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
Correct Answer: C

QUESTION 108
What makes HTTPS traffic difficult to monitor?

A. SSL interception
B. packet header size
C. signature detection time
D. encryption

Correct Answer: D

QUESTION 109
What is a difference between tampered and untampered disk images?

A. Tampered images have the same stored and computed hash.
B. Tampered images are used as evidence.
C. Untampered images are used for forensic investigations.
D. Untampered images are deliberately altered to preserve as evidence

Correct Answer: B

QUESTION 110
What describes a buffer overflow attack?

A. injecting new commands into existing buffers
B. fetching data from memory buffer registers
C. overloading a predefined amount of memory
D. suppressing the buffers in a process

Correct Answer: C

QUESTION 111
What is the difference between an attack vector and 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.

Correct Answer: C

QUESTION 112
Which two elements of the incident response process are stated in NIST SP 800-61 r2? (Choose two.)

A. detection and analysis
B. post-incident activity
C. vulnerability scoring
D. vulnerability management
E. risk assessment

Correct Answer: AB

QUESTION 113
Which category relates to improper use or disclosure of PII data?

A. legal
B. compliance
C. regulated
D. contractual

Correct Answer: C

QUESTION 114
What is the difference between a threat and an exploit?

A. A threat is a result of utilizing flow in a system, and an exploit is a result of gaining control over the system.
B. A threat is a potential attack on an asset and an exploit takes advantage of the vulnerability of the asset
C. An exploit is an attack vector, and a threat is a potential path the attack must go through.
D. An exploit is an attack path, and a threat represents a potential vulnerability

Correct Answer: B

QUESTION 115
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

Correct Answer: D

QUESTION 116
How does TOR alter data content during transit?

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

B. It encrypts content and destination information over multiple layers.
C. It redirects destination traffic through multiple sources avoiding traceability.
D. It traverses source traffic through multiple destinations before reaching the receiver

Correct Answer: B

QUESTION 117
What should an engineer use to aid the trusted exchange of public keys between user tom0411976943 and dan1968754032?

A. central key management server
B. web of trust
C. trusted certificate authorities
D. registration authority data

Correct Answer: C

QUESTION 118
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

Correct Answer: D

QUESTION 119
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

Correct Answer: C

QUESTION 120
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

Correct Answer: A

QUESTION 121

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, resulting in a potential breach.
B. True positive alerts are blocked by mistake as potential attacks affecting application availability.
C. False positives affect security as no alarm is raised when an attack has taken place, resulting in a potential breach.
D. False positive alerts are blocked by mistake as potential attacks affecting application availability.

Correct Answer: C

QUESTION 122
What is a difference between an inline and a tap mode traffic monitoring?

A. Inline monitors traffic without examining other devices, while a tap mode tags traffic and examines the data from monitoring devices.
B. Tap mode monitors traffic direction, while inline mode keeps packet data as it passes through the monitoring devices.
C. Tap mode monitors packets and their content with the highest speed, while the inline mode draws a packet path for analysis.
D. Inline mode monitors traffic path, examining any traffic at a wire speed, while a tap mode monitors traffic as it crosses the network.

Correct Answer: D

QUESTION 123
Which attack method intercepts traffic on a switched network?

A. denial of service
B. ARP cache poisoning
C. DHCP snooping
D. command and control

Correct Answer: B

QUESTION 124
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. by most active source IP
B. by most used ports
C. based on the protocols used
D. based on the most used applications

Correct Answer: A

QUESTION 125
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 tile size

is exceeded. Which action resolves the issue?

A. Add space to the existing partition and lower the retention penod.
B. Use FAT32 to exceed the limit of 4 GB.
C. Use the Ext4 partition because it can hold files up to 16 TB.
D. Use NTFS partition for log file containment

Correct Answer: D

QUESTION 126
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

Correct Answer: C

QUESTION 127
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

Correct Answer: C

QUESTION 128
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

Correct Answer: C

QUESTION 129
Which open-sourced packet capture tool uses Linux and Mac OS X operating systems?

A. NetScout
B. tcpdump
C. SolarWinds
D. netsh

Correct Answer: B