Exam Questions 210-250

Understanding Cisco Cybersecurity Fundamentals

https://www.2passeasy.com/dumps/210-250/

NEW QUESTION 1
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 2
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 3
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

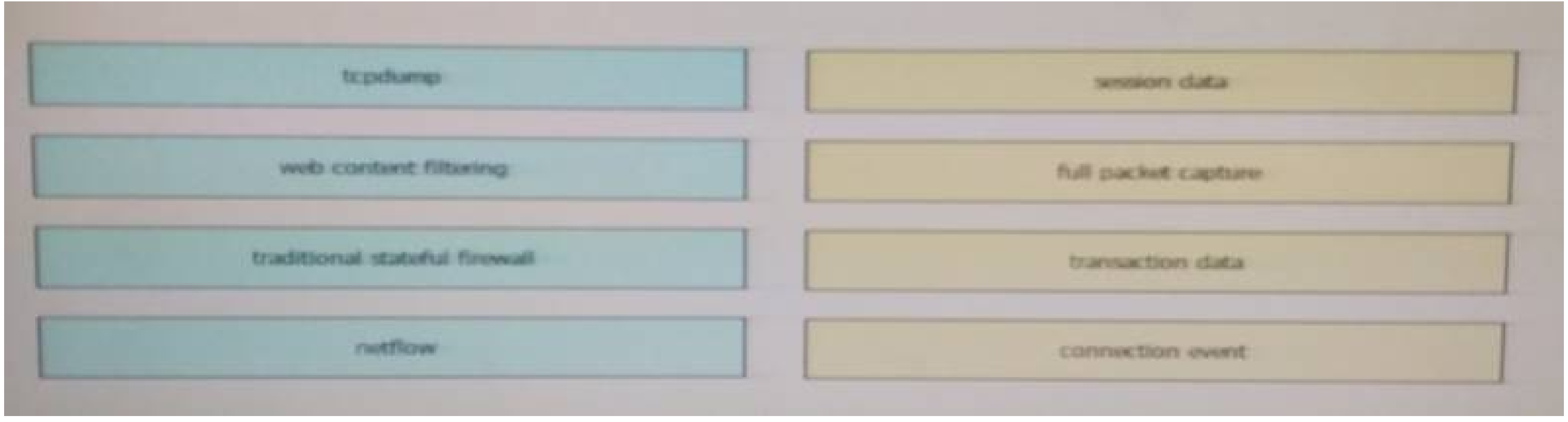
Answer: A

NEW QUESTION 4
Which hashing algorithm is the least secure?

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

Answer: A

NEW QUESTION 5
Drag the technology on the left to the data type the technology provides on the right.



tcpdump	session data
web content filtering	full packet capture
traditional stateful firewall	transaction data
netflow	connection event

Answer:

Explanation: TCPDump = Full packet capture Netflow =Sesion Data
Traditional stateful firewall = Connection Event Web content filtering = Transaction Data

NEW QUESTION 6
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 7
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 8
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 9
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 10
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 10
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 13
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 15
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 18
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 20
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 21
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 26
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 31
Which Linux terminal command can be used to display all the processes?

A. ps –ef
B. ps –u
C. ps –d
D. ps –m

Answer: A

NEW QUESTION 35
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 37
Which type of attack occurs when an attacker utilizes ABotnet to reflect requests off an NTP server to overwhelm their target?

A. man in the middle
B. denial of service
C. distributed denial of service
D. replay

Answer: C

NEW QUESTION 39
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 40
Which identifier is used to describe the application or process that submitted a log message?

A. action
B. selector
C. priority
D. facility

Answer: D

NEW QUESTION 45
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 50
A child process that's permitted to continue on its own after its parent process is terminated. What is that child process called?

A. Leaf.
B. Child tab.
C. Orphan
D. Zombie.

Answer: C

NEW QUESTION 51
Which vulnerability is an example of Heartbleed?

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

Answer: D

NEW QUESTION 53
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 54
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 57
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 61
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 66
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 70
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 75
At which OSI layer does a router typically operate?

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

Answer: B

NEW QUESTION 80
In which technology is network level encrypted not natively incorporated?

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

Answer: A

NEW QUESTION 82
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 87
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 89
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 92
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 96
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 100
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 101
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 106
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 110
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: A

NEW QUESTION 112
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 116
Which information security property is supported by encryption?

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

Answer: C

NEW QUESTION 119
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 124
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 125
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 127
Which cryptographic key is contained in an X.509 certificate?

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

Answer: B

NEW QUESTION 129
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 133
What is PHI?

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

Answer: B

NEW QUESTION 135
Netflow uses which format?

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

Answer: C

NEW QUESTION 139
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 140
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 143
which protocol helps to synchronizes and correlate events across multiple network devices:

A. NTP
B. time zone
C. SNMP
D. CDP

Answer: A

NEW QUESTION 145
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 149
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 152
Which hash algorithm is the weakest?

A. SHA-512
B. RSA 4096
C. SHA-1
D. SHA-256

Answer: C

NEW QUESTION 153
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 154
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

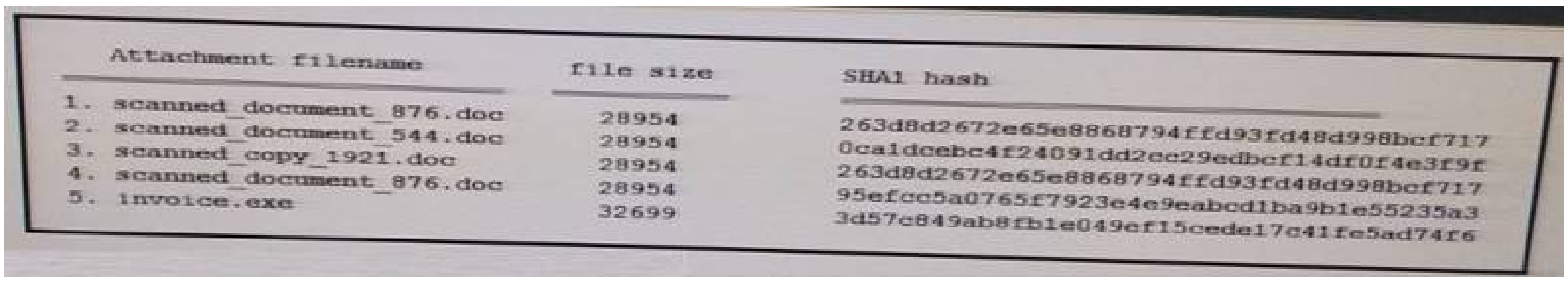
Answer: C

NEW QUESTION 155
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 158
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 159
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 163
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 165
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 166
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 171
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 173
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 174
Which encryption algorithm is the strongest?

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

Answer: A

NEW QUESTION 179
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 180
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 181
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 186
What type of algorithm uses the same key to encrypt and decrypt data?

A. A symmetric algorithm
B. An asymmetric algorithm
C. A public key infrastructure algorithm
D. An IP security algorithm

Answer: A

NEW QUESTION 188
......