

Cisco

Exam Questions 200-201

Understanding Cisco Cybersecurity Operations Fundamentals



NEW QUESTION 1

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

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

Answer: C

NEW QUESTION 2

Which data format is the most efficient to build a baseline of traffic seen over an extended period of time?

- A. syslog messages
- B. full packet capture
- C. NetFlow
- D. firewall event logs

Answer: C

NEW QUESTION 3

Which two elements are assets in the role of attribution in an investigation? (Choose two.)

- A. context
- B. session
- C. laptop
- D. firewall logs
- E. threat actor

Answer: AE

NEW QUESTION 4

Refer to the exhibit.

What is occurring in this network?

- A. ARP cache poisoning
- B. DNS cache poisoning
- C. MAC address table overflow
- D. MAC flooding attack

Answer: A

NEW QUESTION 5

You have identified a malicious file in a sandbox analysis tool. Which piece of file information from the analysis is needed to search for additional downloads of this file by other hosts?

- A. file name
- B. file hash value
- C. file type
- D. file size

Answer: B

NEW QUESTION 6

What is a benefit of agent-based protection when compared to agentless protection?

- A. It lowers maintenance costs
- B. It provides a centralized platform
- C. It collects and detects all traffic locally
- D. It manages numerous devices simultaneously

Answer: B

NEW QUESTION 7

Which two elements of the incident response process are stated in NIST Special Publication 800-61 r2? (Choose two.)

- A. detection and analysis
- B. post-incident activity
- C. vulnerability management
- D. risk assessment
- E. vulnerability scoring

Answer: AB

NEW QUESTION 8

Drag and drop the access control models from the left onto the correct descriptions on the right.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 9

Which category relates to improper use or disclosure of PII data?

- A. legal
- B. compliance
- C. regulated
- D. contractual

Answer: C

NEW QUESTION 10

Which piece of information is needed for attribution in an investigation?

- A. proxy logs showing the source RFC 1918 IP addresses
- B. RDP allowed from the Internet
- C. known threat actor behavior
- D. 802.1x RADIUS authentication pass and fail logs

Answer: C

NEW QUESTION 10

An organization has recently adjusted its security stance in response to online threats made by a known hacktivist group. What is the initial event called in the NIST SP800-61?

- A. online assault
- B. precursor
- C. trigger

D. instigator

Answer: B

NEW QUESTION 15

What does an attacker use to determine which network ports are listening on a potential target device?

- A. man-in-the-middle
- B. port scanning
- C. SQL injection
- D. ping sweep

Answer: B

NEW QUESTION 17

An analyst is investigating a host in the network that appears to be communicating to a command and control server on the Internet. After collecting this packet capture the analyst cannot determine the technique and payload used for the communication.

Which obfuscation technique is the attacker using?

- A. Base64 encoding
- B. transport layer security encryption
- C. SHA-256 hashing
- D. ROT13 encryption

Answer: B

NEW QUESTION 21

How does certificate authority impact a security system?

- A. It authenticates client identity when requesting SSL certificate
- B. It validates domain identity of a SSL certificate
- C. It authenticates domain identity when requesting SSL certificate
- D. It validates client identity when communicating with the server

Answer: B

NEW QUESTION 25

What are two differences in how tampered and untampered disk images affect a security incident? (Choose two.)

- A. Untampered images are used in the security investigation process
- B. Tampered images are used in the security investigation process
- C. The image is tampered if the stored hash and the computed hash match
- D. Tampered images are used in the incident recovery process
- E. The image is untampered if the stored hash and the computed hash match

Answer: BE

NEW QUESTION 26

Which security principle is violated by running all processes as root or administrator?

- A. principle of least privilege
- B. role-based access control
- C. separation of duties
- D. trusted computing base

Answer: A

NEW QUESTION 29

Which metric in CVSS indicates an attack that takes a destination bank account number and replaces it with a different bank account number?

- A. integrity

- B. confidentiality
- C. availability
- D. scope

Answer: A

NEW QUESTION 32

An engineer receives a security alert that traffic with a known TOR exit node has occurred on the network. What is the impact of this traffic?

- A. ransomware communicating after infection
- B. users downloading copyrighted content
- C. data exfiltration
- D. user circumvention of the firewall

Answer: D

NEW QUESTION 34

While viewing packet capture data, an analyst sees that one IP is sending and receiving traffic for multiple devices by modifying the IP header. Which technology makes this behavior possible?

- A. encapsulation
- B. TOR
- C. tunneling
- D. NAT

Answer: D

NEW QUESTION 38

Which artifact is used to uniquely identify a detected file?

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

Answer: D

NEW QUESTION 43

The target web application server is running as the root user and is vulnerable to command injection. Which result of a successful attack is true?

- A. cross-site scripting
- B. cross-site scripting request forgery
- C. privilege escalation
- D. buffer overflow

Answer: B

NEW QUESTION 47

What causes events on a Windows system to show Event Code 4625 in the log messages?

