Cisco

Exam Questions 210-250

Understanding Cisco Cybersecurity Fundamentals

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 purpose of command and control for network aware malware is true?

A. It helps the malware to profile the host
B. It takes over the user account
C. It contacts a remote server for command and updates
D. It controls and down services on the infected host

Answer: C

NEW QUESTION 3
Which security monitoring data type is associated with application server logs?

A. alert data
B. statistical data
C. session data
D. transaction data

Answer: D

NEW QUESTION 4
Based on which statement does the discretionary access control security model grant or restrict access?

A. discretion of the system administrator
B. security policy defined by the owner of an object
C. security policy defined by the system administrator
D. role of a user within an organization

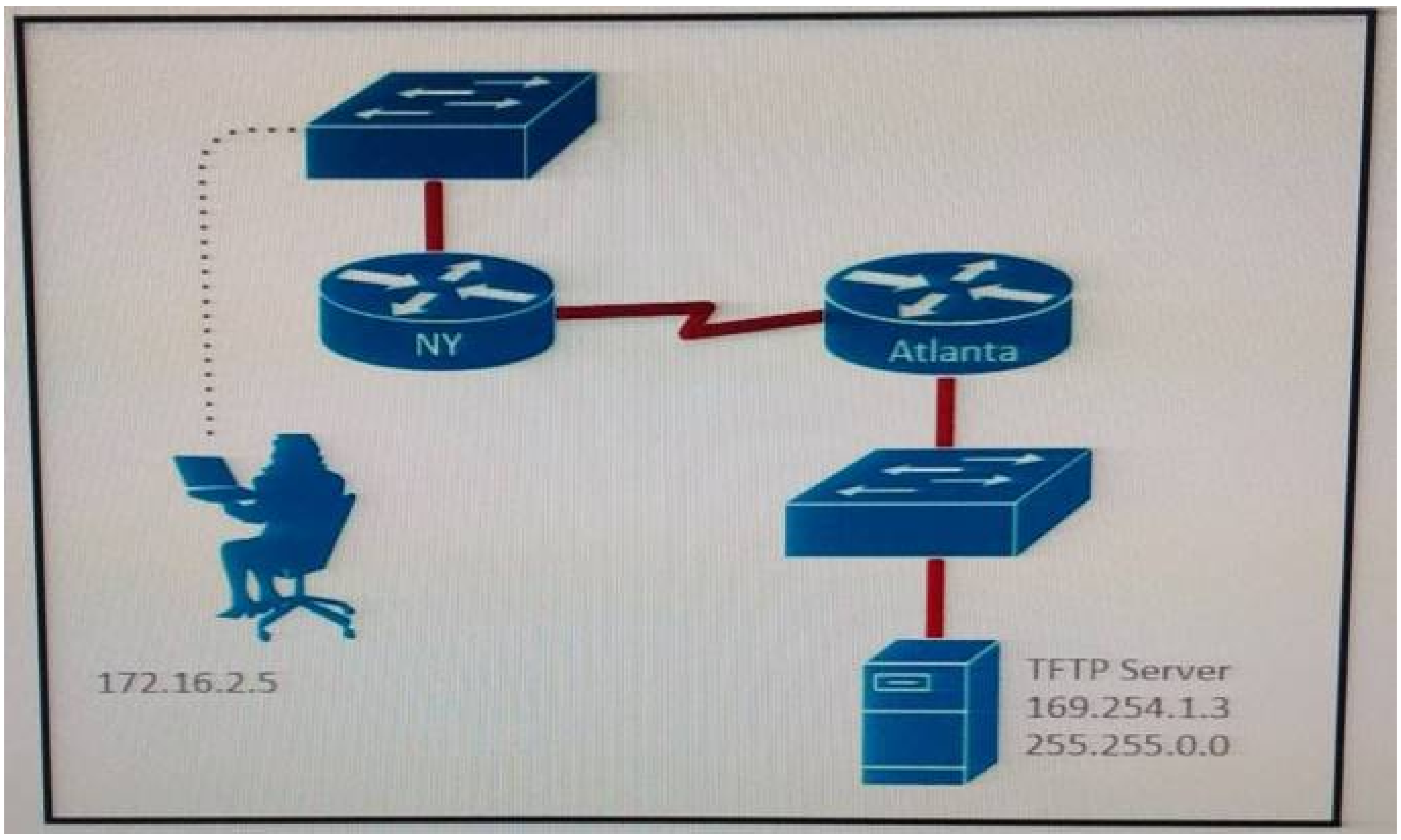
Answer: B

NEW QUESTION 5
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 6
Refer to the exhibit.



A TFTP server has recently been installed in the Atlanta office. The network administrator is located in the NY office and has attempted to make a connection to the TFTP server. They are unable to back up the
configuration file and Cisco IOS of the NY router to the TFTP server Which cause of this problem is true?

A. The TFTP server cannot obtain an address from a DHCP Server.
B. The TFTP server has an incorrect IP address.
C. The network administrator computer has an incorrect IP address
D. The TFTP server has an incorrect subnet mask.

Answer: A

NEW QUESTION 7
Which hashing algorithm is the least secure?

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

Answer: A

NEW QUESTION 8
Which of the following are Cisco cloud security solutions?

A. CloudDLP
B. OpenDNS
C. CloudLock
D. CloudSLS

Answer: BC

NEW QUESTION 9
Which evasion method servers as an important functionality of ransomware?

A. Encoding
B. Encryption
C. Resource exhaustion
D. Extended sleep calls

Answer: B

NEW QUESTION 10
Which NTP command configures the local device as an NTP reference clock source?

A. ntp peer
B. ntp broadcast
C. ntp master
D. ntp server

Answer: C

NEW QUESTION 10
Endpoint logs indicate that a machine has obtained an unusual gateway address and unusual DNS servers via DHCP. Which option is this situation most likely an

example of?

A. Command injection
B. Phishing
C. Man in the middle attack
D. Evasion methods

Answer: C

NEW QUESTION 14
Which protocols is primarily supported by the 3rd layer of the OSI ref models ?

A. HTTP/TLS
B. ATM/MPLS
C. Ipv4/IPv6
D. TCP/UDP

Answer: C

NEW QUESTION 18
Which term represents a weakness in a system that could lead to the system being compromised?

A. vulnerability
B. threat
C. exploit
D. risk

Answer: A

NEW QUESTION 22
Which tool is commonly used by threat actors on a webpage to take advantage of the software vulnerabilities of a system to spread malware?

A. exploit kit
B. root kit
C. vulnerability kit
D. script kiddie kit

Answer: B

NEW QUESTION 25
Which purpose of the certificate revocation list is true?

A. Provide a list of certificates that are trusted regardless of other validity makers.
B. Provide a list of certificates used in the chain of trust
C. Provide a list of alternate device identifiers.
D. Provide a list of certificates of certificates that are untrusted regardless of other validity makers.

Answer: D

NEW QUESTION 30
which definition of common event format in terms of a security information and event management solution is true?

A. type of event log used to identify a successful user login.
B. TCP network media protocol.
C. Event log analysis certificate that stands for certified event forensics.
D. A standard log event format that is used for log collection.

Answer: D

NEW QUESTION 34
Which definition of a daemon on Linux is true?

A. error check right after the call to fork a process
B. new process created by duplicating the calling process
C. program that runs unobtrusively in the background
D. set of basic CPU instructions

Answer: C

NEW QUESTION 36
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 37
As per RFC 1035 which transport layer protocol is used for DNS zone transfer?

A. HTTP
B. RDP
C. UDP
D. TCP

Answer: D

NEW QUESTION 39
Which definition of a fork in Linux is true?

A. daemon to execute scheduled commands
B. parent directory name of a file pathname
C. macros for manipulating CPU sets
D. new process created by a parent process

Answer: D

NEW QUESTION 44
What does the sum of the risks presented by an application represent for that application?

A. Application attack surface
B. Security violation
C. Vulnerability
D. HIPPA violation

Answer: A

NEW QUESTION 45
Which of the following are some useful reports you can collect from Cisco ISE related to endpoints? (Select all that apply.)

