

200-201 Dumps

Understanding Cisco Cybersecurity Operations Fundamentals

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



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

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

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 4

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 5

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

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

D. contractual

Answer: C

NEW QUESTION 6

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 7

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 8

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 9

Which attack method intercepts traffic on a switched network?

- A. denial of service
- B. ARP cache poisoning
- C. DHCP snooping
- D. command and control

Answer: C

NEW QUESTION 10

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 10

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 14

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 16

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 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

What is the practice of giving employees only those permissions necessary to perform their specific role within an organization?

- A. least privilege
- B. need to know
- C. integrity validation
- D. due diligence

Answer: A

NEW QUESTION 25

Which evasion technique is a function of ransomware?

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

Answer: B

NEW QUESTION 27

Which regex matches only on all lowercase letters?

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

Answer: A

NEW QUESTION 28

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 33

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 38

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 41

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 44

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 46

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 48

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 53

What is an attack surface as compared to a vulnerability?

- A. any potential danger to an asset
- B. the sum of all paths for data into and out of the application
- C. an exploitable weakness in a system or its design
- D. the individuals who perform an attack

Answer: B

NEW QUESTION 54

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 vector identifies 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 59

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 60

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 61

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 66

Which utility blocks a host portscan?

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

Answer: C

NEW QUESTION 69

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 73

An analyst is investigating an incident in a SOC environment. Which method is used to identify a session from a group of logs?

- A. sequence numbers
- B. IP identifier
- C. 5-tuple
- D. timestamps

Answer: C

NEW QUESTION 77

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 78

What does cyber attribution identify 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 81

How is attacking a vulnerability categorized?

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

Answer: C

NEW QUESTION 85

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

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

Answer: C

NEW QUESTION 89

Refer to the exhibit.

Date	Flow Start	Duration	Proto	Src IP Addr:Port	Dst IP Addr:Port	Packets	Bytes	Flows
2020-01-05	21:15:28.389	0.000	UDP	127.0.0.1:25678	→ 192.168.0.1:20521	1	82	1

Which type of log is displayed?

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

Answer: B

NEW QUESTION 90

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 94

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 95

Which two compliance frameworks require that data be encrypted when it is transmitted over a public network?
(Choose two.)

- A. PCI
- B. GLBA
- C. HIPAA
- D. SOX
- E. COBIT

Answer: AC

NEW QUESTION 96

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 100

Which action prevents buffer overflow attacks?

- A. variable randomization
- B. using web based applications
- C. input sanitization
- D. using a Linux operating system

Answer: C

NEW QUESTION 104

Refer to the exhibit.

	First Packet	Last Packet	Action	Reason	Initiator IP	Initiator Country	Initiator User	Responder IP	Responder Country	Security Intelligence Category	Ingress Security Zone	Egress Security Zone	Source Port/ICMP Type
2018-03-07 13:42:01			Sinkhole DNS Block		10.0.10.75		JERI LABORDE (DCLOUD-SOC LDAP)	10.110.10.11		DNS Intelligence-CnC	External	Internal	54925 / udp
2018-03-07 13:42:01			Sinkhole DNS Block		10.0.0.100		AMPARO GIVENS (DCLOUD-SOC LDAP)	10.110.10.11		DNS Intelligence-CnC	External	Internal	54925 / udp
2018-03-07 13:42:01			Sinkhole DNS Block		10.112.10.158		VERNETTA DONNEL (DCLOUD-SOC LDAP)	192.168.1.153		DNS Intelligence-CnC	External	Internal	54925 / udp

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 108

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 111

.....

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>