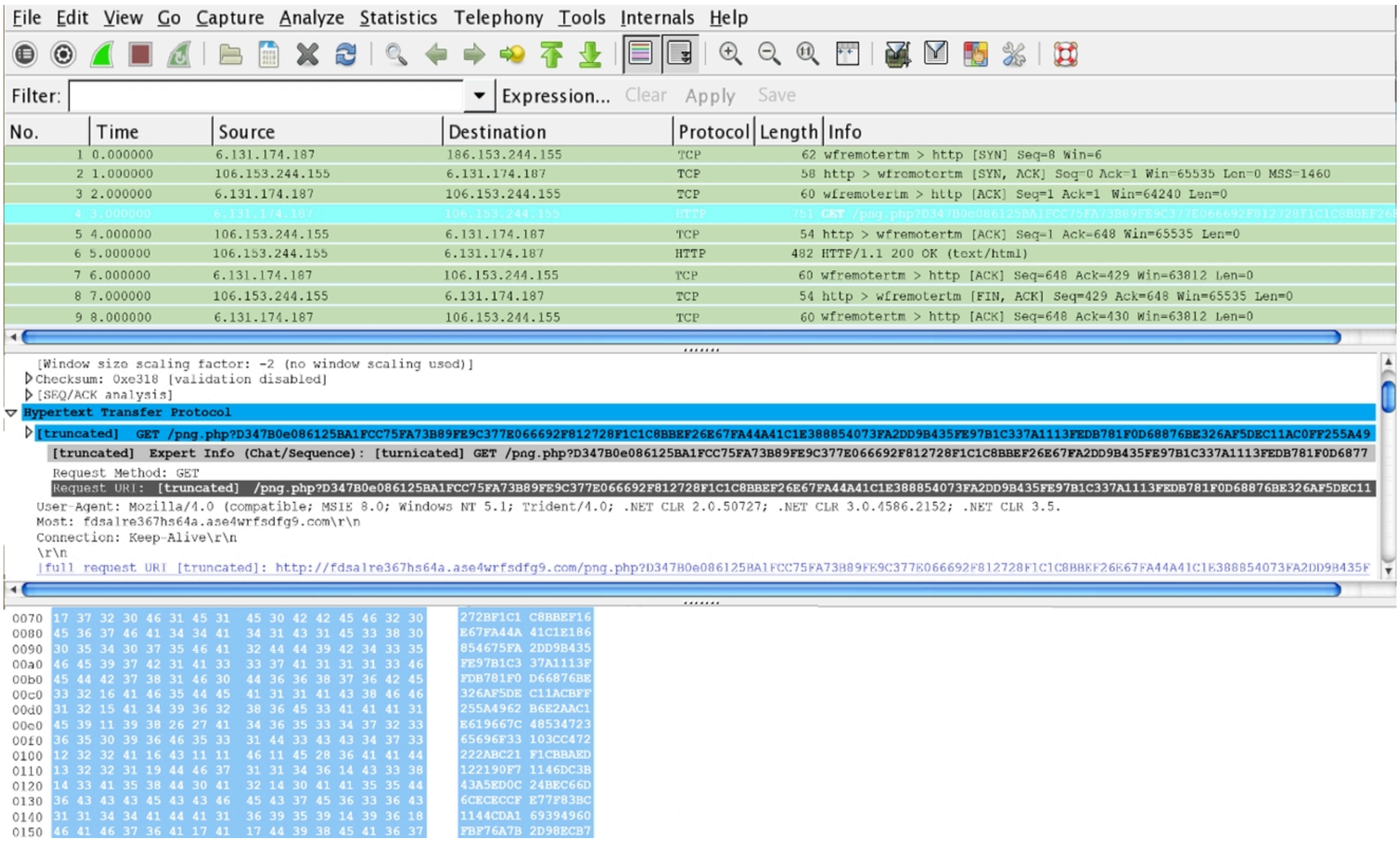
A. incorrect TCP handshake

B. incorrect UDP handshake

C. incorrect OSI configuration

D. incorrect snaplen configuration

Question #162 *Topic 1*


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    186.153.244.155  TCP       62 wfremotertm > http [SYN] Seq=8 Win=6
  2 1.000000  106.153.244.155  6.131.174.187    TCP       58 http > wfremotertm [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 wfremotertm > http [ACK] Seq=1 Ack=1  Win=64240 Len=0
  4 3.000000  6.131.174.187    106.153.244.155  HTTP     751 GET /png.php?D347B0e086125BA1FCC75FA73B89FE9C377E066692F812728F1C1C8BBEF26E
  5 4.000000  106.153.244.155  6.131.174.187    TCP       54 http > wfremotertm [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 wfremotertm > http [ACK] Seq=648 Ack=429 Win=63812 Len=0
  8 7.000000  106.153.244.155  6.131.174.187    TCP       54 http > wfremotertm [FIN, ACK] Seq=429 Ack=648 Win=65535 Len=0
  9 8.000000  6.131.174.187    106.153.244.155  TCP       60 wfremotertm > 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?D347B0e086125BA1FCC75FA73B89FE9C377E066692F812728F1C1C8BBEF26E67FA44A41C1E388854073FA2DD9B435FE97B1C337A1113FEDB781F0D68876BE326AF5DEC11AC0FF255A49
     [truncated]  Expert Info (Chat/Sequence): [turnicated] GET /png.php?D347B0e086125BA1FCC75FA73B89FE9C377E066692F812728F1C1C8BBEF26E67FA2DD9B435FE97B1C337A1113FEDB781F0D6877
     Request Method: GET
     Request URI:  [truncated]  /png.php?D347B0e086125BA1FCC75FA73B89FE9C377E066692F812728F1C1C8BBEF26E67FA44A41C1E388854073FA2DD9B435FE97B1C337A1113FEDB781F0D68876BE326AF5DEC11
   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.
   Most: fdsalre367hs64a.ase4wrfsdfg9.com\r\n
   Connection: Keep-Alive\r\n
   \r\n
   [full request URI [truncated]: http://fdsalre367hs64a.ase4wrfsdfg9.com/png.php?D347B0e086125BA1FCC75FA73B89FE9C377E066692F812728F1C1C8BBEF26E67FA44A41C1E388854073FA2DD9B435F
```

```
0070  17 37 32 30 46 31 45 31  45 30 42 42 45 46 32 30   272BF1C1 C8BBEF16
0080  45 36 37 46 41 34 34 41  34 31 43 31 45 33 38 30   E67FA44A 41C1E186
0090  30 35 34 30 37 35 46 41  32 44 44 39 42 34 33 35   854675FA 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   E619667C 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 33 41 35 38 44 30 41  32 14 30 41 41 35 35 44   43A5ED0C 24BEC66D
0130  36 43 43 43 45 43 43 46  45 43 37 45 36 33 36 43   6CECECCF 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   FBF76A7B 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.

Question #163 *Topic 1*

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})

Question #164 *Topic 1*

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?

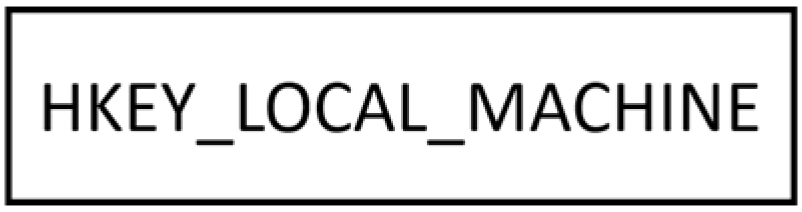
A. Run ג€ps -uג€ to find out who executed additional processes that caused a high load on a server

B. Run ג€ps -efג€ to understand which processes are taking a high amount of resources

C. Run ג€ps -dג€ to decrease the priority state of high load processes to avoid resource exhaustion

D. Run ג€ps -mג€ to capture the existing state of daemons and map required processes to find the gap

Question #165 *Topic 1*



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

Question #166 *Topic 1*

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

Question #167 *Topic 1*

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

Question #168 *Topic 1*

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

Question #169 *Topic 1*

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

Question #170 *Topic 1*

Which category relates to improper use or disclosure of PII data?

A. legal

B. compliance

C. regulated

D. contractual

Question #171 *Topic 1*

Which type of evidence supports a theory or an assumption that results from initial evidence?

A. probabilistic

B. indirect

C. best

D. corroborative

Question #172 *Topic 1*

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

Question #173 *Topic 1*

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

Question #174 *Topic 1*

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

Question #175 *Topic 1*

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

Question #176 *Topic 1*

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

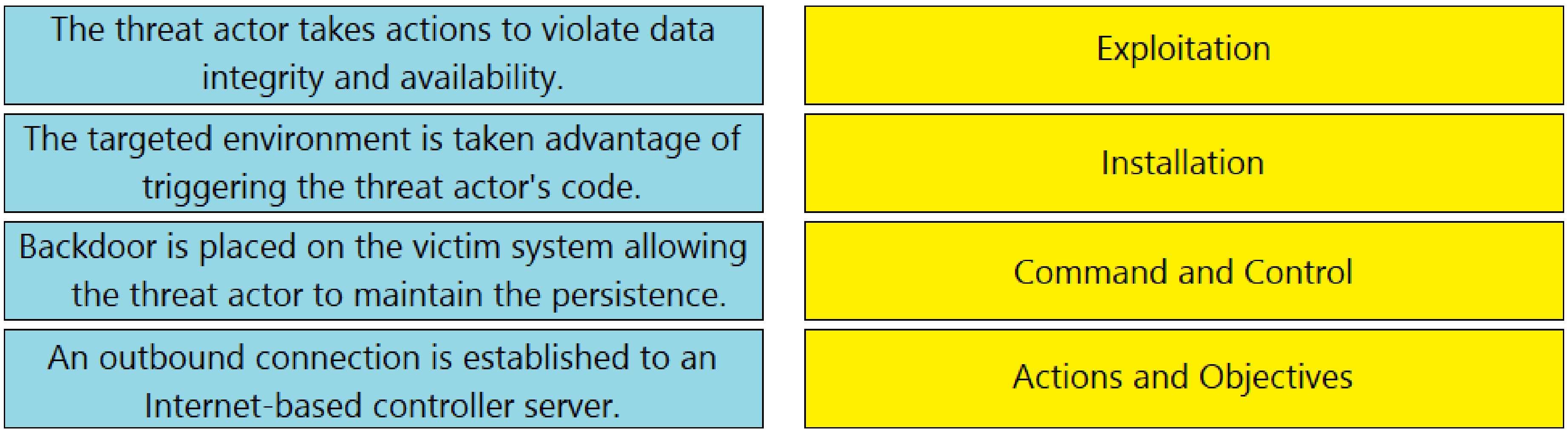
E. vulnerability scoring

Question #177 *Topic 1*

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.

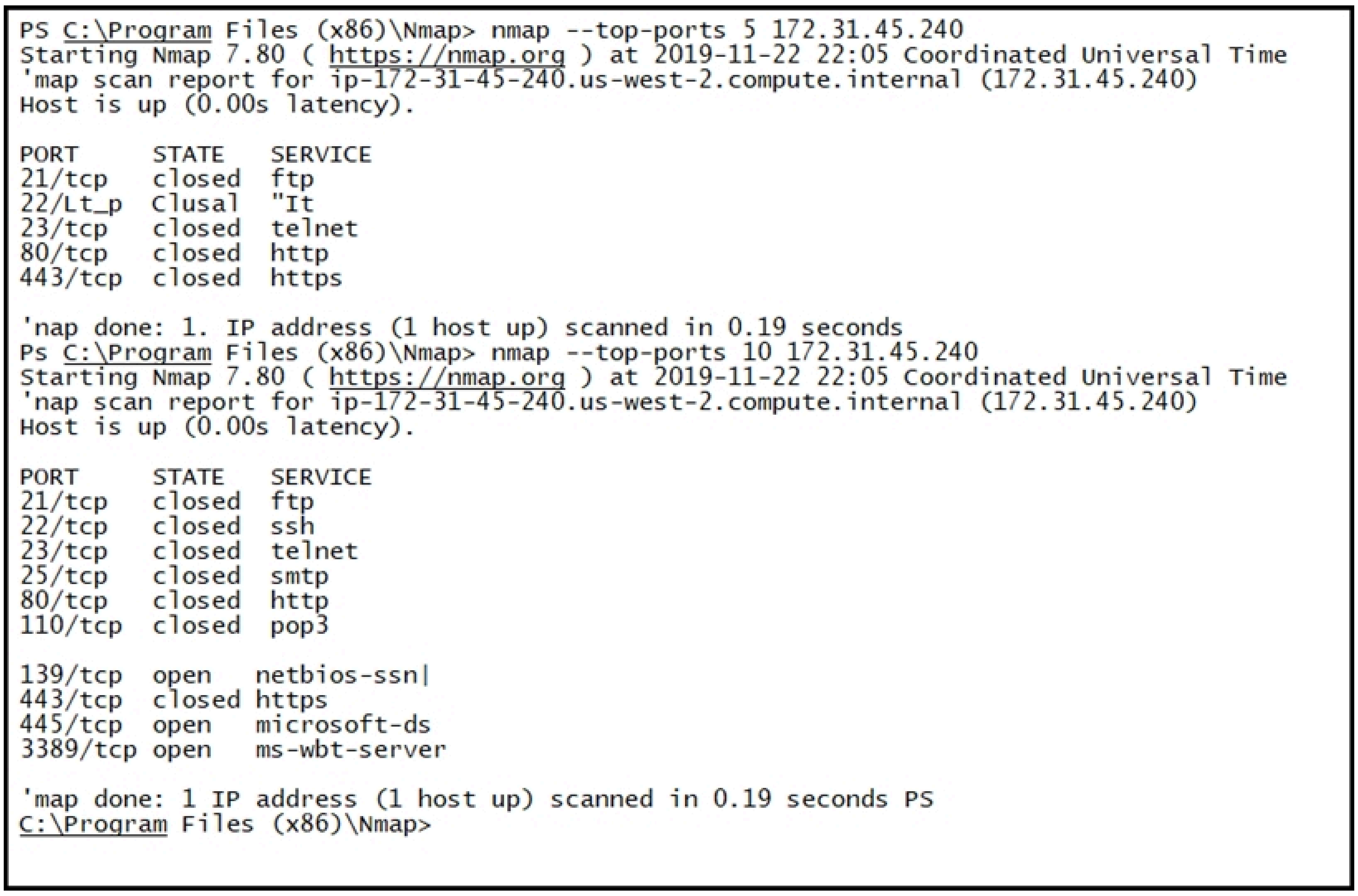
Select and Place:



