Cisco.210-250.v2018-06-05.q61

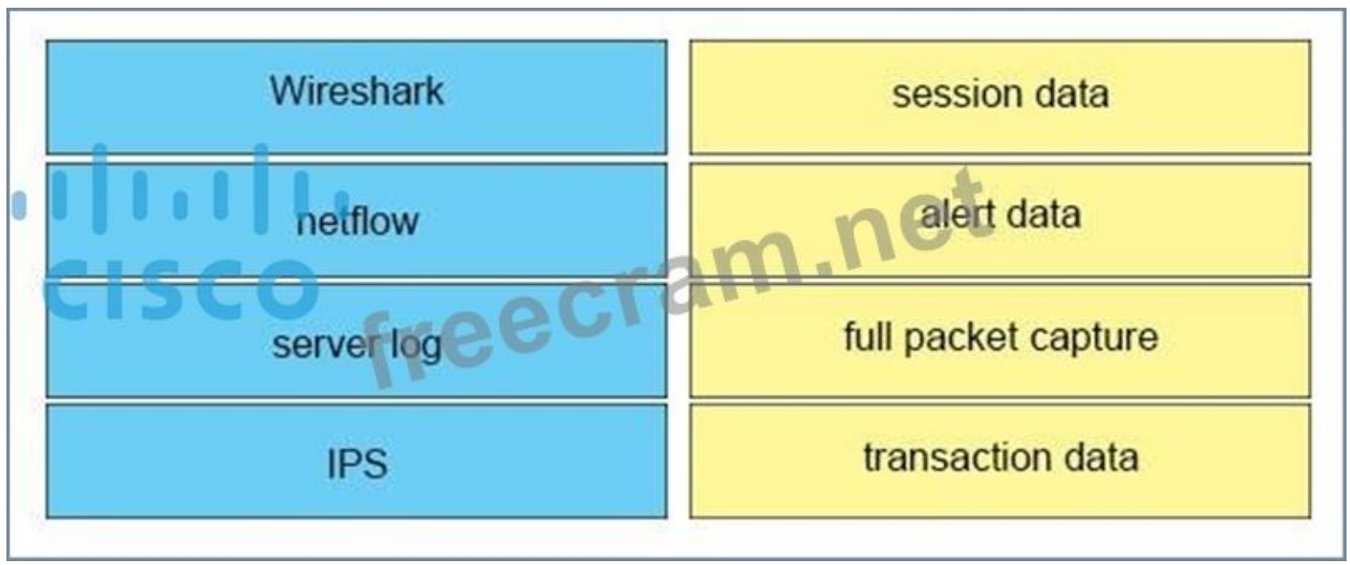
Exam Code:	210-250
Exam Name:	Understanding Cisco Cybersecurity Fundamentals
Certification Provider:	Cisco
Free Question Number:	61
Version:	v2018-06-05
# of views:	1126
# of Questions views:	37940
https://www.freecram.net/torrent/Cisco.210-250.v2018-06-05.q61.html	

