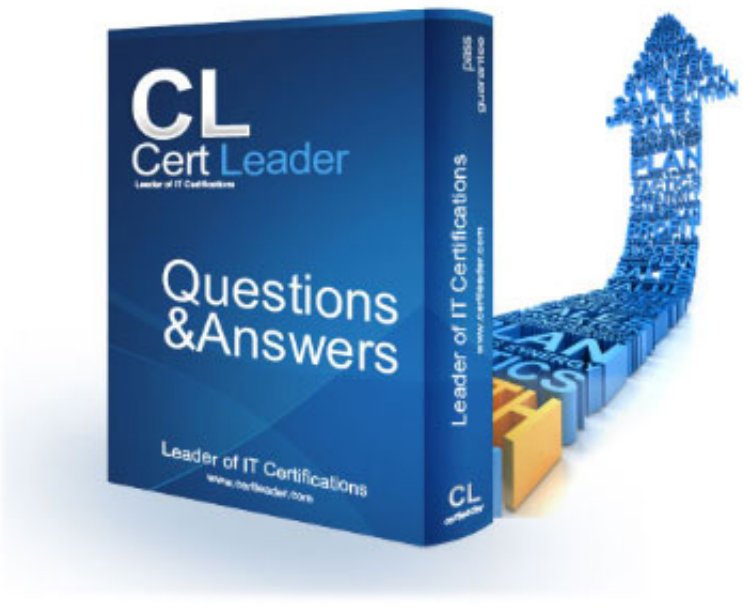
210-250 Dumps

Understanding Cisco Cybersecurity Fundamentals

https://www.certleader.com/210-250-dumps.html



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
you get an alert on your desktop computer showing that an attack was successful on the host but up on investigation you see that occurred duration the attack. Which reason is true?

A. The computer has HIDS installed on it
B. The computer has NIDS installed on it
C. The computer has HIPS installed on it
D. The computer has NIPS installed on it

Answer: A

NEW QUESTION 4
According to the common vulnerability scoring system, which term is associated with scoring multiple vulnerabilities that are exploit in the course of a single attack?

A. chained score
B. risk analysis
C. Vulnerability chaining
D. Confidentiality

Answer: C

NEW QUESTION 5
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 6
For which kind of attack does an attacker use known information in encrypted files to break the encryption scheme for the rest of the file