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

Question #178

Topic 1



```
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

'nap 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
'nap 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.

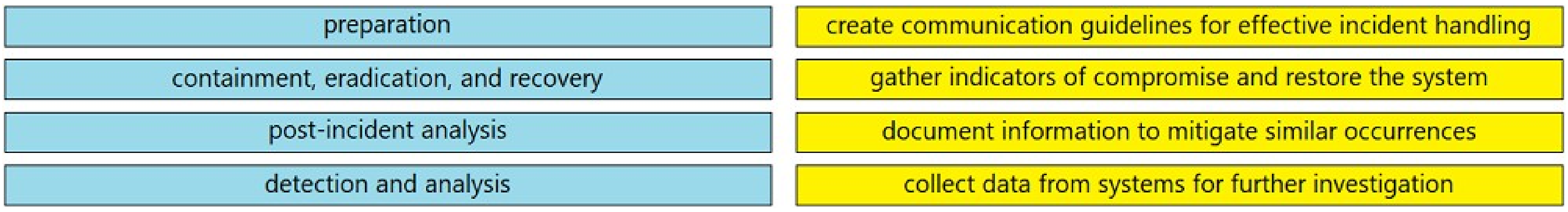
Question #179

Topic 1

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

Question #180

Topic 1

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.

Question #181 *Topic 1*

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

Question #182 *Topic 1*

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.

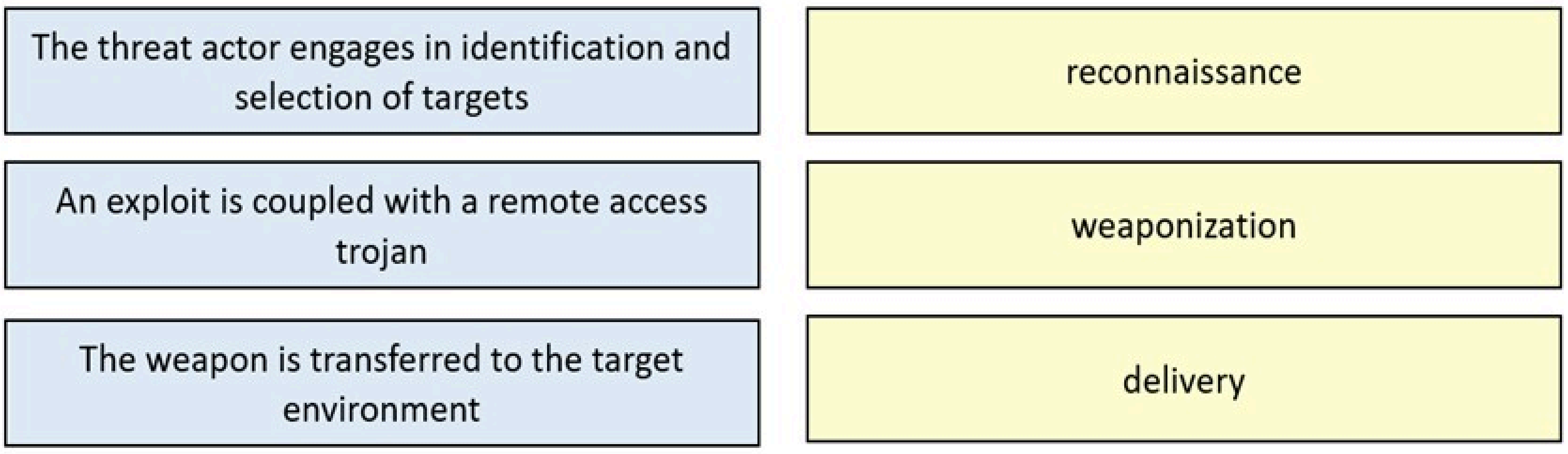
D. Reduce the probability of similar threats.

Question #183 *Topic 1*

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

An exploit is coupled with a remote access trojan

The weapon is transferred to the target environment

reconnaissance

weaponization

delivery

Question #184 *Topic 1*

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

Question #185 *Topic 1*

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

Question #186 *Topic 1*

The SOC team has confirmed a potential indicator of compromise on an endpoint. The team has narrowed the executable file's type to a new trojan family.
According to the NIST Computer Security Incident Handling Guide, what is the next step in handling this event?

A. Perform forensics analysis on the infected endpoint

B. Isolate the infected endpoint from the network

C. Prioritize incident handling based on the impact

D. Collect public information on the malware behavior

Question #187 *Topic 1*

What is an incident response plan?

A. an organizational approach to events that could lead to asset loss or disruption of operations

B. an organizational approach to security management to ensure a service lifecycle and continuous improvements

C. an organizational approach to disaster recovery and timely restoration of operational services

D. an organizational approach to system backup and data archiving aligned to regulations

Question #188 *Topic 1*

What are two categories of DDoS attacks? (Choose two.)

A. direct

B. reflected

C. split brain

D. scanning

E. phishing

Question #189 *Topic 1*

What is the impact of encryption?

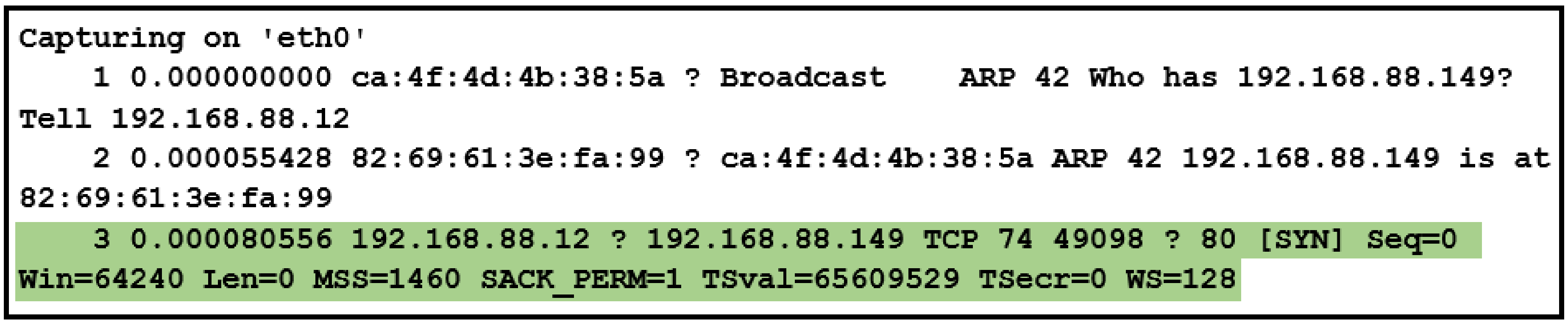
A. Data is unaltered and its integrity is preserved.

B. Data is accessible and available to permitted individuals.

C. Confidentiality of the data is kept secure and permissions are validated.

D. Data is secure and unreadable without decrypting it.

Question #190 *Topic 1*



