

# Cisco

## Exam 500-280

### Securing Cisco Networks with Open Source Snort

Version: 6.0

[ Total Questions: 60 ]

**Question No : 1**

Which protocol operates below the network layer?

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

**Answer: C**

**Question No : 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 No : 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 No : 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 No : 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 No : 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**

**Question No : 7**

Which IPS placement option is the noisiest?

- A. inside the firewall
- B. outside the firewall
- C. inside the DMZ
- D. inside general user segments

**Answer: B**

**Question No : 8**

What is the purpose of using a span or monitor port on a switch?

- A. to aggregate traffic from multiple switch ports
- B. to tap data off network media
- C. to overcome problems that switches have in accurately reproducing desired traffic
- D. to limit the amount of traffic that passes through the switch

**Answer: A**

**Question No : 9**

Which item examines packets for malformation, anomalies, and protocol compliance and gathers and presents packets in one consistent fashion?

- A. Sniffer
- B. preprocessors
- C. detection engine
- D. output and alerting module

**Answer: B**

**Question No : 10**

Which component is one of the four primary components of Snort?