SPOTO CCNA 200-201 Free Demo

QUESTION 1
What are two denial-of-service attacks? (Choose two.)

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

Correct Answer: BC

QUESTION 2
According to the September 2020 threat intelligence feeds, new malware called Egregor was introduced and used in many attacks. Distribution of Egregor is primarily 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. ransomware attack
B. whale-phishing
C. malware attack
D. insider threat

Correct Answer: A

QUESTION 3
What is the principle of defense-in-depth?

A. Agentless and agent-based protection for security are used.
B. Authentication, authorization, and accounting mechanisms are used.
C. Access control models are involved.
D. Several distinct protective layers are involved.

Correct Answer: D

QUESTION 4

What is an advantage of symmetric over asymmetric encryption?

A. It is suited for transmitting large amounts of data.
B. It is a faster encryption mechanism for sessions.
C. A one-time encryption key is generated for data transmission.
D. A key is generated on demand according to data type.

Correct Answer: A

QUESTION 5
What describes the concept of data consistently and readily being accessible for legitimate users?

A. Integrity
B. Confidentiality
C. Accessibility
D. Availability

Correct Answer: D

QUESTION 6
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 7
Which data format is the most efficient to build a baseline of traffic seen over an extended period of time?

A. syslog messages
B. firewall event logs
C. full packet capture
D. NetFlow

Correct Answer: D

QUESTION 8
What is a difference between signature-based and behavior-based detection?

A. Signature-based identifies behaviors that may be linked to attacks, while behavior-based has a predefined set of rules to match before an alert.
B. Signature-based uses a known vulnerability database, while behavior-based intelligently summarizes existing data.
C. Behavior-based identifies behaviors that may be linked to attacks, while signature-based has a predefined set of rules to match before an alert
D. Behavior-based uses a known vulnerability database, while signature-based intelligently summarizes existing data.

Correct Answer: C

QUESTION 9
Which two components reduce the attack surface on an endpoint? (Choose two.)

A. secure boot
B. load balancing
C. increased audit log levels
D. restricting USB ports

E. full packet captures at the endpoint

Correct Answer: AD

QUESTION 10
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