```
Capturing on 'eth0'
    1 0.000000000 ca:4f:4d:4b:38:5a ? Broadcast    ARP 42 Who has 192.168.88.149?
Tell 192.168.88.12
    2 0.000055428 82:69:61:3e:fa:99 ? ca:4f:4d:4b:38:5a ARP 42 192.168.88.149 is at
82:69:61:3e:fa:99
    3 0.000080556 192.168.88.12 ? 192.168.88.149 TCP 74 49098 ? 80 [SYN] Seq=0
Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=65609529 TSecr=0 WS=128
```

Refer to the exhibit. What must be interpreted from this packet capture?

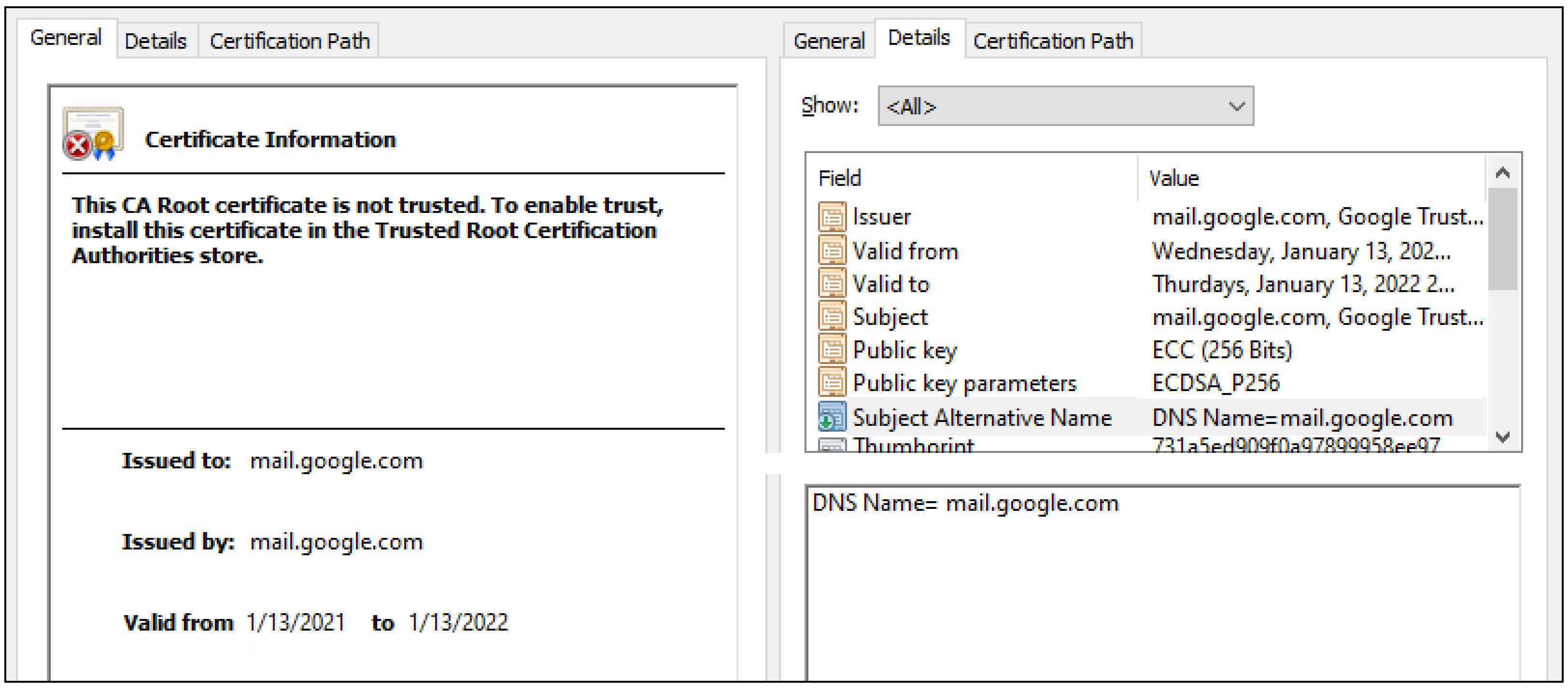
A. IP address 192.168.88.12 is communicating with 192.168.88.149 with a source port 49098 to destination port 80 using TCP protocol.

B. IP address 192.168.88.149 is communicating with 192.168.88.12 with a source port 49098 to destination port 80 using TCP protocol.

C. IP address 192.168.88.149 is communicating with 192.168.88.12 with a source port 80 to destination port 49098 using TCP protocol.

D. IP address 192.168.88.12 is communicating with 192.168.88.149 with a source port 74 to destination port 49098 using TCP protocol.

Question #191 *Topic 1*



Certificate Information

This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

Issued to: mail.google.com

Issued by: mail.google.com

Valid from 1/13/2021 **to** 1/13/2022

Show: <All>

Field	Value
Issuer	mail.google.com, Google Trust...
Valid from	Wednesday, January 13, 202...
Valid to	Thurdays, January 13, 2022 2...
Subject	mail.google.com, Google Trust...
Public key	ECC (256 Bits)
Public key parameters	ECDSA_P256
Subject Alternative Name	DNS Name=mail.google.com
Thumbprint	731a5ed909f0a97899958ee97

DNS Name= mail.google.com

Refer to the exhibit. A company employee is connecting to mail.google.com from an endpoint device. The website is loaded but with an error. What is occurring?

A. man-in-the-middle attack

B. Certificate is not in trusted roots.

C. DNS hijacking attack.

D. Endpoint local time is invalid.

Question #192 *Topic 1*

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

A. Stateful inspection is more secure due to its complex signatures, and deep packet inspection requires less human intervention.

B. Deep packet inspection is more secure due to its complex signatures, and stateful inspection requires less human intervention.

C. Deep packet inspection gives insights up to Layer 7, and stateful inspection gives insights only up to Layer 4.

D. Stateful inspection verifies data at the transport layer, and deep packet inspection verifies data at the application layer.

Question #193 *Topic 1*

What is the difference between the ACK flag and the RST flag?

A. The RST flag approves the connection, and the ACK flag indicates that a packet needs to be resent.

B. The ACK flag marks the connection as reliable, and the RST flag indicates the failure within TCP Handshake.

C. The RST flag approves the connection, and the ACK flag terminates spontaneous connections.

D. The ACK flag confirms the received segment, and the RST flag terminates the connection.

Question #194 *Topic 1*

An automotive company provides new types of engines and special brakes for rally sports cars. The company has a database of inventions and patents for their engines and technical information. Customers can acces the database through the company's website after they register and identify themselves. Which type of protected data is accessed by customers?

A. IP data

B. PII data

C. PSI data

D. PHI data

Question #195 *Topic 1*

What is the difference between vulnerability and risk?

A. A vulnerability represents a flaw in a security that can be exploited, and the risk is the potential damage it might cause.

B. A risk is potential threat that adversaries use to infiltrate the network, and a vulnerability is an exploit.

C. A risk is a potential threat that an exploit applies to, and a vulnerability represents the threat itself.

D. A vulnerability is a sum of possible malicious entry points, and a risk represents the possibility of the unauthorized entry itself.

Question #196 *Topic 1*

The security team has detected an ongoing spam campaign targeting the organization. The team's approach is to push back the cyber kill chain and mitigate ongoing incidents. At which phase of the cyber kill chain should the security team mitigate this type of attack?

A. installation

B. reconnaissance

C. actions

D. delivery

Question #197 *Topic 1*

What describes the concept of data consistently and readily being accessible for legitimate users?

A. accessibility

B. availability

C. integrity

D. confidentiality

Question #198

Topic 1

How does an attack surface differ from an attack vector?

A. An attack vector recognizes the potential outcomes of an attack, and the attack surface is choosing a method of an attack.

B. An attack vector matches components that can be exploited, and an attack surface classifies the potential path for exploitation.

C. An attack surface mitigates external vulnerabilities, and an attack vector identifies mitigation techniques and possible workarounds.

D. An attack surface identifies vulnerable parts for an attack, and an attack vector specifies which attacks are feasible to those parts.

Question #199

Topic 1

What describes the defense-in-depth principle?

A. defining precise guidelines for new workstation installations

B. implementing alerts for unexpected asset malfunctions

C. categorizing critical assets within the organization

D. isolating guest Wi-Fi from the local network

Question #200

Topic 1

How does statistical detection differ from rule-based detection?

A. Statistical detection involves the evaluation of events, and rule-based detection requires an evaluated set of events to function.

B. Rule-based detection involves the evaluation of events, and statistical detection requires an evaluated set of events to function.

C. Statistical detection defines legitimate data over time, and rule-based detection works on a predefined set of rules.

D. Rule-based detection defines legitimate data over a period of time, and statistical detection works on a predefined set of rules.

Question #201

Topic 1

Which type of access control depends on the job function of the user?

A. role-based access control

B. rule-based access control

C. nondiscretionary access control

D. discretionary access control

Question #202 *Topic 1*

What is a collection of compromised machines that attackers use to carry out a DDoS attack?

A. subnet

B. VLAN

C. command and control

D. botnet

Question #203 *Topic 1*

What is the difference between inline traffic interrogation (TAPS) and traffic mirroring (SPAN)?

A. SPAN ports filter out physical layer errors, making some types of analyses more difficult, and TAPS receives all packets, including physical errors.

B. TAPS replicates the traffic to preserve integrity, and SPAN modifies packets before sending them to other analysis tools.

C. TAPS interrogation is more complex because traffic mirroring applies additional tags to data, and SPAN does not alter integrity and provides full visibility within full-duplex networks.

D. SPAN results in more efficient traffic analysis, and TAPS is considerably slower due to latency caused by mirroring.

Question #204 *Topic 1*

A security engineer notices confidential data being exfiltrated to a domain `Ransome4144-mware73-978` address that is attributed to a known advanced persistent threat group. The engineer discovers that the activity is part of a real attack and not a network misconfiguration. Which category does this event fall under as defined in the Cyber Kill Chain?

A. reconnaissance

B. delivery

C. action on objectives

D. weaponization

Question #205 *Topic 1*

Which of these describes SOC metrics in relation to security incidents?

A. probability of outage caused by the incident

B. probability of compromise and impact caused by the incident

C. time it takes to assess the risks of the incident

D. time it takes to detect the incident

Question #206 *Topic 1*

What is a benefit of using asymmetric cryptography?

A. encrypts data with one key

B. decrypts data with one key

C. secure data transfer

D. fast data transfer

Question #207 *Topic 1*

What is obtained using NetFlow?

A. full packet capture

B. session data

C. application logs

D. network downtime report

Question #208 *Topic 1*

What are the two differences between stateful and deep packet inspection? (Choose two.)

A. Deep packet inspection is capable of TCP state monitoring only, and stateful inspection can inspect TCP and UDP.

B. Stateful inspection is capable of packet data inspections, and deep packet inspection is not.

C. Deep packet inspection is capable of malware blocking, and stateful inspection is not.

D. Stateful inspection is capable of TCP state tracking, and deep packet filtering checks only TCP source and destination ports.

E. Deep packet inspection operates on Layer 3 and 4, and stateful inspection operates on Layer 3 of the OSI model.

Question #209 *Topic 1*

An engineer received a flood of phishing emails from HR with the source address HRjacobrn@company.com. What is the threat actor in this scenario?

A. sender

B. phishing email

C. receiver

D. HR

Question #210 *Topic 1*

How does agentless monitoring differ from agent-based monitoring?

A. Agentless can access the data via API, while agent-based uses a less efficient method and accesses log data through WMI.

B. Agent-based monitoring has a lower initial cost for deployment, while agentless requires resource-intensive deployment.

C. Agent-based monitoring is less intrusive in gathering log data, while agentless requires open ports to fetch the logs.

D. Agent-based has a possibility to locally filter and transmit only valuable data, while agentless has much higher network utilization.

Question #211 *Topic 1*

Syslog collecting software is installed on the server. For the log containment, a disk with FAT type partition is used. An engineer determined that log files are being corrupted when the 4 GB file size is exceeded. Which action resolves the issue?

A. Use NTFS partition for log containment.

B. Use the Ext4 partition because it can hold files up to 16 TB.

C. Use FAT32 to exceed the limit of 4 GB.

D. Add space to the existing partition and lower the retention period.

Question #212 *Topic 1*

Which type of verification consists of using tools to compute the message digest of the original and copied data, then comparing the similarity of the digests?

A. evidence collection order

B. volatile data collection

C. data integrity

D. data preservation

Question #213 *Topic 1*

What are two denial-of-service (DoS) attacks? (Choose two.)

A. port scan

B. phishing

C. man-in-the-middle

D. teardrop

E. SYN flood

Question #214 *Topic 1*

What is threat hunting?

A. Focusing on proactively detecting possible signs of intrusion and compromise.

B. Managing a vulnerability assessment report to mitigate potential threats.

C. Attempting to deliberately disrupt servers by altering their availability.

D. Pursuing competitors and adversaries to infiltrate their system to acquire intelligence data.

Question #215 *Topic 1*

According to the September 2020 threat intelligence feeds, a new malware called Egregor was introduced and used in many attacks. Distribution of Egregor is primarily through a Cobalt Strike that has been installed on victim's workstations using RDP exploits. Malware exfiltrates the victim's data to a command and control server. The data is used to force victims pay or lose it by publicly releasing it. Which type of attack is described?

A. malware attack

B. insider threat

C. ransomware attack

D. whale-phishing

Question #216 *Topic 1*

A company encountered a breach on its web servers using IIS 7.5. During the investigation, an engineer discovered that an attacker read and altered the data on a secure communication using TLS 1.2 and intercepted sensitive information by downgrading a connection to export-grade cryptography. The engineer must mitigate similar incidents in the future and ensure that clients and servers always negotiate with the most secure protocol versions and cryptographic parameters.
Which action does the engineer recommend?

A. Upgrade to TLS v1.3.

B. Install the latest IIS version.

C. Deploy an intrusion detection system.

D. Downgrade to TLS 1.1.

Question #217 *Topic 1*

What is the difference between discretionary access control (DAC) and role-based access control (RBAC)?

A. DAC administrators pass privileges to users and groups, and in RBAC, permissions are applied to specific groups.

B. DAC requires explicit authorization for a given user on a given object, RBAC requires specific conditions.

C. RBAC is an extended version of DAC where you can add an extra level of authorization based on time.

D. RBAC access is granted when a user meets specific conditions, and in DAC, permissions are applied on user and group levels.

Question #218 *Topic 1*

The SOC team has confirmed a potential indicator of compromise on an isolated endpoint. The team has narrowed the potential malware type to a new trojan family. According to the NIST Computer Security Incident Handling Guide, what is the next step in handling the event?

A. Perform an AV scan on the infected endpoint.

B. Isolate the infected endpoint from the network.

C. Prioritize incident handling based on the impact.

D. Analyze the malware behavior.

Question #219 *Topic 1*

An engineer is working with the compliance teams to identify the data passing through the network. During analysis, the engineer informs the compliance team that external perimeter data flows contain records, writings, and artwork. Internal segregated network flows contain the customer choices by gender, addresses, and product preferences by age? The engineer must identify protected data. Which two types of data must be identified? (Choose two.)

A. SOX

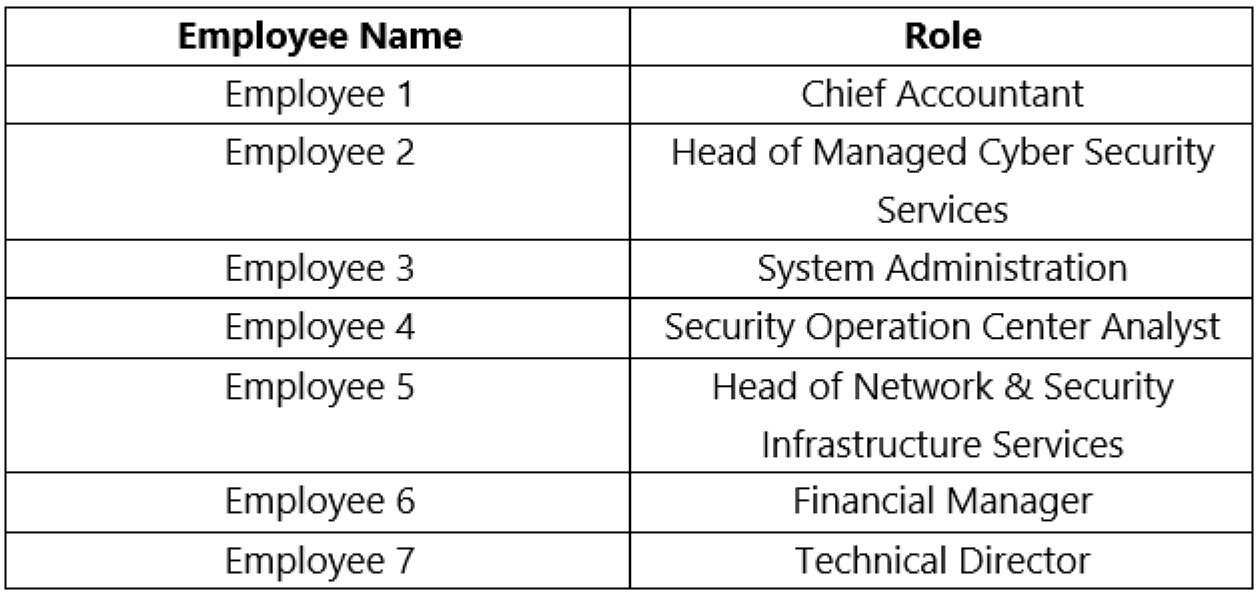
B. PII

C. PCI

D. PHI

E. copyright

Question #220 *Topic 1*



Employee Name	Role
Employee 1	Chief Accountant
Employee 2	Head of Managed Cyber Security Services
Employee 3	System Administration
Employee 4	Security Operation Center Analyst
Employee 5	Head of Network & Security Infrastructure Services
Employee 6	Financial Manager
Employee 7	Technical Director

Refer to the exhibit. Which stakeholders must be involved when a company workstation is compromised?

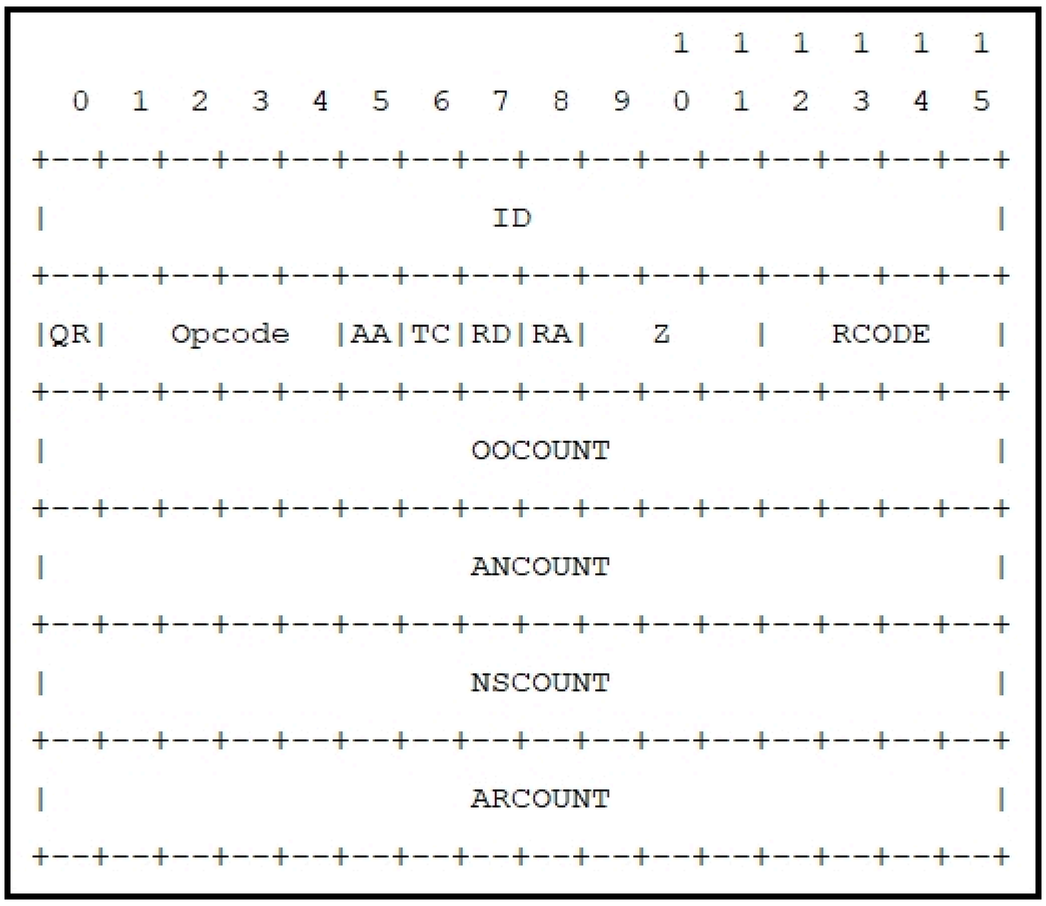
A. Employee 1, Employee 2, Employee 3, Employee 4, Employee 5, Employee 7

B. Employee 4, Employee 6, Employee 7

C. Employee 1, Employee 2, Employee 4, Employee 5

D. Employee 2, Employee 3, Employee 4, Employee 5

Question #221 Topic 1



