Vendor: Cisco

Exam Code: 200-201

Exam Name: Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS)

Version: Demo

QUESTION 1
An engineer needs to configure network systems to detect command and control communications by decrypting ingress and egress perimeter traffic and allowing network security devices to detect malicious outbound communications. Which technology should be used to accomplish the task?

A. digital certificates
B. static IP addresses
C. signatures
D. cipher suite

Correct Answer: A

QUESTION 2
What is rule-based detection when compared to statistical detection?

A. proof of a user's identity
B. proof of a user's action
C. likelihood of user's action
D. falsification of a user's identity

Correct Answer: B

QUESTION 3
What are two social engineering techniques? (Choose two.)

A. privilege escalation
B. DDoS attack
C. phishing
D. man-in-the-middle
E. pharming

Correct Answer: CE

QUESTION 4
Which security principle requires more than one person is required to perform a critical task?

A. least privilege
B. need to know
C. separation of duties
D. due diligence

Correct Answer: C

QUESTION 5
A security incident occurred with the potential of impacting business services. Who performs the attack?

A. malware author
B. threat actor
C. bug bounty hunter
D. direct competitor

Correct Answer: B

QUESTION 6
While viewing packet capture data, an analyst sees that one IP is sending and receiving traffic for multiple devices by modifying the IP header. Which technology makes this behavior possible?

A. encapsulation
B. TOR
C. tunneling
D. NAT

Correct Answer: D

QUESTION 7
Which type of data consists of connection level, application-specific records generated from network traffic?

A. transaction data
B. location data
C. statistical data
D. alert data

Correct Answer: A

QUESTION 8
A user received a malicious attachment but did not run it. Which category classifies the intrusion?

A. weaponization
B. reconnaissance
C. installation
D. delivery

Correct Answer: D

QUESTION 9
What is an attack surface as compared to a vulnerability?

A. any potential danger to an asset
B. the sum of all paths for data into and out of the environment
C. an exploitable weakness in a system or its design
D. the individuals who perform an attack

Correct Answer: C

QUESTION 10
Which metric should be used when evaluating the effectiveness and scope of a Security Operations Center?

A. The average time the SOC takes to register and assign the incident.
B. The total incident escalations per week.
C. The average time the SOC takes to detect and resolve the incident.
D. The total incident escalations per month.

Correct Answer: C

QUESTION 11
What is a purpose of a vulnerability management framework?

A. identifies, removes, and mitigates system vulnerabilities
B. detects and removes vulnerabilities in source code
C. conducts vulnerability scans on the network
D. manages a list of reported vulnerabilities

Correct Answer: A

QUESTION 12
What is threat hunting?

A. Managing a vulnerability assessment report to mitigate potential threats.
B. Focusing on proactively detecting possible signs of intrusion and compromise.
C. Pursuing competitors and adversaries to infiltrate their system to acquire intelligence data.
D. Attempting to deliberately disrupt servers by altering their availability

Correct Answer: B

QUESTION 13
What is a benefit of agent-based protection when compared to agentless protection?

A. It lowers maintenance costs
B. It provides a centralized platform
C. It collects and detects all traffic locally
D. It manages numerous devices simultaneously

Correct Answer: C

QUESTION 14
Which tool gives the ability to see session data in real time?

A. tcpdstat
B. trafdump
C. tcptrace
D. trafshow

Correct Answer: C

QUESTION 15
The SOC team has confirmed a potential indicator of compromise on an endpoint. The team has narrowed the executable file's type to a new trojan family. According to the NIST Computer

Security Incident Handling Guide, what is the next step in handling this event?

A. Isolate the infected endpoint from the network.
B. Perform forensics analysis on the infected endpoint.
C. Collect public information on the malware behavior.
D. Prioritize incident handling based on the impact.

Correct Answer: C

QUESTION 16
A security expert is working on a copy of the evidence, an ISO file that is saved in CDFS format. Which type of evidence is this file?

A. CD data copy prepared in Windows
B. CD data copy prepared in Mac-based system
C. CD data copy prepared in Linux system
D. CD data copy prepared in Android-based system

Correct Answer: A

QUESTION 17
What is the principle of defense-in-depth?

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

Correct Answer: B

QUESTION 18
An engineer needs to discover alive hosts within the 192.168.1.0/24 range without triggering intrusive portscan alerts on the IDS device using Nmap. Which command will accomplish this goal?

A. nmap --top-ports 192.168.1.0/24
B. nmap -sP 192.168.1.0/24
C. nmap -sL 192.168.1.0/24
D. nmap -sV 192.168.1.0/24

Correct Answer: B

QUESTION 19
An engineer is analyzing a recent breach where confidential documents were altered and stolen by the receptionist Further analysis shows that the threat actor connected an externa USB device to bypass security restrictions and steal data The engineer could not find an external USB device Which piece of information must an engineer use for attribution in an investigation?

A. list of security restrictions and privileges boundaries bypassed
B. external USB device