Cisco

Exam Questions 210-255

Implementing Cisco Cybersecurity Operations

NEW QUESTION 1
Which option is unnecessary for determining the appropriate containment strategy according to NIST.SP800-61 r2?

A. effectiveness of the strategy
B. time and resource needed to implement the strategy
C. need for evidence preservation
D. attack vector used to compromise the system

Answer: D

NEW QUESTION 2
The united State CERT provides cybersecurity protection to Federal, civilian, and executive branch agencies through intrusion detection and prevention capabilities. Which type of incident response team is this an example of?

A. Federal PSIRT
B. National PSIRT
C. National CSIRT
D. Federal CSIRT

Answer: B

NEW QUESTION 3
Which statement about the collected evidence data when performing digital forensics is true?

A. it must be preserved and its integrity verified.
B. It must be copied to external storage media and immediately distributed to the CISO.
C. It must be stored in a forensics lab only by the data custodian.
D. It must be deleted as soon as possible due to PCI compliance.

Answer: A

NEW QUESTION 4
Which value in profiling servers in a system is true?

A. it can identify when network performance has decreased
B. it can identify servers that have been exploited
C. it can identify when network ports have been connected
D. it can protect the address space of critical hosts.

Answer: A

NEW QUESTION 5
Which of the following is typically a responsibility of a PSIRT?

A. Configure the organization's firewall
B. Monitor security logs
C. Investigate security incidents in a security operations center (SOC)
D. Disclose vulnerabilities in the organization's products and services

Answer: D

NEW QUESTION 6
Which option allows a file to be extracted from a TCP stream within Wireshark?

A. File > Export Objects
B. Analyze > Extract
C. Tools > Export > TCP
D. View > Extract

Answer: A

NEW QUESTION 7
Which file system has 32 bits assigned to the address clusters of the allocation table?

A. FAT32
B. NTFS
C. EXT4
D. FAT16

Answer: A

NEW QUESTION 8
Which of the following has been used to evade IDS and IPS devices?

A. SNMP
B. HTTP
C. TNP
D. Fragmentation

Answer: D

NEW QUESTION 9
Which of the following is not true about listening ports?

A. A listening port is a port held open by a running application in order to accept inbound connections.
B. Seeing traffic from a known port will identify the associated service.
C. Listening ports use values that can range between 1 and 65535.
D. TCP port 80 is commonly known for Internet traffic.

Answer: B

NEW QUESTION 10
Which statement about threat actors is true?

A. They are any company assets that are threatened.
B. They are any assets that are threatened.
C. They are perpetrators of attacks.
D. They are victims of attacks.

Answer: C

Explanation: A threat actor is an individual or a group of individuals who are responsible for a malicious incident that negatively impacts the security posture of an organization. Threat actors can be further categorized by a combination of skill level, type of activity within the network, and their pursuing motivations.

NEW QUESTION 10
Which option is generated when a file is run through an algorithm and generates a string specific to the contents of that file?

A. URL
B. hash
C. IP address
D. destination port

Answer: B

NEW QUESTION 12
Which CVSSv3 metric captures the level of access that is required for a successful attack?

A. attack vector
B. attack complexity
C. privileges required
D. user interaction

Answer: C

Explanation: Privileges RequiredThe new metric, Privileges Required, replaces the Authentication metric of v2.0. Instead of measuring the number of times an attacker must separately authenticate to a system, Privileges Required captures the level of access required for a successful attack. Specifically, the metric values High, Low, and None reflect the privileges required by an attacker in order to exploit the vulnerability.

NEW QUESTION 14
Which example of a precursor is true?

A. An admin finds their password has been changed.
B. A log indicating a port scan was run against a host.
C. A notification that a host is infected with malware.
D. A device configuration changed from the baseline without an audit log entry.

Answer: B

NEW QUESTION 19
Which string matches the regular expression r(ege)+x?

A. rx
B. regeegex
C. r(ege)x
D. rege+x

Answer: B

NEW QUESTION 24
Which element can be used by a threat actor to discover a possible opening into a target network and can also be used by an analyst to determine the protocol of the malicious traffic?

A. TTLs
B. ports
C. SMTP replies
D. IP addresses

Answer: B

NEW QUESTION 28
Which regular expression matches "color" and "colour"?

A. col[0-9]+our
B. colo?ur
C. colou?r
D.]a-z]{7}

Answer: C

NEW QUESTION 31
Which option can be addressed when using retrospective security techniques?

A. if the affected host needs a software update
B. how the malware entered our network
C. why the malware is still in our network
D. if the affected system needs replacement

Answer: C

NEW QUESTION 36
Based on nistsp800-61R2 what are the recommended protections against malware? Malware prevention software

Answer:

NEW QUESTION 41
Which of the following steps in the kill chain would come before the others?

A. C2
B. Delivery
C. Installation
D. Exploitation

Answer: B

NEW QUESTION 44
Which Linux file system allows unlimited folder subdirectory structure

A. ext4
B. ext3
C. ext2
D. NTFS

Answer: A

NEW QUESTION 47
Which two options can be used by a threat actor to determine the role of a server? (Choose two.)

A. PCAP
B. tracert
C. running processes
D. hard drive configuration
E. applications

Answer: CE

NEW QUESTION 51
You see 100 HTTP GET and POST requests for various pages on one of your web servers. The user agent in the requests contain php code that, if executed, creates and writes to a new php file on the webserver. Which category does this event fall under as defined in the Diamond Model of Intrusion?

A. delivery
B. reconnaissance

C. action on objectives
D. installation
E. exploitation

Answer: A

NEW QUESTION 56
Which two potions about deterministic and probabilistic analysis are true? (Choose two.)

A. probabilistic analysis uses data known beforehand and deterministic analysis is based off assumptions.
B. Deterministic analysis uses data known beforehand and probabilistic analysis based off of assumptions.
C. Deterministic analysis is based off of assumptions
D. Probabilistic analysis result in a result that is definitive.
E. probabilistic analysis results in a result that is not definitive.

Answer: BE

NEW QUESTION 57
Refer to the exhibit.