```
                                1  1  1  1  1  1
  0  1  2  3  4  5  6  7  8  9  0  1  2  3  4  5
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|                      ID                       |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|QR|   Opcode  |AA|TC|RD|RA|   Z    |   RCODE   |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|                    OOCOUNT                    |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|                    ANCOUNT                    |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|                    NSCOUNT                    |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|                    ARCOUNT                    |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
```

Refer to the exhibit. Which field contains DNS header information if the payload is a query or response?

A. ID

B. Z

C. QR

D. TC

Question #222 Topic 1

What is the difference between a threat and an exploit?

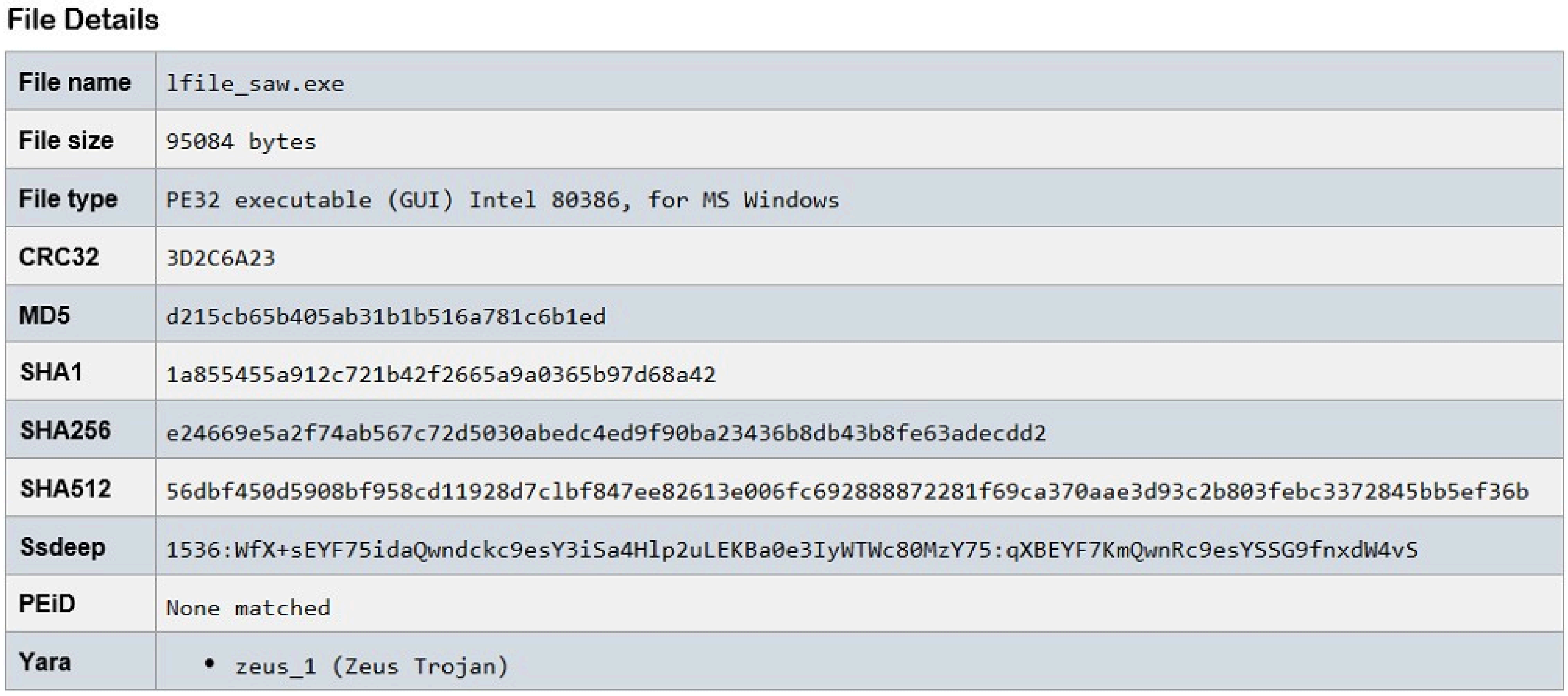
A. An exploit is an attack path, and a threat represents a potential vulnerability.

B. An exploit is an attack vector, and a threat is a potential path the attack must go through.

C. A threat is a potential attack on an asset, and an exploit takes advantage of the vulnerability of the asset.

D. A threat is a result of utilizing flow in a system, and an exploit is a result of gaining control over the system.

Question #223 *Topic 1*



File Details

File name	`1file_saw.exe`
File size	`95084 bytes`
File type	`PE32 executable (GUI) Intel 80386, for MS Windows`
CRC32	`3D2C6A23`
MD5	`d215cb65b405ab31b1b516a781c6b1ed`
SHA1	`1a855455a912c721b42f2665a9a0365b97d68a42`
SHA256	`e24669e5a2f74ab567c72d5030abedc4ed9f90ba23436b8db43b8fe63adecdd2`
SHA512	`56dbf450d5908bf958cd11928d7c1bf847ee82613e006fc692888872281f69ca370aae3d93c2b803febc3372845bb5ef36b`
Ssdeep	`1536:WfX+sEYF75idaQwndckc9esY3iSa4Hlp2uLEKBa0e3IyWTWc80MzY75:qXBEYF7KmQwnRc9esYSSG9fnxdW4vS`
PEiD	`None matched`
Yara	• `zeus_1 (Zeus Trojan)`

Refer to the exhibit. A SOC engineer is analyzing the provided Cuckoo Sandbox report for a file that has been downloaded from an URL, received via email. What is the state of this file?

A. The file was identified as PE32 executable for MS Windows and the Yara filed lists it as Trojan.

B. The file was detected as executable and was matched by PEiD threat signatures for further analysis.

C. The file was detected as executable, but no suspicious features are identified.

D. The calculated SHA256 hash of the file was matched and identified as malicious.

Question #224 *Topic 1*

A security analyst notices a sudden surge of incoming traffic and detects unknown packets from unknown senders. After further investigation, the analyst learns that customers claim that they cannot access company servers. According to NIST SP800-61, in which phase of the incident response process is the analyst?

A. preparation

B. post-incident activity

C. containment, eradication, and recovery

D. detection and analysis

Question #225 *Topic 1*

An engineer is analyzing a recent breach where confidential documents were altered and stolen by the receptionist. Further analysis shows that the threat actor connected an external USB device to bypass security restrictions and steal data. The engineer could not find an external USB device. Which piece of information must an engineer use for attribution in an investigation?

A. receptionist and the actions performed

B. stolen data and its criticality assessment

C. external USB device

D. list of security restrictions and privileges boundaries bypassed

Question #226 *Topic 1*

How does TOR alter data content during transit?

A. It encrypts content and destination information over multiple layers.

B. It traverses source traffic through multiple destinations before reaching the receiver.

C. It redirects destination traffic through multiple sources avoiding traceability.

D. It spoofs the destination and source information protecting both sides.

Question #227 *Topic 1*

Which information must an organization use to understand the threats currently targeting the organization?

A. vendor suggestions

B. threat intelligence

C. risk scores

D. vulnerability exposure

Question #228 *Topic 1*

An analyst is using the SIEM platform and must extract a custom property from a Cisco device and capture the phrase, `File: Clean.` Which regex must the analyst import?

A. File: Clean (.*)

B. ^Parent File: Clean$

C. File: Clean

D. ^File: Clean$

Question #229 *Topic 1*

Which technology prevents end-device to end-device IP traceability?

A. encryption

B. tunneling

C. load balancing

D. NAT/PAT

Question #230 *Topic 1*

What is the difference between inline traffic interrogation and traffic mirroring?

A. Inline replicates the traffic to preserve integrity rather than modifying packets before sending them to other analysis tools.

B. Traffic mirroring results in faster traffic analysis and inline is considerably slower due to latency.

C. Inline interrogation is less complex as traffic mirroring applies additional tags to data.

D. Traffic mirroring copies the traffic rather than forwarding it directly to the analysis tools.

Question #231 *Topic 1*

What is an advantage of symmetric over asymmetric encryption?

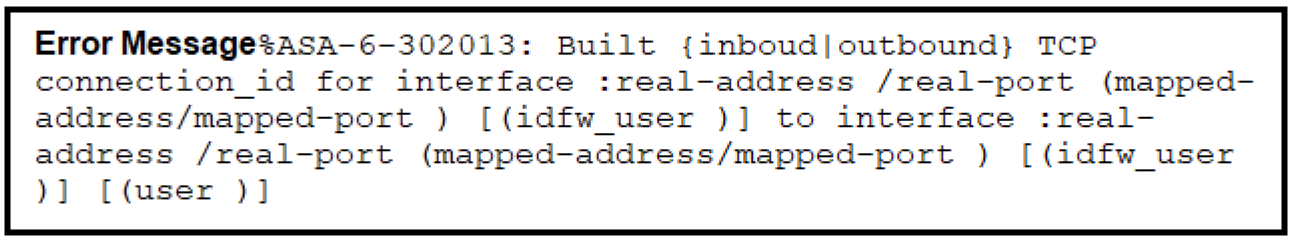
A. It is a faster encryption mechanism for sessions.

B. A one-time encryption key is generated for data transmission.

C. A key is generated on demand according to data type.

D. It is suited for transmitting large amounts of data.

Question #232 *Topic 1*



