policies
D. Inline interrogation detects malicious traffic but does not block the traffic

Correct Answer: A

QUESTION 152
Which regular expression is needed to capture the IP address 192.168.20.232?

A. ^ (?:[0-9]{1,3}\.){3}[0-9]{1,3}
B. ^ (?:[0-9]f1,3}\.){1,4}
C. ^ (?:[0-9]{1,3}\.)'
D. ^ ([0-9]-{3})

Correct Answer: A

QUESTION 153
An analyst received an alert on their desktop computer showing that an attack was successful on the host. After investigating, the analyst discovered that no mitigation action occurred during the attack. What is the reason for this discrepancy?

A. The computer has a HIPS installed on it.
B. The computer has a NIPS installed on it.
C. The computer has a HIDS installed on it.
D. The computer has a NIDS installed on it.

Correct Answer: C

QUESTION 154
What is a difference between SIEM and SOAR?

A. SOAR predicts and prevents security alerts, while SIEM checks attack patterns and applies the mitigation.
B. SIEM's primary function is to collect and detect anomalies, while SOAR is more focused on security operations automation and response.
C. SIEM predicts and prevents security alerts, while SOAR checks attack patterns and applies the mitigation.
D. SOAR's primary function is to collect and detect anomalies, while SIEM is more focused on security operations automation and response.

Correct Answer: B

QUESTION 155
Which attack represents the evasion technique of resource exhaustion?

A. SQL injection
B. man-in-the-middle
C. bluesnarfing
D. denial-of-service

Correct Answer: D

QUESTION 156
At which layer is deep packet inspection investigated on a firewall?

A. internet
B. transport
C. application
D. data link

Correct Answer: C

QUESTION 157
Which regular expression matches "color" and "colour"?

A. colo?ur
B. col[08]+our
C. colou?r
D. col[09]+our

Correct Answer: C

QUESTION 158
A security engineer deploys an enterprise-wide host/endpoint technology for all of the company's corporate PCs. Management requests the engineer to block a selected set of applications on all PCs. Which technology should be used to accomplish this task?

A. application whitelisting/blacklisting
B. network NGFW
C. host-based IDS
D. antivirus/antispyware software

Correct Answer: A

QUESTION 159
Which evasion technique is a function of ransomware?

A. extended sleep calls
B. encryption
C. resource exhaustion
D. encoding

Correct Answer: B

QUESTION 160
Which type of access control depends on the job function of the user?

A. discretionary access control
B. nondiscretionary access control
C. role-based access control
D. rule-based access control

Correct Answer: C

QUESTION 161
A company receptionist received a threatening call referencing stealing assets and did not take any action assuming it was a social engineering attempt. Within 48 hours, multiple assets were breached, affecting the confidentiality of sensitive information. What is the threat actor in this incident?

A. company assets that are threatened
B. customer assets that are threatened
C. perpetrators of the attack
D. victims of the attack

Correct Answer: B

QUESTION 162
What is the difference between a threat and a risk?

A. Threat represents a potential danger that could take advantage of a weakness in a system
B. Risk represents the known and identified loss or danger in the system
C. Risk represents the nonintentional interaction with uncertainty in the system
D. Threat represents a state of being exposed to an attack or a compromise, either physically or logically.

Correct Answer: A

QUESTION 163
What causes events on a Windows system to show Event Code 4625 in the log messages?

A. The system detected an XSS attack
B. Someone is trying a brute force attack on the network
C. Another device is gaining root access to the system
D. A privileged user successfully logged into the system

Correct Answer: B

QUESTION 164
Which type of attack occurs when an attacker is successful in eavesdropping on a conversation between two IP phones?

A. known-plaintext
B. replay
C. dictionary
D. man-in-the-middle

Correct Answer: D

QUESTION 165
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

Correct Answer: A

QUESTION 166
What is the difference between the ACK flag and the RST flag in the NetFlow log session?

A. The RST flag confirms the beginning of the TCP connection, and the ACK flag responds when the data for the payload is complete
B. The ACK flag confirms the beginning of the TCP connection, and the RST flag responds when the data for the payload is complete
C. The RST flag confirms the receipt of the prior segment, and the ACK flag allows for the spontaneous termination of a connection
D. The ACK flag confirms the receipt of the prior segment, and the RST flag allows for the spontaneous termination of a connection

Correct Answer: D

QUESTION 167
What specific type of analysis is assigning values to the scenario to see expected outcomes?

A. deterministic
B. exploratory
C. probabilistic
D. descriptive

Correct Answer: A
QUESTION 168
According to the September 2020 threat intelligence feeds a new malware called Egregor was introduced and used in many attacks. Distnbution of Egregor is pnmanly through a Cobalt Strike that has been installed on victim's workstations using RDP exploits Malware exfiltrates the victim's data to a command and control server. The data is used to force victims pay or lose it by publicly releasing it. Which type of attack is described?

A. malware attack
B. ransomware attack
C. whale-phishing
D. insider threat

Correct Answer: B

QUESTION 169
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

Correct Answer: A

QUESTION 170
An engineer runs a suspicious file in a sandbox analysis tool to see the outcome. The analysis report shows that outbound callouts were made post infection. Which two pieces of information from the analysis report are needed to investigate the callouts? (Choose two.)

A.   signatures
B.   host IP addresses
C.   file size
D.   dropped files
E.   domain names

Correct Answer: BE

QUESTION 171
How does an attack surface differ from an attack vector?

A.   An attack vector recognizes the potential outcomes of an attack, and the attack surface is choosing a method of an attack.
B.   An attack surface identifies vulnerable parts for an attack, and an attack vector specifies which attacks are feasible to those parts.
C.   An attack surface mitigates external vulnerabilities, and an attack vector identifies mitigation techniques and possible workarounds.
D.   An attack vector matches components that can be exploited, and an attack surface classifies the potential path for exploitation

Correct Answer: B

QUESTION 172
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

Correct Answer: B

QUESTION 173
What is a sandbox interprocess communication service?

A.   A collection of rules within the sandbox that prevent the communication between sandboxes.
B.   A collection of network services that are activated on an interface, allowing for inter-port communication.
C.   A collection of interfaces that allow for coordination of activities among processes.
D.   A collection of host services that allow for communication between sandboxes.

Correct Answer: C