# 200-201 Dumps

# Understanding Cisco Cybersecurity Operations Fundamentals

## https://www.certleader.com/200-201-dumps.html

**NEW QUESTION 1**
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 2**
What is the difference between a threat and a risk?

A. Threat represents a potential danger that could take advantage of a weakness in a system
B. Risk represents the known and identified loss or danger in the system
C. Risk represents the nonintentional interaction with uncertainty in the system
D. Threat represents a state of being exposed to an attack or a compromise either physically or logically

**Answer:** A


**NEW QUESTION 3**
Refer to the exhibit.

```
Interface: 192.168.1.29 --- 0x11
Internet Address      Physical Address      Type
192.168.1.10          d8-a7-56-d7-19-ea     dynamic
192.168.1.67          d8-a7-56-d7-19-ea     dynamic
192.168.1.1           01-00-5e-00-00-16     static
```

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 4**
What is the difference between deep packet inspection and stateful inspection?

A. Deep packet inspection is more secure than stateful inspection on Layer 4
B. Stateful inspection verifies contents at Layer 4 and deep packet inspection verifies connection at Layer 7
C. Stateful inspection is more secure than deep packet inspection on Layer 7
D. Deep packet inspection allows visibility on Layer 7 and stateful inspection allows visibility on Layer 4

**Answer:** D


**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**
Drag and drop the technology on the left onto the data type the technology provides on the right.

| | |
|---|---|
| tcpdump | session data |
| web content filtering | full packet capture |
| traditional stateful firewall | transaction data |
| NetFlow | connection event |

A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**

| | |
|---|---|
| tcpdump | web content filtering |
| web content filtering | tcpdump |
| traditional stateful firewall | NetFlow |
| NetFlow | traditional stateful firewall |

**NEW QUESTION 7**
Drag and drop the access control models from the left onto the correct descriptions on the right.

| | |
|---|---|
| MAC | object owner determines permissions |
| ABAC | OS determines permissions |
| RBAC | role of the subject determines permissions |
| DAC | attributes of the subject determines permissions |

A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**

| | |
|---|---|
| MAC | DAC |
| ABAC | MAC |
| RBAC | RBAC |
| DAC | ABAC |

**NEW QUESTION 8**
Which category relates to improper use or disclosure of PII data?

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

**Answer:** C

**NEW QUESTION 9**
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 arid fail logs

**Answer:** C

**NEW QUESTION 10**
What is a purpose of a vulnerability management framework?

A. identifies, removes, and mitigates system vulnerabilities
B. detects and removes vulnerabilities in source code
C. conducts vulnerability scans on the network
D. manages a list of reported vulnerabilities

**Answer:** A

**NEW QUESTION 10**
Refer to the exhibit.

<IMG SRC=j%41vascript:alert('attack')>

Which kind of attack method is depicted in this string?

A. cross-site scripting
B. man-in-the-middle
C. SQL injection
D. denial of service

**Answer:** A

**NEW QUESTION 11**
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 12**
What is the function of a command and control server?

A. It enumerates open ports on a network device
B. It drops secondary payload into malware
C. It is used to regain control of the network after a compromise
D. It sends instruction to a compromised system

**Answer:** D

**NEW QUESTION 17**
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 21**
Refer to the exhibit.

```
- Internet Protocol version 4, Src: 192.168.122.100 (192.168.122.100), Dst:
81.179.179.69 (81.179.179.69)
    Version: 4
    Header Length: 20 bytes
 + Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT
(Not ECN-Capable Transport))
    Total Length: 538
    Identification: 0x6bse (27534)
 + Flags: 0x02 (Don't Fragment)
    Fragment offset: 0
    Time to live: 128
    Protocol: TCP (6)
 + Header checksum: 0x000 [Validation disabled]
    Source: 192.168.122.100 (192.168.122.100)
    Destination: 81.179.179.69 (81.179.179.69)
    [Source GeoIP: Unknown]




+ Transmission control protocol. src port: 50272 (50272) Dst Port: 80 (80).
Seq: 419451624. Ack: 970444123. Len: 490
```

What should be interpreted from this packet capture?

A. IP address 179.179.69/50272/192.168.122.100/80/6 is sending a packet from port 80 of IP address 192.168.122.100 that is going to port 50272 of IP address 81.179.179.69 using IP protocol 6.
B. IP address 192.168.122.100/50272/81.179.179.69/80/6 is sending a packet from port 50272 of IP address 192.168.122.100 that is going to port 80 of IP address 81.179.179.69 using IP protocol 6.
C. IP address 192.168.122.100/50272/81.179.179.69/80/6 is sending a packet from port 80 of IP address 192.168.122.100 that is going to port 50272 of IP address 81.179.179.69 using IP protocol 6.7E503B693763E0113BE0CD2E4A16C9C4
D. IP address 179.179.69/50272/192.168.122.100/80/6 is sending a packet from port 50272 of IP address 192.168.122.100 that is going to port 80 of IP address 81.179.179.69 using IP protocol 6.

**Answer:** B


**NEW QUESTION 22**
Which type of data collection requires the largest amount of storage space?

A. alert data
B. transaction data
C. session data
D. full packet capture

**Answer:** D


**NEW QUESTION 25**
Refer to the exhibit.

```
No.   Time       Source       Destination   Protocol   Length Info
   1 0.000000  10.0.0.2     10.128.0.2     TCP       54 3341 - 66 [SYN] Seq=0 Win=512 Len=0
   2 0.003987  10.128.0.2   10.0.0.2       TCP       58 88 - 3222 [SYN, ACK] Seq=0 Ack=1 Win=29288 Len=0 NSS=1468
   3 0.005514  10.128.0.2   10.0.0.2       TCP       58 88 - 3341 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 NSS=1460
   4 0.008429  10.0.0.2     10.128.0.2     TCP       54 3342 - 80 [SYN] Seq=0 Win=512 Len=0
   5 0.010233  10.128.0.2   10.0.0.2       TCP       58 88 - 3220 [SYN, ACK] Seq=0 Ack=1 Win=2988 Len=0 NSS=1468
   6 0.014072  10.128.0.2   10.0.0.2       TCP       58 80 - 3342 [SYN, ACK] Seq=0 Ack=1 Win=2900 Len=0 NSS=1460
   7 0.016830  10.0.0.2     10.128.0.2     TCP       54 3343 - 88 [SYN] Seq=0 Win=512 Len=0
   8 0.022220  10.128.0.2   10.0.0.2       TCP       58 89 - 3343 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
   9 0.023496  10.128.0.2   10.0.0.2       TCP       58 89 - 3219 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
  10 0.025243  10.0.0.2     10.128.0.2     TCP       54 3344 - 88 [SYN] Seq=0 Win=512 Len=0
  11 0.026672  10.128.0.2   10.0.0.2       TCP       58 89 - 3218 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
  12 0.028038  10.128.0.2   10.0.0.2       TCP       58 80 - 3221 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
  13 0.030523  10.128.0.2   10.0.0.2       TCP       58 88 - 3344 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460

Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
Ethernet II, Src: 42:01:0a:f0:00:17 (42:01:0a:f0:00:17), Dst: 42:01:0a:f0:00:01 (42:01:0a:f0:00:01)
Internet Protocol Version 4, Src: 18.0.0.2, Dst: 10.128.0.2
Transmission Control Protocol, Src Port: 3341, Dst Port: 80, Seq: 0, Len: 0
   Source Port: 3341
   Destination Port: 80
   [Stream index: 0]
   [TCP Segment Len: 0]
   Sequence number: 0 (relative sequence number)
   [Next sequence number: 0 (relative sequence number)]
 , Acknowledgement number: 1023350884
   0101 .... = Header Length: 20 bytes (5)
 , Flags: 0x002 (SYN)
   Windows Size Value: 512
   [Calculated window size: 512]
   Checksum: 0x8d5a [unverified]
   [Checksum Status: Unverified]
   Urgent pointer: 0
 , [Timestamps]
```

What is occurring in this network traffic?