```
Error Message%ASA-6-302013: Built {inboud|outbound} TCP
connection_id for interface :real-address /real-port (mapped-
address/mapped-port ) [(idfw_user )] to interface :real-
address /real-port (mapped-address/mapped-port ) [(idfw_user
)] [(user )]
```

Refer to the exhibit. During the analysis of a suspicious scanning activity incident, an analyst discovered multiple local TCP connection events. Which technology provided these logs?

A. antivirus

B. IDS/IPS

C. firewall

D. proxy

Question #233 *Topic 1*

An organization is cooperating with several third-party companies. Data exchange is on an unsecured channel using port 80. Internal employees use the FTP service to upload and download sensitive data. An engineer must ensure confidentiality while preserving the integrity of the communication. Which technology must the engineer implement in this scenario?

A. RADIUS server

B. web application firewall

C. X.509 certificates

D. CA server

Question #234 *Topic 1*

What describes the impact of false-positive alerts compared to false-negative alerts?

A. A false negative is alerting for an XSS attack. An engineer investigates the alert and discovers that an XSS attack happened. A false positive is when an XSS attack happens and no alert is raised.

B. A false positive is an event altering for an SQL injection attack. An engineer investigates the alert and discovers that an attack attempt was blocked by IPS. A false negative is when the attack gets detected but succeeds and results in a breach.

C. A false positive is an event altering for a brute-force attack. An engineer investigates the alert and discovers that a legitimate user entered the wrong credential several times. A false negative is when a threat actor tries to brute-force attack a system and no alert is raised.

D. A false negative is a legitimate attack triggering a brute-force alert. An engineer investigates the alert and finds out someone intended to break into the system. A false positive is when no alert and no attack is occurring.

Question #235 *Topic 1*

Which vulnerability type is used to read, write, or erase information from a database?

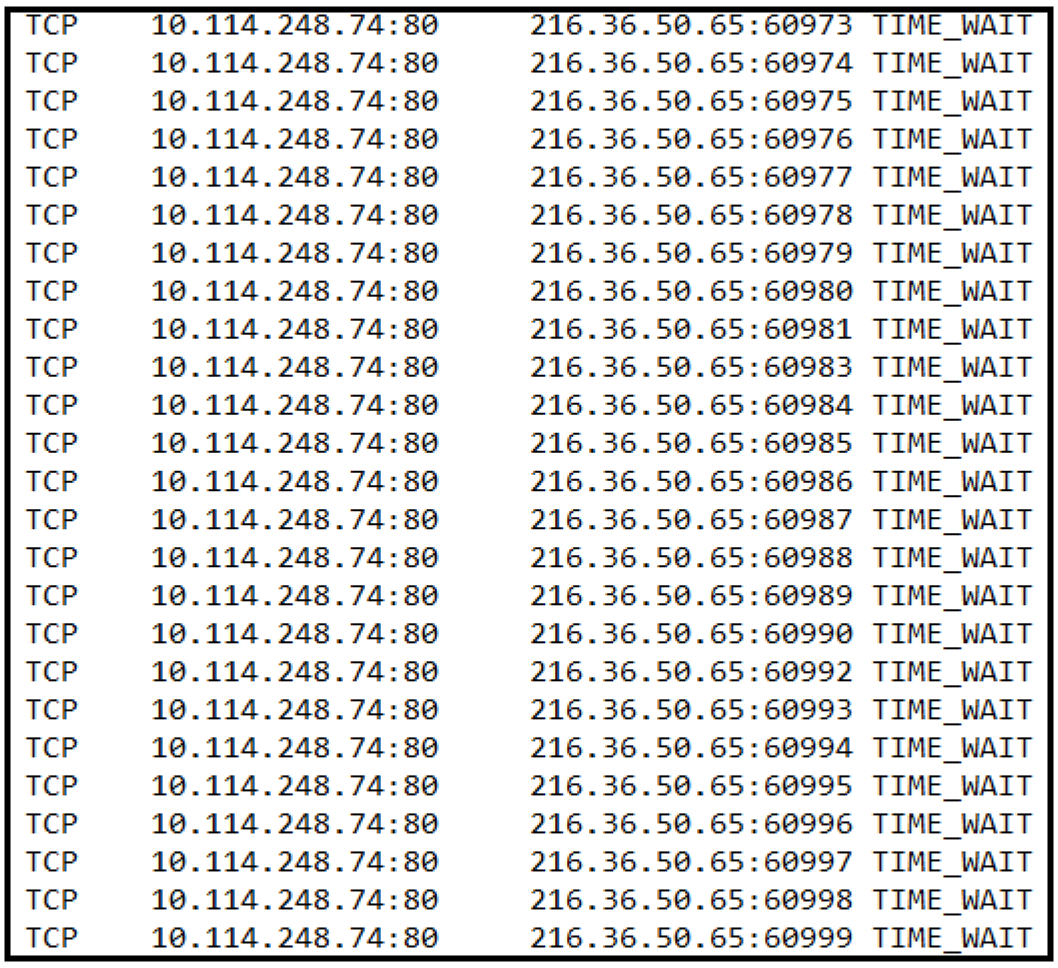
A. cross-site request forgery

B. SQL injection

C. cross-site scripting

D. buffer overflow

Question #236 *Topic 1*



```
TCP    10.114.248.74:80      216.36.50.65:60973 TIME_WAIT
TCP    10.114.248.74:80      216.36.50.65:60974 TIME_WAIT
TCP    10.114.248.74:80      216.36.50.65:60975 TIME_WAIT
TCP    10.114.248.74:80      216.36.50.65:60976 TIME_WAIT
TCP    10.114.248.74:80      216.36.50.65:60977 TIME_WAIT
TCP    10.114.248.74:80      216.36.50.65:60978 TIME_WAIT
TCP    10.114.248.74:80      216.36.50.65:60979 TIME_WAIT
TCP    10.114.248.74:80      216.36.50.65:60980 TIME_WAIT
TCP    10.114.248.74:80      216.36.50.65:60981 TIME_WAIT
TCP    10.114.248.74:80      216.36.50.65:60983 TIME_WAIT
TCP    10.114.248.74:80      216.36.50.65:60984 TIME_WAIT
TCP    10.114.248.74:80      216.36.50.65:60985 TIME_WAIT
TCP    10.114.248.74:80      216.36.50.65:60986 TIME_WAIT
TCP    10.114.248.74:80      216.36.50.65:60987 TIME_WAIT
TCP    10.114.248.74:80      216.36.50.65:60988 TIME_WAIT
TCP    10.114.248.74:80      216.36.50.65:60989 TIME_WAIT
TCP    10.114.248.74:80      216.36.50.65:60990 TIME_WAIT
TCP    10.114.248.74:80      216.36.50.65:60992 TIME_WAIT
TCP    10.114.248.74:80      216.36.50.65:60993 TIME_WAIT
TCP    10.114.248.74:80      216.36.50.65:60994 TIME_WAIT
TCP    10.114.248.74:80      216.36.50.65:60995 TIME_WAIT
TCP    10.114.248.74:80      216.36.50.65:60996 TIME_WAIT
TCP    10.114.248.74:80      216.36.50.65:60997 TIME_WAIT
TCP    10.114.248.74:80      216.36.50.65:60998 TIME_WAIT
TCP    10.114.248.74:80      216.36.50.65:60999 TIME_WAIT
```

#netstat -an

Refer to the exhibit. An engineer received a ticket about a slowed-down web application. The engineer runs the command. How must the engineer interpret the results?

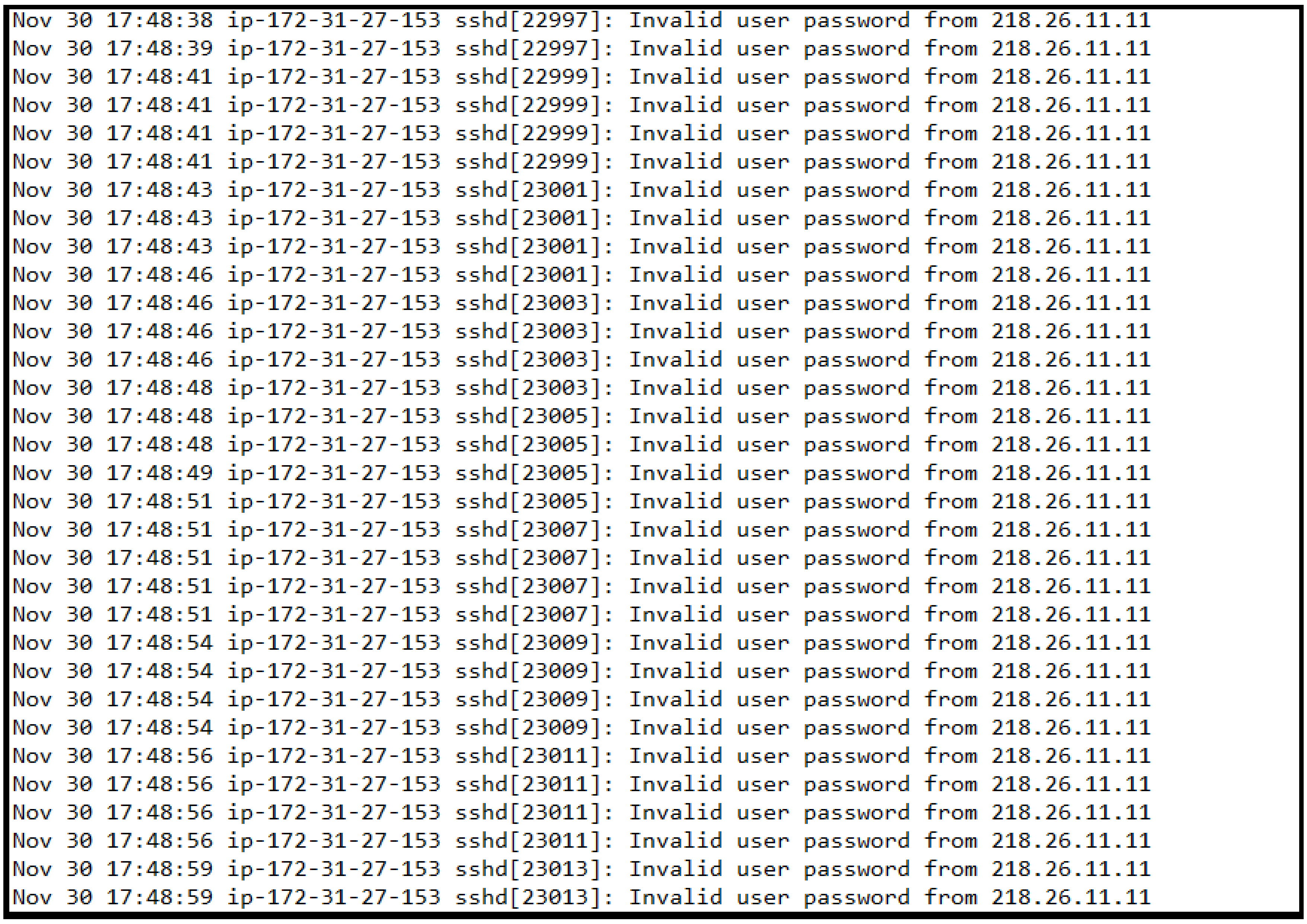
A. The web application is receiving a common, legitimate traffic.

B. The engineer must gather more data.

C. The server is under a man-in-the-middle attack between the web application and its database.

D. The web application server is under a denial-of-service attack.

Question #237 *Topic 1*



