Exam Questions 210-255
SECOPS 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
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 3
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 4
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 5
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 6
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 7
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

Guaranteed success with Our exam guides visit - https://www.certshared.com
NEW QUESTION 8
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 facie evidence
D. indirect evidence
Answer: D

NEW QUESTION 9
Which source provides reports of vulnerabilities in software and hardware to a Security Operations Center?
A. Analysis Center
B. National CSIRT
C. Internal CSIRT
D. Physical Security
Answer: C
Explanation:
Vendor teams handle reports of vulnerabilities in their software or hardware products. They may work within the organization to determine if their products are vulnerable and to develop remediation and mitigation strategies. A vendor team may also be the internal CSIRT for a vendor organization. For example, the Cisco Product Security Incident Response Team (PSIRT) is a dedicated global team that manages the receipt, investigation, and public reporting of security vulnerability information related to Cisco products and networks. Cisco PSIRT provides security advisories and security responses.

NEW QUESTION 10
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 11
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 12
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 well as 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 13
According to NIST 86, which action describes the volatile data collection?
NEW QUESTION 14
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 15
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 16
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 17
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 18
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 19
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 20
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 21

-----
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