Cisco

500-280 Exam

Securing Cisco Networks with Open Source Snort

Question: 1

Which protocol operates below the network layer?

A. UDP
B. ICMP
C. ARP
D. DNS

Answer: C

Question: 2

Which area is created between screening devices in an egress/ingress path for housing web, mail, or DNS servers?

A. EMZ
B. DMZ
C. harbor
D. inlet

Answer: B

Question: 3

What does protocol normalization do?

A. compares evaluated packets to normal, daily network-traffic patterns
B. removes any protocol-induced or protocol-allowable ambiguities
C. compares a packet to related traffic from the same session, to determine whether the packet is out of sequence
D. removes application layer data, whether or not it carries protocol-induced anomalies, so that packet headers can be inspected more accurately for signs of abuse

Answer: B

Question: 4

On which protocol does Snort focus to decode, process, and alert on suspicious network traffic?

A. Apple talk
B. TCP/IP
C. IPX/SPX
D. ICMP

Answer: B

Question: 5

Which technique can an intruder use to try to evade detection by a Snort sensor?

A. exceed the maximum number of fragments that a sensor can evaluate
B. split the malicious payload over several fragments to mask the attack signature
C. disable a sensor by exceeding the number of packets that it can fragment before forwarding
D. send more packet fragments than the destination host can reassemble, to disable the host without regard to any intrusion-detection devices that might be on the network

Answer: B

Question: 6

An IPS addresses evasion by implementing countermeasures. What is one such countermeasure?

A. periodically reset statistical buckets to zero for memory utilization, maximization, and performance
B. send packets to the origination host of a given communication session, to confirm or eliminate spoofing
C. perform pattern and signature analysis against the entire packet, rather than against individual fragments
D. automate scans of suspicious source IP addresses

Answer: C