No.	Time	Source	Destination	Protocol	Length	Info
1878	6.473353	173.37.145.84	10.0.2.15	TCP	62	80-49522 [ACK] Seq=14404 ACK=2987 Win=65535 Len=0
1986	6.736855	173.37.145.84	10.0.2.15	HTTP	245	HTTP/1.1 304 Not Modified
1987	6.736873	10.0.2.15	173.37.145.84	TCP	56	49522-80 [ACK] Seq=2987 ACK=14593 Win=59640 Len=0
2317	7.245088	10.0.2.15	173.37.145.84	TCP	2976	[TCP segment of a reassembled PDU]
2318	7.245192	10.0.2.15	173.37.145.84	HTTP	1020	GET /web/fw/1/ntpagetag.gif?js=14ts=1476292607552.2866tc
2321	7.246633	173.37.145.84	10.0.2.15	TCP	62	80-49522 [ACK] Seq=14593 ACK=4447 Win=65535 Len=0
2322	7.246640	173.37.145.84	10.0.2.15	TCP	62	80-49522 [ACK] Seq=14593 ACK=5907 Win=65535 Len=0
2323	7.246642	173.37.145.84	10.0.2.15	TCP	62	80-49522 [ACK] Seq=14593 ACK=6871 Win=65535 Len=0
2542	7.512750	173.37.145.84	10.0.2.15	HTTP	442	HTTP/1.1 200 OK (GIF89a)
2543	7.512781	10.0.2.15	173.37.145.84	TCP	56	49522-80 [ACK] Seq=6871 ACK=14979 Win=62480 Len=0

Which packet contains a file that is extractable within Wireshark?

A. 1986
B. 2318
C. 2542
D. 2317

Answer: C

NEW QUESTION 59
Which information must be left out of a final incident report?

A. server hardware configurations
B. exploit or vulnerability used
C. impact and/or the financial loss
D. how the incident was detected

Answer: A

NEW QUESTION 60
How do you enforce network access control automatically?

A. IGMP
B. SNMP
C. 802.1X
D. Port Security

Answer: C

NEW QUESTION 61
A user on your network receives an email in their mailbox that contains a malicious attachment. There is no indication that the file was run. Which category as defined in the Diamond Model of Intrusion does this activity fall under?

A. reconnaissance
B. weaponization
C. delivery
D. installation

Answer: C

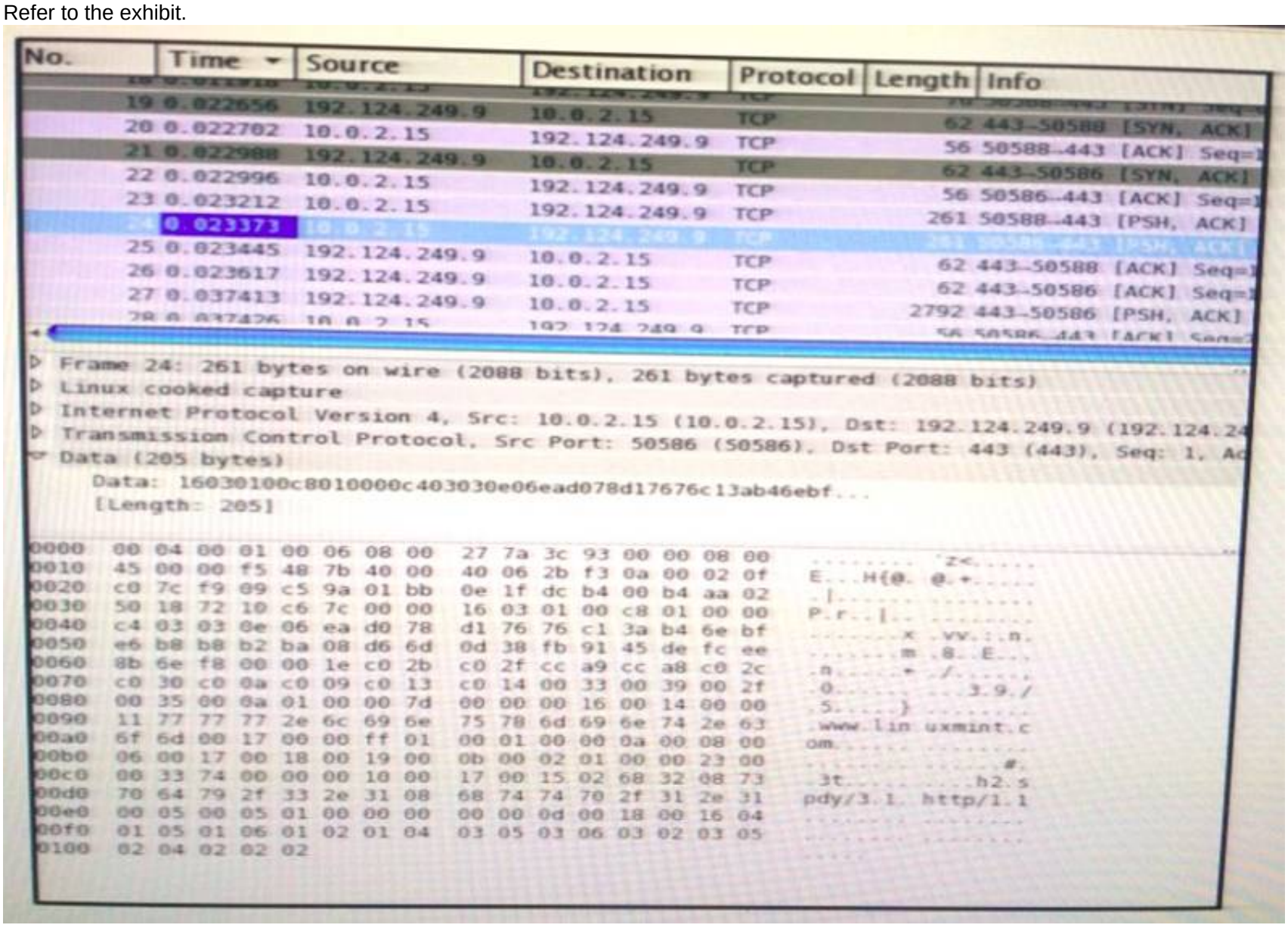
NEW QUESTION 65
Which data type is protected under the PCI compliance framework?