A. Web Server Log reports
B. Top Application reports
C. RADIUS Authentication reports
D. Administrator Login reports

Answer: ABD

NEW QUESTION 48
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 51
Which actions can a promiscuous IPS take to mitigate an attack? Choose three

A. Denying Frames
B. Resetting the TCP Connection
C. Requesting host blocking
D. Modifying packets
E. Denying packets
F. Requesting connection blocking

Answer: BCF

NEW QUESTION 52
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

Answer: A

NEW QUESTION 56
Which option is an advantage to using network-based anti-virus versus host-based anti-virus?

A. Network-based has the ability to protect unmanaged devices and unsupported operating systems.
B. There are no advantages compared to host-based antivirus.
C. Host-based antivirus does not have the ability to collect newly created signatures.
D. Network-based can protect against infection from malicious files at rest.

Answer: A

NEW QUESTION 57
You have deployed an enterprise-wide-host/endpoint technology for all of the company corporate PCs Management asks you to block a selected set application on all corporate PCs. Which technology is the option?

A. Application whitelisting/blacklisting
B. Antivirus/antispyware software.
C. Network NGFW
D. Host-based IDS

Answer: A

NEW QUESTION 60
Which of the following are metrics that can measure the effectiveness of a runbook?

A. Mean time to repair (MTTR)
B. Mean time between failures (MTBF)
C. Mean time to discover a security incident
D. All of the above

Answer: D

NEW QUESTION 65
A zombie process occurs when which of the following happens?

A. A process holds its associated memory and resources but is released from the entry table.
B. A process continues to run on its own.
C. A process holds on to associate memory but releases resources.
D. A process releases the associated memory and resources but remains in the entry table.

Answer: D

NEW QUESTION 67
Which Statement about personal firewalls is true?

A. They are resilient against kernel attacks
B. They can protect email messages and private documents in a similar way to a VPN
C. They can protect the network against attacks
D. They can protect a system by denying probing requests

Answer: D

NEW QUESTION 69
Which type of attack occurs when an attacker is successful in eavesdropping on a conversation between two IP phones?

A. replay
B. man-in-the-middle
C. dictionary
D. known-plaintext

Answer: B

NEW QUESTION 74
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 ate modified before capture
D. Packet payloads are lost

Answer: A

NEW QUESTION 77
Which of the following are public key standards?

A. IPSEC
B. PKCS #10
C. PKCS #12
D. ISO33012
E. AES

Answer: BC

NEW QUESTION 79
Which definition of the virtual address space for a Windows process is true?

A. actual physical location of an object in memory
B. set of virtual memory addresses that it can use
C. set of pages that are currently resident in physical memory
D. system-level memory protection feature that is built into the operating system

Answer: B

NEW QUESTION 82
If a web server accepts input from the user and passes it to ABash shell, to which attack method is it vulnerable?

A. input validation
B. hash collision
C. command injection
D. integer overflow

Answer: C

NEW QUESTION 87
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 92
The other one was, something similar to, what cryptography is used on Digital Certificates? The answers included:

A. SHA-256
B. SHA-512
C. RSA 4096

Answer: A

NEW QUESTION 96
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 97
Which protocol is expected to have NTP a user agent, host, and referrer headers in a packet capture?

A. NTP
B. HTTP
C. DNS
D. SSH

Answer: B

NEW QUESTION 98
Which data can be obtained using NetFlow?

A. session data
B. application logs
C. network downtime
D. report full packet capture

Answer: A

NEW QUESTION 103
Which two options are recognized forms of phishing? (Choose two)

A. spear
B. whaling
C. mailbomb
D. hooking
E. mailnet

Answer: AB

NEW QUESTION 107
Which definition of the IIS Log Parser tool is true?

A. a logging module for IIS that allows you to log to a database
B. a data source control to connect to your data source
C. a powerful, versatile tool that makes it possible to run SQL-like queries against log flies
D. a powerful versatile tool that verifies the integrity of the log files

Answer: C

NEW QUESTION 110
Which two features must a next generation firewall include? (Choose two.)

A. data mining
B. host-based antivirus
C. application visibility and control
D. Security Information and Event Management
E. intrusion detection system

Answer: CE

NEW QUESTION 114
At which OSI layer does a router typically operate?

A. Transport
B. Network
C. Data link
D. Application

Answer: B

NEW QUESTION 119
Which NTP service is ABest practice to ensure that all network devices are synchronized with a reliable and trusted time source?

A. Redundant authenticated NTP
B. Redundant unauthenticated NTP
C. Authenticated NTP services from one of the local AD domain controllers
D. Local NTP within each network device

Answer: A

NEW QUESTION 123
In which technology is network level encrypted not natively incorporated?

A. Kerberos
B. ssl
C. tls
D. IPsec

Answer: A

NEW QUESTION 124
which data type is the most beneficial to recreate ABinary file for malware analysis

A. Alert
B. Session
C. Statistical
D. Extracted Content Data

Answer: B

NEW QUESTION 127
Which vulnerability is an example of Shellshock?

A. SQL injection
B. heap Overflow
C. cross site scripting
D. command injection

Answer: D

NEW QUESTION 130
Which term represents the practice of giving employees only those permissions necessary to perform their specific role within an organization?

A. integrity validation
B. due diligence
C. need to know
D. least privilege

Answer: D

NEW QUESTION 133
Which term represents the chronological record of how evidence was collected- analyzed, preserved, and transferred?

A. chain of evidence
B. evidence chronology
C. chain of custody
D. record of safekeeping

Answer: C

NEW QUESTION 135
Which three statements about host-based IPS are true? (Choose three.)

A. It can view encrypted files.
B. It can have more restrictive policies than network-based IPS.
C. It can generate alerts based on behavior at the desktop level.
D. It can be deployed at the perimeter.
E. It uses signature-based policies.
F. It works with deployed firewalls.

Answer: ABC

NEW QUESTION 138
Which definition of an antivirus program is true?

A. program used to detect and remove unwanted malicious software from the system
B. program that provides real time analysis of security alerts generated by network hardware and application
C. program that scans a running application for vulnerabilities
D. rules that allow network traffic to go in and out

Answer: A

NEW QUESTION 140
Which purpose of a security risk assessment is true?

A. Find implementation issues that could lead to vulnerability
B. Notify the customer of a vulnerability
C. Set the SIR value of a vulnerability
D. Score a vulnerability

Answer: A

NEW QUESTION 141
Which process continues to be recorded in the process table after it has ended and the status is returned to the parent?

A. daemon
B. zombie
C. orphan
D. child

Answer: B

NEW QUESTION 146
According to the attribute-based access control (ABAC) model, what is the subject location considered?

A. Part of the environmental attributes
B. Part of the object attributes
C. Part of the access control attributes

D. None of the above

Answer: A

NEW QUESTION 150
What event types does FMC record?

A. standard common event logs types
B. successful login event logs
C. N/A

Answer: C

NEW QUESTION 155
Which description is an example of whaling?

A. When attackers target specific individuals
B. When attackers target a group of individuals
C. When attackers go after the CEO
D. When attackers use fraudulent websites that look like legitimate ones

Answer: C

NEW QUESTION 157
Which protocol is primarily supported by the third layer of the Open Systems Interconnection reference model?

A. HTTP/TLS
B. IPv4/IPv6
C. TCP/UDP
D. ATM/ MPLS

Answer: B

NEW QUESTION 159
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 160
Which definition of Windows Registry is true?

A. set of pages that are currently resident m physical memory
B. basic unit to which the operating system allocates processor time
C. set of virtual memory addresses
D. database that stores low-level settings for the operating system

Answer: D

NEW QUESTION 164
Which type of technology is used for detecting unusual patterns and anomalous behavior on a network?

A. Host intrusion detection
B. Host malware prevention
C. NetFlow analysis
D. Web content filtering

Answer: C

NEW QUESTION 166
Which two activities are examples of social engineering? (Choose two)

A. receiving call from the IT department asking you to verify your username/password to maintain the account
B. receiving an invite to your department's weekly WebEx meeting
C. sending a verbal request to an administrator to change the password to the account of a user the administrator does know
D. receiving an email from MR requesting that you visit the secure HR website and update your contract information
E. receiving an unexpected email from an unknown person with an uncharacteristic attachment from someone in the same company

Answer: AD

NEW QUESTION 170
Which three options are types of Layer 2 network attack? (Choose three.)