NEW QUESTION: 1

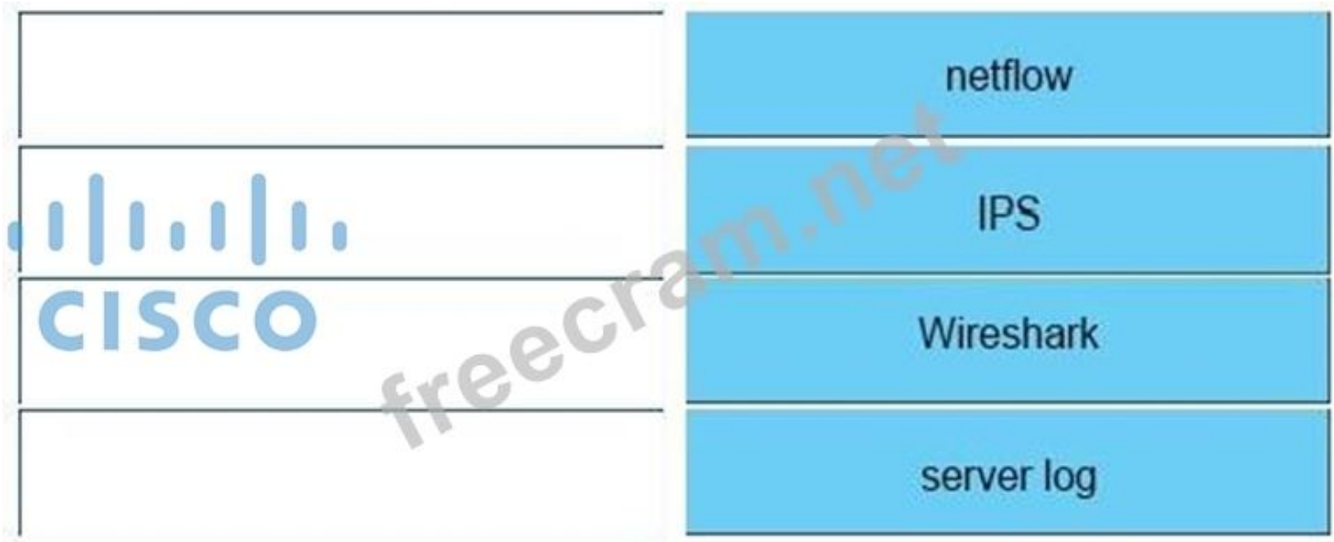
DRAG DROP

Drag the data source on the left to the correct data type on the right.

Select and Place:



Answer:



NEW QUESTION: 2
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: (SHOW ANSWER)
Explanation/Reference:
Explanation:

NEW QUESTION: 3
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: (SHOW ANSWER)
Explanation/Reference:
Explanation:

NEW QUESTION: 4
Which hash algorithm is the weakest?
A. SHA-512
B. RSA 4096
C. SHA-1
D. SHA-256
Answer: (SHOW ANSWER)
Explanation/Reference:

Explanation:

NEW QUESTION: 5
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: (SHOW ANSWER)
Explanation/Reference:
Explanation:

NEW QUESTION: 6
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.
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:

NEW QUESTION: 7
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: (SHOW ANSWER)
Explanation/Reference:
Explanation:

NEW QUESTION: 8
Which information security property is supported by encryption?
A. sustainability
B. integrity
C. confidentiality
D. availability
Answer: (SHOW ANSWER)

Explanation/Reference:
Explanation:

NEW QUESTION: 9
Which definition of a fork in Linux is true?
A. daemon to execute scheduled commands
B. parentdirectory name of a file path name
C. macros for manipulating CPU sets
D. new process created by a parent process
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:

NEW QUESTION: 10
Which definition of Windows Registry is true?

A. set of pages that are currently resident in 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: (SHOW ANSWER)
Explanation/Reference:
Explanation:

NEW QUESTION: 11
Which encryption algorithm is the strongest?
A. AES
B. CES
C. DES
D. 3DES
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:

NEW QUESTION: 12
Which two options are recognized forms of phishing? (Choose two.)
A. spear
B. whaling
C. mailbomb
D. hooking
E. mailnet
Answer: (SHOW ANSWER)

Explanation/Reference:
Explanation:

NEW QUESTION: 13
Which statement about digitally signing a document is true?
A. The document is hashed and then thedocument 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 isencrypted with the public key.
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:

NEW QUESTION: 14
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: (SHOW ANSWER)
Explanation/Reference:
Explanation:

NEW QUESTION: 15
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: (SHOW ANSWER)
Explanation/Reference:
Explanation:

NEW QUESTION: 16
Which identifier is used to describe the application or process that submitted a log message?
A. action
B. selector
C. priority
D. facility
Answer: (SHOW ANSWER)

Explanation/Reference:
Reference:
https://www.tutorialspoint.com/unix/unix-system-logging.htm

NEW QUESTION: 17
Which security monitoring data type requires the most storage space?
A. full packet capture
B. transaction data
C. statistical data
D. session data
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:

NEW QUESTION: 18
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: (SHOW ANSWER)
Explanation/Reference:
Explanation:

NEW QUESTION: 19
Which two terms are types of cross site scripting attacks? (Choose two.)
A. directed
B. encoded
C. stored
D. reflected
E. cascaded

Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:

NEW QUESTION: 20
Which definition of the IIS Log Parser tool is true?
A. a logging module for IIS that allows you to logto 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 files
D. a powerful, versatile tool that verifies the integrity of the log files
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:

NEW QUESTION: 21
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: (SHOW ANSWER)
Explanation/Reference:
Explanation:

NEW QUESTION: 22
In computer security, which information is the term PHI used to describe?
A. private host information
B. protected health information
C. personal health information
D. protected host information
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:

NEW QUESTION: 23
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: (SHOW ANSWER)

Explanation/Reference:

Explanation:

NEW QUESTION: 24

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: (SHOW ANSWER)

Explanation/Reference:

Explanation:

NEW QUESTION: 25

Which protocol is expected to have a user agent, host, and referrer header in a packet capture?

