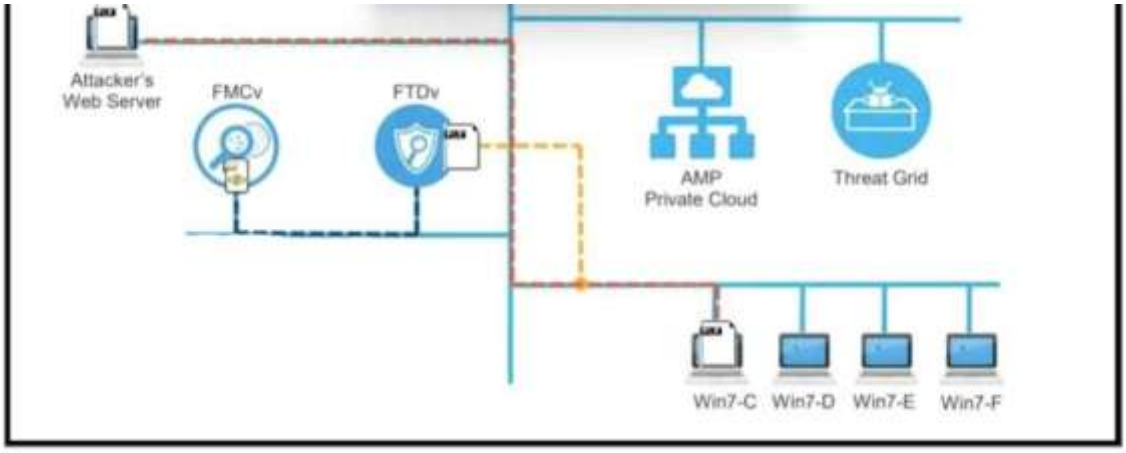
QUESTION 224
What describes the defense-m-depth principle?

A. defining precise guidelines for new workstation installations
B. categorizing critical assets within the organization
C. isolating guest Wi-Fi from the focal network
D. implementing alerts for unexpected asset malfunctions

Answer: B

QUESTION 225
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 tile event is recorded. What would have occurred with stronger data visibility?



A. The traffic would have been monitored at any segment in the network.
B. Malicious traffic would have been blocked on multiple devices
C. An extra level of security would have been in place
D. Detailed information about the data in real time would have been provided

Answer: B

QUESTION 226
What is the impact of encryption?

A. Confidentiality of the data is kept secure and permissions are validated
B. Data is accessible and available to permitted individuals
C. Data is unaltered and its integrity is preserved
D. Data is secure and unreadable without decrypting it

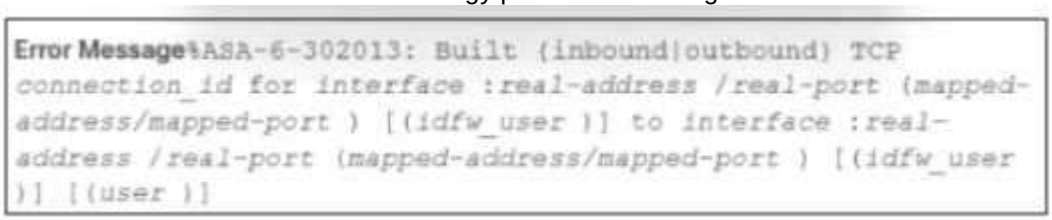
Answer: A

QUESTION 227
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 externa 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. list of security restrictions and privileges boundaries bypassed
B. external USB device
C. receptionist and the actions performed
D. stolen data and its criticality assessment

Answer: A

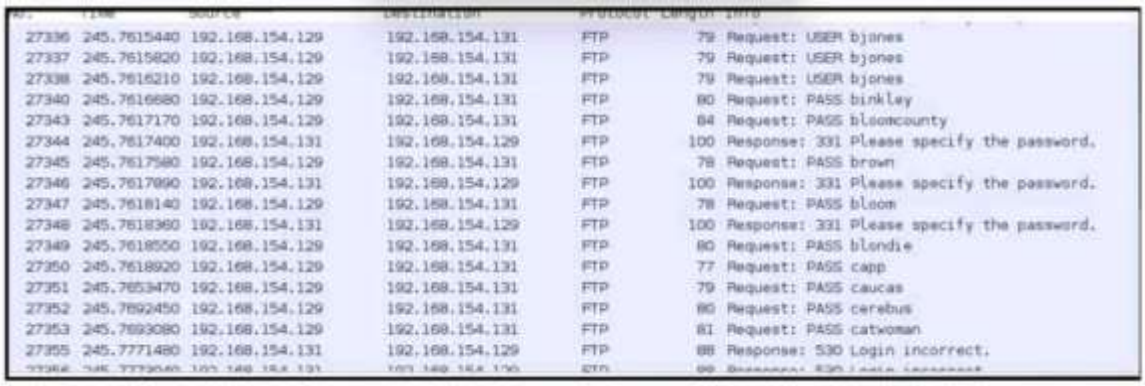
QUESTION 228
Refer to the exhibit. During the analysis of a suspicious scanning activity incident, an analyst discovered multiple local TCP connection events. Which technology provided these logs?



A. antivirus
B. proxy
C. IDS/IPS
D. firewall

Answer: D

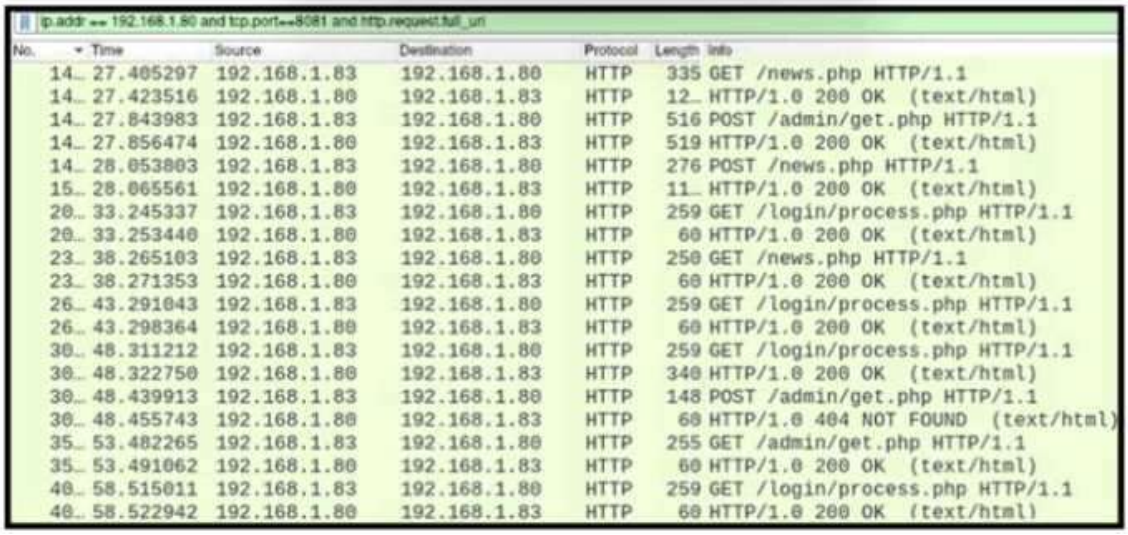
QUESTION 229
Refer to the exhibit. An analyst was given a PCAP file, which is associated with a recent intrusion event in the company FTP server. Which display filters should the analyst use to filter the FTP traffic?



A. dstport == FTP
B. tcp.port==21
C. tcpport = FTP
D. dstport = 21

Answer: C

QUESTION 230
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. garbage flood attack attacker is sending garbage binary data to open ports
C. indicators of data exfiltration HTTP requests must be plain text
D. cache bypassing attack: attacker is sending requests for noncacheable content

Answer: C

QUESTION 231
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 1.3.
B. Install the latest IIS version.
C. Downgrade to TLS 1.1.
D. Deploy an intrusion detection system

Answer: B

QUESTION 232
What is the difference between discretionary access control (DAC) and role-based access control (RBAC)?

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

B. RBAC access is granted when a user meets specific conditions, and in DAC, permissions are applied on user and group levels.
C. RBAC is an extended version of DAC where you can add an extra level of authorization based on time.
D. DAC administrators pass privileges to users and groups, and in RBAC, permissions are applied to specific groups

Answer: A

QUESTION 233
Which technology prevents end-device to end-device IP traceability?

A. encryption
B. load balancing
C. NAT/PAT
D. tunneling

Answer: C

QUESTION 234
What are the two differences between stateful and deep packet inspection? (Choose two)

A. Stateful inspection is capable of TCP state tracking, and deep packet filtering checks only TCP source and destination ports
B. Deep packet inspection is capable of malware blocking, and stateful inspection is not
C. Deep packet inspection operates on Layer 3 and 4. and stateful inspection operates on Layer 3 of the OSI model
D. Deep packet inspection is capable of TCP state monitoring only, and stateful inspection can inspect TCP and UDP.
E. Stateful inspection is capable of packet data inspections, and deep packet inspection is not

Answer: AB

QUESTION 235
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. data integrity
C. data preservation
D. volatile data collection

Answer: B

QUESTION 236
What is the difference between inline traffic interrogation (TAPS) and traffic mirroring (SPAN)?