```
Nov 30 17:48:38 ip-172-31-27-153 sshd[22997]: Invalid user password from 218.26.11.11
Nov 30 17:48:39 ip-172-31-27-153 sshd[22997]: Invalid user password from 218.26.11.11
Nov 30 17:48:41 ip-172-31-27-153 sshd[22999]: Invalid user password from 218.26.11.11
Nov 30 17:48:41 ip-172-31-27-153 sshd[22999]: Invalid user password from 218.26.11.11
Nov 30 17:48:41 ip-172-31-27-153 sshd[22999]: Invalid user password from 218.26.11.11
Nov 30 17:48:41 ip-172-31-27-153 sshd[22999]: Invalid user password from 218.26.11.11
Nov 30 17:48:43 ip-172-31-27-153 sshd[23001]: Invalid user password from 218.26.11.11
Nov 30 17:48:43 ip-172-31-27-153 sshd[23001]: Invalid user password from 218.26.11.11
Nov 30 17:48:43 ip-172-31-27-153 sshd[23001]: Invalid user password from 218.26.11.11
Nov 30 17:48:46 ip-172-31-27-153 sshd[23001]: Invalid user password from 218.26.11.11
Nov 30 17:48:46 ip-172-31-27-153 sshd[23003]: Invalid user password from 218.26.11.11
Nov 30 17:48:46 ip-172-31-27-153 sshd[23003]: Invalid user password from 218.26.11.11
Nov 30 17:48:46 ip-172-31-27-153 sshd[23003]: Invalid user password from 218.26.11.11
Nov 30 17:48:48 ip-172-31-27-153 sshd[23003]: Invalid user password from 218.26.11.11
Nov 30 17:48:48 ip-172-31-27-153 sshd[23005]: Invalid user password from 218.26.11.11
Nov 30 17:48:48 ip-172-31-27-153 sshd[23005]: Invalid user password from 218.26.11.11
Nov 30 17:48:49 ip-172-31-27-153 sshd[23005]: Invalid user password from 218.26.11.11
Nov 30 17:48:51 ip-172-31-27-153 sshd[23005]: Invalid user password from 218.26.11.11
Nov 30 17:48:51 ip-172-31-27-153 sshd[23007]: Invalid user password from 218.26.11.11
Nov 30 17:48:51 ip-172-31-27-153 sshd[23007]: Invalid user password from 218.26.11.11
Nov 30 17:48:51 ip-172-31-27-153 sshd[23007]: Invalid user password from 218.26.11.11
Nov 30 17:48:51 ip-172-31-27-153 sshd[23007]: Invalid user password from 218.26.11.11
Nov 30 17:48:54 ip-172-31-27-153 sshd[23009]: Invalid user password from 218.26.11.11
Nov 30 17:48:54 ip-172-31-27-153 sshd[23009]: Invalid user password from 218.26.11.11
Nov 30 17:48:54 ip-172-31-27-153 sshd[23009]: Invalid user password from 218.26.11.11
Nov 30 17:48:54 ip-172-31-27-153 sshd[23009]: Invalid user password from 218.26.11.11
Nov 30 17:48:56 ip-172-31-27-153 sshd[23011]: Invalid user password from 218.26.11.11
Nov 30 17:48:56 ip-172-31-27-153 sshd[23011]: Invalid user password from 218.26.11.11
Nov 30 17:48:56 ip-172-31-27-153 sshd[23011]: Invalid user password from 218.26.11.11
Nov 30 17:48:56 ip-172-31-27-153 sshd[23011]: Invalid user password from 218.26.11.11
Nov 30 17:48:59 ip-172-31-27-153 sshd[23013]: Invalid user password from 218.26.11.11
Nov 30 17:48:59 ip-172-31-27-153 sshd[23013]: Invalid user password from 218.26.11.11
```

Refer to the exhibit. A security analyst is investigating unusual activity from an unknown IP address. Which type of evidence is this file?

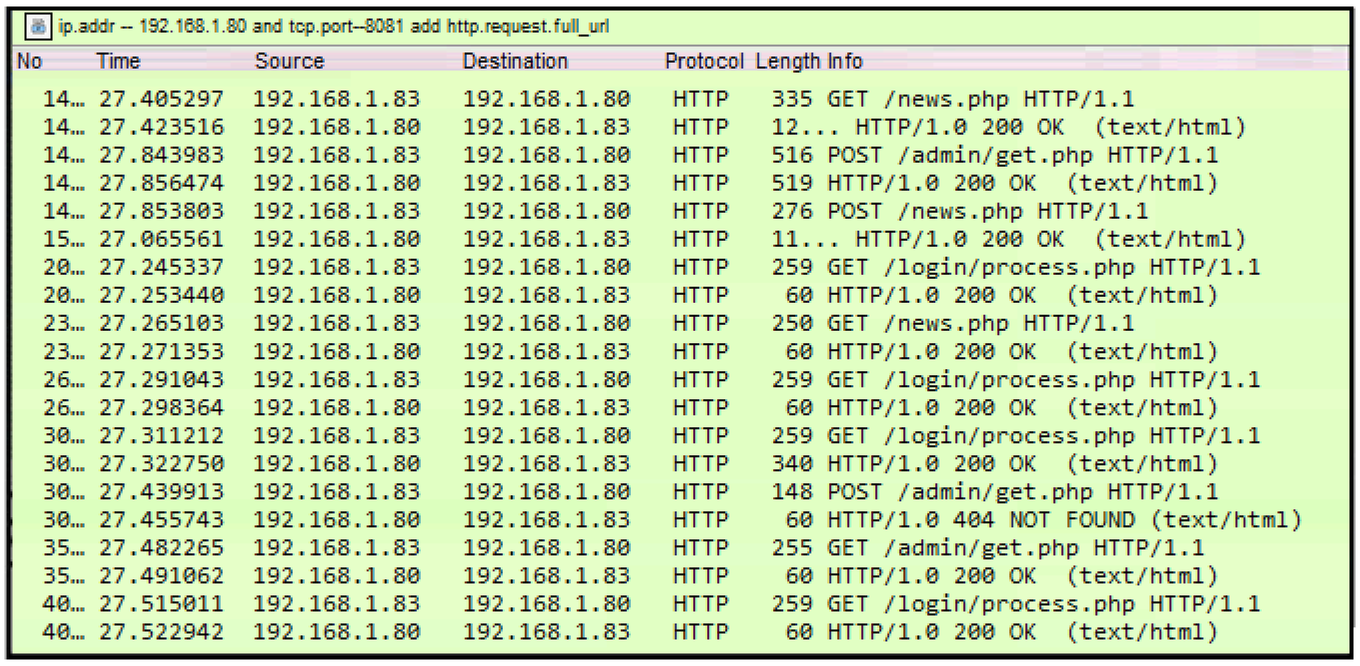
A. indirect evidence

B. best evidence

C. direct evidence

D. corroborative evidence

Question #238 *Topic 1*



```
ip.addr -- 192.168.1.80 and tcp.port--8081 add http.request.full_url
No      Time       Source         Destination    Protocol Length Info
 14… 27.405297  192.168.1.83   192.168.1.80   HTTP    335 GET /news.php HTTP/1.1
 14… 27.423516  192.168.1.80   192.168.1.83   HTTP    12... HTTP/1.0 200 OK  (text/html)
 14… 27.843983  192.168.1.83   192.168.1.80   HTTP    516 POST /admin/get.php HTTP/1.1
 14… 27.856474  192.168.1.80   192.168.1.83   HTTP    519 HTTP/1.0 200 OK  (text/html)
 14… 27.853803  192.168.1.83   192.168.1.80   HTTP    276 POST /news.php HTTP/1.1
 15… 27.065561  192.168.1.80   192.168.1.83   HTTP    11... HTTP/1.0 200 OK  (text/html)
 20… 27.245337  192.168.1.83   192.168.1.80   HTTP    259 GET /login/process.php HTTP/1.1
 20… 27.253440  192.168.1.80   192.168.1.83   HTTP     60 HTTP/1.0 200 OK  (text/html)
 23… 27.265103  192.168.1.83   192.168.1.80   HTTP    250 GET /news.php HTTP/1.1
 23… 27.271353  192.168.1.80   192.168.1.83   HTTP     60 HTTP/1.0 200 OK  (text/html)
 26… 27.291043  192.168.1.83   192.168.1.80   HTTP    259 GET /login/process.php HTTP/1.1
 26… 27.298364  192.168.1.80   192.168.1.83   HTTP     60 HTTP/1.0 200 OK  (text/html)
 30… 27.311212  192.168.1.83   192.168.1.80   HTTP    259 GET /login/process.php HTTP/1.1
 30… 27.322750  192.168.1.80   192.168.1.83   HTTP    340 HTTP/1.0 200 OK  (text/html)
 30… 27.439913  192.168.1.83   192.168.1.80   HTTP    148 POST /admin/get.php HTTP/1.1
 30… 27.455743  192.168.1.80   192.168.1.83   HTTP     60 HTTP/1.0 404 NOT FOUND (text/html)
 35… 27.482265  192.168.1.83   192.168.1.80   HTTP    255 GET /admin/get.php HTTP/1.1
 35… 27.491062  192.168.1.80   192.168.1.83   HTTP     60 HTTP/1.0 200 OK  (text/html)
 40… 27.515011  192.168.1.83   192.168.1.80   HTTP    259 GET /login/process.php HTTP/1.1
 40… 27.522942  192.168.1.80   192.168.1.83   HTTP     60 HTTP/1.0 200 OK  (text/html)
```

Refer to the exhibit. A network administrator is investigating suspicious network activity by analyzing captured traffic. An engineer notices abnormal behavior and discovers that the default user agent is present in the headers of requests and data being transmitted. What is occurring?

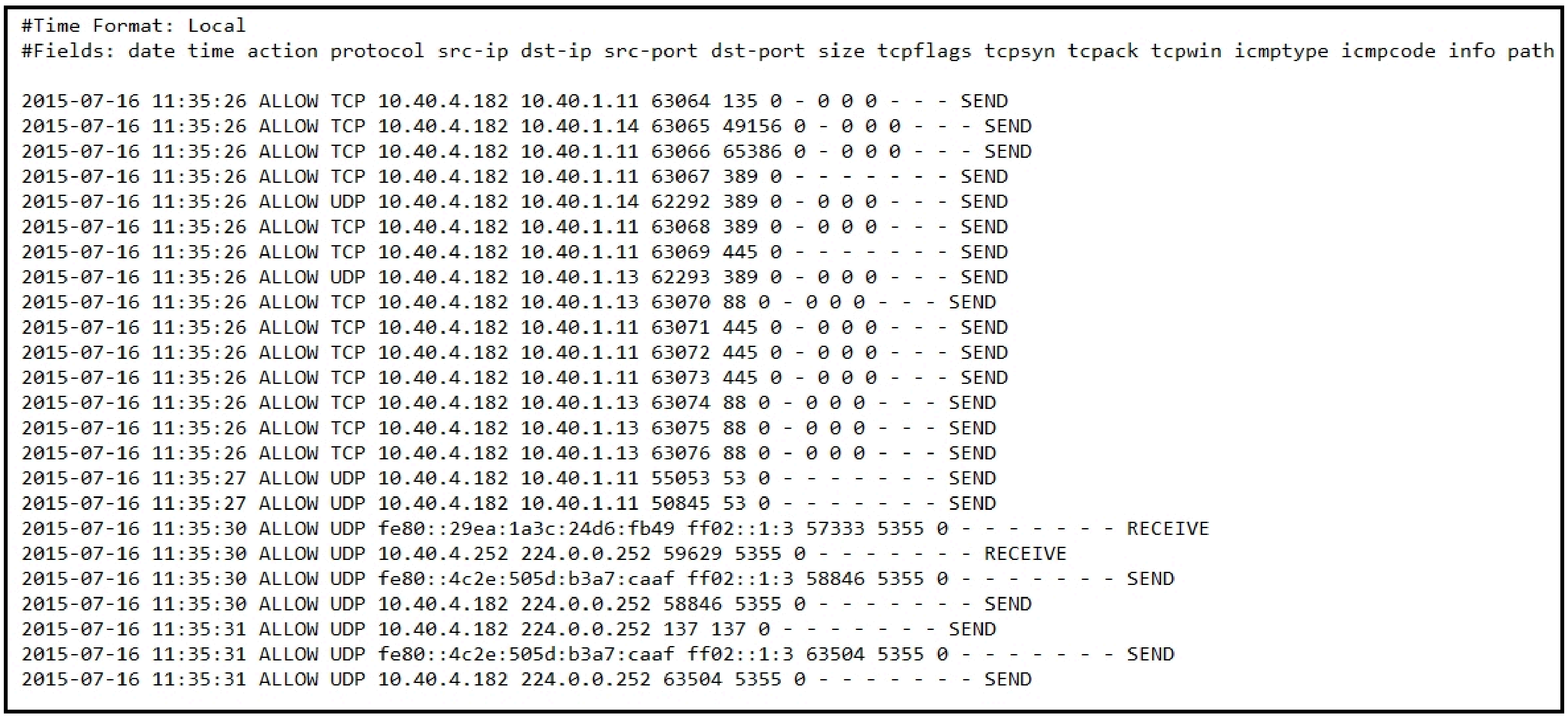
A. indicators of denial-of-service attack: due to the frequency of requests

B. indicators of data exfiltration: HTTP requests must be plain text

C. cache bypassing attack: attacker is sending requests for noncacheable content

D. garbage flood attack: attacker is sending garbage binary data to open ports

Question #239 *Topic 1*



