Cisco

Exam Questions 200-201

Understanding Cisco Cybersecurity Operations Fundamentals

NEW QUESTION 1
Refer to the exhibit.

What information is depicted?

A. IIS data
B. NetFlow data
C. network discovery event
D. IPS event data

Answer: B

NEW QUESTION 2
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 3
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 4
What is the difference between statistical detection and rule-based detection models?

A. Rule-based detection involves the collection of data in relation to the behavior of legitimate users over a period of time
B. Statistical detection defines legitimate data of users over a period of time and rule-based detection defines it on an IF/THEN basis
C. Statistical detection involves the evaluation of an object on its intended actions before it executes that behavior
D. Rule-based detection defines legitimate data of users over a period of time and statistical detection defines it on an IF/THEN basis

Answer: B

NEW QUESTION 5
Refer to the exhibit.

Which packet contains a file that is extractable within Wireshark?

A. 2317
B. 1986
C. 2318
D. 2542

Answer: D

NEW QUESTION 6
Which type of evidence supports a theory or an assumption that results from initial evidence?

A. probabilistic
B. indirect
C. best
D. corroborative

Answer: D

NEW QUESTION 7
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 8
Refer to the exhibit.

In which Linux log file is this output found?

A. /var/log/authorization.log
B. /var/log/dmesg
C. var/log/var.log
D. /var/log/auth.log

Answer: D

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
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 10
Refer to the exhibit.

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 12
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 13
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 15
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 20
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 22
Refer to the exhibit.

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 24
What is a difference between inline traffic interrogation and traffic mirroring?

A. Inline inspection acts on the original traffic data flow
B. Traffic mirroring passes live traffic to a tool for blocking
C. Traffic mirroring inspects live traffic for analysis and mitigation
D. Inline traffic copies packets for analysis and security

Answer: B

NEW QUESTION 28
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
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 33
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 38
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 43
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 47
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 48
Which signature impacts network traffic by causing legitimate traffic to be blocked?

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

Answer: D

NEW QUESTION 51
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 56
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 59
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 60
A security specialist notices 100 HTTP GET and POST requests for multiple pages on the web servers. The agent in the requests contains PHP code that, if executed, creates and writes to a new PHP file on the webserver. Which event category is described?

A. reconnaissance
B. action on objectives
C. installation
D. exploitation

Answer: C

NEW QUESTION 64
Refer to the exhibit.

What does the message indicate?

A. an access attempt was made from the Mosaic web browser
B. a successful access attempt was made to retrieve the password file
C. a successful access attempt was made to retrieve the root of the website
D. a denied access attempt was made to retrieve the password file

Answer: C

NEW QUESTION 68
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 70
What is the virtual address space for a Windows process?

A. physical location of an object in memory
B. set of pages that reside in the physical memory
C. system-level memory protection feature built into the operating system
D. set of virtual memory addresses that can be used

Answer: D

NEW QUESTION 72
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 76
Refer to the exhibit.

Which type of log is displayed?

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

Answer: D

NEW QUESTION 79
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 84
An investigator is examining a copy of an ISO file that is stored in CDFS format. What type of evidence is this file?

A. data from a CD copied using Mac-based system
B. data from a CD copied using Linux system
C. data from a DVD copied using Windows system
D. data from a CD copied using Windows

Answer: B

NEW QUESTION 88
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 92
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 95
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 99
Which utility blocks a host portscan?

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

Answer: C

NEW QUESTION 100
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 101
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 106
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 111
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 113
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 117
Which access control model does SELinux use?

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

Answer: C

NEW QUESTION 122
Refer to the exhibit.

Which type of log is displayed?

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

Answer: B

NEW QUESTION 124
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 128
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 130
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 133
......