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

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

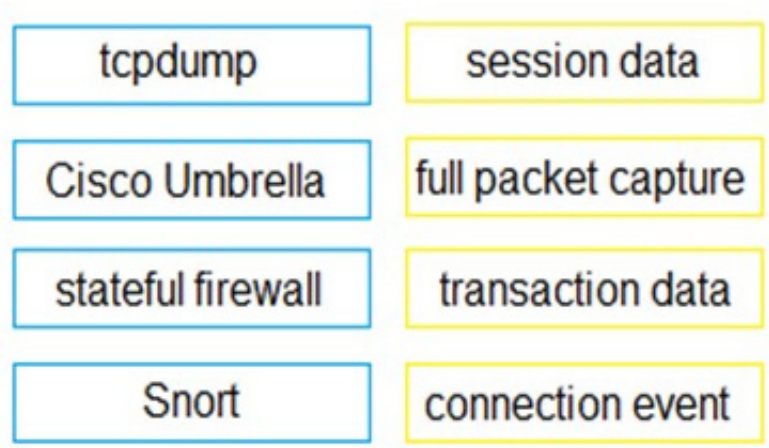
Correct Answer: A

QUESTION 6

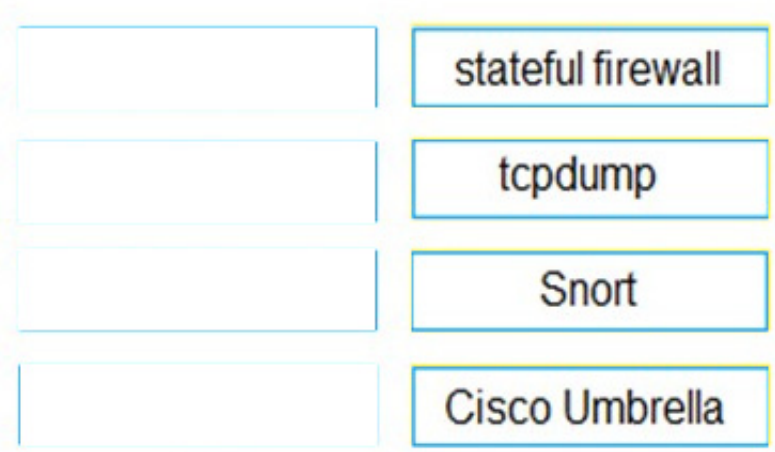
DRAG DROP

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

Select and Place:



Correct Answer:



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

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.

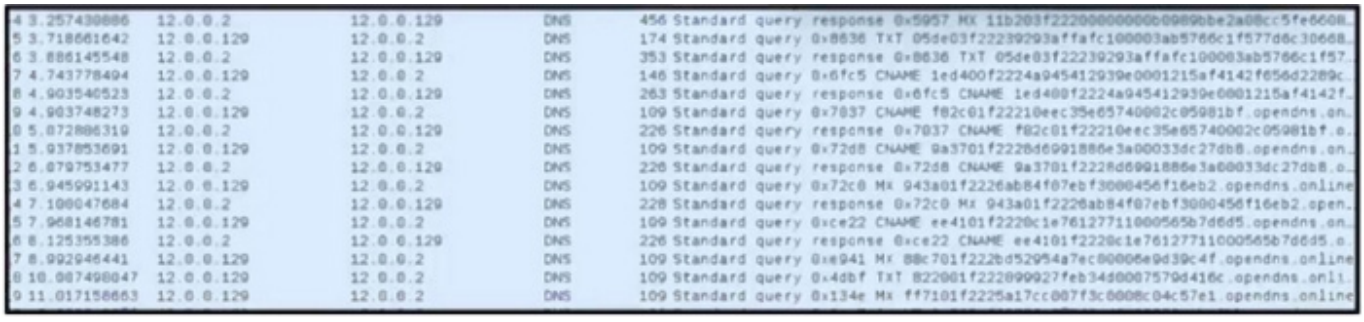
D. Run "ps -m" to capture the existing state of daemons and map required processes to find the gap.

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?



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

ference: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf