Cisco

Exam Questions 210-250

SECFND Understanding Cisco Cybersecurity Fundamentals

Guaranteed success with Our exam guides
visit - https://www.certshared.com
NEW QUESTION 1
Which term describes the act of a user, without authority or permission, obtaining rights on a system, beyond what were assigned?

A. authentication tunneling
B. administrative abuse
C. rights exploitation
D. privilege escalation

Answer: D

NEW QUESTION 2
Which protocol maps IP network addresses to MAC hardware addresses so that IP packets can be sent across networks?

A. Internet Control Message Protocol
B. Address Resolution Protocol
C. Session Initiation Protocol
D. Transmission Control Protocol/Internet Protocol

Answer: B

NEW QUESTION 3
Which hashing algorithm is the least secure?

A. MD5
B. RC4
C. SHA-3
D. SHA-2

Answer: A

NEW QUESTION 4
Company XX must filter/control some application and limited connection based on location across the network, which technology can be used?

A. HIDS.
B. NGFW.
C. Web proxy.
D. Load balancers.

Answer: B

NEW QUESTION 5
If a router has four interfaces and each interface is connected to four switches, how many broadcast domains are present on the router?

A. 1
B. 2
C. 4
D. 8

Answer: C

NEW QUESTION 6
Which event occurs when a signature-based IDS encounters network traffic that triggers an alert?

A. connection event
B. endpoint event
C. NetFlow event
D. intrusion event

Answer: D

NEW QUESTION 7
How many broadcast domains are created if three hosts are connected to a Layer 2 switch in full-duplex mode?

A. 4
B. 3
C. None
D. 1

Answer: D

NEW QUESTION 8
How does NTP help with monitoring?
A. Using TCP allows you to view HTTP connections between servers and clients.
B. By synchronizing the time of day allows correlation of events from different system logs.
C. To receive system generated emails
D. To look up IP addresses in the system using the FQDN.

Answer: B

NEW QUESTION 9
Which option is true when using the traffic mirror feature in a switch?

A. Full packet captures are possible
B. Packets are automatically decrypted
C. Ethernet header are modified before capture
D. Packet payloads are lost

Answer: A

NEW QUESTION 10
What is one of the advantages of the mandatory access control (MAC) model?

A. Easy and scalable.
B. Stricter control over the information access.
C. The owner can decide whom to grant access to.

Answer: B

NEW QUESTION 11
In NetFlow records, which flags indicate that an HTTP connection was stopped by a security appliance, like a firewall, before it could be built fully?

A. ACK
B. SYN ACK
C. RST
D. PSH, ACK

Answer: D

NEW QUESTION 12
Which term describes reasonable effort that must be made to obtain relevant information to facilitate appropriate courses of action?

A. Due diligence
B. ethical behavior
C. decision making
D. data mining.

Answer: A

NEW QUESTION 13
One of the objectives of information security is to protect the CIA of information and systems. What does CIA mean in this context?

A. Confidentiality, Integrity, and Availability
B. Confidentiality, Identity, and Availability
C. Confidentiality, Integrity, and Authorization
D. Confidentiality, Identity, and Authorization

Answer: A

NEW QUESTION 14
Which statement about digitally signing a document is true?

A. The document is hashed and then the document is encrypted with the private key.
B. The document is hashed and then the hash is encrypted with the private key.
C. The document is encrypted and then the document is hashed with the public key
D. The document is hashed and then the document is encrypted with the public key.

Answer: B

NEW QUESTION 15
According to RFC 1035 which transport protocol is recommended for use with DNS queries?

A. Transmission Control Protocol
B. Reliable Data Protocol
C. Hypertext Transfer Protocol
D. User Datagram Protocol

Answer: D
NEW QUESTION 16
Which tool provides universal query access to text-based data such as event logs and file system?

A. Service viewer
B. Log parser
C. Windows management instrumentation
D. Handles

Answer: B

NEW QUESTION 17
Which cryptographic key is contained in an X.509 certificate?

A. symmetric
B. public
C. private
D. asymmetric

Answer: B

NEW QUESTION 18
What are two Features of NGFW:

A. Data Mining.
B. Host Based AV
C. Application visibility and control
D. SIEM
E. IDS

Answer: CE

NEW QUESTION 19
Which of the following access control models use security labels to make access decisions?

A. Role-based access control (RBAC)
B. Mandatory access control (MAC)
C. Identity-based access control (IBAC)

Answer: B

NEW QUESTION 20
Which encryption algorithm is the strongest?

A. AES
B. CES
C. DES
D. 3DES

Answer: A

NEW QUESTION 21
......
Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

210-250 Practice Exam Features:

* 210-250 Questions and Answers Updated Frequently
* 210-250 Practice Questions Verified by Expert Senior Certified Staff
* 210-250 Most Realistic Questions that Guarantee you a Pass on Your First Try
* 210-250 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

100% Actual & Verified — Instant Download, Please Click Order The 210-250 Practice Test Here