A. high rate of SYN packets being sent from a multiple source towards a single destination IP
B. high rate of SYN packets being sent from a single source IP towards multiple destination IPs
C. flood of ACK packets coming from a single source IP to multiple destination IPs
D. flood of SYN packets coming from a single source IP to a single destination IP

**Answer:** D


**NEW QUESTION 29**
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 31**
Which metric is used to capture the level of access needed to launch a successful attack?

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

**Answer:** A


**NEW QUESTION 36**
What should a security analyst consider when comparing inline traffic interrogation with traffic tapping to determine which approach to use in the network?

A. Tapping interrogation replicates signals to a separate port for analyzing traffic
B. Tapping interrogations detect and block malicious traffic
C. Inline interrogation enables viewing a copy of traffic to ensure traffic is in compliance with security policies
D. Inline interrogation detects malicious traffic but does not block the traffic

**Answer:** A


**NEW QUESTION 37**
Refer to the exhibit.



What is the potential threat identified in this Stealthwatch dashboard?

A. Host 10.201.3.149 is sending data to 152.46.6.91 using TCP/443.
B. Host 152.46.6.91 is being identified as a watchlist country for data transfer.
C. Traffic to 152.46.6.149 is being denied by an Advanced Network Control policy.
D. Host 10.201.3.149 is receiving almost 19 times more data than is being sent to host 152.46.6.91.

**Answer:** D

**NEW QUESTION 41**
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 44**
Which step in the incident response process researches an attacking host through logs in a SIEM?

A. detection and analysis
B. preparation
C. eradication
D. containment

**Answer:** A

**NEW QUESTION 46**
An intruder attempted malicious activity and exchanged emails with a user and received corporate information, including email distribution lists. The intruder asked the user to engage with a link in an email. When the fink launched, it infected machines and the intruder was able to access the corporate network.
Which testing method did the intruder use?

A. social engineering
B. eavesdropping
C. piggybacking
D. tailgating

**Answer:** A

**NEW QUESTION 50**
Which evasion technique is indicated when an intrusion detection system begins receiving an abnormally high volume of scanning from numerous sources?

A. resource exhaustion
B. tunneling
C. traffic fragmentation
D. timing attack

**Answer:** A

**NEW QUESTION 54**
Which event artifact is used to identity HTTP GET requests for a specific file?

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

**Answer:** D

**NEW QUESTION 58**
How does an SSL certificate impact security between the client and the server?

A. by enabling an authenticated channel between the client and the server
B. by creating an integrated channel between the client and the server
C. by enabling an authorized channel between the client and the server
D. by creating an encrypted channel between the client and the server

**Answer:** D

**NEW QUESTION 61**
Which system monitors local system operation and local network access for violations of a security policy?

A. host-based intrusion detection
B. systems-based sandboxing
C. host-based firewall

D. antivirus

**Answer:** C


**NEW QUESTION 62**
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 65**
What does cyber attribution identify in an investigation?

A. exploit of an attack
B. threat actors of an attack
C. vulnerabilities exploited
D. cause of an attack

**Answer:** B


**NEW QUESTION 70**
What is the difference between an attack vector and attack surface?

A. An attack surface identifies vulnerabilities that require user input or validation; and an attack vectoridentifies vulnerabilities that are independent of user actions.
B. An attack vector identifies components that can be exploited; and an attack surface identifies the potential path an attack can take to penetrate the network.
C. An attack surface recognizes which network parts are vulnerable to an attack; and an attack vector identifies which attacks are possible with these vulnerabilities.
D. An attack vector identifies the potential outcomes of an attack; and an attack surface launches an attack using several methods against the identified vulnerabilities.

**Answer:** C


**NEW QUESTION 74**
Refer to the exhibit.

```
$ cuckoo submit --machine cuckoo1 /path/to/binary
```

Which event is occurring?