A. NTP

B. HTTP

C. DNS

D. SSH

Answer: (SHOW ANSWER)

Explanation/Reference:

Explanation:

NEW QUESTION: 26

Which definition of permissions in Linux is true?

A. rules that allow network traffic to go in and out

B. table maintenance program

C. written affidavit that you have to sign before using the system

D. attributes of ownership and control of an object

Answer: (SHOW ANSWER)

Explanation/Reference:

Explanation:

NEW QUESTION: 27

Which hashing algorithm is the least secure?

A. MD5

B. RC4

C. SHA-3

D. SHA-2

Answer: (SHOW ANSWER)

Explanation/Reference:

Explanation:

NEW QUESTION: 28

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: (SHOW ANSWER)

Explanation/Reference:

Explanation:

NEW QUESTION: 29

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: (SHOW ANSWER)

Explanation/Reference:

Explanation:

NEW QUESTION: 30

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: (SHOW ANSWER)

Explanation/Reference:

Explanation:

NEW QUESTION: 31

Attachment filename	file size	SHA1 hash
1. scanned_document_876.doc	28954	263d8d2672e65e8868794ffd93fd48d998bcf717
2. scanned_document_544.doc	28954	0caldcebc4f24091dd2cc29edbcf14df0f4e3f9f
3. scanned_copy_1921.doc	28954	263d8d2672e65e8868794ffd93fd48d998bcf717
4. scanned_document_876.doc	28954	95efcc5a0765f7923e4e9eabcd1ba9b1e55235a3
5. invoice.exe	32699	3d57c849ab8fb1e049ef15cede17c41fe5ad74f6

Refer to the exhibit. 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: (SHOW ANSWER)

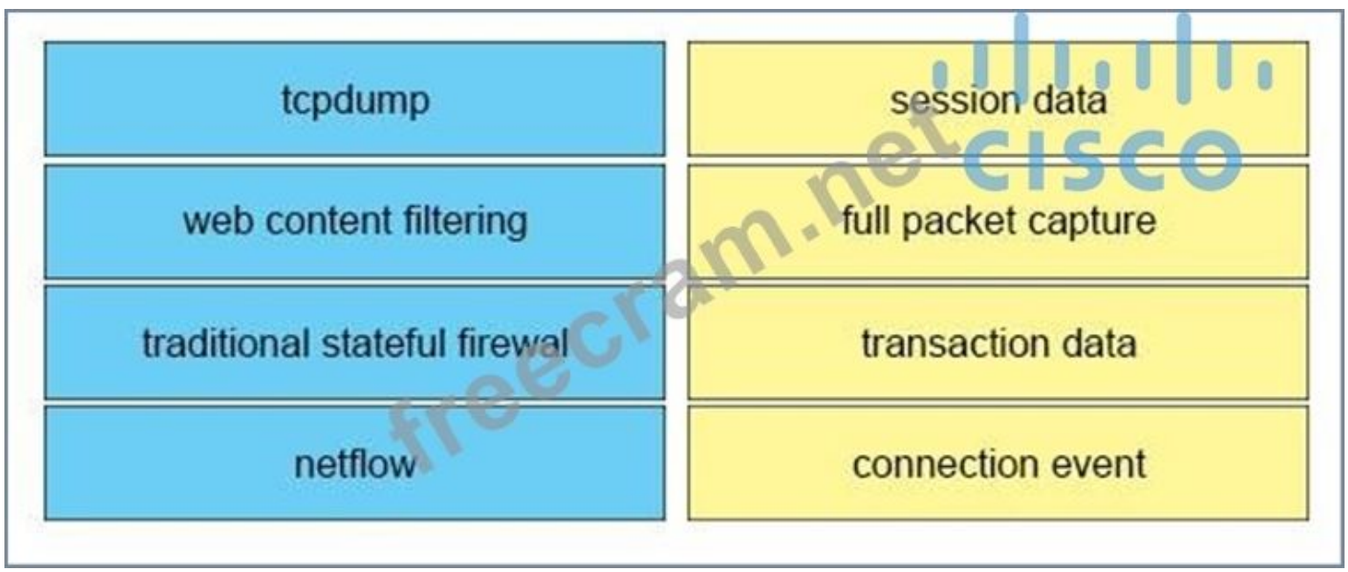
Explanation/Reference:
Explanation:

