600-199Q&As

Securing Cisco Networks with Threat Detection and Analysis

Pass Cisco 600-199 Exam with 100% Guarantee

QUESTION 1

Which will be provided as output when issuing the show processes cpu command on a Cisco IOS router?

A. router configuration

B. CPU utilization of device

C. memory used by device processes

D. interface processing statistics

Correct Answer: B

QUESTION 2

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

Correct Answer: A

QUESTION 3

When an IDS generates an alert for a correctly detected network attack, what is this event called?

A. false positive

B. true negative

C. true positive

D. false negative

Correct Answer: C

QUESTION 4

What are four steps to manage incident response handling? (Choose four.)

A. preparation

B. qualify

C. identification

D. who

E. containment

F. recovery

G. eradication

H. lessons learned

Correct Answer: ACEH

QUESTION 5

Which two activities would you typically be expected to perform as a Network Security Analyst? (Choose two.)

A. Verify user login credentials.

B. Troubleshoot firewall performance.

C. Monitor database applications.

D. Create security policies on routers.

Correct Answer: BD

QUESTION 6

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 7

Which two measures would you recommend to reduce the likelihood of a successfully executed network attack from the Internet? (Choose two.)

A. Completely disconnect the network from the Internet.

B. Deploy a stateful edge firewall.

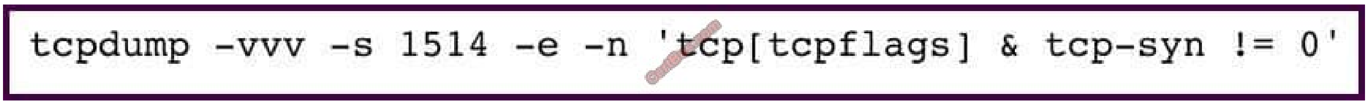
C. Buy an insurance policy against attack-related business losses.

D. Implement a password management policy for remote users.

Correct Answer: BD

QUESTION 8

Refer to the exhibit.



```
tcpdump -vvv -s 1514 -e -n 'tcp[tcpflags] & tcp-syn != 0'
```

What does the tcpdump command do?

A. Capture all packets sourced from TCP port 1514, resolve DNS names, print all TCP packets with the SYN flag not equaling 0, and print the Ethernet header and all version information.

B. Capture all packets sourced from TCP port 1514, resolve DNS names, print all TCP packets except those containing the SYN flag, and print the Ethernet header and all version information.

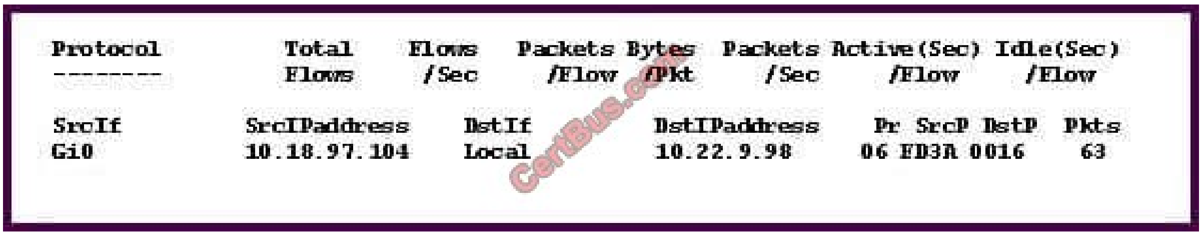
C. Capture up to 1514 bytes, do not resolve DNS names, print all TCP packets except for those containing the SYN flag, and print the Ethernet header and be very verbose.

D. Capture up to 1514 bytes, do not resolve DNS names, print only TCP packets containing the SYN flag, and print the Ethernet header and be very verbose.

Correct Answer: D

QUESTION 9

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 10

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 11

The IHL is a 4-bit field containing what measurement?

A. the number of 32-bit words in the IP header

B. the size of the IP header, in bytes

C. the size of the entire IP datagram, in bytes

D. the number of bytes in the IP header

E. the number of 32-bit words in the entire IP datagram

Correct Answer: A

QUESTION 12

Which event is actionable?

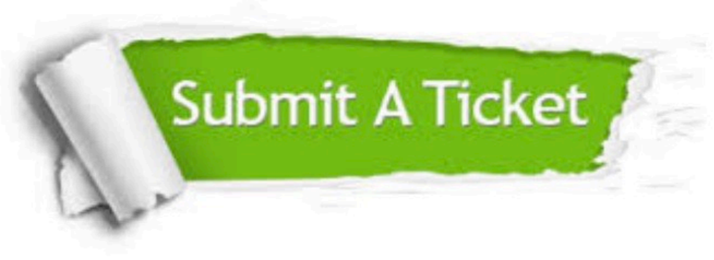
A. SSH login failed

B. Telnet login failed

C. traffic flow started

D. reverse shell detected

Correct Answer: D


Submit A Ticket

100%