

200-201^{Q&As}

Understanding Cisco Cybersecurity Operations Fundamentals
(CBROPS)

Pass Cisco 200-201 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.leads4pass.com/200-201.html>

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Cisco
Official Exam Center

- ⚙ **Instant Download** After Purchase
- ⚙ **100% Money Back** Guarantee
- ⚙ **365 Days** Free Update
- ⚙ **800,000+** Satisfied Customers



QUESTION 1

Which process represents the application-level allow list?

- A. allowing everything and denying specific executable files
- B. allowing everything and denying specific applications protocols
- C. allowing specific files and deny everything else
- D. allowing specific format files and deny executable files

Correct Answer: C

QUESTION 2

Which statement describes patch management?

- A. scanning servers and workstations for missing patches and vulnerabilities
- B. process of appropriate distribution of system or software updates
- C. managing and keeping previous patches lists documented for audit purposes
- D. workflow of distributing mitigations of newly found vulnerabilities

Correct Answer: B

QUESTION 3

What is a Shellshock vulnerability?

- A. command injection
- B. cross site scripting
- C. heap overflow
- D. SQL injection

Correct Answer: A

QUESTION 4

What is obtained using NetFlow?

- A. session data
- B. application logs
- C. network downtime report
- D. full packet capture

Correct Answer: A

QUESTION 5

A cyberattacker notices a security flaw in a software that a company is using. They decide to tailor a specific worm to exploit this flaw and extract saved passwords from the software. To which category of the Cyber Kill Chain model does this event belong?

- A. weaponization
- B. reconnaissance
- C. delivery
- D. exploitation

Correct Answer: A

QUESTION 6

DRAG DROP

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

Select and Place:

tcpdump	session data
Cisco Umbrella	full packet capture
stateful firewall	transaction data
Snort	connection event

Correct Answer:

	stateful firewall
	tcpdump
	Snort
	Cisco Umbrella

QUESTION 7

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

Correct Answer: B

QUESTION 8

Which incidence response step includes identifying all hosts affected by an attack?

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

Correct Answer: A

The correct answer is A, detection and analysis.

The detection and analysis phase of an incident response process involves identifying and confirming the presence of a security incident. This includes identifying all hosts that may have been affected by the attack.

During this phase, incident responders collect and analyze information about the incident, such as network traffic, system logs, and other data, to determine the nature and scope of the incident. This information is used to develop an initial

understanding of the incident, including which hosts have been affected.

QUESTION 9

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

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

Correct Answer: C

QUESTION 10

An employee reports that someone has logged into their system and made unapproved changes, files are out of order, and several documents have been placed in the recycle bin. The security specialist reviewed the system logs, found nothing suspicious, and was not able to determine what occurred. The software is up to date; there are no alerts from antivirus and no failed login attempts. What is causing the lack of data visibility needed to detect the attack?

- A. The threat actor used a dictionary-based password attack to obtain credentials.
- B. The threat actor gained access to the system by known credentials.
- C. The threat actor used the teardrop technique to confuse and crash login services.
- D. The threat actor used an unknown vulnerability of the operating system that went undetected.

Correct Answer: C

QUESTION 11

A security incident occurred with the potential of impacting business services. Who performs the attack?

- A. malware author
- B. threat actor
- C. bug bounty hunter

D. direct competitor

Correct Answer: B

Reference: [https://www.paubox.com/blog/what-is-threat-actor/#:~:text=The%20term%20threat%20actor%20refers,CTA\)%20when%20referencing%20cybersecurity%20issues](https://www.paubox.com/blog/what-is-threat-actor/#:~:text=The%20term%20threat%20actor%20refers,CTA)%20when%20referencing%20cybersecurity%20issues)

QUESTION 12

An engineer received an alert affecting the degraded performance of a critical server. Analysis showed a heavy CPU and memory load. What is the next step the engineer should take to investigate this resource usage?

- A. Run "ps -d" to decrease the priority state of high load processes to avoid resource exhaustion.
- B. Run "ps -u" to find out who executed additional processes that caused a high load on a server.
- C. Run "ps -ef" to understand which processes are taking a high amount of resources.
- D. Run "ps -m" to capture the existing state of daemons and map required processes to find the gap.

Correct Answer: C

Reference: <https://unix.stackexchange.com/questions/62182/please-explain-this-output-of-ps-ef-command>

QUESTION 13

Refer to the exhibit. What is occurring?

4 3.257439886	12.0.0.2	12.0.0.129	DNS	456 Standard query response 0x5997 MX 11b263f22209000000000989b6e2a08cc5fe6608.
5 3.718661642	12.0.0.129	12.0.0.2	DNS	174 Standard query 0x8636 Txt 05de03f22239293affafc100003ab5766c1f577d6c30668.
6 3.886145548	12.0.0.2	12.0.0.129	DNS	353 Standard query response 0x8636 Txt 05de03f22239293affafc100003ab5766c1f57.
7 4.743778494	12.0.0.129	12.0.0.2	DNS	146 Standard query 0x6fc5 CNAME 1ed400f2224a945412939e0001215af4142f656d2289c.
8 4.903540523	12.0.0.2	12.0.0.129	DNS	263 Standard query response 0x6fc5 CNAME 1ed400f2224a945412939e0001215af4142f.
9 4.903748273	12.0.0.129	12.0.0.2	DNS	109 Standard query 0x7837 CNAME f82c01f22210e0c35e65740062c05981bf.opendns.on.
10 5.072886310	12.0.0.2	12.0.0.129	DNS	226 Standard query response 0x7837 CNAME f82c01f22210e0c35e65740062c05981bf.o.
11 5.937853691	12.0.0.129	12.0.0.2	DNS	109 Standard query 0x72d8 CNAME 9a3701f2226d6991886e3a00033dc27db8.opendns.on.
12 6.079753477	12.0.0.2	12.0.0.129	DNS	226 Standard query response 0x72d8 CNAME 9a3701f2226d6991886e3a00033dc27db8.o.
13 6.945991143	12.0.0.129	12.0.0.2	DNS	109 Standard query 0x72c0 Mx 943a01f2226ab84f07ebf3000456f16eb2.opendns.online
14 7.100047684	12.0.0.2	12.0.0.129	DNS	226 Standard query response 0x72c0 Mx 943a01f2226ab84f07ebf3000456f16eb2.open.
15 7.968146781	12.0.0.129	12.0.0.2	DNS	109 Standard query 0xce22 CNAME ee4101f2220c1e76127711000565b7d6d5.opendns.on.
16 8.125355386	12.0.0.2	12.0.0.129	DNS	226 Standard query response 0xce22 CNAME ee4101f2220c1e76127711000565b7d6d5.o.
17 8.992946441	12.0.0.129	12.0.0.2	DNS	109 Standard query 0xe941 Mx 88c701f222bd52954a7ec00006e9d39c4f.opendns.online
18 10.007498047	12.0.0.129	12.0.0.2	DNS	109 Standard query 0x48bf Txt 822061f222099927feb3480007579d416c.opendns.onli.
19 11.017158863	12.0.0.129	12.0.0.2	DNS	109 Standard query 0x134e Mx ff7101f2225a17cc007f3c0008c04c57e1.opendns.online

- A. possible DNS amplification attack with requests that maximize data quantity
- B. possible DNS tunneling with encrypted communication through CNAMEs
- C. possible DNS cache poisoning with misdirects toward a fraudulent website
- D. possible botnet traffic with random MX querying to generate increased traffic

Correct Answer: B

QUESTION 14

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

Correct Answer: C

QUESTION 15

The SOC team has confirmed a potential indicator of compromise on an endpoint. The team has narrowed the executable file's type to a new trojan family. According to the NIST Computer Security Incident Handling Guide, what is the next step in handling this event?

- A. Isolate the infected endpoint from the network.
- B. Perform forensics analysis on the infected endpoint.
- C. Collect public information on the malware behavior.
- D. Prioritize incident handling based on the impact.

Correct Answer: C

reference: <https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf>

[Latest 200-201 Dumps](#)

[200-201 Study Guide](#)

[200-201 Exam Questions](#)