```
#Time Format: Local
#Fields: date time action protocol src-ip dst-ip src-port dst-port size tcpflags tcpsyn tcpack tcpwin icmptype icmpcode info path

2015-07-16 11:35:26 ALLOW TCP 10.40.4.182 10.40.1.11 63064 135 0 - 0 0 0 - - - SEND
2015-07-16 11:35:26 ALLOW TCP 10.40.4.182 10.40.1.14 63065 49156 0 - 0 0 0 - - - SEND
2015-07-16 11:35:26 ALLOW TCP 10.40.4.182 10.40.1.11 63066 65386 0 - 0 0 0 - - - SEND
2015-07-16 11:35:26 ALLOW TCP 10.40.4.182 10.40.1.11 63067 389 0 - - - - - - - SEND
2015-07-16 11:35:26 ALLOW UDP 10.40.4.182 10.40.1.14 62292 389 0 - 0 0 0 - - - SEND
2015-07-16 11:35:26 ALLOW TCP 10.40.4.182 10.40.1.11 63068 389 0 - 0 0 0 - - - SEND
2015-07-16 11:35:26 ALLOW TCP 10.40.4.182 10.40.1.11 63069 445 0 - - - - - - - SEND
2015-07-16 11:35:26 ALLOW UDP 10.40.4.182 10.40.1.13 62293 389 0 - 0 0 0 - - - SEND
2015-07-16 11:35:26 ALLOW TCP 10.40.4.182 10.40.1.13 63070 88 0 - 0 0 0 - - - SEND
2015-07-16 11:35:26 ALLOW TCP 10.40.4.182 10.40.1.11 63071 445 0 - 0 0 0 - - - SEND
2015-07-16 11:35:26 ALLOW TCP 10.40.4.182 10.40.1.11 63072 445 0 - 0 0 0 - - - SEND
2015-07-16 11:35:26 ALLOW TCP 10.40.4.182 10.40.1.11 63073 445 0 - 0 0 0 - - - SEND
2015-07-16 11:35:26 ALLOW TCP 10.40.4.182 10.40.1.13 63074 88 0 - 0 0 0 - - - SEND
2015-07-16 11:35:26 ALLOW TCP 10.40.4.182 10.40.1.13 63075 88 0 - 0 0 0 - - - SEND
2015-07-16 11:35:26 ALLOW TCP 10.40.4.182 10.40.1.13 63076 88 0 - 0 0 0 - - - SEND
2015-07-16 11:35:27 ALLOW UDP 10.40.4.182 10.40.1.11 55053 53 0 - - - - - - - SEND
2015-07-16 11:35:27 ALLOW UDP 10.40.4.182 10.40.1.11 50845 53 0 - - - - - - - SEND
2015-07-16 11:35:30 ALLOW UDP fe80::29ea:1a3c:24d6:fb49 ff02::1:3 57333 5355 0 - - - - - - - RECEIVE
2015-07-16 11:35:30 ALLOW UDP 10.40.4.252 224.0.0.252 59629 5355 0 - - - - - - - RECEIVE
2015-07-16 11:35:30 ALLOW UDP fe80::4c2e:505d:b3a7:caaf ff02::1:3 58846 5355 0 - - - - - - - SEND
2015-07-16 11:35:30 ALLOW UDP 10.40.4.182 224.0.0.252 58846 5355 0 - - - - - - - SEND
2015-07-16 11:35:31 ALLOW UDP 10.40.4.182 224.0.0.252 137 137 0 - - - - - - - SEND
2015-07-16 11:35:31 ALLOW UDP fe80::4c2e:505d:b3a7:caaf ff02::1:3 63504 5355 0 - - - - - - - SEND
2015-07-16 11:35:31 ALLOW UDP 10.40.4.182 224.0.0.252 63504 5355 0 - - - - - - - SEND
```

Refer to the exhibit. An engineer received an event log file to review. Which technology generated the log?

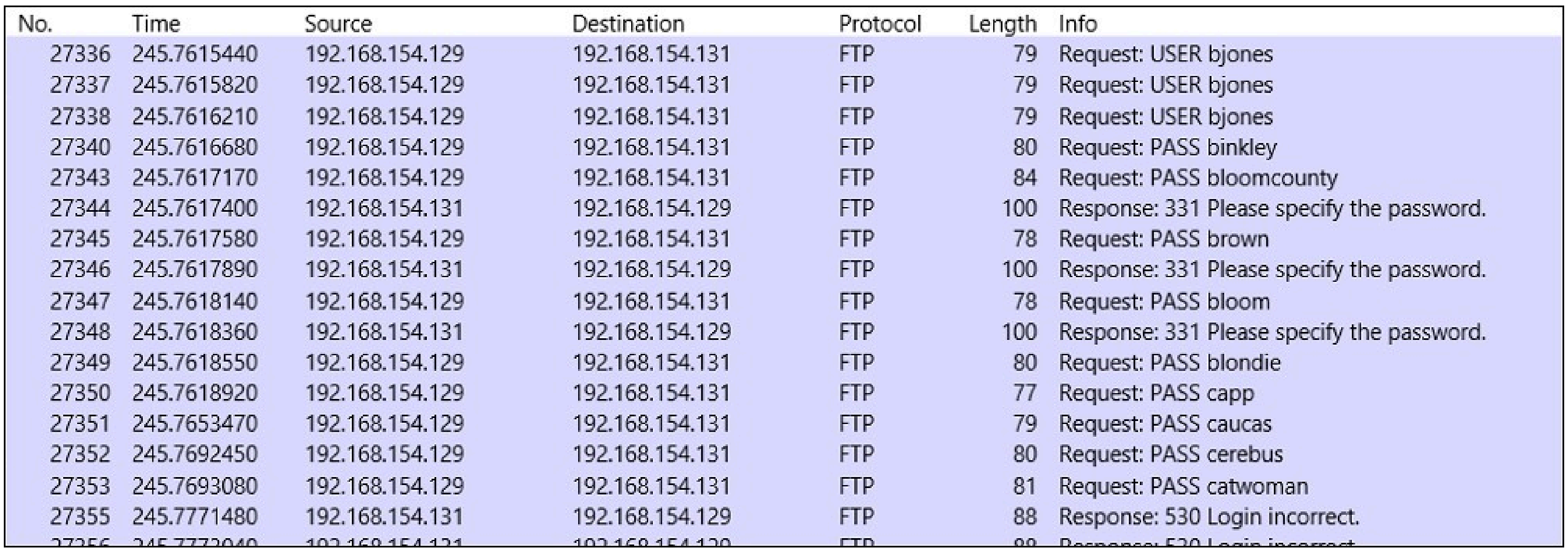
A. IDS/IPS

B. firewall

C. proxy

D. NetFlow

Question #240 *Topic 1*