NEW QUESTION: 32

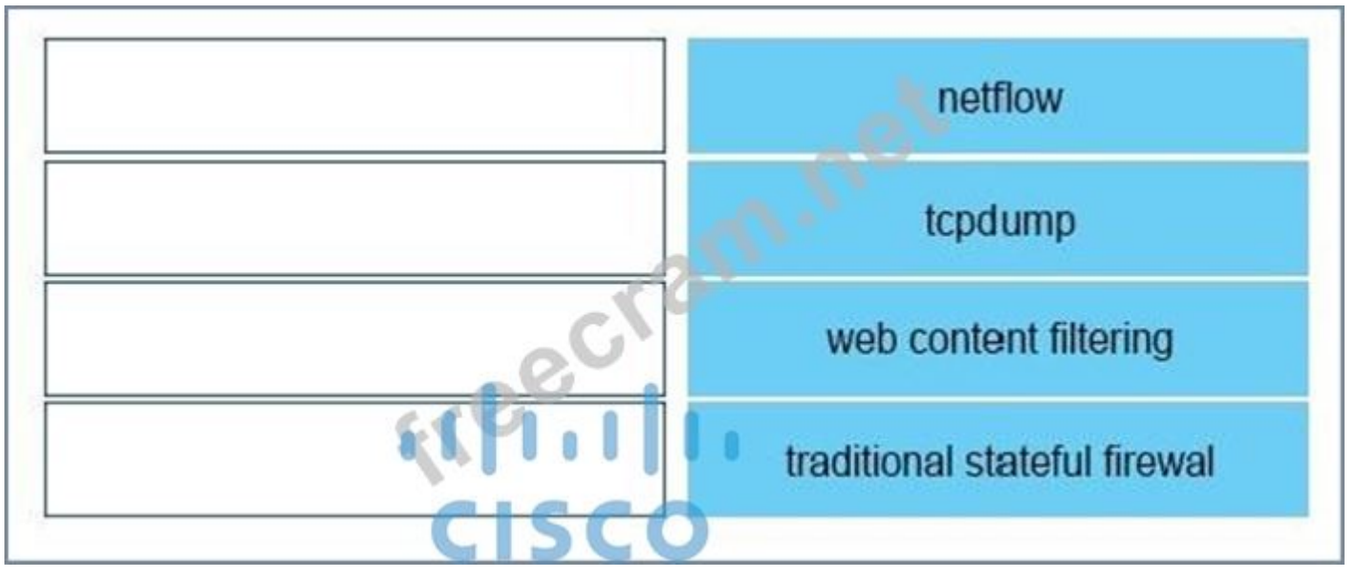
DRAG DROP

Drag the technology on the left to the data type the technology provides on the right.

Select and Place:



Answer:



NEW QUESTION: 33
Which cryptographic key is contained in an X.509 certificate?
A. symmetric
B. public
C. private
D. asymmetric
Answer: C (LEAVE A REPLY)
Explanation/Reference:
Explanation:

NEW QUESTION: 34
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: (SHOW ANSWER)
Explanation/Reference:
Explanation:

NEW QUESTION: 35
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: A (LEAVE A REPLY)

Explanation/Reference:
Explanation:

NEW QUESTION: 36
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: (SHOW ANSWER)
Explanation/Reference:
Explanation:

