



Cisco

Exam Questions 210-255

Implementing Cisco Cybersecurity Operations

NEW QUESTION 1

During which phase of the forensic process are tools and techniques used to extract the relevant information from the collective data?

- A. examination
- B. reporting
- C. collection
- D. investigation

Answer: A

Explanation: Examinations involve forensically processing large amounts of collected data using a combination of automated and manual methods to assess and extract data of particular interest, while preserving the integrity of the data. Forensic tools and techniques appropriate to the types of data that were collected are executed to identify and extract the relevant information from the collected data while protecting its integrity. Examination may use a combination of automated tools and manual processes.

NEW QUESTION 2

Which network device creates and sends the initial packet of a session?

- A. source
- B. origination
- C. destination
- D. network

Answer: A

NEW QUESTION 3

During which phase of the forensic process is data that is related to a specific event labeled and recorded to preserve its integrity?

- A. collection
- B. examination
- C. reporting
- D. investigation

Answer: A

NEW QUESTION 4

The United States 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 5

Which process is being utilized when IPS events are removed to improve data integrity?

- A. data normalization
- B. data availability
- C. data protection
- D. data signature

Answer: A

Explanation: Data normalization is the process of intercepting and storing incoming data so it exists in one form only. This eliminates redundant data and protects the data's integrity.

Link: <https://www.helpnetsecurity.com/2013/01/07/the-importance-of-data-normalization-in-ips/>

NEW QUESTION 6

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 7

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 8

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 9

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 10

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 10

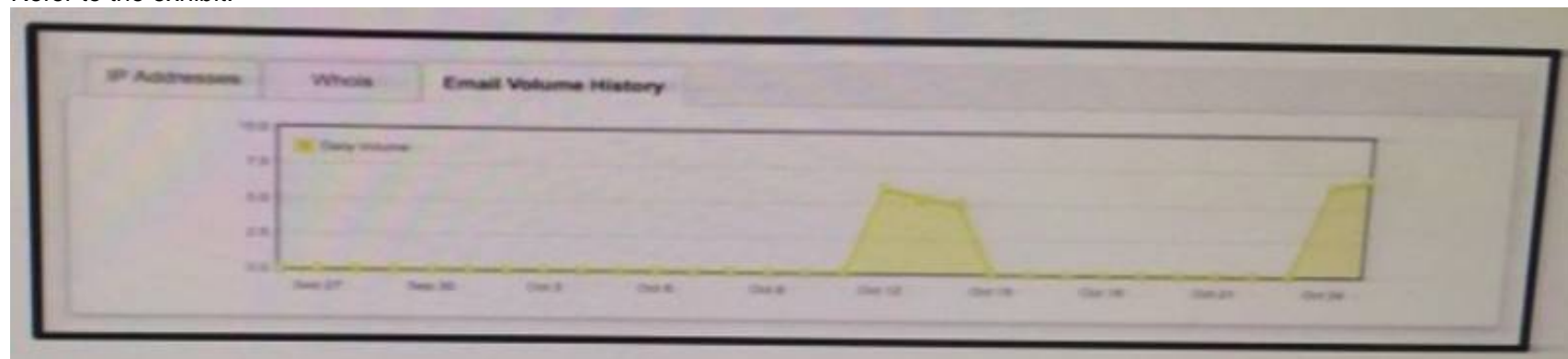
Which of the following is one of the main goals of the CSIRT?

- A. To configure the organization's firewalls
- B. To monitor the organization's IPS devices
- C. To minimize and control the damage associated with incidents, provide guidance for mitigation, and work to prevent future incidents
- D. To hire security professionals who will be part of the InfoSec team of the organization.

Answer: C

NEW QUESTION 15

Refer to the exhibit.



You notice that the email volume history has been abnormally high. Which potential result is true?

- A. Email sent from your domain might be filtered by the recipient.
- B. Messages sent to your domain may be queued up until traffic dies down.
- C. Several hosts in your network may be compromised.
- D. Packets may be dropped due to network congestion.

Answer: C

NEW QUESTION 20

Which identifies both the source and destination location?

