

Cisco

Exam 600-199

Securing Cisco Networks with Threat Detection and Analysis

Version: Demo

[Total Questions: 10]

Question No : 1

Which source should be used to recommend preventative measures against security vulnerabilities regardless of operating system or platform?

- A. Microsoft security bulletins
- B. Cisco PSIRT notices
- C. Common Vulnerabilities and Exposure website
- D. Mozilla Foundation security advisories
- E. zero-day attack wiki

Answer: C

Question No : 2

Which two tools are used to help with traffic identification? (Choose two.)

- A. network sniffer
- B. ping
- C. traceroute
- D. route table
- E. NetFlow
- F. DHCP

Answer: A,E

Question No : 3

In what sequence do the proper eradicate/recovery steps take place?

- 1) Re-image
- 2) Restore
- 3) Patch
- 4) Backup

- A. 1, 2, 3, 4
- B. 4, 3, 2, 1
- C. 1, 3, 4, 2
- D. 4, 1, 3, 2

Answer: D

Question No : 4

When is it recommended to establish a traffic profile baseline for your network?

- A. outside of normal production hours
- B. during a DDoS attack
- C. during normal production hours
- D. during monthly file server backup

Answer: C

Question No : 5

Which event is likely to be a false positive?

- A. Internet Relay Chat signature with an alert context buffer containing #IPS_ROCS Yay
- B. a signature addressing an ActiveX vulnerability alert on a Microsoft developer network documentation page
- C. an alert for a long HTTP request with an alert context buffer containing a large HTTP GET request
- D. BitTorrent activity detected on ephemeral ports

Answer: B

Question No : 6

In the context of a network security device like an IPS, which event would qualify as having the highest severity?

- A. remote code execution attempt

- B. brute force login attempt
- C. denial of service attack
- D. instant messenger activity

Answer: A

Question No : 7

Refer to the exhibit.

```
15:59:06.480292 IP 10.10.10.10.http > 192.168.10.2.58320: Flags [.], seq 82080, ack 1, win 16416, options [nop,nop,TS val 1991638787 ecr 459929244], length 1368
15:59:06.480375 IP 10.10.10.10.http > 192.168.10.2.58320: Flags [.], seq XXXXX, ack 1, win 16416, options [nop,nop,TS val 1991638787 ecr 459929244], length 1368
```

In the tcpdump output, what is the sequence number that is represented by XXXXX?

- A. 82080
- B. 82081
- C. 83448
- D. 83449
- E. 98496
- F. 98497

Answer: C

Question No : 8

Which three symptoms are best used to detect a TCP SYN flood attack? (Choose three.)

- A. high memory utilization on target server
- B. large number of sockets in SYN_RECV state on target server
- C. network monitoring devices report large number of unACKed SYNs sent to target server
- D. target server crashes repeatedly
- E. user experience with target server is slow or unresponsive

Answer: B,C,E

Question No : 9

Refer to the exhibit.

```

16:44:56.916908 00:1b:78:42:00:58 > 00:19:bb:2f:0a:73, ethertype IPv4 (0x0800),
length 74, tos 0x0, ttl 64, offset 0, flags [DF], proto TCP (6), length
60) 192.168.10.111:57274 > 192.168.10.113:443, cksum 0x0c75 (correct),
734417495:734417495(0) 5840 <mss 1460,sackOK,timestamp 502169031 0,nop,wscale 6>

```

In the packet captured from tcpdump, which fields match up with the lettered parameters?

- A.** A.Source and destination IP addresses,B.Source and destination Ethernet addresses,C.Source and destination TCP port numbers,D.TCP acknowledgement number,E.IP options
- B.** A.Source and destination Ethernet addresses,B.Source and destination IP addresses,C.Source and destination TCP port numbers,D.TCP sequence number,E.TCP options
- C.** A.Source and destination Ethernet addresses,B.Source and destination IP addresses,C.Source and destination TCP port numbers,D.TCP acknowledgement number,E.IP options
- D.** A.Source and destination Ethernet addresses,B.Source and destination IP addresses,C.Source and destination TCP port numbers,D.TCP sequence number,E.IP options

Answer: B

Question No : 10

What is the maximum size of an IP datagram?

- A.** There is no maximum size.
- B.** It is limited only by the memory on the host computers at either end of the connection and the intermediate routers.
- C.** 1024 bytes
- D.** 65535 bytes
- E.** 32768 bytes

Answer: D