NEW QUESTION: 37
Which evasion method involves performing actions slower than normal to prevent detection?
A. traffic fragmentation
B. tunneling
C. timing attack
D. resource exhaustion
Answer: (SHOW ANSWER)
Explanation/Reference:
Reference:https://books.google.com/books?id=KIwLSddtAWsC&pg=PA58&lpg=PA58&dq=timing+attack+performing+actions+slower+than+normal+to+prevent+detection&source=bl&ots=9qu7ywV-mX&sig=_9lwcDDq-WNaYlEeP7VkR0MPAOE&hl=en&sa=X&ved=0ahUKEwiRwo_P8vvRAhVKyoMKHaUlAUQQ6AEIITAB#v=onepage&q=timing%20attack%20performing%20actions%20slower%20than%20normal%20to%20prevent%20detection&f=false

NEW QUESTION: 38
Which definition of a process in Windows is true?
A. running program
B. unit of execution that must be manually scheduled by the application
C. database that stores low-level settings for the OS and for certain applications
D. basic unit to which the operating system allocates processor time
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:

NEW QUESTION: 39

Which data can be obtained using NetFlow?

A. session data

B. applicationlogs

C. network downtime report

D. full packet capture

Answer: (SHOW ANSWER)

Explanation/Reference:

Explanation:

NEW QUESTION: 40

If a web server accepts input from the user and passes it to a bash shell, to which attack method if it vulnerable?

A. input validation

B. hash collision

C. command injection

D. integer overflow

Answer: (SHOW ANSWER)

Explanation/Reference:

Explanation:

NEW QUESTION: 41

Which two protocols are used for email? (Choose two.)

A. NTP

B. DNS

C. HTTP

D. IMAP

E. SMTP

Answer: (SHOW ANSWER)

Explanation/Reference:

Explanation:

NEW QUESTION: 42

Which definition of vulnerability is true?

A. an exploitable, unpatched and unmitigated weakness in software

B. an incompatible piece of software

C. software that does not have the most current patch applied

D. software that was not approved for installation

Answer: (SHOW ANSWER)

Explanation/Reference:

Explanation:

NEW QUESTION: 43
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 HR 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: (SHOW ANSWER)
Explanation/Reference:
Explanation:

NEW QUESTION: 44
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: (SHOW ANSWER)
Explanation/Reference:
Explanation:

NEW QUESTION: 45
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: (SHOW ANSWER)
Explanation/Reference:
Explanation:

NEW QUESTION: 46
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 offull packet capture solution
C. misconfiguration of web filter
D. TCP injection
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:

NEW QUESTION: 47
Which definition of a daemon on Linux is true?
A. error check right afterthe 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: (SHOW ANSWER)
Explanation/Reference:
Explanation:

NEW QUESTION: 48
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: (SHOW ANSWER)
Explanation/Reference:
Explanation:

NEW QUESTION: 49
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: (SHOW ANSWER)
Explanation/Reference:
Explanation:

NEW QUESTION: 50
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: C (LEAVE A REPLY)
Explanation/Reference:
Explanation:

NEW QUESTION: 51
Which situation indicates application-level whitelisting?
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: (SHOW ANSWER)
Explanation/Reference:
Explanation:

NEW QUESTION: 52
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
Answer: (SHOW ANSWER)
Explanation/Reference:

NEW QUESTION: 53
Which definition describes the main purpose of a Security Information and Event Management solution?

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 of an environment
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:

NEW QUESTION: 54
A firewall requires deep packet inspection to evaluate which layer?
A. application
B. internet
C. link
D. transport
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:

NEW QUESTION: 55
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: (SHOW ANSWER)
Explanation/Reference:
Explanation:

NEW QUESTION: 56
Which network device is used to separate broadcast domains?
A. router
B. repeater
C. switch
D. bridge
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:

NEW QUESTION: 57

One of the objectives of information security if 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: (SHOW ANSWER)

Explanation/Reference:

Explanation:

NEW QUESTION: 58

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.

