600-199$^{\text{Q\&As}}$

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.pass4itsure.com/600-199.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

Which event is actionable?

A. SSH login failed

B. Telnet login failed

C. traffic flow started

D. reverse shell detected

Correct Answer: D

QUESTION 2

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 3

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 4

Which would be classified as a remote code execution attempt?

A. OLE stack overflow detected

B. null login attempt

C. BitTorrent activity detected

D. IE ActiveX DoS

Correct Answer: A

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

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 7

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 8

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 9

As a part of incident response, which action should be performed?

A. watch to see if the incident reoccurs

B. custody of information

C. maintain data security and custody for future forensics use

D. classify the problem

Correct Answer: C

QUESTION 10

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 11

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 12

In what sequence do the proper eradicate/recovery steps take place? 1) Re-image2) Restore3) Patch4) Backup

A. 1, 2, 3, 4

B. 4, 3, 2, 1

C. 1, 3, 4, 2

D. 4, 1, 3, 2

Correct Answer: D