A. known-plaintext
B. known-ciphertext
C. unknown key
D. man in the middle

Answer: A

NEW QUESTION 7
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

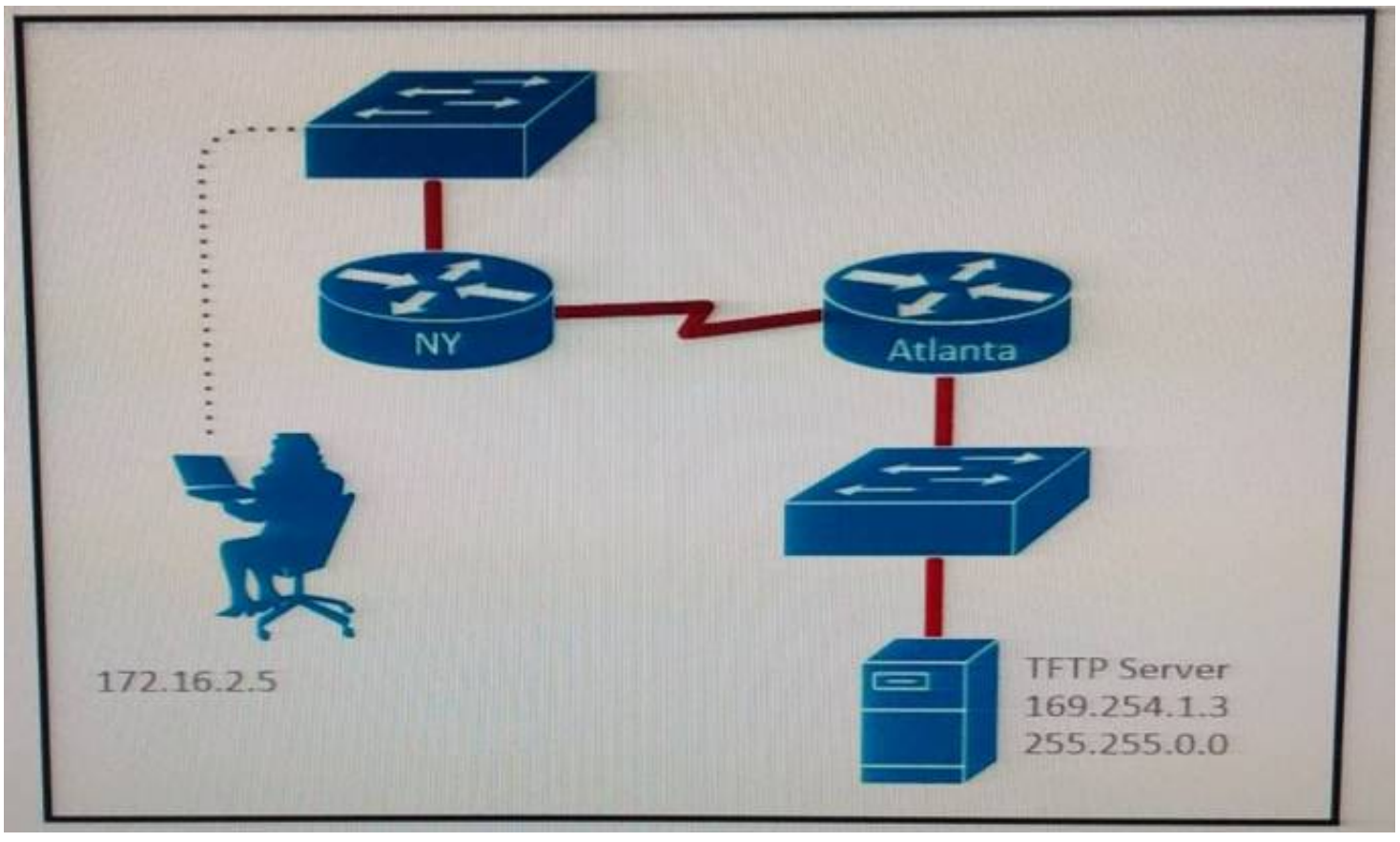
NEW QUESTION 8

Which definition of a Linux daemon is true?

A. Process that is causing harm to the system by either using up system resources or causing a critical crash.
B. Long – running process that is the child at the init process
C. process that has no parent process
D. process that is starved at the CPU.

Answer: B

NEW QUESTION 9
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 10
Which hashing algorithm is the least secure?

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

Answer: A

NEW QUESTION 10
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 13
Which of the following are Cisco cloud security solutions?

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

Answer: BC

NEW QUESTION 15

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 18
DNS query uses which protocol

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

Answer: B

NEW QUESTION 19
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 20
Which evasion method involves performing actions slower than normal to prevent detection?

A. traffic fragmentation
B. tunneling
C. timing attack
D. resource exhaustion

Answer: C

NEW QUESTION 22
An intrusion detection system begins receiving an abnormally high volume of scanning from numerous sources. Which evasion technique does this attempt indicate?

A. traffic fragmentation
B. resource exhaustion
C. timing attack
D. tunneling

Answer: B

NEW QUESTION 26
What Does the sum of the risk presented by an application represent for that application ?

A. Security violation
B. Application Attack Surface
C. HIPPA violation
D. Vulnerability

Answer: B

NEW QUESTION 29
For which purpose can Windows management instrumentation be used?

A. Remote viewing of a computer
B. Remote blocking of malware on a computer
C. Remote reboot of a computer
D. Remote start of a computer

Answer: A

NEW QUESTION 33
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 34
Which term represents the likely hood of potential danger that could take advantage of a weakness in a system?

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

Answer: B

NEW QUESTION 39
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 44
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 49
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 52
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 54
You must create a vulnerability management framework. Which main purpose of this framework is true?

A. Conduct vulnerability scans on the network.
B. Manage a list of reported vulnerabilities.
C. Identify, remove and mitigate system vulnerabilities.
D. Detect and remove vulnerabilities in source code.

Answer: C

NEW QUESTION 55
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 57
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 61
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 62
Which statement about an attack surface is true?

A. It is the sum of all paths for data/commands into and out of the application
B. It is an exploitable weakness in a system or design
C. It is the individual who perform an attack.
D. It is any potential danger to an asset.

Answer: A

NEW QUESTION 63
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 64
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 69
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 72
Which vulnerability is an example of Heartbleed?

A. Buffer overflow
B. Denial of service
C. Command injection
D. Information disclosure

Answer: D

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 81
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 86
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 91
Which concern is important when monitoring NTP servers for abnormal levels of traffic?

A. Being the cause of a distributed reflection denial of service attack.
B. Users changing the time settings on their systems.
C. A critical server may not have the correct time synchronized.
D. Watching for rogue devices that have been added to the network.

Answer: A

NEW QUESTION 94
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 98
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 99
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 104
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 107
Which two options are recognized forms of phishing? (Choose two)

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

Answer: AB

NEW QUESTION 110
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 113
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 115
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 116
At which OSI layer does a router typically operate?

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

Answer: B

NEW QUESTION 118
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
What Linux commands show the process for all users?

A. ps –a
B. ps –u
C. ps –d
D. ps –m

Answer: A

NEW QUESTION 127
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 131
Stateful and traditional firewalls can analyze packets and judge them against a set of predetermined rules called access control lists (ACLs). They inspect which of the following elements within a packet? (Choose Two)

A. Session headers
B. NetFlow flow information
C. Source and destination ports and source and destination IP addresses
D. Protocol information

Answer: CD

NEW QUESTION 135
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 137
Which vulnerability is an example of Shellshock?

