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
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 4
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 5
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 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
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 8
Which incidence response step includes identifying all hosts affected by an attack'?

A. post-incident activity
B. detection and analysis
C. containment eradication and recovery
D. preparation

Answer: A

NEW QUESTION 9
Refer to the exhibit.

```
GET /item.php?id=34' or sleep(10)
```

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
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 10
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.

```
File     Actions    Edit     View      Help

   48  41.270348133 185.199.111.153 → 192.168.88.164 TLSv1.2 123 Application Data
   49  41.270348165 185.199.111.153 → 192.168.88.164 TLSv1.2 104 Application Data
   50  41.270356290 192.168.88.164 → 185.199.111.153 TCP 66 44736 → 443 [ACK]
Seq=834 Ack=3104 Win=64128 Len=0 TSval=3947973757 TSecr=2989424849
   51  41.270369874 192.168.88.164 → 185.199.111.153 TCP 66 44736 → 443 [ACK]
Seq=834 Ack=3142 Win=64128 Len=0 TSval=3947973757 TSecr=2989424849
   52  41.270430171 192.168.88.164 → 185.199.111.153 TLSv1.2 104 Application Data
   53  41.271767772 185.199.111.153 → 192.168.88.164 TLSv1.2 2854 Application Data
   54  41.271767817 185.199.111.153 → 192.168.88.164 TLSv1.2 904 Application Data
   55  41.271788996 192.168.88.164 → 185.199.111.153 TCP 66 44736 → 443 [ACK]
Seq=872 Ack=6768 Win=62592 Len=0 TSval=3947973758 TSecr=2989424849
   56  41.271973293 192.168.88.164 → 185.199.111.153 TLSv1.2 97 Encrypted Alert
   57  41.272411701 192.168.88.164 → 185.199.111.153 TCP 66 44736 → 443 [FIN, ACK]
Seq=903 Ack=6768 Win=64128 Len=0 TSval=3947973759 TSecr=2989424849
   58  41.283301751 185.199.111.153 → 192.168.88.164 TCP 66 443 → 44736 [ACK]
Seq=6768 Ack=903 Win=28160 Len=0 TSval=2989424852 TSecr=3947973757
   59  41.283301808 185.199.111.153 → 192.168.88.164 TLSv1.2 97 Encrypted Alert
   60  41.283321947 192.168.88.164 → 185.199.111.153 TCP 54 44736 → 443 [RST]
Seq=903 Win=0 Len=0
   61  41.283939151 185.199.111.153 → 192.168.88.164 TCP 66 443 → 44736 [FIN, ACK]
Seq=6799 Ack=903 Win=28160 Len=0 TSval=2989424852 TSecr=3947973757
   62  41.283945760 192.168.88.164 → 185.199.111.153 TCP 54 44736 → 443 [RST]
Seq=903 Win=0 Len=0
   63  41.284635561 185.199.111.153 → 192.168.88.164 TCP 66 443 → 44736 [ACK]
Seq=6800 Ack=904 Win=28160 Len=0 TSval=2989424853 TSecr=3947973759
   64  41.284642324 192.168.88.164 → 185.199.111.153 TCP 54 44736 → 443 [RST]
Seq=904 Win=0 Len=0
```

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 19
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 20
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 23
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 25
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 30
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 31
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 32
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 37
A security expert is working on a copy of the evidence, an ISO file that is saved in CDFS format. Which type of evidence is this file?

A. CD data copy prepared in Windows
B. CD data copy prepared in Mac-based system
C. CD data copy prepared in Linux system
D. CD data copy prepared in Android-based system

Answer: A

NEW QUESTION 40
Refer to the exhibit.

Severity	Date	Time	Sig ID	Source IP	Source Port	Dest IP	Dest Port	Description
6	Jan 15 2020	05:15:22	33883	62.5.22.54	22557	198.168.5.22	53	*

Which type of log is displayed?

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

Answer: D

NEW QUESTION 42
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 45
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 48
Refer to the exhibit.

```
# nmap -sV 172.18.104.139

Starting Nmap 7.01 ( https://nmap.org ) at 2020-03-07 11:36 EST
Nmap scan report for 172.18.104.139
Host is up (0.000018s latency).
Not shown: 996 closed ports
PORT      STATE  SERVICE    VERSION
22/tcp    open   ssh        OpenSSH 7.2p2 Ubuntu 4ubuntu2.4 (Ubuntu Linux; protocol 2.0)
25/tcp    open   smtp       Postfix smtpd
110/tcp   open   pop3       Dovecot pop3d
143/tcp   open   imap       Dovecot imapd
Service Info: Host:    172.18.108.139; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

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 53
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 58
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 61
Which utility blocks a host portscan?

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

Answer: C

NEW QUESTION 62
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 64
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 65
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 67
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 70
Refer to the exhibit.

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

source address	10.0.2.15
destination address	50588
source port	443
destination port	192.124.249.9
Network Protocol	Transmission Control Protocol
Transport Protocol	Internet Protocol v4
Application Protocol	Transport Layer Security v1.2

A. Mastered
B. Not Mastered

Answer: A

Explanation:

source address	source address
destination address	source port
source port	destination port
destination port	destination address
Network Protocol	Transport Protocol
Transport Protocol	Network Protocol
Application Protocol	Application Protocol

NEW QUESTION 73
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 76
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 79
An analyst is exploring the functionality of different operating systems.
What is a feature of Windows Management Instrumentation that must be considered when deciding on an operating system?

A. queries Linux devices that have Microsoft Services for Linux installed
B. deploys Windows Operating Systems in an automated fashion
C. is an efficient tool for working with Active Directory
D. has a Common Information Model, which describes installed hardware and software

Answer: D

NEW QUESTION 82
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 84
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 89
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 90
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 95
......

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons 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 FirstTry

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

100% Actual & Verified — Instant Download, Please Click
Order The 200-201 Practice Test Here