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.

Correct Answer: C

QUESTION 41
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

Correct Answer: D

QUESTION 42
What is a collection of compromised machines that attackers use to carry out a DDoS attack?

A. subnet
B. botnet
C. VLAN
D. command and control

Correct Answer: B

QUESTION 43
According to the NIST SP 800-86. which two types of data are considered volatile? (Choose two.)

A. swap files
B. temporary files
C. login sessions
D. dump files
E. free space

Correct Answer: CE

QUESTION 44
A security engineer notices confidential data being exfiltrated to a domain "Ranso4134-mware31-895" 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

Correct Answer: D

QUESTION 45
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 host name
B. protocol, source IP, source port, destination IP, and destination port
C. event name, log source, time, source IP, and username
D. protocol, log source, source IP, destination IP, and host name

Correct Answer: B

QUESTION 46
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

Correct Answer: C

QUESTION 47
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

Correct Answer: AB

QUESTION 48
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

Correct Answer: D

QUESTION 49
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.

Correct Answer: B

QUESTION 50
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

Correct Answer: CD

QUESTION 51
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

Correct Answer: B

QUESTION 52
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

Correct Answer: C

QUESTION 53
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

Correct Answer: B

QUESTION 54
What is vulnerability management?

A. A security practice focused on clarifying and narrowing intrusion points.
B. A security practice of performing actions rather than acknowledging the threats.
C. A process to identify and remediate existing weaknesses.
D. A process to recover from service interruptions and restore business-critical applications

Correct Answer: C

QUESTION 55
Why is HTTPS traffic difficult to screen?

A. HTTPS is used internally and screening traffic (or external parties is hard due to isolation.
B. The communication is encrypted and the data in transit is secured.
C. Digital certificates secure the session, and the data is sent at random intervals.
D. Traffic is tunneled to a specific destination and is inaccessible to others except for the receiver.

Correct Answer: B

QUESTION 56
During which phase of the forensic process are tools and techniques used to extract information from the collected data?

A. investigation
B. examination
C. reporting
D. collection

Correct Answer: D

QUESTION 57
Which action prevents buffer overflow attacks?

A. variable randomization
B. using web based applications
C. input sanitization
D. using a Linux operating system

Correct Answer: C

QUESTION 58
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

Correct Answer: C

QUESTION 59
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

Correct Answer: A

QUESTION 60
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

Correct Answer: A

QUESTION 61
What is the difference between deep packet inspection and stateful inspection?

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

Correct Answer: D

QUESTION 62
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.

Correct Answer: A

QUESTION 63