
**Vendor:**Cisco

**Exam Code:**600-199

**Exam Name:**Securing Cisco Networks with Threat Detection and Analysis

**Version:**Demo

**QUESTION 1**

If a company has a strict policy to limit potential confidential information leakage, which three alerts would be of concern? (Choose three.)

A. P2P activity detected

B. Skype activity detected

C. YouTube viewing activity detected

D. Pastebin activity detected

E. Hulu activity detected

Correct Answer: ABD

---

**QUESTION 2**

Which data from previous network attacks should be used to recommend architectural changes based on potential future impact?

A. SNMP statistics

B. known vulnerabilities

C. security audit reports

D. IPS signature logs

E. STP topology changes

Correct Answer: A

---

**QUESTION 3**

Which attack exploits incorrect boundary checking in network software?

A. Slowloris

B. buffer overflow

C. man-in-the-middle

D. Smurf

Correct Answer: B

---

**QUESTION 4**

A server administrator tells you that the server network is potentially under attack. Which piece of information is critical to begin your network investigation?

A. cabinet location of the servers

B. administrator password for the servers

C. OS that is used on the servers

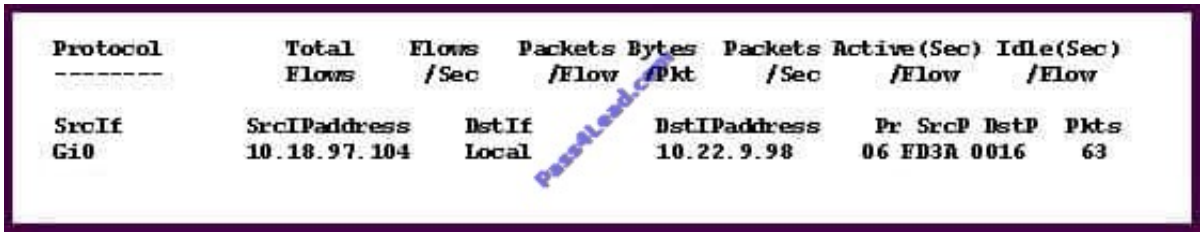
D. IP addresses/subnets used for the servers

Correct Answer: D

---

**QUESTION 5**

Refer to the exhibit.



```
Protocol        Total    Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------        Flows     /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Gi0           10.18.97.104    Local         10.22.9.98      06 FD3A 0016   63
```

Which protocol is used in this network traffic flow?

A. SNMP

B. SSH

C. DNS

D. Telnet

Correct Answer: B

---

**QUESTION 6**

What does the acronym "CSIRT" stand for?

A. Computer Security Identification Response Team

B. Cisco Security Incident Response Team

C. Cisco Security Identification Response Team

D. Computer Security Incident Response Team

Correct Answer: D

---

**QUESTION 7**

Which two statements about the IPv4 TTL field are true? (Choose two.)

A. If the TTL is 0, the datagram is automatically retransmitted.

B. Each router that forwards an IP datagram reduces the TTL value by one.

C. It is used to limit the lifetime of an IP datagram on the Internet.

D. It is used to track IP datagrams on the Internet.

Correct Answer: BC

---

**QUESTION 8**

Which three tools should be used for incident response? (Choose three.)

A. screwdriver

B. sniffer

C. antivirus/anti-malware software

D. video player

E. CPU

F. RAM

Correct Answer: ABC

---

**QUESTION 9**

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

Correct Answer: B

---

**QUESTION 10**

If an alert that pertains to a remote code execution attempt is seen on your network, which step is unlikely to help?

A. looking for anomalous traffic

B. looking for reconnaissance activity

C. restoring the machine to a known good backup

D. clearing the event store to see if future events indicate malicious activity

Correct Answer: D

---

**QUESTION 11**

Refer to the exhibit.

```
17:39:48.549310 40:6c:8f:10:11:12 > ff:ff:ff:ff:ff:ff, ARP, length 42: Ethernet (len 6), IPv4 (len 4),
Request who-has 10.10.10.20 (ff:ff:ff:ff:ff:ff) tell 10.10.10.10, length 28
17:39:48.549571 3c:97:0e:20:21:22 > 40:6c:8f:10:11:12, ARP, length 60: Ethernet (len 6), IPv4 (len 4), Reply
10.10.10.20 is-at 3c:97:0e:20:21:22, length 46
```

Based on the tcpdump capture, which three statements are true? (Choose three.)

A. Host 10.10.10.20 is requesting the MAC address of host 10.10.10.10 using ARP.

B. Host 10.10.10.10 is requesting the MAC address of host 10.10.10.20.

C. The ARP request is unicast.

D. The ARP response is unicast.

E. The ARP request is broadcast.

F. Host 10.10.10.20 is using the MAC address of ffff.ffff.ffff.

Correct Answer: BDE

---

**QUESTION 12**

What is the purpose of the TCP SYN flag?

A. to sequence each byte of data in a TCP connection

B. to synchronize the initial sequence number contained in the Sequence Number header field with the other end of the connection

C. to acknowledge outstanding data relative to the byte count contained in the Sequence Number header field

D. to sequence each byte of data in a TCP connection relative to the byte count contained in the Sequence Number header field

Correct Answer: B