200-201$^{\text{Q\&As}}$

Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS)

Pass Cisco 200-201 Exam with 100% Guarantee

QUESTION 1

The SOC team detected an ongoing port scan. After investigation, the team concluded that the scan was targeting the company servers. According to the Cyber Kill Chain model, which step must be assigned to this type of event?

A. delivery

B. exploitation

C. reconnaissance

D. actions on objectives

Correct Answer: C

QUESTION 2

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

Host-based antivirus protection is also known as agent-based. Agent-based antivirus runs on every protected machine. Agentless antivirus protection performs scans on hosts from a centralized system. Agentless systems have become popular for virtualized environments in which multiple OS instances are running on a host simultaneously. Agent-based antivirus running in each virtualized system can be a serious drain on system resources. Agentless antivirus for virtual hosts involves the use of a special security virtual appliance that performs optimized scanning tasks on the virtual hosts. An example of this is VMware\\'s vShield.

QUESTION 3

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.

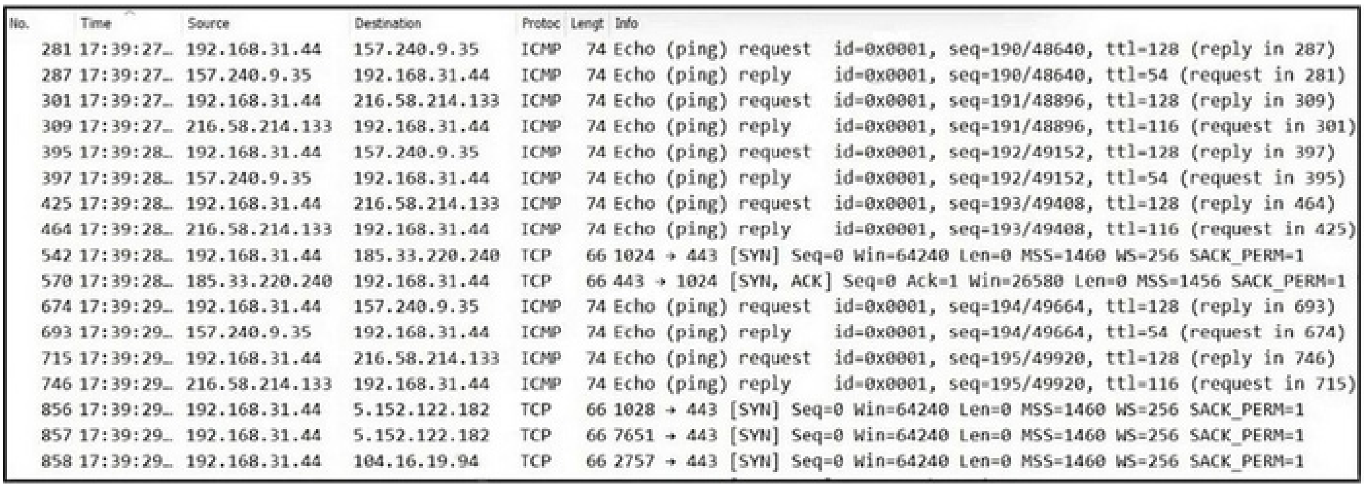
C. Tap mode monitors packets and their content with the highest speed, while the inline mode draws a packet path for analysis.

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

Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/650/configuration/guide/fpmc-config-guide-v65/inline_sets_and_passive_interfaces_for_firepower_threat_defense.html

QUESTION 4



```
No.     Time          Source           Destination      Protoc Lengt Info
    281 17:39:27… 192.168.31.44    157.240.9.35     ICMP    74 Echo (ping) request  id=0x0001, seq=190/48640, ttl=128 (reply in 287)
    287 17:39:27… 157.240.9.35     192.168.31.44    ICMP    74 Echo (ping) reply    id=0x0001, seq=190/48640, ttl=54 (request in 281)
    301 17:39:27… 192.168.31.44    216.58.214.133   ICMP    74 Echo (ping) request  id=0x0001, seq=191/48896, ttl=128 (reply in 309)
    309 17:39:27… 216.58.214.133   192.168.31.44    ICMP    74 Echo (ping) reply    id=0x0001, seq=191/48896, ttl=116 (request in 301)
    395 17:39:28… 192.168.31.44    157.240.9.35     ICMP    74 Echo (ping) request  id=0x0001, seq=192/49152, ttl=128 (reply in 397)
    397 17:39:28… 157.240.9.35     192.168.31.44    ICMP    74 Echo (ping) reply    id=0x0001, seq=192/49152, ttl=54 (request in 395)
    425 17:39:28… 192.168.31.44    216.58.214.133   ICMP    74 Echo (ping) request  id=0x0001, seq=193/49408, ttl=128 (reply in 464)
    464 17:39:28… 216.58.214.133   192.168.31.44    ICMP    74 Echo (ping) reply    id=0x0001, seq=193/49408, ttl=116 (request in 425)
    542 17:39:28… 192.168.31.44    185.33.220.240   TCP     66 1024 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
    570 17:39:28… 185.33.220.240   192.168.31.44    TCP     66 443 → 1024 [SYN, ACK] Seq=0 Ack=1 Win=26580 Len=0 MSS=1456 SACK_PERM=1
    674 17:39:29… 192.168.31.44    157.240.9.35     ICMP    74 Echo (ping) request  id=0x0001, seq=194/49664, ttl=128 (reply in 693)
    693 17:39:29… 157.240.9.35     192.168.31.44    ICMP    74 Echo (ping) reply    id=0x0001, seq=194/49664, ttl=54 (request in 674)
    715 17:39:29… 192.168.31.44    216.58.214.133   ICMP    74 Echo (ping) request  id=0x0001, seq=195/49920, ttl=128 (reply in 746)
    746 17:39:29… 216.58.214.133   192.168.31.44    ICMP    74 Echo (ping) reply    id=0x0001, seq=195/49920, ttl=116 (request in 715)
    856 17:39:29… 192.168.31.44    5.152.122.182    TCP     66 1028 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
    857 17:39:29… 192.168.31.44    5.152.122.182    TCP     66 7651 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
    858 17:39:29… 192.168.31.44    104.16.19.94     TCP     66 2757 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
```

Refer to the exhibit. What is occurring in this network traffic?

A. legitimate network traffic

B. flood of SYN-ACK packets

C. ICMP flood

D. flood of SYN packets

Correct Answer: C

QUESTION 5

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

An attack surface is the total sum of vulnerabilities that can be exploited to carry out a security attack. Attack surfaces can be physical or digital. The term attack surface is often confused with the term attack vector, but they are not the same thing. The surface is what is being attacked; the vector is the means by which an intruder gains access.