210-250$^{Q\&As}$

Cisco Cybersecurity Fundamentals

Pass Cisco 210-250 Exam with 100% Guarantee

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

QUESTION 1

What is an amplification attack?

A. An amplification attack is a form of directed DDoS attack in which the attacker\\'s packets are sent at a much faster rate than the victim\\'s packets.

B. An amplification attack is a form of reflected attack in which the response traffic (sent by the unwitting participant) is made up of packets that are much larger than those that were initially sent by the attacker (spoofing the victim).

C. An amplification attack is a type of man-in-the-middle attack.

D. An amplification attack is a type of data exfiltration attack.

Correct Answer: B

QUESTION 2

Which of the following functions are typically provided by an SIEM? (Select all that apply.)

A. Log correlation

B. Log archiving

C. Log normalization

D. Log correction

Correct Answer: ABC

QUESTION 3

Which of the following shows giving permissions to the group owners for read and execute, giving file owner permission for read, write, and execute, and giving all others permissions for execute?

A. -rwx-rx-x

B. -rx-rwx-x

C. -rx-x-rwx

D. -rwx-rwx-x

Correct Answer: A

QUESTION 4

What does a digital certificate certify about an entity?

A. A digital certificate certifies the ownership of the public key of the named subject of the certificate.

B. A digital certificate certifies the ownership of the private key of the named subject of the certificate.

C. A digital certificate certifies the ownership of the symmetric key of the named subject of the certificate.

D. A digital certificate certifies the ownership of the bulk encryption key of the named subject of the certificate.

Correct Answer: A

QUESTION 5

The ECDHE_ECDSA part of the cipher list identifies which one of the following algorithms?

A. authentication and key exchange

B. encryption

C. message authentication code

D. pseudorandom function

Correct Answer: A

QUESTION 6

What are three key components of a threat-centric SOC? (Choose three.)

A. people

B. compliances

C. processes

D. regulations

E. technologies

Correct Answer: ACE

QUESTION 7

Which three of the following statements best describe the limitations of network taps? (Choose three.)

A. Separate Rx and Tx make it difficult to determine which side of the connection sent the traffic.

B. Taps that are inserted at the physical layer can impact the performance on the inserted link.

C. Taps are unable to filter traffic.

D. Separating Rx and Tx requires multiple NICs to capture both sides of the connection.

E. Taps are expensive.

Correct Answer: CDE

QUESTION 8

Which type of attack occurs when an attacker utilizes a botnet to reflect requests off an NTP server to overwhelm their target?

A. main in the middle

B. denial of service

C. distributed denial of service

D. replay

Correct Answer: C

QUESTION 9

What is a backdoor?

A. A backdoor is a social engineering attack to get access back to the victim.

B. A backdoor is a privilege escalation attack designed to get access from the victim.

C. A backdoor is an application or code used by an attacker either to allow future access or to collect information to use in further attacks.

D. A backdoor is malware installed using man-in-the-middle attacks.

Correct Answer: C

QUESTION 10

What is the maximum number of hosts that a Class B network can have?

A. 254

B. 32,766

C. 65,534

D. 16,777,214

Correct Answer: C

QUESTION 11

Given the scenario where the Downloads directory is in the home directory, which three of the following commands will navigate you to the Downloads directory? (Choose three.)

A. cd /home//Downloads

B. cd /etc/home/bob/Downloads

C. cd Downloads

D. cd ~/Downloads

Correct Answer: ACD

QUESTION 12

What is the primary goal of an attacker when using an iFrame or HTTP 302 cushioning?

A. help the user find the correct web page location

B. ensure that the victim\\'s web browser ends up on the attacker\\'s web page, which serves out the malicious exploit to the victim

C. offer a secure transaction in a web page

D. protect against malware infiltration

Correct Answer: B

QUESTION 13

How can a user test the logging process on a Linux device?

A. ping the logging server

B. perform a show run command and verify the entry

C. use the logger command

D. traceroute to the syslog server

Correct Answer: C

QUESTION 14

Cisco AVC uses which of the following technologies to provide deep packet inspection (DPI) technology to identify a wide variety of applications within the network traffic flow, using Layer 3 to Layer 7 data?

A. Cisco NetFlow

B. IPFIX

C. Cisco AMP

D. Cisco Network-Based Application Recognition Version 2 (NBAR2)

Correct Answer: D

QUESTION 15

Which two of the following are UDP applications? (Choose two.)

A. SMTP

B. TFTP

C. FTP

D. SNMP

Correct Answer: BD