- A. The system detected an XSS attack
- B. Someone is trying a brute force attack on the network
- C. Another device is gaining root access to the system
- D. A privileged user successfully logged into the system

Answer: B

NEW QUESTION 50

Which two components reduce the attack surface on an endpoint? (Choose two.)

- A. secure boot
- B. load balancing
- C. increased audit log levels
- D. restricting USB ports
- E. full packet captures at the endpoint

Answer: AD

NEW QUESTION 51

A security engineer deploys an enterprise-wide host/endpoint technology for all of the company's corporate PCs. Management requests the engineer to block a selected set of applications on all PCs.

Which technology should be used to accomplish this task?

- A. application whitelisting/blacklisting
- B. network NGFW

- C. host-based IDS
- D. antivirus/antispysware software

Answer: A

NEW QUESTION 54

Which security principle requires more than one person is required to perform a critical task?

- A. least privilege
- B. need to know
- C. separation of duties
- D. due diligence

Answer: C

NEW QUESTION 57

Which type of attack occurs when an attacker is successful in eavesdropping on a conversation between two IP phones?

- A. known-plaintext
- B. replay
- C. dictionary
- D. man-in-the-middle

Answer: D

NEW QUESTION 59

A network engineer discovers that a foreign government hacked one of the defense contractors in their home country and stole intellectual property. What is the threat agent in this situation?

- A. the intellectual property that was stolen
- B. the defense contractor who stored the intellectual property
- C. the method used to conduct the attack
- D. the foreign government that conducted the attack

Answer: D

NEW QUESTION 62

A system administrator is ensuring that specific registry information is accurate. Which type of configuration information does the HKEY_LOCAL_MACHINE hive contain?

- A. file extension associations
- B. hardware, software, and security settings for the system
- C. currently logged in users, including folders and control panel settings
- D. all users on the system, including visual settings

Answer: B

NEW QUESTION 64

Which event artifact is used to identify HTTP GET requests for a specific file?

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

Answer: B

NEW QUESTION 66

Refer to the exhibit.

Drag and drop the element name from the left onto the correct piece of the PCAP file on the right.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 69

Which access control model does SELinux use?

- A. RBAC
- B. DAC
- C. MAC
- D. ABAC

Answer: C

NEW QUESTION 73

How is attacking a vulnerability categorized?

- A. action on objectives
- B. delivery
- C. exploitation
- D. installation

Answer: C

NEW QUESTION 75

Refer to the exhibit.

What is the expected result when the "Allow subdissector to reassemble TCP streams" feature is enabled?

- A. insert TCP subdissectors
- B. extract a file from a packet capture
- C. disable TCP streams
- D. unfragment TCP

Answer: D

NEW QUESTION 77

How does an attacker observe network traffic exchanged between two users?

- A. port scanning
- B. man-in-the-middle
- C. command injection
- D. denial of service

Answer: B

NEW QUESTION 78

At which layer is deep packet inspection investigated on a firewall?

- A. internet
- B. transport
- C. application
- D. data link

Answer: C

NEW QUESTION 81

What is a difference between SOAR and SIEM?

- A. SOAR platforms are used for threat and vulnerability management, but SIEM applications are not
- B. SIEM applications are used for threat and vulnerability management, but SOAR platforms are not
- C. SOAR receives information from a single platform and delivers it to a SIEM
- D. SIEM receives information from a single platform and delivers it to a SOAR

Answer: A

NEW QUESTION 83

How is NetFlow different than traffic mirroring?

- A. NetFlow collects metadata and traffic mirroring clones data
- B. Traffic mirroring impacts switch performance and NetFlow does not
- C. Traffic mirroring costs less to operate than NetFlow
- D. NetFlow generates more data than traffic mirroring

Answer: A

NEW QUESTION 86

Drag and drop the security concept on the left onto the example of that concept on the right.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 87

Which type of data consists of connection level, application-specific records generated from network traffic?

- A. transaction data
- B. location data
- C. statistical data
- D. alert data

Answer: A

NEW QUESTION 92

Why is encryption challenging to security monitoring?

- A. Encryption analysis is used by attackers to monitor VPN tunnels.
- B. Encryption is used by threat actors as a method of evasion and obfuscation.
- C. Encryption introduces additional processing requirements by the CPU.
- D. Encryption introduces larger packet sizes to analyze and store.

Answer: B

NEW QUESTION 94

In a SOC environment, what is a vulnerability management metric?

- A. code signing enforcement
- B. full assets scan

- C. internet exposed devices
- D. single factor authentication

Answer: D

NEW QUESTION 99

.....

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

200-201 Practice Exam Features:

- * 200-201 Questions and Answers Updated Frequently
- * 200-201 Practice Questions Verified by Expert Senior Certified Staff
- * 200-201 Most Realistic Questions that Guarantee you a Pass on Your First Try
- * 200-201 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The 200-201 Practice Test Here](#)