A. ARP attacks
B. brute force attacks
C. spoofing attacks
D. DDOS attacks
E. VLAN hopping
F. botnet attacks

Answer: ACE

NEW QUESTION 174
The FMC can share HTML, Pdf and csv data type that relate to a specific event type which event type:

A. Connection
B. Host
C. Netflow
D. Intrusion

Answer: D

NEW QUESTION 179
What is PHI?

A. Protected HIPAA information
B. Protected health information
C. Personal health information
D. Personal human information

Answer: B

NEW QUESTION 184
which international standard is for general risk management, including the principles and guidelines for managing risk?

A. ISO 27001
B. ISO 27005
C. IS0 31000
D. ISO 27002

Answer: C

NEW QUESTION 189
Which definition describes the purpose of a Security Information and Event Management?

A. a database that collects and categorizes indicators of compromise to evaluate and search for potential security threats
B. a monitoring interface that manages firewall access control lists for duplicate firewall filtering
C. a relay server or device that collects then forwards event logs to another log collection device
D. a security product that collects, normalizes, and correlates event log data to provide holistic views of the security posture

Answer: D

NEW QUESTION 191
An attacker installs a rogue switch that sends superior BPDUs on your network. What is a possible result of this activity?

A. The switch could offer fake DHCP addresses.
B. The switch could become the root bridge.
C. The switch could be allowed to join the VTP domain
D. The switch could become a transparent bridge.

Answer: B

NEW QUESTION 192
Which two actions are valid uses of public key infrastructure? (Choose two)

A. ensuring the privacy of a certificate
B. revoking the validation of a certificate
C. validating the authenticity of a certificate
D. creating duplicate copies of a certificate
E. changing ownership of a certificate

Answer: AC

NEW QUESTION 196
Netflow uses which format?

A. base 10
B. ASCII
C. Binary
D. Hexadecimal

Answer: C

NEW QUESTION 199
A user reports difficulties accessing certain external web pages, when examining traffic to and from the external domain in full packet captures, you notice many SYNs that have the same sequence number, source, and destination IP address, but have different payloads. Which problem is a possible explanation of this situation?

A. insufficient network resources
B. failure of full packet capture solution
C. misconfiguration of web filter
D. TCP injection

Answer: D

NEW QUESTION 204
Where is a host-based intrusion detection system located?

A. on a particular end-point as an agent or a desktop application
B. on a dedicated proxy server monitoring egress traffic
C. on a span switch port
D. on a tap switch port

Answer: A

NEW QUESTION 205
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 208
While viewing packet capture data, you notice that one IP is sending and receiving traffic for multiple devices by modifying the IP header,
Which option is making this behavior possible?

A. TOR
B. NAT
C. encapsulation
D. tunneling

Answer: B

NEW QUESTION 212
Which two tasks can be performed by analyzing the logs of a traditional stateful firewall? (Choose two.)

A. Confirm the timing of network connections differentiated by the TCP 5-tuple
B. Audit the applications used within a social networking web site.
C. Determine the user IDs involved in an instant messaging exchange.
D. Map internal private IP addresses to dynamically translated external public IP addresses
E. Identify the malware variant carried by SMTP connection

Answer: AD

NEW QUESTION 217
Which security monitoring data type requires the most storage space?

A. full packet capture
B. transaction data
C. statistical data
D. session data

Answer: A

NEW QUESTION 219
Which two protocols are often used for DDoS amplification attacks (choose two)

A. HTTP
B. TCP
C. DNS
D. ICMPv6
E. NTP

Answer: CE

NEW QUESTION 224
Which type of exploit normally requires the culprit to have prior access to the target system?

A. local exploit
B. denial of service
C. system vulnerability
D. remote exploit

Answer: A

NEW QUESTION 225
A firewall requires deep packet inspection to evaluate which layer?

A. application
B. Internet
C. link
D. transport

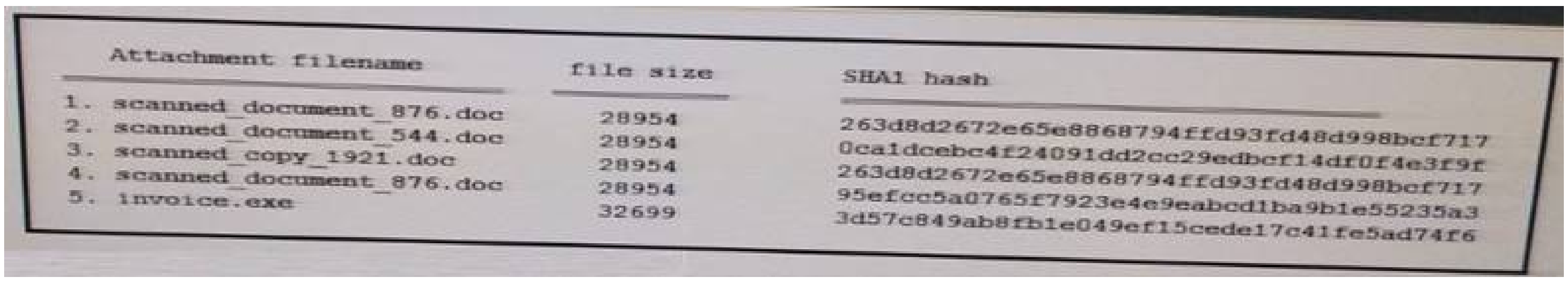
Answer: A

NEW QUESTION 230
which security principle is violated by running all processes as root/admin

A. RBAC
B. Principle of least privilege
C. Segregation of duty

Answer: B

NEW QUESTION 233
Refer to the exhibit.



Attachment filename	file size	SHA1 hash
1. scanned_document_876.doc	28954	263d8d2672e65e8868794ffd93fd48d998bcf717
2. scanned_document_544.doc	28954	0ca1dcebc4f24091dd2cc29edbcf14df0f4e3f9f
3. scanned_copy_1921.doc	28954	263d8d2672e65e8868794ffd93fd48d998bcf717
4. scanned_document_876.doc	28954	95efcc5a0765f7923e4e9eabcd1ba9b1e55235a3
5. invoice.exe	32699	3d57c849ab8fb1e049ef15cede17c41fe5ad74f6

During an analysis this list of email attachments is found. Which files contain the same content?

A. 1 and 4
B. 3 and 4
C. 1 and 3
D. 1 and 2

Answer: C

NEW QUESTION 237
which options is true when using the traffic mirror feature in a switch

A. Ethernet headers are modified
B. packets payloads are lost
C. packets are not processed
D. full capture is possible

Answer: D

NEW QUESTION 242
Which protocol is primarily supported by the Fourth layer of the Open Systems Interconnection reference model?

A. HTTP/TLS
B. IPv4/IPv6
C. TCP/UDP
D. ATM/ MPLS

Answer: C

NEW QUESTION 243
Which directory is commonly used on Linux systems to store log files, including syslog and apache access logs?

A. /etc/log
B. /root/log
C. /lib/log
D. /var/log

Answer: D

NEW QUESTION 246
In which context is it inappropriate to use a hash algorithm?

A. Telnet logins
B. Verifying file integrity
C. SSH logins
D. Digital signature verification

Answer: A

NEW QUESTION 251
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 254
Which network device is used to separate broadcast domains?

A. Router
B. Repeater
C. Switch
D. Bridge

Answer: A

NEW QUESTION 258
Which encryption algorithm is the strongest?

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

Answer: A

NEW QUESTION 260
Which of the following are examples of system-based sandboxing implementations? (Select all that apply.)

A. Google Project Zero
B. Google Chromium sandboxing
C. Java JVM sandboxing
D. Threat Grid
E. HTML5 “sandbox” attribute for use with iframes.

Answer: BCE

NEW QUESTION 262
Which security principle states that more than one person is required to perform a critical task?

A. due diligence
B. separation of duties
C. need to know
D. least privilege

Answer: B

NEW QUESTION 266
......