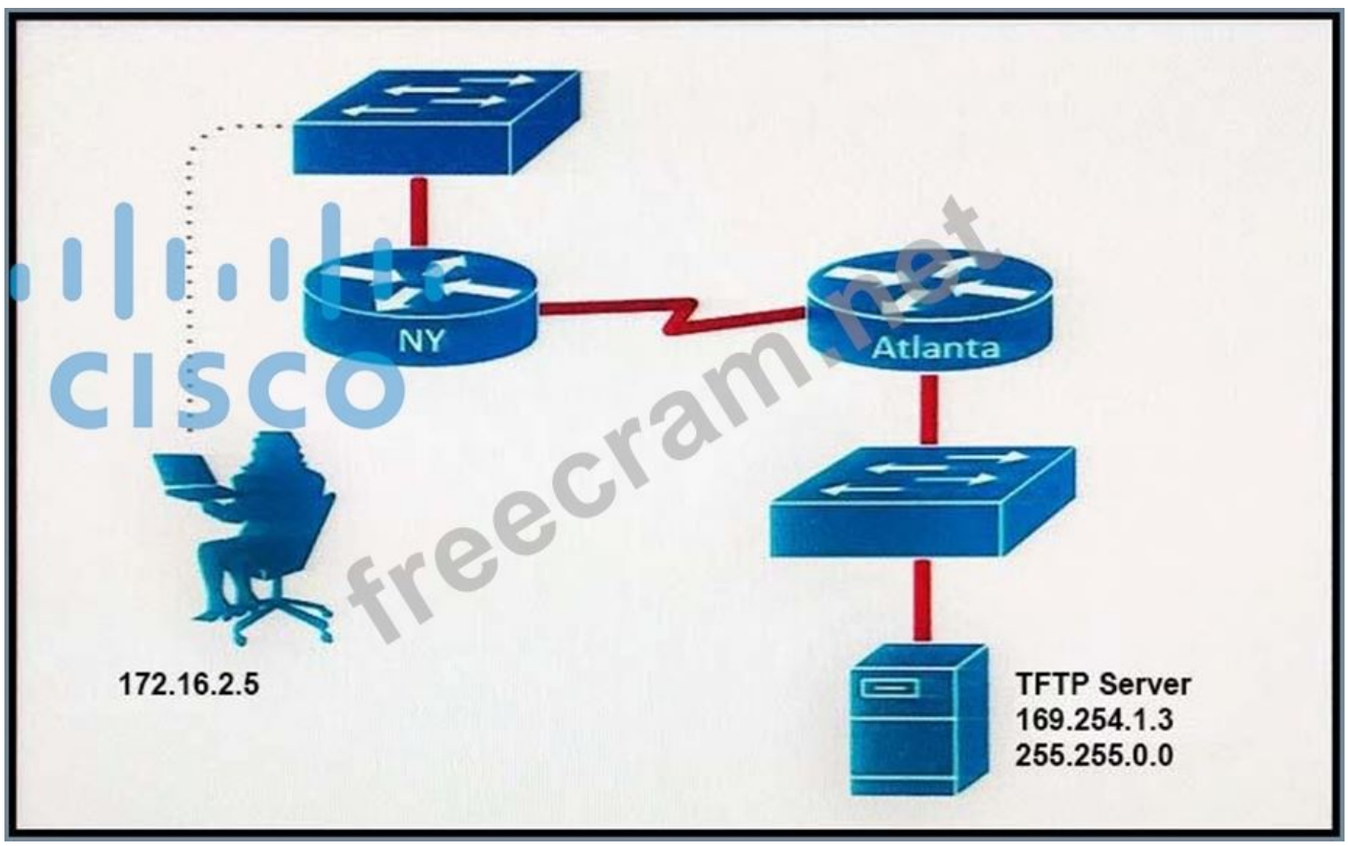
E. Identify the malware variant carried by an SMTP connection

Answer: (SHOW ANSWER)

Explanation/Reference:

Explanation:

NEW QUESTION: 59



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 backup 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: (SHOW ANSWER)

Explanation/Reference:

Explanation:

NEW QUESTION: 60

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

A. alert data

B. statistical data

C. session data

D. transaction data

Answer: (SHOW ANSWER)

Explanation/Reference:

Explanation:

NEW QUESTION: 61

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: (SHOW ANSWER)

Explanation/Reference:

Explanation:

https://www.examdiscuss.com/Cisco/exam/210-250/premium/ (**185** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

Valid 210-250 Dumps shared by ExamDiscuss.com for Helping Passing 210-250 Exam! ExamDiscuss.com now offer the **newest 210-250 exam dumps**, the ExamDiscuss.com 210-250 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com 210-250 dumps with Test Engine here: https://www.examdiscuss.com/Cisco/exam/210-250/premium/ (**185** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)