

350-201 Dumps

Performing CyberOps Using Core Security Technologies (CBRCOR)

<https://www.certleader.com/350-201-dumps.html>



NEW QUESTION 1

Which command does an engineer use to set read/write/execute access on a folder for everyone who reaches the resource?

- A. chmod 666
- B. chmod 774
- C. chmod 775
- D. chmod 777

Answer: D

NEW QUESTION 2

A patient views information that is not theirs when they sign in to the hospital's online portal. The patient calls the support center at the hospital but continues to be put on hold because other patients are experiencing the same issue. An incident has been declared, and an engineer is now on the incident bridge as the CyberOps Tier 3 Analyst. There is a concern about the disclosure of PII occurring in real-time. What is the first step the analyst should take to address this incident?

- A. Evaluate visibility tools to determine if external access resulted in tampering
- B. Contact the third-party handling provider to respond to the incident as critical
- C. Turn off all access to the patient portal to secure patient records
- D. Review system and application logs to identify errors in the portal code

Answer: C

NEW QUESTION 3

Refer to the exhibit.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.0.0.2	10.128.0.2	TCP	54	3341 -> 80 [SYN] Seq=0 Win=512 Len=0
2	0.003987	10.128.0.2	10.0.0.2	TCP	58	80 -> 3222 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
3	0.005514	10.128.0.2	10.0.0.2	TCP	54	80 -> 3341 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
4	0.008429	10.0.0.2	10.128.0.2	TCP	54	3342 -> 80 [SYN] Seq=0 Win=512 Len=0
5	0.010233	10.128.0.2	10.0.0.2	TCP	58	80 -> 3220 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
6	0.014072	10.128.0.2	10.0.0.2	TCP	58	80 -> 3342 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
7	0.016830	10.0.0.2	10.128.0.2	TCP	54	3343 -> 80 [SYN] Seq=0 Win=512 Len=0
8	0.022220	10.128.0.2	10.0.0.2	TCP	58	80 -> 3343 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
9	0.023496	10.128.0.2	10.0.0.2	TCP	58	80 -> 3219 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
10	0.025243	10.0.0.2	10.128.0.2	TCP	58	3344 -> 80 [SYN] Seq=0 Win=512 Len=0
11	0.026672	10.128.0.2	10.0.0.2	TCP	58	80 -> 3218 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
12	0.028038	10.128.0.2	10.0.0.2	TCP	58	80 -> 3221 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
13	0.030523	10.128.0.2	10.0.0.2	TCP	58	80 -> 3344 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460

Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)	
Ethernet II, Src: 42:01:0a:f0:00:17 (42:01:0a:f0:00:17), Dst: 42:01:0a:f0:00:01 (42:01:0a:f0:00:01)	
Internet Protocol Version 4, Src: 10.0.0.2, Dst: 10.128.0.2	
Transmission Control Protocol, Src Port: 3341, Dst Port: 80, Seq: 0, Len: 0	
Source port: 3341 Destination port: 80 [Stream index: 0] [TCP Segment Len: 0] Sequence number: 0 (relative sequence number) [Next sequence number: 0 (relative sequence number)] Acknowledgment number: 1023350804 0101 = Header Length: 20 bytes (5) Flags: 0x002 (SYN) Window size value: 512 [Calculated window size: 512] Checksum: 0x8d5a [unverified] [Checksum Status: Unverified] Urgent pointer: 0 [Timestamps]	

What is the threat in this Wireshark traffic capture?

- A. A high rate of SYN packets being sent from multiple sources toward a single destination IP
- B. A flood of ACK packets coming from a single source IP to multiple destination IPs
- C. A high rate of SYN packets being sent from a single source IP toward multiple destination IPs
- D. A flood of SYN packets coming from a single source IP to a single destination IP

Answer: D

NEW QUESTION 4

An engineer is investigating several cases of increased incoming spam emails and suspicious emails from the HR and service departments. While checking the event sources, the website monitoring tool showed several web scraping alerts overnight. Which type of compromise is indicated?

