Correct Answer: A

QUESTION 85
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.

Correct Answer: D

QUESTION 86
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

Correct Answer: A

QUESTION 87
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

Correct Answer: CD

QUESTION 88
What is indicated by an increase in IPv4 traffic carrying protocol 41 ?

A. additional PPTP traffic due to Windows clients
B. unauthorized peer-to-peer traffic
C. deployment of a GRE network on top of an existing Layer 3 network
D. attempts to tunnel IPv6 traffic through an IPv4 network

Correct Answer: D

QUESTION 89
Which technology prevents end-device to end-device IP traceability?

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

Correct Answer: C

QUESTION 90
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. actions
B. delivery
C. reconnaissance
D. installation

Correct Answer: B

QUESTION 91
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

Correct Answer: C

QUESTION 92
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

Correct Answer: D

QUESTION 93
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

Correct Answer: B

QUESTION 94
Which regex matches only on all lowercase letters?

A. [az]+
B. [^az]+
C. az+
D. a*z+

Correct Answer: A

QUESTION 95
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.

Correct Answer: A

QUESTION 96
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

Correct Answer: C

QUESTION 97
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

Correct Answer: D

QUESTION 98
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

Correct Answer: B

QUESTION 99
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

Correct Answer: D

QUESTION 100
Which event is a vishing attack?

A. obtaining disposed documents from an organization
B. using a vulnerability scanner on a corporate network
C. setting up a rogue access point near a public hotspot
D. impersonating a tech support agent during a phone call

Correct Answer: D

QUESTION 101
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

Correct Answer: B

QUESTION 102
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

Correct Answer: B

QUESTION 103
How is attacking a vulnerability categorized?

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

Correct Answer: C

QUESTION 104
Which technology on a host is used to isolate a running application from other applications?

A. sandbox
B. application allow list
C. application block list
D. host-based firewall

Correct Answer: A

QUESTION 105
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

Correct Answer: D

QUESTION 106
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

Correct Answer: C

QUESTION 107
Which piece of information is needed for attribution in an investigation?