A. APS interrogation is more complex because traffic mirroring applies additional tags to data and SPAN does not alter integrity and provides full duplex network.
B. SPAN results in more efficient traffic analysis, and TAPS is considerably slower due to latency caused by mirroring.
C. TAPS replicates the traffic to preserve integrity, and SPAN modifies packets before sending them to other analysis tools
D. SPAN ports filter out physical layer errors, making some types of analyses more difficult, and TAPS receives all packets, including physical errors.

Answer: A

QUESTION 237
Which information must an organization use to understand the threats currently targeting the organization?

A. threat intelligence
B. risk scores
C. vendor suggestions
D. vulnerability exposure

Answer: A

QUESTION 238
What is threat hunting?

A. Managing a vulnerability assessment report to mitigate potential threats.
B. Focusing on proactively detecting possible signs of intrusion and compromise.
C. Pursuing competitors and adversaries to infiltrate their system to acquire intelligence data.
D. Attempting to deliberately disrupt servers by altering their availability

Answer: A

QUESTION 239
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 penmeter 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. PHI
D. PCI
E. copyright

Answer: BC

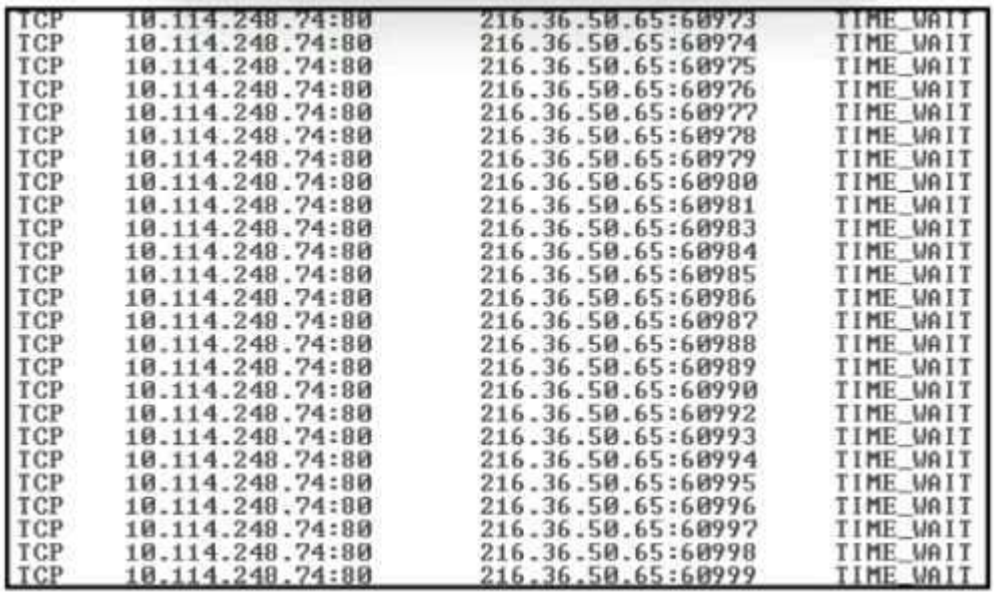
QUESTION 240
What describes the impact of false-positive alerts compared to false-negative alerts?

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 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
C. A false positive is an event alerting 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 positive is an event alerting 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.

Answer: C

QUESTION 241

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



```
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
```

A. The web application is receiving a common, legitimate traffic
B. The engineer must gather more data.
C. The web application server is under a denial-of-service attack.
D. The server is under a man-in-the-middle attack between the web application and its database

Answer: C

QUESTION 242
When an event is investigated, which type of data provides the investigate capability to determine if data exfiltration has occurred?

A. full packet capture
B. NetFlow data
C. session data
D. firewall logs

Answer: A

QUESTION 243
What is the difference between deep packet inspection and stateful inspection?

A. Deep packet inspection gives insights up to Layer 7, and stateful inspection gives insights only up to Layer 4.
B. Deep packet inspection is more secure due to its complex signatures, and stateful inspection requires less human intervention.
C. Stateful inspection is more secure due to its complex signatures, and deep packet inspection requires less human intervention.
D. Stateful inspection verifies data at the transport layer and deep packet inspection verifies data at the application layer

Answer: B

QUESTION 244
What is obtained using NetFlow?

A. session data
B. application logs
C. network downtime report
D. full packet capture

Answer: A

QUESTION 245
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. Statistical detection defines legitimate data over time, and rule-based detection works on a predefined set of rules
C. Rule-based detection involves the evaluation of events, and statistical detection requires an evaluated set of events to function Rule-based detection defines
D. legitimate data over a period of time, and statistical detection works on a predefined set of rules

Answer: B

QUESTION 246
Refer to the exhibit. What must be interpreted from this packet capture?

```
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
```

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

Answer: B