600-199 Q&As

Securing Cisco Networks with Threat Detection and Analysis

Pass Cisco 600-199 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.passapply.com/600-199.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Cisco Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

Which is considered to be anomalous activity?

A. an alert context buffer containing traffic to amazon.com

B. an alert context buffer containing SSH traffic

C. an alert context buffer containing an FTP server SYN scanning your network

D. an alert describing an anonymous login attempt to an FTP server

Correct Answer: C

QUESTION 2

Which four tools are used during an incident to collect data? (Choose four.)

A. Sniffer

B. TCPDump

C. FTK

D. EnCase

E. ABC

F. ASA

G. Microsoft Windows 7

Correct Answer: ABCD

QUESTION 3

Refer to the exhibit.

Which protocol is used in this network traffic flow?

A. SNMP

B. SSH

C. DNS

D. Telnet

Correct Answer: B

QUESTION 4

When investigating potential network security issues, which two pieces of useful information would be found in a syslog message? (Choose two.)

A. product serial number

B. MAC address

C. IP address

D. product model number

E. broadcast address

Correct Answer: BC

QUESTION 5

Refer to the exhibit.

Based on the tcpdump output, which two statements are true? (Choose two.)

A. The reply is sent via unicast.

B. All devices in the same subnet on a switched network will see the reply because it was broadcast.

C. The device is coming up for the first time and is requesting an IP address.

D. The ARP request is being sent as a broadcast.

E. The device is requesting an ARP.

F. Host 192.168.10.7 is requesting the operational status of host 192.168.10.8.

Correct Answer: AD

QUESTION 6

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

Correct Answer: D

QUESTION 7

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

QUESTION 8

Refer to the exhibit.

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

Correct Answer: B

QUESTION 9

Given a Linux machine running only an SSH server, which chain of alarms would be most concerning?

A. brute force login attempt from outside of the network, followed by an internal network scan

B. root login attempt followed by brute force login attempt

C. Microsoft RPC attack against the server

D. multiple rapid login attempts

Correct Answer: A

QUESTION 10

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 11

Which step should be taken first when a server on a network is compromised?

A. Refer to the company security policy.

B. Email all server administrators.

C. Determine which server has been compromised.

D. Find the serial number of the server.

Correct Answer: A

QUESTION 12

After an attack has occurred, which two options should be collected to help remediate the problem? (Choose two.)

A. packet captures

B. NAT translation table

C. syslogs from affected devices

D. connection table information

E. NetFlow data

Correct Answer: CE