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.pass2lead.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

An employee received an email from a colleague\\'s address asking for the password for the domain controller. The employee noticed a missing letter within the sender\\'s address. What does this incident describe?

A. brute-force attack

B. insider attack

C. shoulder surfing

D. social engineering

Correct Answer: B

QUESTION 2

Which option describes indicators of attack?

A. blocked phishing attempt on a company

B. spam emails on an employee workstation

C. virus detection by the AV software

D. malware reinfection within a few minutes of removal

Correct Answer: D

QUESTION 3

What specific type of analysis is assigning values to the scenario to see expected outcomes?

A. deterministic

B. exploratory

C. probabilistic

D. descriptive

Correct Answer: A

QUESTION 4

What is a collection of compromised machines that attackers use to carry out a DDoS attack?

A. subnet

B. botnet

C. VLAN

D. command and control

Correct Answer: B

QUESTION 5

How does agentless monitoring differ from agent-based monitoring?

A. Agentless can access the data via API. while agent-base uses a less efficient method and accesses log data through WMI.

B. Agent-based monitoring is less intrusive in gathering log data, while agentless requires open ports to fetch the logs

C. Agent-based monitoring has a lower initial cost for deployment, while agentless monitoring requires resource-intensive deployment.

D. Agent-based has a possibility to locally filter and transmit only valuable data, while agentless has much higher network utilization

Correct Answer: D

Agent-based monitoring: With agent-based monitoring, software agents are installed on the monitored systems or devices. These agents collect data locally, perform filtering or preprocessing of the data, and then transmit the relevant or valuable information to the monitoring system. Agent-based monitoring allows for local processing and filtering, which can reduce network utilization by only transmitting essential data.

Agentless monitoring: Agentless monitoring, on the other hand, does not require software agents to be installed on the monitored systems or devices. Instead, it relies on leveraging existing protocols and interfaces, such as APIs (Application Programming Interfaces) or SNMP (Simple Network Management Protocol), to remotely access and retrieve monitoring data from the target systems. Agentless monitoring generally involves higher network utilization as the monitoring system needs to gather data from remote systems over the network.

QUESTION 6

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

Correct Answer: B

QUESTION 7

An organization\\'s security team has detected network spikes coming from the internal network. An investigation has concluded that the spike in traffic was from intensive network scanning How should the analyst collect the traffic to isolate the suspicious host?

A. by most active source IP

B. by most used ports

C. based on the protocols used

D. based on the most used applications

Correct Answer: A

QUESTION 8

A security engineer has a video of a suspect entering a data center that was captured on the same day that files in the same data center were transferred to a competitor. Which type of evidence is this?

A. best evidence

B. prima facie evidence

C. indirect evidence

D. physical evidence

Correct Answer: C

There are three general types of evidence:

--> Best evidence: can be presented in court in the original form (for example, an exact copy of a hard disk drive).

--> Corroborating evidence: tends to support a theory or an assumption deduced by some initial evidence. This corroborating evidence confirms the proposition. --> Indirect or circumstantial evidence: extrapolation to a conclusion of fact (such

as fingerprints, DNA evidence, and so on).

QUESTION 9

What matches the regular expression c(rgr)+e?

A. c(rgr)e

B. crgrrgre

C. crgr+e

D. ce

Correct Answer: B

QUESTION 10

An engineer is working on a ticket for an incident from the incident management team. A week ago, an external web application was targeted by a DDoS attack. Server resources were exhausted and after two hours, it crashed. An engineer was able to identify the attacker and technique used. Three hours after the attack, the server was restored and the engineer recommended implementing mitigation by Blackhole filtering and transferred the incident ticket back to the IR team. According to NIST.SP800-61, at which phase of the incident response did the engineer finish work?

A. post-incident activity

B. preparation

C. detection and analysis

D. containment, eradication, and recovery

Correct Answer: D

QUESTION 11

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

Correct Answer: D

QUESTION 12

Which tool gives the ability to see session data in real time?

A. tcpdstat

B. trafdump

C. tcptrace

D. trafshow

Correct Answer: C

QUESTION 13

What is the impact of false positive alerts on business compared to true positive?

A. True positives affect security as no alarm is raised when an attack has taken place, resulting in a potential breach.

B. True positive alerts are blocked by mistake as potential attacks affecting application availability.

C. False positives affect security as no alarm is raised when an attack has taken place, resulting in a potential breach.

D. False positive alerts are blocked by mistake as potential attacks affecting application availability.

Correct Answer: C

QUESTION 14

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

Correct Answer: C

QUESTION 15

Which security model assumes an attacker within and outside of the network and enforces strict verification before connecting to any system or resource within the organization?

A. Biba

B. Object-capability

C. Take-Grant

D. Zero Trust

Correct Answer: D

Zero Trust security is an IT security model that requires strict identity verification for every person and device trying to access resources on a private network, regardless of whether they are sitting within or outside of the network perimeter.