```
No.    Time         Source           Destination      Protocol  Length  Info
27336  245.7615440  192.168.154.129  192.168.154.131  FTP           79  Request: USER bjones
27337  245.7615820  192.168.154.129  192.168.154.131  FTP           79  Request: USER bjones
27338  245.7616210  192.168.154.129  192.168.154.131  FTP           79  Request: USER bjones
27340  245.7616680  192.168.154.129  192.168.154.131  FTP           80  Request: PASS binkley
27343  245.7617170  192.168.154.129  192.168.154.131  FTP           84  Request: PASS bloomcounty
27344  245.7617400  192.168.154.131  192.168.154.129  FTP          100  Response: 331 Please specify the password.
27345  245.7617580  192.168.154.129  192.168.154.131  FTP           78  Request: PASS brown
27346  245.7617890  192.168.154.131  192.168.154.129  FTP          100  Response: 331 Please specify the password.
27347  245.7618140  192.168.154.129  192.168.154.131  FTP           78  Request: PASS bloom
27348  245.7618360  192.168.154.131  192.168.154.129  FTP          100  Response: 331 Please specify the password.
27349  245.7618550  192.168.154.129  192.168.154.131  FTP           80  Request: PASS blondie
27350  245.7618920  192.168.154.129  192.168.154.131  FTP           77  Request: PASS capp
27351  245.7653470  192.168.154.129  192.168.154.131  FTP           79  Request: PASS caucas
27352  245.7692450  192.168.154.129  192.168.154.131  FTP           80  Request: PASS cerebus
27353  245.7693080  192.168.154.129  192.168.154.131  FTP           81  Request: PASS catwoman
27355  245.7771480  192.168.154.131  192.168.154.129  FTP           88  Response: 530 Login incorrect.
27356  245.7772040  192.168.154.131  192.168.154.129  FTP           88  Response: 530 Login incorrect.
```

Refer to the exhibit. An analyst was given a PCAP file, which is associated with a recent intrusion event in the company FTP server. Which display filters should the analyst use to filter the FTP traffic?

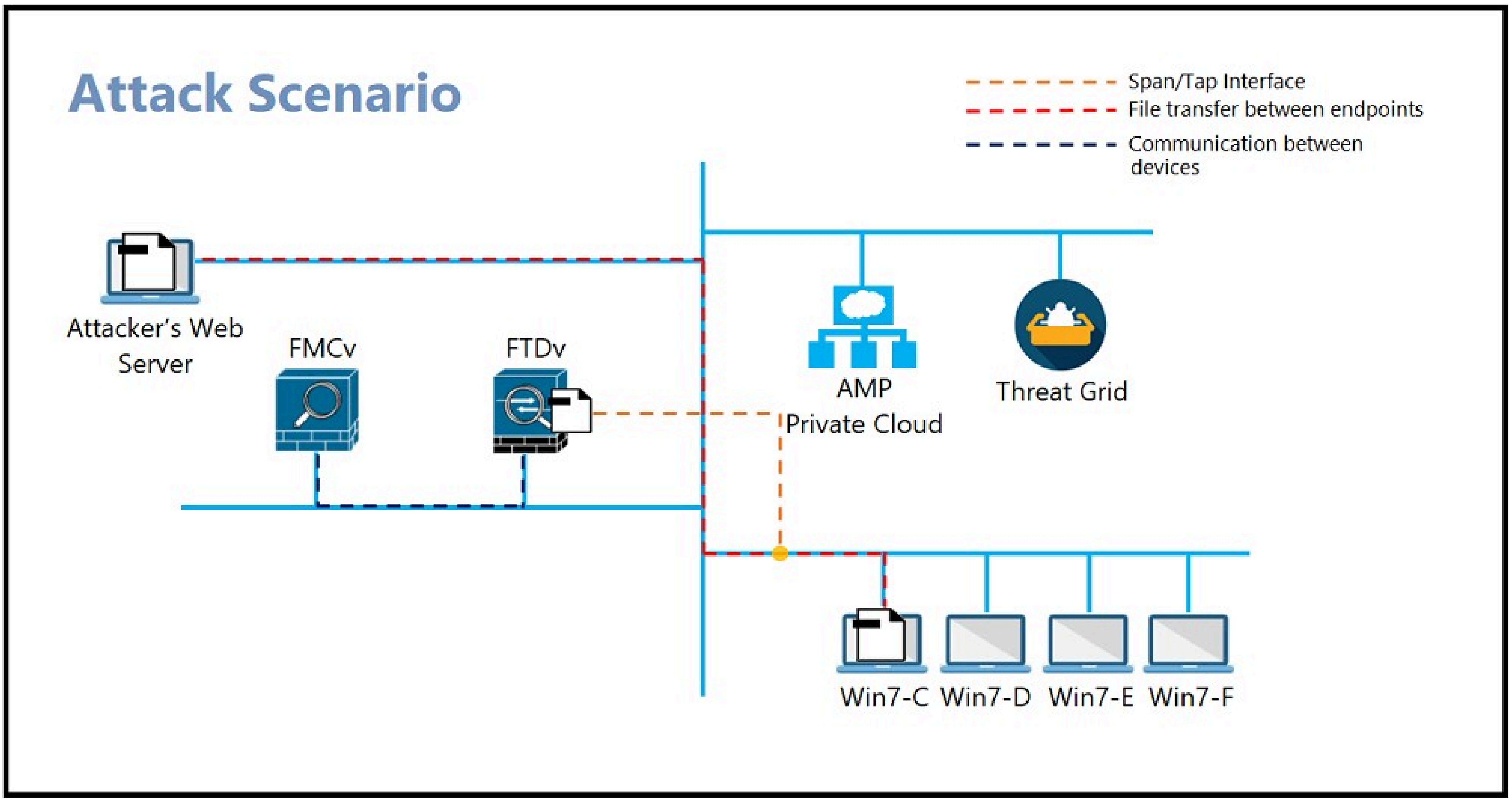
A. dst.port = 21

B. tcp.port == 21

C. dstport == FTP

D. tcpport = FTP

Question #241 *Topic 1*



Refer to the exhibit. A workstation downloads a malicious .docx file from the Internet and a copy is sent to FTDv. The FTDv sends the file hash to FMC and the file event is recorded. What would have occurred with stronger data visibility?

A. An extra level of security would have been in place.

B. Malicious traffic would have been blocked on multiple devices.

C. The traffic would have been monitored at any segment in the network.

D. Detailed information about the data in real time would have been provided.

Question #242 *Topic 1*

Refer to the exhibit. Which frame numbers contain a file that is extractable via TCP stream within Wireshark?

A. 7 to 21

B. 7 and 21

C. 7, 14, and 21

D. 14, 16, 18, and 19

Question #243 *Topic 1*

Refer to the exhibit. What is occurring?

A. DNS tunneling

B. DNS amplification

C. ARP poisoning

D. ARP flood

Question #244 *Topic 1*

Refer to the exhibit. An engineer is analyzing a PCAP file after a recent breach. An engineer identified that the attacker used an aggressive ARP scan to scan the hosts and found web and SSH servers. Further analysis showed several SSH Server Banner and Key Exchange Initiations. The engineer cannot see the exact data being transmitted over an encrypted channel and cannot identify how the attacker gained access. How did the attacker gain access?

A. by using an SSH Tectia Server vulnerability to enable host-based authentication

B. by using brute force on the SSH service to gain access

C. by using the buffer overflow in the URL catcher feature for SSH

D. by using an SSH vulnerability to silently redirect connections to the local host

Question #245 *Topic 1*

What describes a buffer overflow attack?

A. suppressing the buffers in a process

B. injecting new commands into existing buffers

C. overloading a predefined amount of memory

D. fetching data from memory buffer registers

Question #246 *Topic 1*

What should an engineer use to aid the trusted exchange of public keys between user tom0426871442 and dan1968754032?

A. central key management server

B. web of trust

C. registration authority data

D. trusted certificate authorities

Question #247 *Topic 1*

Which tool gives the ability to see session data in real time?

A. tcpdstat

B. trafdump

C. trafshow

D. tcptrace

Question #248 *Topic 1*

Refer to the exhibit. An engineer needs to identify certificate information on server1234567890. What does the exhibit indicate?

A. Elliptic-curve cryptography is used for the public keys.

B. Key exchange is not secure as the SHA256 hashing algorithm is used.

C. The certificate is signed by GTS CA on May 24 and is invalid.

D. Asymmetric cryptography is used for key exchange.

Question #249 *Topic 1*

Which of these describes volatile evidence?

A. logs

B. registers and cache

C. disk and removable drives

D. usernames

Question #250 *Topic 1*

Which security model assumes an attacker within and outside of the network and enforces strict verification before connecting to any system or resource within the organization?

A. Take-Grant

B. Object-capability

C. Zero Trust

D. Biba

Question #251 *Topic 1*

Why is HTTPS traffic difficult to screen?

A. HTTPS is used internally and screening traffic for external parties is hard due to isolation.

B. Digital certificates secure the session, and the data is sent at random intervals.

C. Traffic Is tunneled to a specific destination and is inaccessible to others except for the receiver.

D. The communication is encrypted and the data in transit is secured.

Question #252 *Topic 1*

A user received a targeted spear-phishing email and identified it as suspicious before opening the content. To which category of the Cyber Kill Chain model does to this type of event belong?

A. exploitation

B. weaponization

C. reconnaissance

D. delivery

Question #253 *Topic 1*

Refer to the exhibit. An engineer is reviewing a Cuckoo report of a file. What must the engineer interpret from the report?

A. The file will monitor user activity and send the information to an outside source.

B. The file will Insert itself into an application and execute when the application is run.

C. The file will appear legitimate by evading signature-based detection.

D. The file will not execute its behavior in a sandbox environment to avoid detection.

Question #254 *Topic 1*

What are two differences between tampered disk images and untampered disk images? (Choose two.)

A. The image is tampered if the stored hash and the computed hash are identical.

B. Tampered images are used as an element for the root cause analysis report.

C. Untampered images can be used as law enforcement evidence.

D. Tampered images are used in a security Investigation process.

E. The image is untampered if the existing stored hash matches the computed one.

Question #255 *Topic 1*

Which system monitors local system operation and local network access for violations of a security policy?

A. host-based data loss prevention

B. host-based intrusion detection

C. antivirus

D. sandbox

Question #256 *Topic 1*

What is the difference between indicator of attack (IoA) and indicators of compromise (IoC)?

A. IoA refers to the individual responsible for the security breach, and IoC refers to the resulting loss.

B. IoA is the evidence that a security breach has occurred, and IoC allows organizations to act before the vulnerability can be exploited.

C. IoC refers to the individual responsible for the security breach, and IoA refers to the resulting loss.

D. IoC is the evidence that a security breach has occurred, and IoA allows organizations to act before the vulnerability can be exploited.

Question #257 *Topic 1*

What is the functionality of an IDS?

A. forensic tool used to perform an in-depth analysis and debugging

B. software or device which monitors and identifies malicious network activity

C. device or software that detects and blocks suspicious files

D. endpoint protection software that prevents viruses and malware

Question #258 *Topic 1*

What is a description of "phishing" as a social engineering attack?

A. Fake Social Security Administration personnel contact random individuals, inform them that there has been a computer problem on their end, and ask that those individuals confirm their Social Security Number, all for the purpose of committing identity theft.

B. A hacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message. The recipient is then tricked into clicking a malicious link.

C. The attacker focuses on creating a good pretext, or a fabricated scenario, that is used to try and steal victims' personal information.

D. Someone without the proper authentication follows an authenticated employee into a restricted area. The attacker might impersonate a delivery driver and wait outside a building to get things started.

Question #259 *Topic 1*

According to the NIST SP 800-86, which two types of data are considered volatile? (Choose two.)

A. temporary files

B. login sessions

C. swap files

D. dump files

E. free space

Question #260 *Topic 1*

Which technique describes altering the data content and avoiding identification?

A. data modification, such as hashing

B. catching clear text data transfer

C. data in transit hijacking

D. obfuscation, such as tunneling

Question #261 *Topic 1*

Refer to the exhibit. An employee received an email from an unknown sender with an attachment and reported it as a phishing attempt. An engineer uploaded the file to Cuckoo for further analysis. What should an engineer interpret from the provided Cuckoo report?

A. MD5 of the file was not identified as malicious.

B. Win32.polip.a.exe is an executable file and should be flagged as malicious.

C. The file is clean and does not represent a risk.

D. Cuckoo cleaned the malicious file and prepared it for usage.

Question #262 *Topic 1*

Which CVSS metric group identifies other components that are affected by a successful security attack?

A. scope

B. privileges required

C. integrity

D. attack vendor

Question #263 *Topic 1*

Refer to the exhibit. A suspicious IP address is tagged by Threat Intelligence as a brute-force attempt source. After the attacker produces many of failed login entries it successfully compromises the account. Which stakeholder is responsible for the incident response detection step?

A. employee 2

B. employee 3

C. employee 4

D. employee 5

Question #264 *Topic 1*

An engineer is working on a ticket for an incident from the incident management team. A week ago, an external web application was targeted by a DDoS attack. Server resources were exhausted and after two hours, it crashed. An engineer was able to identify the attacker and technique used. Three hours after the attack, the server was restored and the engineer recommended implementing mitigation by Blackhole filtering and transferred the incident ticket back to the IR team. According to NIST.SP800-61, at which phase of the incident response did the engineer finish work?

A. post-incident activity

B. preparation

C. detection and analysis

D. containment, eradication, and recovery

Question #265 *Topic 1*

What is the difference between attack surface and vulnerability?

A. A vulnerability is a way of taking advantage of a system or resource, and an attack surface is a specific technique utilized by the vulnerability.

B. An attack surface is a way of taking advantage of a system or resource, and a vulnerability is a specific technique utilized by the vulnerability.

C. An attack surface describes how software or a system is exposed to potential attacks, and a vulnerability is an actual weakness that exposes the potential risk.

D. A vulnerability describes how software or a system is exposed to potential attacks, and an attack surface is an actual weakness that exposes the potential risk.

Question #266 *Topic 1*

What is a scareware attack?

A. inserting malicious code that causes popup windows with flashing colors

B. overwhelming a targeted website with fake traffic

C. gaining access to your computer and encrypting data stored on it

D. using the spoofed email addresses to trick people into providing login credentials

Question #267 *Topic 1*

What is the communication channel established from a compromised machine back to the attacker?

A. man-in-the-middle

B. command and control

C. IDS evasion

D. port scanning

Question #268 *Topic 1*

During which phase of the forensic process are tools and techniques used to extract information from the collected data?

A. examination

B. investigation

C. collection

D. reporting

Question #269 *Topic 1*

An information security analyst inspects the .pcap file and observes encrypted unusual SSH traffic flow over nonstandard ports Which technology makes this behavior feasible?+

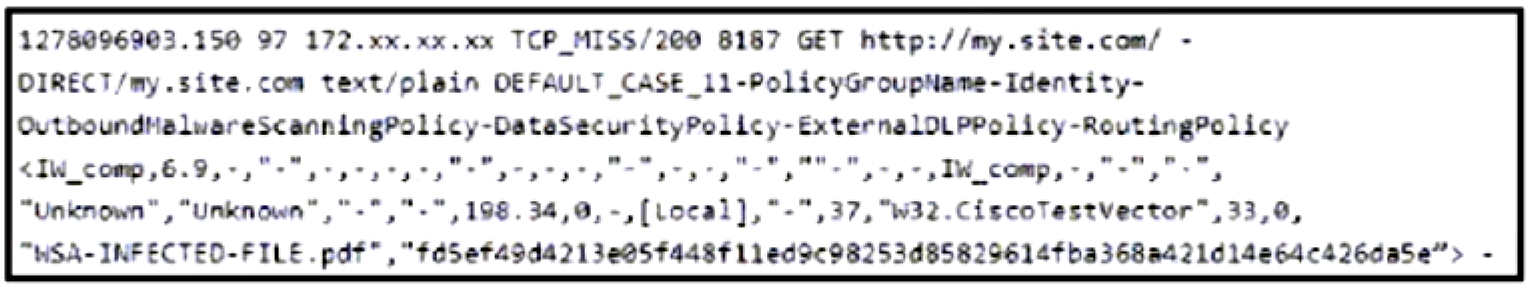
A. NAT

B. tunneling

C. P2P

D. TOR

Question #270 *Topic 1*



```
1278096903.150 97 172.xx.xx.xx TCP_MISS/200 8187 GET http://my.site.com/ -
DIRECT/my.site.com text/plain DEFAULT_CASE_11-PolicyGroupName-Identity-
OutboundMalwareScanningPolicy-DataSecurityPolicy-ExternalDLPPolicy-RoutingPolicy
<IW_comp,6.9,-,"-",-,-,-,-,"-",-,-,-,"-",-,-,"-",""-",-,-,IW_comp,-,"-","-",
"Unknown","Unknown","-","-",198.34,0,-,[Local],"-",37,"W32.CiscoTestVector",33,0,
"WSA-INFECTED-FILE.pdf","fd5ef49d4213e05f448f11ed9c98253d85829614fba368a421d14e64c426da5e"> -
```

Refer to the exhibit. Which technology produced the log?

A. antivirus

B. IPS/IDS

C. firewall

D. proxy

Question #271 *Topic 1*

What is the role of NAT in data visibility?

A. load balancing

B. hiding IP addresses

C. web filtering

D. encrypting files

Question #272 *Topic 1*

What is the purpose of command and control for network-aware malware?

A. It controls and shuts down services on the infected host.

B. It helps the malware to profile the host.

C. It contacts a remote server for commands and updates.

D. It takes over the user account for analysis.

Question #273 *Topic 1*

Which element is included in an incident response plan as stated in NIST.SP800-617

A. security of sensitive information

B. individual approach to incident response

C. consistent threat identification

D. approval of senior management