



210-250^{Q&As}

Cisco Cybersecurity Fundamentals

Pass Cisco 210-250 Exam with 100% Guarantee

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

<https://www.passapply.com/210-250.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 statement is true about sandboxing?

- A. Using a sandbox technique ensures that no malware infected files can get in the network.
- B. Running a file in a sandbox guarantees that the disposition will show the threat that it poses to your environment.
- C. Malware authors deploy several techniques to bypass sandbox analysis.
- D. Using a sandbox replaces the need for expensive antivirus and firewall software.

Correct Answer: C

QUESTION 2

After attackers gain access to a system, what method can they use to expand their access to other systems without exploiting vulnerabilities on other systems in the network?

- A. change the network gateway address to the attacker's command and control server
- B. establish a Metasploit session to 127.0.0.1 and pass the user's account hash to it
- C. take advantage of domain trust to make connections to a partner network
- D. block employees from visiting social media web sites on the company network

Correct Answer: C

QUESTION 3

Which three of the following statements are true regarding the router? (Choose three.)

- A. Longer prefixes are always preferred over shorter ones when forwarding a packet.
- B. Routers use administrative distance to determine the trustworthiness of the routes
- C. Routers use routing tables to route between networks.
- D. Routers populate the routing table by dynamically learning the source IP address of incoming packets
- E. Routers are considered Layer 2 devices.

Correct Answer: ABC

QUESTION 4

Which two of the following statements are true about Windows virtual memory? (Choose two.)



- A. Virtual memory combines the RAM memory with the hard disk space to compensate for lack of RAM.
- B. Adding a larger disk drive to a system automatically increases its virtual memory allocation.
- C. A virtual address does not represent the actual physical location of an object in memory. Instead, the system maintains a page table for each process, which is an internal data structure that is used to translate virtual addresses into their corresponding physical addresses.
- D. Adding more RAM to a system automatically increases the need for more virtual memory on the system.

Correct Answer: AC

QUESTION 5

Which field in the IP header represents the sender's logical address?

- A. destination MAC address field
- B. source IP address field
- C. destination IP address field
- D. source MAC address field

Correct Answer: B

QUESTION 6

Which of the following statements is true about clientless SSL VPN?

- A. The client must use a digital certificate to authenticate.
- B. The remote client needs only an SSL-enabled web browser to access resources on the private network of the security appliances.
- C. Clientless SSL VPNs do not provide the same level of encryption as client based SSL VPNs.
- D. Clientless SSL VPN sessions expire every hour.

Correct Answer: B

QUESTION 7

Which option is a purpose of port scanning?

- A. Identify the Internet Protocol of the target system.
- B. Determine if the network is up or down.
- C. Identify which ports and services are open on the target host.



D. Identify legitimate users of a system.

Correct Answer: C

QUESTION 8

What is one way of mitigating DHCP attacks by using a Cisco switch?

- A. VLAN segmentation
- B. MAC address security
- C. DHCP snooping
- D. DHCP authentication

Correct Answer: C

QUESTION 9

Regarding the Cisco CTA dashboard, what is the primary purpose of the "relative threat exposure"?

- A. Using a single pane, it quickly identifies, which device on the network is compromised.
- B. It provides an instant view into existing CnC channels within the network infrastructure.
- C. It answers the question, "Who has infiltrated the network?"
- D. It answers the question, "How is my organization doing as it relates to others?"
- E. It identifies which known CVE vulnerabilities are present within the configured network devices, included routers, switches, and NGFWs.

Correct Answer: D

QUESTION 10

What is the key to the success of an MITM attack?

- A. The hacked machine becomes overwhelmed with responses.
- B. TCP/IP bugs make it easy to crash older operating systems.
- C. The attacker waits until after a communication session is established.
- D. Packet flooding consumes resources.

Correct Answer: C



QUESTION 11

A host on an isolated port can communicate with which of the following?

- A. A host on another isolated port
- B. A host on a community port
- C. A server on a community port
- D. With the promiscuous port only

Correct Answer: D

QUESTION 12

What entity requests access to a resource?

- A. Object
- B. Subject
- C. File
- D. Database

Correct Answer: B

QUESTION 13

A change that is low risk and might not need to follow the full change management process is classified as which of the following?

- A. Standard
- B. Emergency
- C. Normal
- D. Controlled

Correct Answer: A

QUESTION 14

Where are configuration records stored?

- A. In a CMDB
- B. In a MySQL DB



C. In a XLS file

D. There is no need to store them

Correct Answer: A

QUESTION 15

Which of the following is a true statement?

A. A remote access VPN must include a host installed on the client.

B. A clientless VPN can connect multiple concentrators together.

C. A remote access VPN may include a host installed on the client.

D. A clientless VPN installs software on the host to establish the VPN connection.

Correct Answer: C

[210-250 Practice Test](#)

[210-250 Study Guide](#)

[210-250 Exam Questions](#)