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

Answer: D

NEW QUESTION 139
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 143
For which reason can HTTPS traffic make security monitoring difficult?

A. encryption
B. large packet headers
C. Signature detection takes longer.
D. SSL interception

Answer: A

NEW QUESTION 144
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 145
Which term represents a potential danger that could take advantage of a weakness in a system?

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

Answer: D

NEW QUESTION 150
Which two protocols are used for email (Choose two)

A. NTP
B. DNS
C. HTTP
D. IMAP
E. SMTP

Answer: DE

NEW QUESTION 152
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 153
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 155
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 158
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 163
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 168
which statement about the difference between a denial-of-service attack and a distributed denial-of service attack is true?

A. dos attacks only use flooding to compromise a network, and DDOS attacks m=only use other methods?
B. Dos attacks are launched from one host, and DDOS attacks are lunched from multiple hosts.
C. Dos attacks are lunched from one host, and DDOS attacks are lunched from multiple hosts
D. DDos attacks are lunched from one host, and DOS attacks are lunched from multiple hosts
E. Dos attacks and DDOS attacks have no differences?

Answer: B

NEW QUESTION 173
What event types does FMC record?

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

Answer: C

NEW QUESTION 178
Which information security property is supported by encryption?

A. sustainability
B. integrity
C. confidentiality
D. availability

Answer: C

NEW QUESTION 183
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 184
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 186
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 187
Which situation indicates application-level white listing?

A. Allow everything and deny specific executable files.
B. Allow specific executable files and deny specific executable files.
C. Writing current application attacks on a whiteboard daily.
D. Allow specific files and deny everything else.

Answer: D

NEW QUESTION 190
Where does routing occur within the DoD TCP/IP reference model?

A. application
B. internet
C. network
D. transport

Answer: B

NEW QUESTION 192
Which two terms are types of cross site scripting attacks? (Choose two)

A. directed

B. encoded
C. stored
D. reflected
E. cascaded

Answer: CD

NEW QUESTION 196
What is PHI?

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

Answer: B

NEW QUESTION 198
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 203
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 207
Which action is an attacker taking when they attempt to gain root access on the victim's system?

A. privilege escalation
B. command injections
C. root kit
D. command and control

Answer: A

NEW QUESTION 212
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 213
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 214
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 217
After a large influx of network traffic to externally facing devices, you begin investigating what appear to be a denial of service attack. When you review packets capture data, you notice that the traffic is a single SYN packet to each port. Which kind of attack is this?

A. SYN flood.
B. Host porfiling.
C. Traffic fragmentation.
D. Port scanning.

Answer: D

NEW QUESTION 219
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 223
A firewall requires deep packet inspection to evaluate which layer?

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

Answer: A

NEW QUESTION 227
In which case should an employee return his laptop to the organization?

A. When moving to a different role
B. Upon termination of the employment
C. As described in the asset return policy
D. When the laptop is end of lease

Answer: C

NEW QUESTION 232
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 237
What is a trunk link used for?

A. To pass multiple virtual LANs
B. To connect more than two switches
C. To enable Spanning Tree Protocol
D. To encapsulate Layer 2 frames

Answer: A

NEW QUESTION 241
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 243
Which of the following is true about heuristic-based algorithms?

A. Heuristic-based algorithms may require fine tuning to adapt to network traffic and minimize the possibility of false positives.
B. Heuristic-based algorithms do not require fine tuning.
C. Heuristic-based algorithms support advanced malware protection.
D. Heuristic-based algorithms provide capabilities for the automation of IPS signature creation and tuning.

Answer: A

NEW QUESTION 244
You discover that a foreign government hacked one of the defense contractors in your country and stole intellectual property. In this situation, which option is considered the threat agent?

A. method in which the hack occurred
B. defense contractor that stored the intellectual property
C. intellectual property that was stolen
D. foreign government that conducted the attack

Answer: D

NEW QUESTION 249
Which network device is used to separate broadcast domains?

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

Answer: A

NEW QUESTION 251
Which encryption algorithm is the strongest?

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

Answer: A

NEW QUESTION 255
Cisco pxGrid has a unified framework with an open API designed in a hub-and-spoke architecture. pxGrid is used to enable the sharing of contextual-based information from which devices?

A. From a Cisco ASA to the Cisco OpenDNS service
B. From a Cisco ASA to the Cisco WSA
C. From a Cisco ASA to the Cisco FMC
D. From a Cisco ISE session directory to other policy network systems, such as Cisco IOS devices and the Cisco ASA

Answer: D

NEW QUESTION 258
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 267
.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your 210-250 Exam with Our Prep Materials Via below:

https://www.certleader.com/210-250-dumps.html