A. credit card type
B. primary account number
C. health conditions
D. provision of individual care

Answer: B

Explanation: From PCI security standards, PAN or Primary Account Number is the correct Answer
https://www.pcisecuritystandards.org/documents/PCI%20SSC%20Quick%20Reference%20Guide.pdf

NEW QUESTION 66
Refer to the exhibit.



Which application protocol is in this PCAP file?

A. TCP
B. SSH
C. HTTP
D. SSL

Answer: D

Explanation: If we are looking at the OSI model then SSL/TLS would sit at the presentation layer as it provides encryption services, but SSL/TLS also establishes an encrypted communication session therefore SSL/TLS is also seen as part of session layer (layer 5 of the OSI model). It will also guarantee the authenticity of a Server by properly authenticating the required authentication challenges. Authentication works at Layer 7.If we are referring to the TCP/IP model, then it is entirely acceptable that SSL is seen as an application layer protocol as layers 5,6 & 7 of the OSI are mapped to the Application layer in TCP/IP model.TCP is not an application layer protocol – it is seen as the Transport layer protocol in both models.

NEW QUESTION 69
Which element is part of an incident response plan?

A. organizational approach to incident response
B. organizational approach to security
C. disaster recovery
D. backups

Answer: A

NEW QUESTION 73
In VERIS, an incident is viewed as a series of events that adversely affects the information assets of an organization. Which option contains the elements that every event is comprised of according to VERIS incident model'?

A. victim demographics, incident description, incident details, discovery & response
B. victim demographics, incident details, indicators of compromise, impact assessment
C. actors, attributes, impact, remediation
D. actors, actions, assets, attributes

Answer: D

NEW QUESTION 78
What is the process of remediation the network and systems and/or reconstructing so the responsible threat actor can be revealed?

A. Data analysis
B. Assets distribution
C. Evidence collection
D. Threat actor distribution

Answer: A

NEW QUESTION 81
Which of the following are examples of some of the responsibilities of a corporate CSIRT and the policies it helps create? (Select all that apply.)

A. Scanning vendor customer networks
B. Incident classification and handling
C. Information classification and protection
D. Information dissemination
E. Record retentions and destruction

Answer: BCDE

NEW QUESTION 85
Which of the following is an example of a managed security offering where incident response experts monitor and respond to security alerts in a security operations center (SOC)?

A. Cisco CloudLock
B. Cisco's Active Threat Analytics (ATA)
C. Cisco Managed Firepower Service
D. Cisco Jasper

Answer: B

NEW QUESTION 89
Which CVSSv3 metric value increases when attacks consume network bandwidth, processor cycles, or disk space?

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

Answer: C

Explanation: Availability Impact (A): This metric measures the impact to the availability of the impacted component resulting from a successfully exploited vulnerability. While the confidentiality and integrity impact metrics apply to the loss of confidentiality or integrity of data such as information and files used by the impacted component, this metric refers to the loss of availability of the impacted component itself, such as a networked service such as web, database, and email. Because availability refers to the accessibility of information resources, attacks that consume network bandwidth, processor cycles, or disk space all impact the availability of an impacted component.

NEW QUESTION 94
According to NIST-SP800-61R2, which option should be contained in the issue tracking system?

A. incidents related to the current incident
B. incident unrelated to the current incident
C. actions taken by nonincident handlers
D. latest public virus signatures

Answer: A

NEW QUESTION 99
What is the difference between deterministic and probabilistic assessment method? (Choose Two)

A. At deterministic method we know the facts beforehand and at probabilistic method we make assumptions
B. At probabilistic method we know the facts beforehand and at deterministic method we make assumptions
C. Probabilistic method has an absolute nature

D. Determinstc method has an absolute nature

Answer: AD

NEW QUESTION 104
Which are two security goals of data normalization? (Choose two.)

A. increase data exposure
B. purge redundant data
C. create data for attraction
D. maintain data integrity
E. reduce size of data on disk

Answer: BD

NEW QUESTION 106
What is the common artifact that is used to uniquely identify a detected file?

A. Hash
B. Timestamp
C. File size

Answer: A

NEW QUESTION 109
You have run a suspicious file in a sandbox analysis tool to see what the file does. The analysis report shows that outbound callouts were made post infection. Which two pieces of information from the analysis report are needed or required to investigate the callouts? (Choose two.)

A. file size
B. domain names
C. dropped files
D. signatures
E. host IP addresses

Answer: BE

NEW QUESTION 110
Which HTTP header field is usually used in forensics to identify the type of browser used?

A. accept-language
B. user-agent
C. referrer
D. host

Answer: B

NEW QUESTION 112
You have a video of a suspect entering a data center that was captured on the same that files in the same data center were transferred to a computer. Which type of is this?

A. Physical evidence
B. best evidence
C. prima faice evidence
D. indirect evidence

Answer: D

NEW QUESTION 114
Which function does an internal CSIRT provide?

A. incident handling services across various CSIRTs
B. incident handling services for a country's government
C. incident handling services for a parent organizationD incident handling services as a service for other organization

Answer: C

NEW QUESTION 118
In addition to cybercrime and attacks, evidence found on a system or network may be presented in a court of law to support accusations of crime or civil action, including which of the following?

A. Fraud, money laundering, and theft
B. Drug-related crime
C. Murder and acts of violence
D. All of the above

Answer: D

NEW QUESTION 122
Which incident handling is focused on minimizing the impact of an incident?

A. Scoping
B. Reporting
C. Containment
D. Eradication

Answer: D

NEW QUESTION 126
Which of the following are core responsibilities of a national CSIRT and CERT?

A. Provide solutions for bug bounties
B. Protect their citizens by providing security vulnerability information, security awareness training, best practices, and other information
C. Provide vulnerability brokering to vendors within a country
D. Create regulations around cybersecurity within the country

Answer: B

NEW QUESTION 130
What are the metric values of the confidentiality based on the CVSS framework?

A. Low-high
B. Low –Medium-high
C. High-Low-none
D. High-none

Answer: C

NEW QUESTION 133
Which type of analysis shows what the outcome is as well how likely each outcome is?

A. exploratory
B. descriptive
C. probabilistic
D. deterministic

Answer: D

NEW QUESTION 134
Which precursor example is true?

A. Admin finds their password has been changed
B. A log scan indicating a port scan against a host
C. A network device configuration has been changed

Answer: B

NEW QUESTION 136
Refer to the exhibit.

Severity	Date	Time	Sig ID	Source IP	Source Port	Dest IP	Dest Port	Description
6	Jan 15 2016	05:15:22	33883	62.5.22.54	22557	198.168.5.22	53	-

Which type of log is this an example of?

A. IDS log
B. proxy log
C. NetFlow log
D. syslog

Answer: C

NEW QUESTION 139
Which of the following are the three metrics, or "scores," of the Common Vulnerability Scoring System (CVSS)? (Select all that apply.)

A. Baseline score
B. Base score
C. Environmental score
D. Temporal score

Answer: BCD

NEW QUESTION 144
Which option filters a LibPCAP capture that used a host as a gateway?

A. tcp|udp] [src|dst] port <port>
B. [src|dst] net <net> [{mask <mask>}|{len <len>}]
C. ether [src|dst] host <ehost>
D. gateway host <host>

Answer: D

Explanation: This primitive allows you to filter on packets that used host as a gateway. That is, where the Ethernet source or destination was host but neither the source nor destination IP address was host.

NEW QUESTION 147
Which component of the NIST SP800-61 r2 incident handling strategy reviews data?

A. preparation
B. detection and analysis
C. containment, eradication, and recovery
D. post-incident analysis

Answer: D

Explanation: 3.4.2 Using Collected Incident Data (which falls under post incident analysis in the aforementioned document)Lessons learned activities should produce a set of objective and subjective data regarding each incident.Over time, the collected incident data should be useful in several capacities. The data, particularly the total hours of involvement and the cost, may be used to justify additional funding of the incident response team. A study of incident characteristics may indicate systemic security weaknesses and threats, as wellas changes in incident trends. This data can be put back into the risk assessment process, ultimately leading to the selection and implementation of additional controls. Another good use of the data is measuring the success of the incident response team. If incident data is collected and stored properly, it should provide several measures of the success (or at least the activities) of the incident response team.Incident data can also be collected to determine if a change to incident response capabilities causes a corresponding change in the team's performance (e.g., improvements in efficiency, reductions in costs).

NEW QUESTION 150
Which command can be used to find open ports on a system?

A. netstat -I
B. netstat -v
C. netstat -r
D. netstat-g

Answer: A

NEW QUESTION 152
Which CSIRT category provides incident handling services to their parent organization such as a bank, a manufacturing company, a university, or a federal agency?

A. internal CSIRT
B. national CSIRT
C. coordination centers
D. analysis centers
E. vendor teams
F. incident response providers

Answer: A

NEW QUESTION 153
Which of the following are examples of some of the responsibility of a corporate CSIRT and the policies it helps create? (Choose four)

A. Scanning vendor customer network
B. incident classification and handling
C. Information classification and protection
D. Information dissemination
E. Record retentions and destruction

Answer: BCDE

NEW QUESTION 158
Which technology is the leading industry approach used to automatically enforce NAC?

A. SNMP
B. port security
C. IGMP

D. 802.1x

Answer: D

NEW QUESTION 162
According to NIST 86, which action describes the volatile data collection?

A. Collect data before rebooting
B. Collect data while rebooting
C. Collect data after rebooting
D. Collect data that contains malware

Answer: A

NEW QUESTION 166
Refer to the exhibit.

Threat Intelligence:

IP Address	Reputation (-100 to 100 higher is safer)
ABC.example.com	25
DEF.example.com	-75
FGH.example.com	0
XYZ.example.com	75

DNS Information:

Domain Name	IP Address
ABC.example.com	209.165.201.10
DEF.example.com	209.165.201.130
FGH.example.com	209.165.200.230
XYZ.example.com	209.165.202.25

Session Logs:

Source	Destination	Protocol
10.0.1.1/5567	209.165.201.130/443	TCP
10.0.1.2/8012	209.165.201.10/80	TCP
10.0.1.10/8125	209.165.200.230/80	TCP
10.0.1.20/9765	209.165.202.25/443	TCP

Which host is likely connecting to a malicious site?

A. 10.0.1.10
B. 10.0.1.20
C. 10.0.12
D. 10.0.1.1

Answer: D

NEW QUESTION 170
Which option is a misuse variety per VERIS enumerations?

A. snooping
B. hacking
C. theft
D. assault

Answer: B

Explanation: Misuse is defined as the use of entrusted organizational resources or privileges for any purpose or manner contrary to that which was intended. Includes administrative abuse, use policy violations, use of non-approved assets, etc. These actions can be malicious or non-malicious in nature. Misuse is

exclusive to parties that enjoy a degree of trust from the organization, such as insiders and partners.VERIS classification note: There is an action category for Hacking and for Misuse. Both can utilize similar vectors and achieve similar results; in Misuse, the actor was granted access/privileges (and used them inappropriately), whereas with Hacking, access/privileges are obtained illegitimately.

NEW QUESTION 172
To which category do attributes belong within the VERIS schema ?

