Exam Questions 200-201

Understanding Cisco Cybersecurity Operations Fundamentals

https://www.2passeasy.com/dumps/200-201/

NEW QUESTION 1
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 2
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 3
An engineer runs a suspicious file in a sandbox analysis tool to see the outcome. The analysis report shows that outbound callouts were made post infection.
Which two pieces of information from the analysis report are needed to investigate the callouts? (Choose two.)

A. signatures
B. host IP addresses
C. file size
D. dropped files
E. domain names

Answer: BE

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

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

Answer: B

NEW QUESTION 6
Drag and drop the technology on the left onto the data type the technology provides on the right.

A. Mastered
B. Not Mastered

Answer: A

Explanation:

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 arid fail logs

Answer: C

NEW QUESTION 10
Refer to the exhibit.

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 15
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
Refer to the exhibit.

This request was sent to a web application server driven by a database. Which type of web server attack is represented?

A. parameter manipulation
B. heap memory corruption
C. command injection
D. blind SQL injection

Answer: D

NEW QUESTION 18
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 21
Which regular expression matches "color" and "colour"?

A. colo?ur
B. col[08]+our
C. colou?r
D. col[09]+our

Answer: C

NEW QUESTION 26
What specific type of analysis is assigning values to the scenario to see expected outcomes?

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

Answer: A

NEW QUESTION 30
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 32
What is the practice of giving an employee access to only the resources needed to accomplish their job?

A. principle of least privilege
B. organizational separation
C. separation of duties
D. need to know principle

Answer: A

NEW QUESTION 34
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 35
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 37
Which principle is being followed when an analyst gathers information relevant to a security incident to determine the appropriate course of action?

A. decision making
B. rapid response
C. data mining
D. due diligence

Answer: A

NEW QUESTION 41
What is rule-based detection when compared to statistical detection?

A. proof of a user's identity
B. proof of a user's action
C. likelihood of user's action
D. falsification of a user's identity

Answer: B

NEW QUESTION 44
Which evasion technique is a function of ransomware?

A. extended sleep calls
B. encryption
C. resource exhaustion
D. encoding

Answer: B

NEW QUESTION 47
Which regex matches only on all lowercase letters?

A. [az]+
B. [^az]+
C. az+
D. a*z+

Answer: A

NEW QUESTION 51
An analyst discovers that a legitimate security alert has been dismissed. Which signature caused this impact on network traffic?

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

Answer: B

NEW QUESTION 53
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 54
A security engineer has a video of a suspect entering a data center that was captured on the same day that files in the same data center were transferred to a competitor.
Which type of evidence is this?

A. best evidence
B. prima facie evidence
C. indirect evidence
D. physical evidence

Answer: C

NEW QUESTION 58
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 61
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 66
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 68
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 69
What do the Security Intelligence Events within the FMC allow an administrator to do?

A. See if a host is connecting to a known-bad domain.
B. Check for host-to-server traffic within your network.
C. View any malicious files that a host has downloaded.
D. Verify host-to-host traffic within your network.

Answer: A

NEW QUESTION 71
What makes HTTPS traffic difficult to monitor?

A. SSL interception
B. packet header size
C. signature detection time
D. encryption

Answer: D

NEW QUESTION 72
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 77
Refer to the exhibit.

Which type of log is displayed?

A. IDS
B. proxy
C. NetFlow
D. sys

Answer: D

NEW QUESTION 81
A malicious file has been identified in a sandbox analysis tool.
Which piece of information is needed to search for additional downloads of this file by other hosts?

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

Answer: D

NEW QUESTION 86
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 89
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 94
When trying to evade IDS/IPS devices, which mechanism allows the user to make the data incomprehensible without a specific key, certificate, or password?

A. fragmentation
B. pivoting
C. encryption
D. stenography

Answer: D

NEW QUESTION 99
Refer to the exhibit.

What does the output indicate about the server with the IP address 172.18.104.139?

A. open ports of a web server
B. open port of an FTP server
C. open ports of an email server
D. running processes of the server

Answer: C

NEW QUESTION 101
Refer to the exhibit.

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 102
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 107
Which utility blocks a host portscan?

A. HIDS
B. sandboxing
C. host-based firewall
D. antimalware

Answer: C

NEW QUESTION 112
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 115
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 117
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 119
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 121
A SOC analyst is investigating an incident that involves a Linux system that is identifying specific sessions. Which identifier tracks an active program?

A. application identification number
B. active process identification number
C. runtime identification number
D. process identification number

Answer: D

NEW QUESTION 122
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 127
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 131

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 135
Which access control model does SELinux use?

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

Answer: C

NEW QUESTION 139
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 144
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 147
At which layer is deep packet inspection investigated on a firewall?

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

Answer: C

NEW QUESTION 152
Refer to the exhibit.

Which type of log is displayed?

A. proxy
B. NetFlow
C. IDS
D. sys

Answer: B

NEW QUESTION 154
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 158
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 160
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 163
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 165
.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual 200-201 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the 200-201 Product From:

https://www.2passeasy.com/dumps/200-201/

Money Back Guarantee

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 FirstTry

* 200-201 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year