# Cisco

## Exam 500-280

### Securing Cisco Networks with Open Source Snort

**Verson: Demo**

**[ Total Questions:  10 ]**

**Question No : 1**

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

**A.** ACL
**B.** postprocessor
**C.** iptables
**D.** output and alerting

**Answer: D**

**Question No : 2**

Which engine or module presents alert and log data in the format that you specify?

**A.** tap
**B.** sniffing
**C.** detection
**D.** output

**Answer: D**

**Question No : 3**

Which statement about the detection engine configuration settings in snort.conf is true?

**A.** All the decoder alerts are on by default.
**B.** All the decoder settings are off by default.
**C.** Some decoder settings are on and others must be uncommented.
**D.** The decoder is no longer in use.

**Answer: B**

**Question No : 4**

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 : 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**

Which output method is the fastest for Snort?

**A.** unified2
**B.** database
**C.** binary (tcpdump)
**D.** CSV

**Answer: A**

**Question No : 7**

Which action is valid for decoder/preprocessor stub rules?

**A.** file I/O
**B.** recurse
**C.** inspect
**D.** reject

**Answer: D**

**Question No : 8**

Which output is in a lightweight, binary form?

**A.** unified2
**B.** PCAP
**C.** SNMP
**D.** CSV

**Answer: A**

**Question No : 9**

What is a GID?

**A.** general intrusion domain
**B.** Generator ID
**C.** Gigabit interface definition
**D.** gradual interrupt detection

**Answer: B**

**Question No : 10**

Barnyard has a mode of operation that reads the most current unified log file and processes new unified files as they become available. What is this mode called?

**A.** one-shot
**B.** continual
**C.** continual with checkpoint

**D.** unified

**Answer: B**