- A. IP address
- B. URL
- C. ports
- D. MAC address

Answer: A

Explanation: The IP Address is used to uniquely identify the desired host we need to contact. This information is not shown in the above packet because it exists in the IP header section located right above the TCP header we are analysing. If we were to expand the IP header, we would (certainly) find the source and destination IP Address fields in there.

NEW QUESTION 23

What is accomplished in the identification phase of incident handling?

- A. determining the responsible user
- B. identifying source and destination IP addresses
- C. defining the limits of your authority related to a security event
- D. determining that a security event has occurred

Answer: D

Explanation: From Cisco SECOPS Elearning course Identification phase is referenced as 'Identification: The SOC analyst performs continuous monitoring, and active cyber threat hunting. When a true positive incident has been detected, the incident response team is activated. During the investigation process, the SOC analyst or the incident response team may also contact the CERT/CC (or other security intelligence sources), which tracks Internet security activity and has the most current threat information.'

NEW QUESTION 27

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

Answer:

NEW QUESTION 29

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 32

Which Linux file system allows unlimited folder subdirectory structure

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

Answer: A

NEW QUESTION 35

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

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

Answer: CE

NEW QUESTION 36

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 39

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 41

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 43

Which of the following are not components of the 5-tuple of a flow in NetFlow? (Choose two.)

- A. Source IP address
- B. Flow record ID
- C. Gateway
- D. Source port
- E. Destination port

Answer: BC

NEW QUESTION 48

What are the metric values for confidentiality impact in the CVSS v3.0 framework?

- A. high, low, none
- B. open, closed, obsolete
- C. high, low
- D. high, medium, none

Answer: A

NEW QUESTION 49

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 51

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 56

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 60

In the context of incident handling phases, which two activities fall under scoping? (Choose two.)

- A. determining the number of attackers that are associated with a security incident
- B. ascertaining the number and types of vulnerabilities on your network
- C. identifying the extent that a security incident is impacting protected resources on the network
- D. determining what and how much data may have been affected
- E. identifying the attackers that are associated with a security incident

Answer: CE

NEW QUESTION 62

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 65

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 67

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. Deterministic method has an absolute nature

Answer: AD

NEW QUESTION 71

Which of the following has been used to evade IDS / IPS devices?

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

Answer: D

NEW QUESTION 73

Which option is the common artifact used to uniquely identify a detected file?

- A. file size
- B. file extension
- C. file timestamp
- D. file hash

Answer: D

NEW QUESTION 75

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 77

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 81

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 86

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 87

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

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

Answer: D

NEW QUESTION 90

How is confidentiality defined in the CVSS v3.0 framework?

- A. confidentiality of the information resource managed by person due to an unsuccessfully exploited vulnerability
- B. confidentiality of the information resource managed by a person due to a successfully vulnerability
- C. confidentiality of the information resources managed by a software component due to a successfully exploited vulnerability
- D. confidentiality of the information resource managed by a software component due to an unsuccessfully exploited vulnerability

Answer: C

Explanation: <https://www.first.org/cvss/specification-document>

NEW QUESTION 94

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 99

Which CVSSv3 metric value increases when the attacker is able to modify all files protected by the vulnerable component?

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

Answer: B

Explanation: Consider a vulnerability in an Internet service such as web, email, or DNS that allows an attacker to modify or delete all web files in a directory would incur an impact to Integrity only, rather than Availability. The reason is that the web service is still performing properly – it just happens to be serving back altered content.

NEW QUESTION 104

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 108

Which of the following is not an example of weaponization?

- A. Connecting to a CnC server
- B. Wrapping software with a RAT
- C. Creating a backdoor in an application
- D. Developing an automated script to inject commands on a USB device

Answer: A

NEW QUESTION 113

Which CVSSv3 Attack Vector metric value requires the attacker to physically touch or manipulate the vulnerable component?

- A. local
- B. physical
- C. network
- D. adjacent

Answer: B

Explanation: Attack Vector (AV): This metric reflects the context by which vulnerability exploitation is possible. This metric value and the base score will correlate with an attacker's proximity to a vulnerable component. The score will be higher the more remote (logically and physically) an attacker is from the vulnerable component.

Local: Exploiting the vulnerability requires either physical access to the target or a local (shell) account on the target.

Adjacent: Exploiting the vulnerability requires access to the local network of the target, and cannot be performed across an OSI Layer 3 boundary.

Network: The vulnerability is exploitable from remote networks. Such a vulnerability is often termed "remotely exploitable," and can be thought of as an attack being exploitable one or more network hops away, such as across Layer 3 boundaries from routers.

Physical: A vulnerability exploitable with physical access requires the attacker to physically touch or manipulate the vulnerable component.

NEW QUESTION 117

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 119

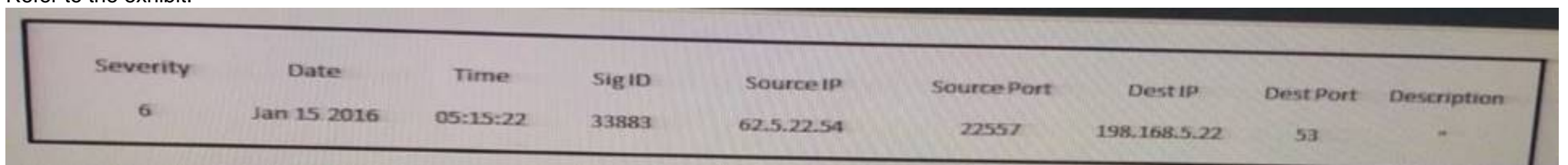
What protocol is related to NAC?

- A. 802.1Q
- B. 802.1X (EAP-TLS, EAP-PEAP or EAP-MSCHAP)
- C. 802.1E
- D. 802.1F

Answer: B

NEW QUESTION 122

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 126

What is the definition of confidentiality according to CVSSv3 framework?

Answer:

Explanation: this metric measures the impact to the confidentiality of the information resources managed by a software component due to a successfully exploited vulnerability.

NEW QUESTION 128

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 132

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 137

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

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

Answer: A

NEW QUESTION 142

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 144

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 147

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 149

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 152

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 153

What attribute belonging VERIS schema?

- A. confidentiality/possession
- B. integrity/authenticity
- C. availability/utility

Answer: ABC

NEW QUESTION 154

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 157

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

direct evidence	log that shows a command and control check-in from verified malware
corroborative evidence	firewall log showing successful communication and threat intelligence stating an IP is known to host malware
indirect evidence	NetFlow-based spike in DNS traffic

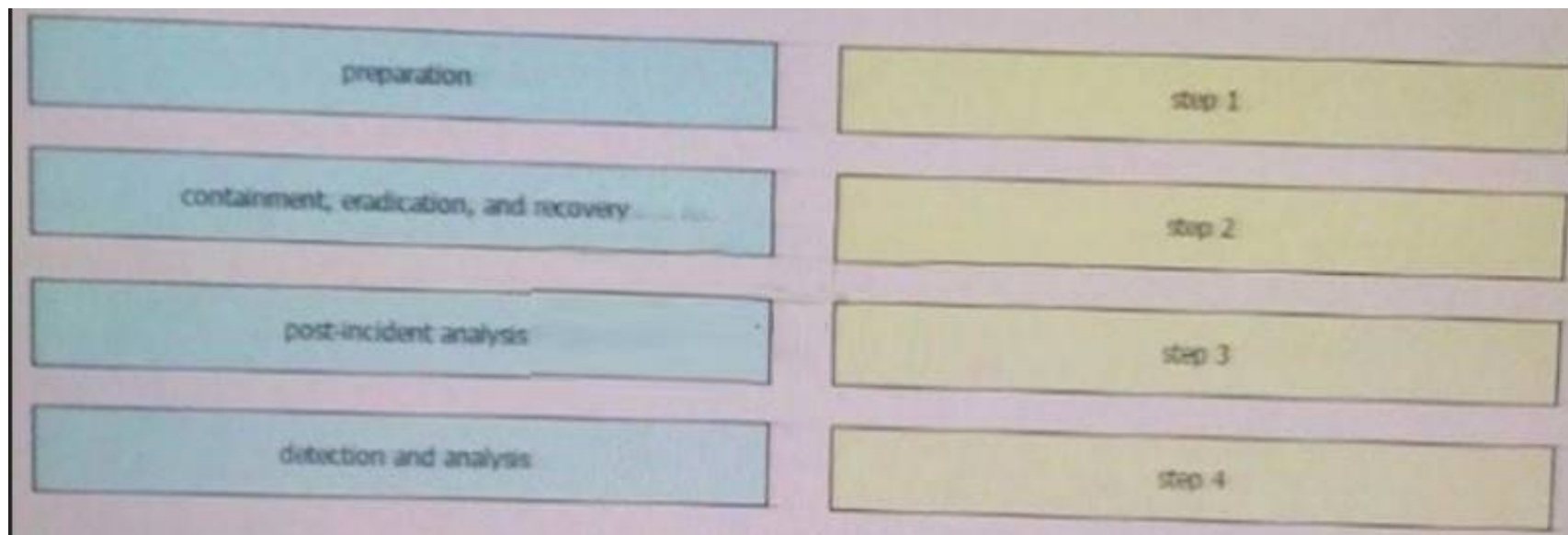
Answer:

Explanation:

direct evidence	indirect evidence
corroborative evidence	direct evidence
indirect evidence	corroborative evidence

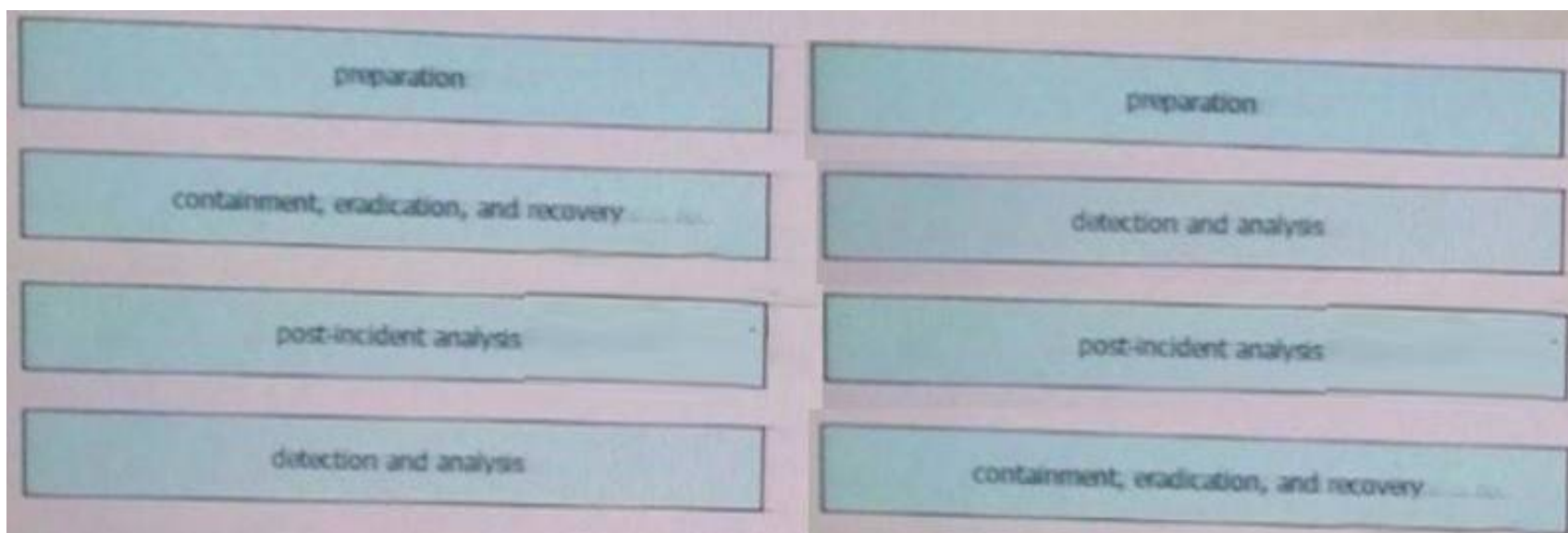
NEW QUESTION 161

Drag and drop the elements of incident handling from the left into the correct order on the right.



