C. receptionist and the actions performed
D. stolen data and its criticality assessment

Correct Answer: C

QUESTION 20
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

Correct Answer: C

QUESTION 21
Which are two denial-of-service attacks? (Choose two.)

A. TCP connections
B. ping of death
C. man-in-the-middle
D. code-red
E. UDP flooding

Correct Answer: BE

QUESTION 22
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

Correct Answer: C

QUESTION 23
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

Correct Answer: B

QUESTION 24
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 an 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

Correct Answer: A

QUESTION 25
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

Correct Answer: C

QUESTION 26
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

Correct Answer: B

QUESTION 27
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

Correct Answer: B

QUESTION 28

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

A. IoA is the evidence that a security breach has occurred, and IoC allows organizations to act before the vulnerability can be exploited.
B. IoA refers to the individual responsible for the security breach, and IoC refers to the resulting loss.
C. IoC is the evidence that a security breach has occurred, and IoA allows organizations to act before the vulnerability can be exploited.
D. IoC refers to the individual responsible for the security breach, and IoA refers to the resulting loss.

Correct Answer: C

QUESTION 29
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

Correct Answer: C

QUESTION 30
Which utility blocks a host portscan?

A. HIDS
B. sandboxing
C. host-based firewall
D. antimalware

Correct Answer: C

QUESTION 31
An engineer must compare NIST vs ISO frameworks The engineer deeded to compare as readable documentation and also to watch a comparison video review. Using Windows 10 OS. the engineer started a browser and searched for a NIST document and then opened a new tab in the same browser and searched for an ISO document for comparison. The engineer tried to watch the video, but there 'was an audio problem with OS so the engineer had to troubleshoot it At first the engineer started CMD and looked fee a driver path then locked for a corresponding registry in the registry editor The engineer enabled "Audiosrv" in task manager and put it on auto start and the problem was solved Which two components of the OS did the engineer touch? (Choose two)

A. permissions
B. PowerShell logs
C. service
D. MBR
E. process and thread

Correct Answer: AC

QUESTION 32

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$

Correct Answer: A

QUESTION 33
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

Correct Answer: D

QUESTION 34
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.

Correct Answer: CE

QUESTION 35
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.

Correct Answer: A

QUESTION 36
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

Correct Answer: B

QUESTION 37
What are two differences in how tampered and untampered disk images affect a security incident? (Choose two.)

A. Untampered images are used in the security investigation process
B. Tampered images are used in the security investigation process
C. The image is tampered if the stored hash and the computed hash match
D. Tampered images are used in the incident recovery process
E. The image is untampered if the stored hash and the computed hash match

Correct Answer: AE

QUESTION 38
How does agentless monitoring differ from agent-based monitoring?

A. Agentless can access the data via API. while agent-base uses a less efficient method and accesses log data through WMI.
B. Agent-based monitoring is less intrusive in gathering log data, while agentless requires open ports to fetch the logs
C. Agent-based monitoring has a lower initial cost for deployment, while agentless monitoring requires resource-intensive deployment.
D. Agent-based has a possibility to locally filter and transmit only valuable data, while agentless has much higher network utilization

Correct Answer: B

QUESTION 39
Which metric in CVSS indicates an attack that takes a destination bank account number and replaces it with a different bank account number?

A. availability
B. confidentiality
C. scope
D. integrity

Correct Answer: D

QUESTION 40
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