A. victim demographics
B. incident tracking
C. Discovery and response
D. incident description

Answer: D

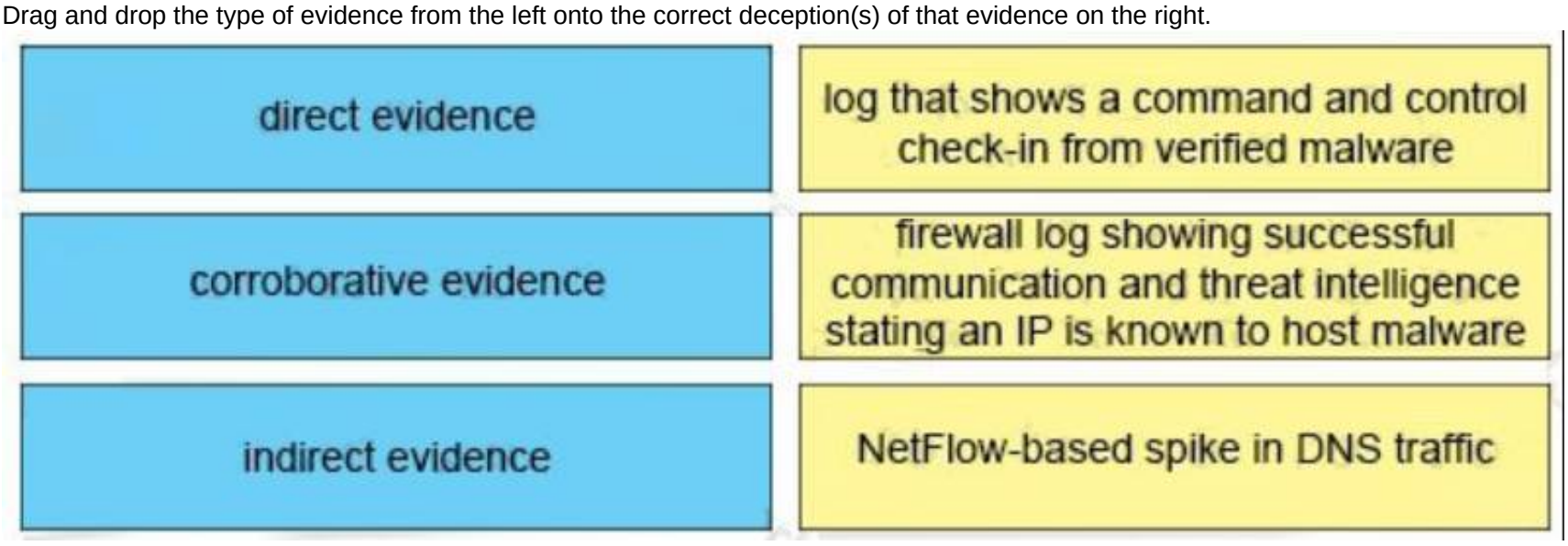
NEW QUESTION 175
Which expression creates a filter on a host IP address or name?

A. [src|dst] host <host >
B. [tcp|udp] [src|dst] port<port>
C. ether [src|dst] host<ehost>
D. gateway host <host>

Answer: A

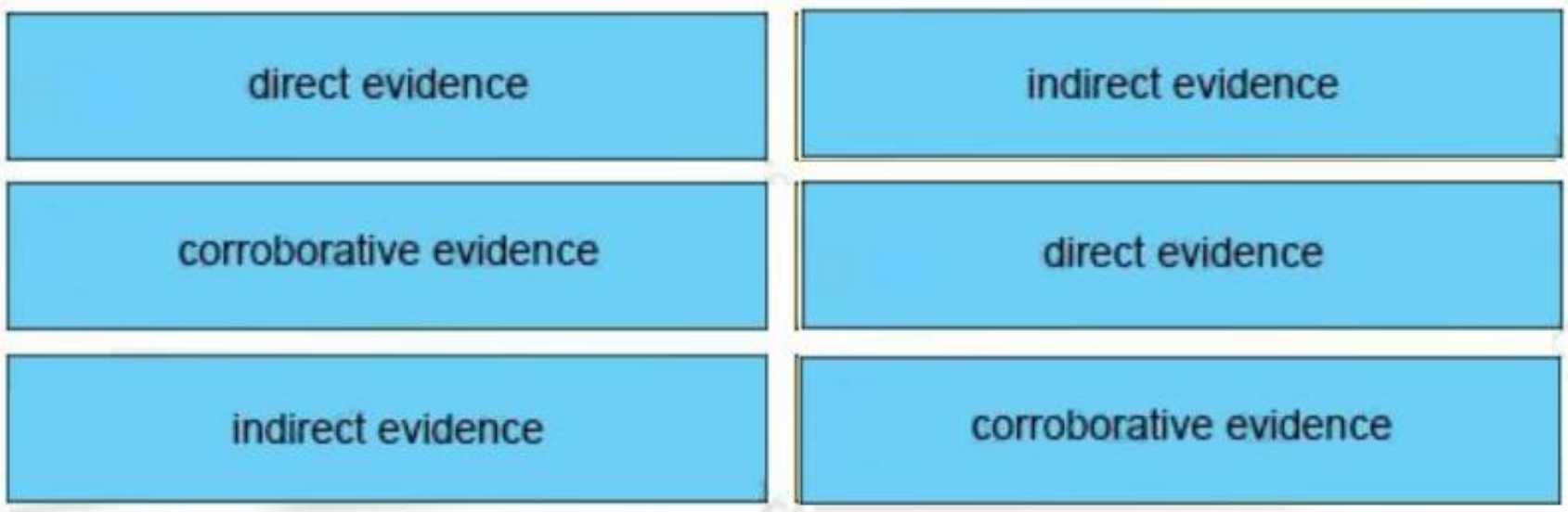
Explanation: https://www.wireshark.org/docs/wsug_html_chunked/ChCapCaptureFilterSection.html

NEW QUESTION 176
Drag and drop the type of evidence from the left onto the correct deception(s) of that evidence on the right.