Answer:

Explanation:



NEW QUESTION 164

Which type of analysis assigns values to scenarios to see what the outcome might be in each scenario?

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

Answer: A

Explanation: Deterministic Versus Probabilistic Analysis

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.

Probabilistic methods institute powerful tools for use in many kinds of decision-making problems—in this case, cybersecurity event analysis. In this type of analysis, the analysis components suggest a “probabilistic Answer” to the results of the investigation, which is not a definitive result.

Deterministic analysis, you know and obtain “facts” about the incident, breach, affected applications, and so on. For instance, by analyzing applications using port-based analysis and similar methods, you can assume that the process is deterministic—especially when applications conform to the specifications of the standards.

NEW QUESTION 167

When incident data is collected, it is important that evidentiary cross-contamination is prevented. How is this accomplished?

- A. by allowing unrestricted access to impacted devices
- B. by not allowing items of evidence to physically touch
- C. by ensuring power is removed to all devices involved
- D. by not permitting a device to store evidence if it is the evidence itself.

Answer: D

NEW QUESTION 171

Which of the following is the team that handles the investigation, resolution, and disclosure of security vulnerabilities in vendor products and services?

- A. CSIRT
- B. ICASI
- C. USIRP
- D. PSIRT

Answer: D

NEW QUESTION 176

Refer to the Exhibit.



A customer reports that they cannot access your organization's website. Which option is a possible reason that the customer cannot access the website?

- A. The server at 10.33.1.5 is using up too much bandwidth causing a denial- of-service.
- B. The server at 10.67.10.5 has a virus.
- C. A vulnerability scanner has shown that 10.67.10.5 has been compromised.
- D. Web traffic sent from 10.67.10.5 has been identified as malicious by Internet sensors.

Answer: D

Explanation: Every firewall has its own database where it maintains the website reputation on terms of security, ease of access, performance etc and below certain score (generally 7 in case of Cisco), firewalls block access to the sites. For example, you can visit www.senderbase.org and enter name of any website and you will see the reputation of that website.

NEW QUESTION 177

In Microsoft Windows, as files are deleted the space they were allocated eventually is considered available for use by other files. This creates alternating used and unused areas of various sizes. What is this called?

- A. network file storing
- B. free space fragmentation
- C. alternate data streaming
- D. defragmentation

Answer: B

Explanation: Free (unallocated) space fragmentation occurs when there are several unused areas of the file system where new files or meta data can be written to. Unwanted free space fragmentation is generally caused by deletion or truncation of files, but file systems may also intentionally insert fragments ("bubbles") of free space in order to facilitate extending nearby files

NEW QUESTION 179

Which analyzing technique describe the outcome as well as how likely each outcome is?

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

Answer: C

NEW QUESTION 181

What information from HTTP logs can be used to find a threat actor?

- A. referer
- B. IP address
- C. user-agent
- D. URL

Answer: B

Explanation: <https://www.sans.org/reading-room/whitepapers/malicious/user-agent-field-analyzing-detecting-abnormal-organization-33874>

NEW QUESTION 186

What can be addressed when using retrospective security techniques?

- A. if the affected host needs a software update
- B. what system are affected

- C. if the affected system needs replacement
- D. why the malware is still in our network

Answer: D

NEW QUESTION 190

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 192

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 196

Which goal of data normalization is true?

- A. Reduce data redundancy.
- B. Increase data redundancy.
- C. Reduce data availability.
- D. Increase data availability

Answer: A

Explanation: Data normalization is the process of intercepting and storing incoming data so it exists in one form only. This eliminates redundant data and protects the data's integrity.

NEW QUESTION 200

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 Flows
2010-09-01 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 202

What is the process of remediation the system from attack so that responsible threat actor can be revealed?

- A. Validating the Attacking Host's IP Address
- B. Researching the Attacking Host through Search Engines.
- C. Using Incident Databases.
- D. Monitoring Possible Attacker Communication Channels.

Answer: A

NEW QUESTION 206

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 211

Which option creates a display filter on Wireshark on a host IP address or name?

