Cisco Exam Questions 210-255
SECOPS Implementing Cisco Cybersecurity Operations

CertShared now are offering 100% pass ensure 210-255 dumps!
https://www.certshared.com/exam/210-255/ (180 Q&As)
NEW QUESTION 1
Which network device creates and sends the initial packet of a session?

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

Answer: A

NEW QUESTION 2
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 3
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 4
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 5
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 6
Which of the following has been used to evade IDS / IPS devices?

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

Answer: D

NEW QUESTION 7
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 8
Which HTTP header field is usually used in forensics to identify the type of browser used?
A. accept-language
B. user-agent
C. referer
D. host

Answer: B

NEW QUESTION 9
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 resource 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 10
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 11
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 12
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 13
Which analyzing technique describe the outcome as well as how likely each outcome is?

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

Answer: C

Explanation:
Probabilistic analysis describes the outcome in terms of the likelihood of occurrence. A probability distribution identifies the likelihood of events or outcomes.
NEW QUESTION 14
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-abnormals-organization-33874

NEW QUESTION 15
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 16
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 17
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 18
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 19
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 20
Which two HTTP header fields relate to intrusion analysis? (Choose two).

Answer: A
A. user-agent  
B. host  
C. connection  
D. language  
E. handshake type  

Answer: AB  

Explanation:  
User-Agent: Contains a characteristic string that allows the network protocol peers to identify the application type, operating system, software vendor or software version of the requesting software user agent. See also the Firefox user agent string reference.  
Host: Specifies the domain name of the server (for virtual hosting), and (optionally) the TCP port number on which the server is listening.
CertShared now are offering 100% pass ensure 210-255 dumps!
https://www.certshared.com/exam/210-255/ (180 Q&As)

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 FirstTry
* 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