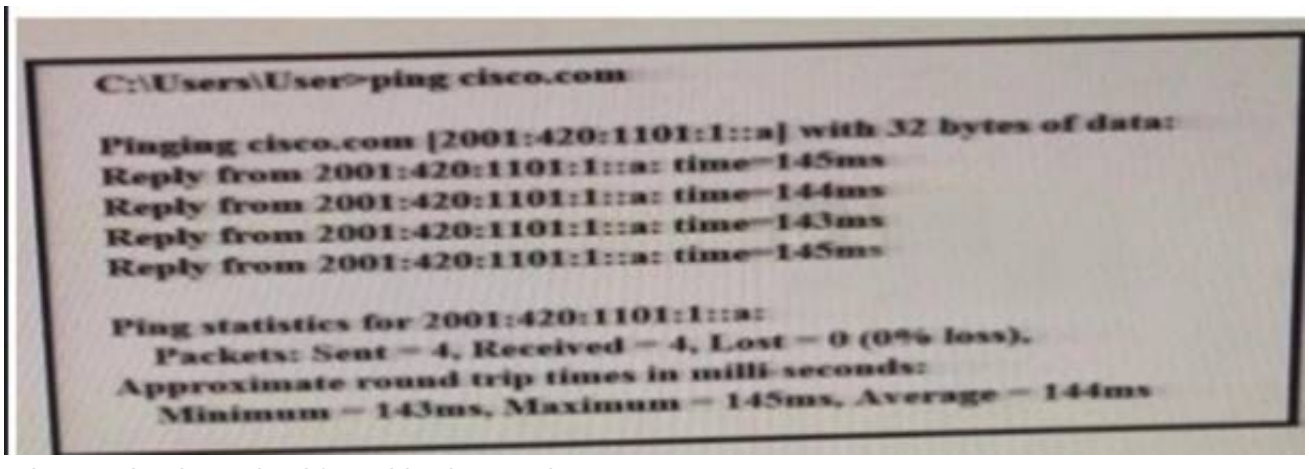


Answer:

Explanation:



NEW QUESTION 178
Refer to the exhibit.



What can be determined from this ping result?

A. The public IP address of cisco.com is 2001:420:1101:1::a.
B. The Cisco.com website is down.
C. The Cisco.com website is responding with an internal IP.
D. The public IP address of cisco.com is an IPv4 address.

Answer: A

NEW QUESTION 180
Which CVSS metric describes the conditions that are beyond the attackers control so that an attack can be successful?

A. User interaction
B. Attack vector
C. attack complexity
D. privileges required

Answer: C

NEW QUESTION 181
Which of the following is not an example of the VERIS main schema categories?

A. Incident tracking
B. Victim demographics
C. Incident descriptions
D. Incident forensics ID

Answer: D

NEW QUESTION 182
Which of the following is one of the main goals of data normalization?

A. To save duplicate logs for redundancy
B. To purge redundant data while maintaining data integrity
C. To correlate IPS and IDS logs with DNS
D. To correlate IPS/IDS logs with firewall logs

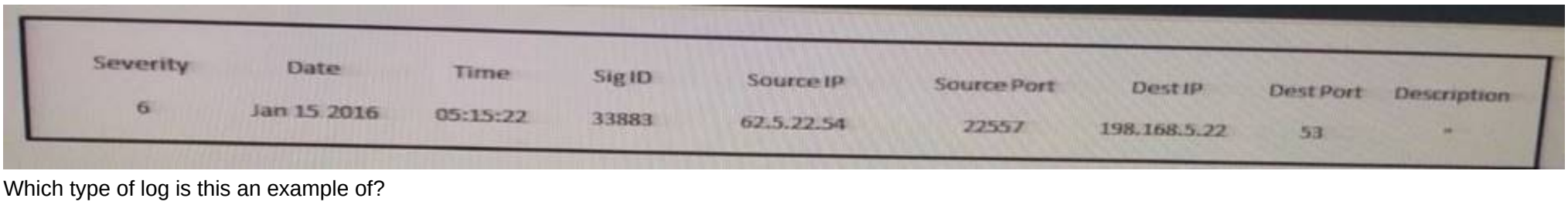
Answer: B

NEW QUESTION 187
Which type of intrusion event is an attacker retrieving the robots. txt file from target site?

A. exploitation
B. weaponization
C. scanning
D. reconnaissance

Answer: D

NEW QUESTION 190
Refer to the exhibit.



Severity	Date	Time	Sig ID	Source IP	Source Port	Dest IP	Dest Port	Description
6	Jan 15 2016	05:15:22	33883	62.5.22.54	22557	198.168.5.22	53	-

Which type of log is this an example of?

A. syslog
B. NetFlow log
C. proxy log
D. IDS log

Answer: B

Explanation: A typical output of a NetFlow command line tool (nfdump in this case) when printing the stored flows may look as follows:
Date flow start Duration Proto Src IP Addr:Port Dst IP Addr:Port Packets Bytes Flows2010-09-01 00:00:00.459 0.000 UDP 127.0.0.1:24920 -> 192.168.0.1:22126 1 46 12010-09-01 00:00:00.363 0.000 UDP 192.168.0.1:22126 -> 127.0.0.1:24920 1 80 1

NEW QUESTION 195
Which description of a retrospective malware detection is true?

A. You use Wireshark to identify the malware source.
B. You use historical information from one or more sources to identify the affected host or file.
C. You use information from a network analyzer to identify the malware source.
D. You use Wireshark to identify the affected host or file.

Answer: B

NEW QUESTION 200
Which two statements correctly describe the victim demographics section of the VERIS schema? (Choose two.)

A. The victim demographics section describes but does not identify the organization that is affected by the incident.
B. The victim demographics section compares different types of organizations or departments within a single organization.
C. The victim demographics section captures general information about the incident.
D. The victim demographics section uses geolocation data to identify the organization name of the victim and the threat actor.

Answer: AB

NEW QUESTION 203
Which type verification typically consists of using tools to compute the message digest of the original and copies data, then comparing the digests to make sure that they are the same?

A. evidence collection order
B. data integrity
C. data preservation
D. volatile data collection

Answer: B

NEW QUESTION 207
Which option has a drastic impact on network traffic because it can cause legitimate traffic to be blocked?

A. true positive
B. true negative
C. false positive
D. false negative

Answer: C

NEW QUESTION 208
You receive an alert for malicious code that exploits Internet Explorer and runs arbitrary code on the site visitor machine. The malicous code is on an external site that is being visited by hosts on your network. Which user agent in the HTTP headers in the requests from your internal hosts warrants further investigation?