- A. ip.address == <address> or ip.network == <network>
- B. [tcp|udp] ip.[src|dst] port <port>
- C. ip.addr == <addr> or ip.name == <name>
- D. ip.addr == <addr> or ip.host == <host>

Answer: D

NEW QUESTION 212

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 217

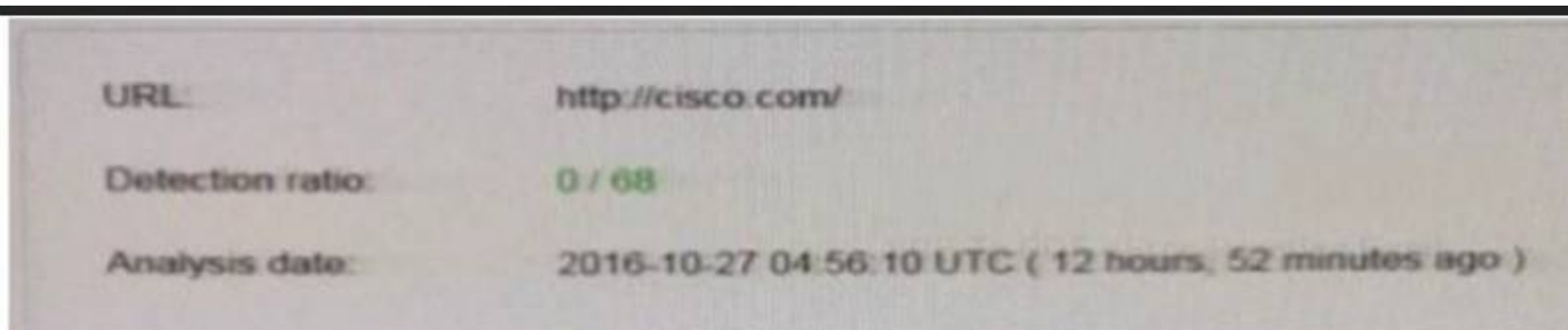
Which option has a drastic impact on network traffic because it can cause legitimate traffic to be blocked?

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

Answer: C

NEW QUESTION 220

Refer to the exhibit.



We have performed a malware detection on the Cisco website. Which statement about the result is true?

- A. The website has been marked benign on all 68 checks.
- B. The threat detection needs to run again.
- C. The website has 68 open threats.
- D. The website has been marked benign on 0 checks.

Answer: A

Explanation: <https://www.virustotal.com/en/url/df05d8e27bd760c33dc709951a5840cc6578d78d544d869890b7b94ea21e46b0>

NEW QUESTION 223

You receive an alert for malicious code that exploits Internet Explorer and runs arbitrary code on the site visitor machine. The malicious 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 (X11; Linux i686; rv: 1.9.2.20) Gecko/20110805
- C. Mozilla/5.0 (Windows NT 6.1; WOW64; rv: 4.0.0) Gecko/20100101
- D. Opera/9.80 (X11; Linux i686; Ubuntu/14.10) Presto/2.12.388 Version/12.16

Answer: A

NEW QUESTION 226

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 228

Which Security Operations Center's goal is to provide incident handling to a country?

- A. Coordination Center
- B. Internal CSIRT
- C. National CSIRT
- D. Analysis Center

Answer: C

NEW QUESTION 230

Which of the following is not a metadata feature of the Diamond Model?

- A. Direction
- B. Result
- C. Devices
- D. Resources

Answer: C

NEW QUESTION 235

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 236

Which stakeholder group is responsible for containment, eradication, and recovery in incident handling?

- A. facilitators
- B. practitioners
- C. leaders and managers
- D. decision makers

Answer: C

NEW QUESTION 239

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 240

Which feature is used to find possible vulnerable services running on a server?

- A. CPU utilization
- B. security policy
- C. temporary internet files
- D. listening ports

Answer: D

NEW QUESTION 241

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 243

Which file system has 32 assigned to the address cluster of the allocation table?

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

Answer: C

NEW QUESTION 245

Which of the following is not an example of reconnaissance?