A. A binary named "submit" is running on VM cuckoo1.
B. A binary is being submitted to run on VM cuckoo1
C. A binary on VM cuckoo1 is being submitted for evaluation
D. A URL is being evaluated to see if it has a malicious binary

**Answer:** C


**NEW QUESTION 75**
Which HTTP header field is used in forensics to identify the type of browser used?

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

**Answer:** C


**NEW QUESTION 79**
What is the difference between the ACK flag and the RST flag in the NetFlow log session?

A. The RST flag confirms the beginning of the TCP connection, and the ACK flag responds when the data for the payload is complete
B. The ACK flag confirms the beginning of the TCP connection, and the RST flag responds when the data for the payload is complete
C. The RST flag confirms the receipt of the prior segment, and the ACK flag allows for the spontaneous termination of a connection
D. The ACK flag confirms the receipt of the prior segment, and the RST flag allows for the spontaneous termination of a connection

**Answer:** D


**NEW QUESTION 81**
When communicating via TLS, the client initiates the handshake to the server and the server responds back with its certificate for identification.
Which information is available on the server certificate?

A. server name, trusted subordinate CA, and private key
B. trusted subordinate CA, public key, and cipher suites
C. trusted CA name, cipher suites, and private key
D. server name, trusted CA, and public key

**Answer:** D


**NEW QUESTION 83**
Which list identifies the information that the client sends to the server in the negotiation phase of the TLS handshake?

A. ClientStart, ClientKeyExchange, cipher-suites it supports, and suggested compression methods
B. ClientStart, TLS versions it supports, cipher-suites it supports, and suggested compression methods
C. ClientHello, TLS versions it supports, cipher-suites it supports, and suggested compression methods
D. ClientHello, ClientKeyExchange, cipher-suites it supports, and suggested compression methods

**Answer:** C


**NEW QUESTION 86**
Which security technology allows only a set of pre-approved applications to run on a system?

A. application-level blacklisting
B. host-based IPS
C. application-level whitelisting
D. antivirus

**Answer:** C


**NEW QUESTION 91**
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 95**
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 97**
What is an example of social engineering attacks?

A. receiving an unexpected email from an unknown person with an uncharacteristic attachment from someone in the same company
B. receiving an email from human resources requesting a visit to their secure website to update contact information
C. sending a verbal request to an administrator who knows how to change an account password
D. receiving an invitation to the department's weekly WebEx meeting

**Answer:** B


**NEW QUESTION 100**
Which event is user interaction?

A. gaining root access
B. executing remote code
C. reading and writing file permission
D. opening a malicious file

**Answer:** D


**NEW QUESTION 104**
Which access control model does SELinux use?

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

**Answer:** C

**NEW QUESTION 108**
What does cyber attribution identity in an investigation?

A. cause of an attack
B. exploit of an attack
C. vulnerabilities exploited
D. threat actors of an attack

**Answer:** D

**NEW QUESTION 113**
What are two social engineering techniques? (Choose two.)

A. privilege escalation
B. DDoS attack
C. phishing
D. man-in-the-middle
E. pharming

**Answer:** CE

**NEW QUESTION 114**
An analyst received an alert on their desktop computer showing that an attack was successful on the host. After investigating, the analyst discovered that no mitigation action occurred during the attack. What is the reason for this discrepancy?

A. The computer has a HIPS installed on it.
B. The computer has a NIPS installed on it.
C. The computer has a HIDS installed on it.
D. The computer has a NIDS installed on it.

**Answer:** C

**NEW QUESTION 116**
Which two elements are used for profiling a network? (Choose two.)

A. session duration
B. total throughput
C. running processes
D. listening ports
E. OS fingerprint

**Answer:** DE

**NEW QUESTION 120**
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 125**
Refer to the exhibit.



Which two elements in the table are parts of the 5-tuple? (Choose two.)

A. First Packet

B. Initiator User
C. Ingress Security Zone
D. Source Port
E. Initiator IP

**Answer:** DE


**NEW QUESTION 127**
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 132**
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 137**
Which IETF standard technology is useful to detect and analyze a potential security incident by recording session flows that occurs between hosts?

A. SFlow
B. NetFlow
C. NFlow
D. IPFIX

**Answer:** D


**NEW QUESTION 138**
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 140**
......

# Thank You for Trying Our Product

* 100% Pass or Money Back

   All our products come with a 90-day Money Back Guarantee.

* One year free update

   You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

   We currently serve more than 30,000,000 customers.

* Shop Securely

   All transactions are protected by VeriSign!

**100% Pass Your 200-201 Exam with Our Prep Materials Via below:**

https://www.certleader.com/200-201-dumps.html