A. Mozilla/5.0 (compatible, MSIE 10.0, Windows NT 6.2, Trident 6.0)
B. Mozilla/5.0 (XII; Linux i686; rv: 1.9.2.20) Gecko/20110805
C. Mozilla/5.0 (Windows NT 6.1; WOW64; rv: 4O0) Gecko/20100101
D. Opera/9.80 (XII; Linux i686; Ubuntu/14.10) Presto/2.12.388 Version/12.16

Answer: A

NEW QUESTION 210
Which of the following are the three broad categories of cybersecurity investigations?

A. Public, private, and individual investigations
B. Judiciary, private, and individual investigations
C. Public, private, and corporate investigations
D. Government, corporate, and private investigations

Answer: A

NEW QUESTION 212
What does the CSIRT incident response provider usually do?

A. provide incident handling services to their parent organization.
B. provide incident handling services to a country
C. coordinate and facilitate the handling of incidents across various CSIRTs

D. focus on synthesizing data from various sources to determine trends and patterns in incident activity
E. handle reports of vulnerabilities in their software or hardware products
F. offer incident handling services as a for-fee service to other organizations

Answer: F

NEW QUESTION 213
Which CVSS metric describes the conditions that are beyond the attacker's control that must be exist to exploit the vulnerability?

A. attack vector
B. attack complexity
C. privileges required
D. user interaction

Answer: C

NEW QUESTION 216
Choose the option that best describes NIST data integrity

A. use only sha-1
B. use only md5
C. you must hash data & backup and compare hashes
D. no need to hash data & backup and compare hashes

Answer: C

NEW QUESTION 219
Which two potions are the primary 5-tuple components? (Choose two)

A. destination IP address
B. header length
C. sequence number
D. checksum
E. source IP address

Answer: AE

NEW QUESTION 220
Filtering ports in wireshark?

A. tcp.port == 80
B. tcp port equals 80
C. tcp.port 80
D. port 80

Answer: A

NEW QUESTION 222
Which file is allocated with 32 bits?

A. NTFS
B. FAT32
C. FAT
D. ExFAT

Answer: D

NEW QUESTION 224
Which option is the process of remediating the network and systems and/or reconstructing the attack so that the responsible threat actor can be revealed?

A. data analytics
B. asset attribution
C. threat actor attribution
D. evidence collection

Answer: A

NEW QUESTION 229
Which of the following is an example of a coordination center?

A. Cisco PSIRT
B. Microsoft MSRC
C. CERT division of the Software Engineering Institute (SEI)
D. FIRST

Answer: C

NEW QUESTION 233
Which type of analysis allows you to see how likely an exploit could affect your network?

A. descriptive
B. casual
C. probabilistic
D. inferential

Answer: C

Explanation: In deterministic analysis, all data used for the analysis is known beforehand. Probabilistic analysis, on the other hand, is done assuming the likelihood that something will or has happened, but you don't know exactly when or how.

NEW QUESTION 234
From a security perspective, why is it important to employ a clock synchronization protocol on a network?

A. so that everyone knows the local time
B. to ensure employees adhere to work schedule
C. to construct an accurate timeline of events when responding to an incident
D. to guarantee that updates are pushed out according to schedule

Answer: C

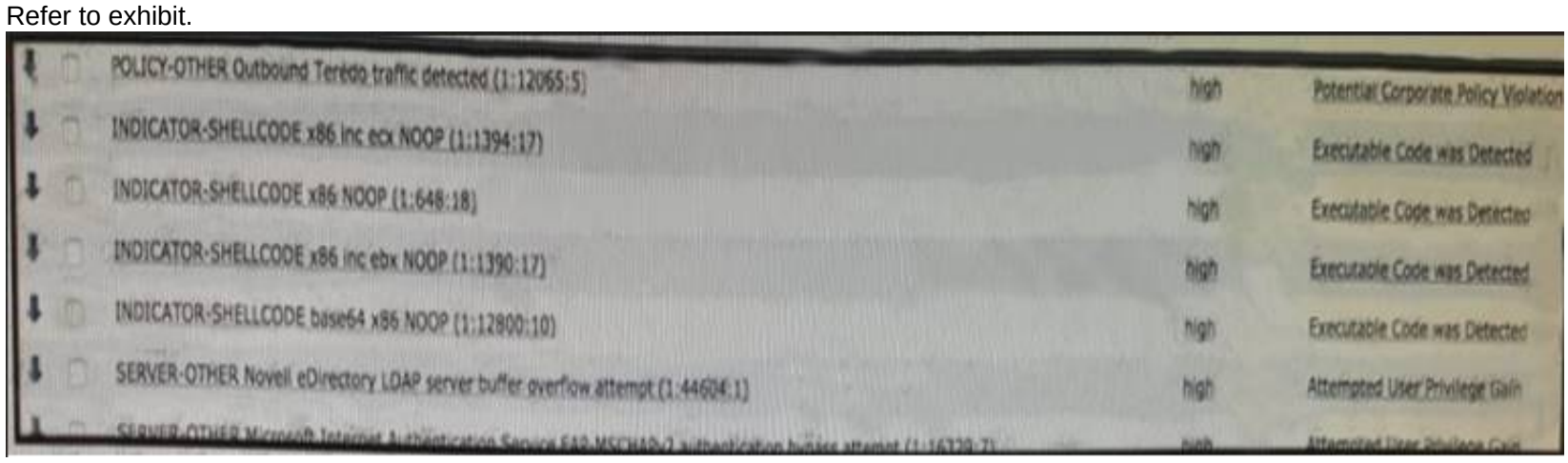
Explanation: The Importance of Time Synchronization for Your NetworkIn modern computer networks time synchronization is critical because every aspect of managing, securing, planning, and debugging a network involves determining when events happen. Time also provides the only frame of reference between all devices on the network. Without synchronized time, accurately correlating log files between these devices is difficult, even impossible. Following are just a few specific reasons:Tracking security breaches, network usage, or problems affecting a large number of components can be nearly impossible if timestamps in logs are inaccurate. Time is often the critical factor that allows an event on one network node to be mapped to a corresponding event on another.To reduce confusion in shared filesystems, it is important for the modification times to be consistent, regardless of what machine the filesystems are on.

NEW QUESTION 237
Which Cyber Kill Model category does attacking vulnerability belong to?

A. Exploitation
B. Installation
C. Deliver
D. Action on Objectives

Answer: A

NEW QUESTION 238
Refer to exhibit.



Which option is the logical source device for these events?

A. web server
B. NetFlow collector
C. proxy server
D. IDS/IPS

Answer: A

NEW QUESTION 242
You see confidential data being exfiltrated to an IP address that is attributed to a known Advanced Persistent Threat group. Assume that this is part of a real attach and not a network misconfiguration. Which category does this event fall under as defined in the Diamond Model of Intrusion?

A. reconnaissance
B. weaponization
C. delivery
D. action on objectives

Answer: D

Explanation: It is an Advanced Persistent Threat group that being exfiltrated confidential data, and Action and Objectives says that adversary is inside the network and starting to achieve his or her objective for launching the attack. An adversary could use this opportunity to steal data.

NEW QUESTION 245
Which event artifact can be used to identify HTTP GET requests for a specific file?

A. HTTP status code
B. TCP ACK
C. destination IP
D. URI

Answer: D

NEW QUESTION 250
Which element is included in an incident response plan?

A. organization mission
B. junior analyst approval
C. day-to-day firefighting
D. siloed approach to communications

Answer: A

Explanation: The incident response plan should include the following elements:
– Mission– Strategies and goals– Senior management approval– Organizational approach to incident response– How the incident response team will communicate with the rest of the organization and with other organizations– Metrics for measuring the incident response capability and its effectiveness– Roadmap for maturing the incident response capability– How the program fits into the overall organization.

NEW QUESTION 255
What define the roadmap for implementing the incident response capability?

A. incident response plan
B. incident response procedure
C. incident handling guide
D. incident response policy

Answer: A

NEW QUESTION 257
When performing threat hunting against a DNS server, which traffic toward the affected domain is considered a starting point?

A. HTTPS traffic
B. TCP traffic
C. HTTP traffic
D. UDP traffic

Answer: D

NEW QUESTION 259
Which statement about collecting data evidence when performing digital forensics is true?

A. Allowing unrestricted access to impacted devices
B. Not allowing items of evidence to be physically touch
C. Powering off the device after collecting the data
D. It must be preserved and integrity checked

Answer: D

NEW QUESTION 261
Which of the following is typically a responsibility of a PSIRT (Product SIRT)?

A. Configure the organization’s firewall
B. Monitor security logs
C. Investigate security incidents in a SOC
D. Disclosure vulnerabilities in the organization’s products and services

Answer: D

NEW QUESTION 265
A CMS plugin creates two files that are accessible from the Internet myplugin.html and exploitable.php. A newly discovered exploit takes advantage of an injection vulnerability in exploitable.php. To exploit the vulnerability, one must send an HTTP POST with specific variables to exploitable.php. You see traffic to your webserver that consists of only HTTP GET requests to myplugin.html. Which category best describes this activity?

A. weaponization
B. exploitation
C. installation
D. reconnaissance

Answer: D

NEW QUESTION 269
Which of the following is an example of a managed security offering where incident response experts monitor and respond to security alerts in a SOC?

A. Cisco CloudLock
B. Cisco's Active Threat Analytics (ATA)
C. Cisco Managed Firepower Service
D. Cisco Jasper

Answer: B

NEW QUESTION 271
Refer to the following packet capture. Which of the following statements is true about this packet capture?
00:00:04.549138 IP omar.cisco.com.34548 > 93.184.216.34.telnet: Flags [S], seq 3152949738, win 29200,options [mss 1460,sackOK,TS val 1193148797 ecr 0,nop,wscale 7], length 000:00:05.547084 IP omar.cisco.com.34548 > 93.184.216.34.telnet: Flags [S], seq3152949738, win 29200,options [mss 1460,sackOK,TS val 1193149047 ecr 0,nop,wscale 7], length 000:00:07.551078 IP omar.cisco.com.34548 > 93.184.216.34.telnet: Flags [S], seq3152949738, win 29200, options [mss 1460,sackOK,TS val 1193149548 ecr 0,nop,wscale 7], length 000:00:11.559081 IP omar.cisco.com.34548 > 93.184.216.34.telnet: Flags [S], seq3152949738, win 29200,options [mss 1460,sackOK,TS val 1193150550 ecr 0,nop,wscale 7], length 0

A. The host with the IP address 93.184.216.34 is the source.
B. The host omar.cisco.com is the destination.
C. This is a Telnet transaction that is timing out and the server is not responding.
D. The server omar.cisco.com is responding to 93.184.216.34 with four data packets.

Answer: C

NEW QUESTION 274
What mechanism does the Linux operating system provide to control access to files?

A. privileges required
B. user interaction
C. file permissions
D. access complexity

Answer: C

NEW QUESTION 277
Which two components are included in a 5-tuple? (Choose two.)

A. port number
B. destination IP address
C. data packet
D. user name
E. host logs

Answer: AB

Explanation: The source and destination addresses are primary 5-tuple components. The source address is the IP address of the network that creates and sends a data packet, and the destination address is the recipient.

NEW QUESTION 281
Employees are allowed access to internal websites. An employee connects to an internal website and IDS reports it as malicious behavior. What is this example of?

A. true positive
B. false negative
C. false positive
D. true negative

Answer: C

NEW QUESTION 286
You have a video of suspect entering your office the day your data has being stolen?

A. Direct evidence
B. Indirect
C. Circumstantial

Answer:

B

NEW QUESTION 291

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons and Answers in PDF Format

210-255 Practice Exam Features:

* 210-255 Questions and Answers Updated Frequently

* 210-255 Practice Questions Verified by Expert Senior Certified Staff

* 210-255 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* 210-255 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year