- A. Searching the robots.txt file
- B. Redirecting users to a source and scanning traffic to learn about the target
- C. Scanning without completing the three-way handshake
- D. Communicating over social media

Answer: B

NEW QUESTION 247

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 Network
 In 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 250

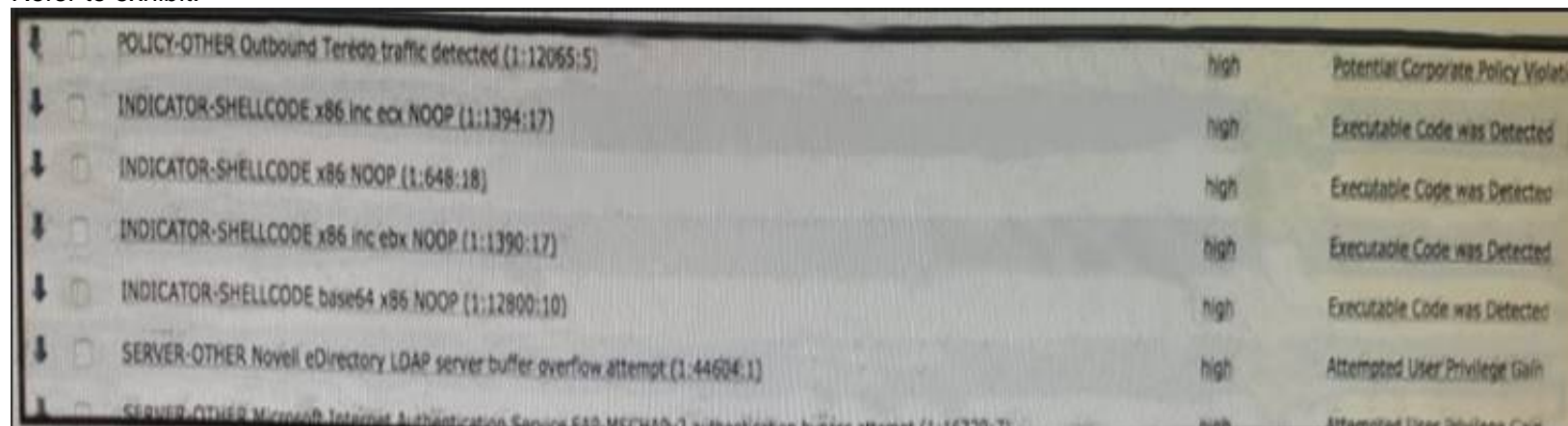
Which Cyber Kill Model category does attacking vulnerability belong to?

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

Answer: A

NEW QUESTION 253

Refer to exhibit.



POLICY-OTHER Outbound Teredo traffic detected (1:12055:5)	high	Potential Corporate Policy Violation
INDICATOR-SHELLCODE x86 inc ecx NOOP (1:1394:17)	high	Executable Code was Detected
INDICATOR-SHELLCODE x86 NOOP (1:648:18)	high	Executable Code was Detected
INDICATOR-SHELLCODE x86 inc ebx NOOP (1:1390:17)	high	Executable Code was Detected
INDICATOR-SHELLCODE base64 x86 NOOP (1:12800:10)	high	Executable Code was Detected
SERVER-OTHER Novell eDirectory LDAP server buffer overflow attempt (1:44604:1)	high	Attempted User Privilege Gain
SERVER-OTHER Microsoft Internet Authentication Service SAS-MSCAD-2 authentication buffer attempt (1:16320:7)	high	Attempted User Privilege Gain

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 258

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 261

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 264

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 268

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 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 275

Which Linux file system supports journaling and an unlimited number of sub directories?

- A. EXT4
- B. EXT2
- C. EXT3
- D. TFS

Answer: A

NEW QUESTION 280

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 282

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 286

Which purpose of data mapping is true?

- A. Visualize data.
- B. Find extra vulnerabilities.
- C. Discover the identities of attackers
- D. Check that data is correct.

Answer: D

NEW QUESTION 289

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 294

At which stage attacking the vulnerability belongs in Cyber kill chain?

Answer:

Explanation: Exploitation

NEW QUESTION 295

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 299

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questions 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 First Try
- * 210-255 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The 210-255 Practice Test Here](#)