- A. phishing
- B. dumpster diving
- C. social engineering
- D. privilege escalation

Answer: C

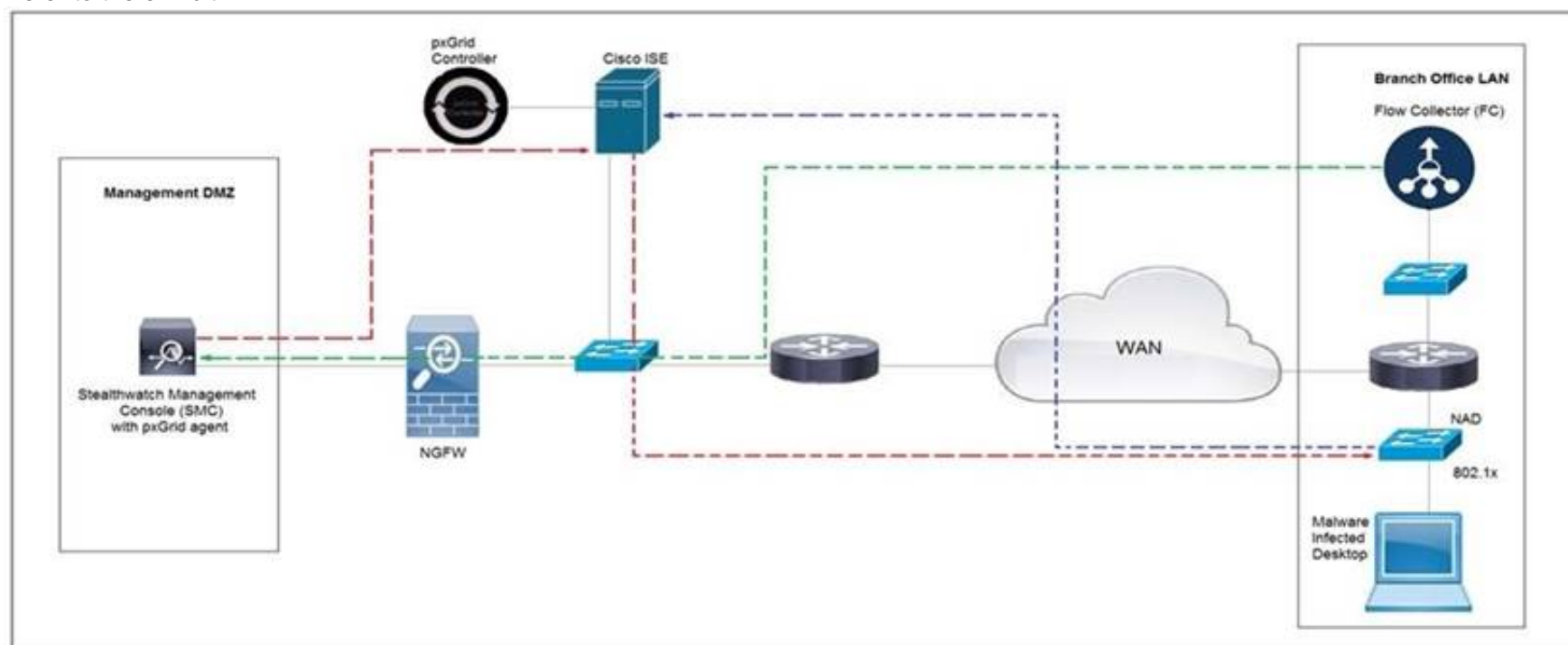
NEW QUESTION 5

Refer to the exhibit.

- /invoker/JMXInvokerServlet
- /CFIDE/adminapi
- /?a=<script>alert%28%22XSS%22%29%3B</script>&b=UNION+SELECT+ALL+FROM+information_schema+AND+%27or+SLEEP%285%29+or+%27&c=../../../../etc/passwd

- A. exploitation
- B. actions on objectives
- C. delivery
- D. reconnaissance

Refer to the exhibit.



A. NetFlow and event data
B. event data and syslog data
C. SNMP and syslog data
D. NetFlow and SNMP

Drag and drop the NIST incident response process steps from the left onto the actions that occur in the steps on the right.

Eradicate	Analyze and document the breach, and strengthen systems against future attacks
Contain	Conduct incident response role training for employees
Post-Incident Handling	Determine where the breach started and prevent the attack from spreading
Recover	Determine how the breach was discovered and the areas that were impacted
Analyze	Eliminate the root cause of the breach and apply updates to the system
Prepare	Get systems and business operations up and running, and ensure that the same type of attack does not occur again

visit - <https://www.certleader.com>

B. Not Mastered

Answer: A

Explanation:

Answer Area

Eradicate	Contain
Contain	Prepare
Post-Incident Handling	Recover
Recover	Analyze
Analyze	Eradicate
Prepare	Post-Incident Handling

NEW QUESTION 8

What is a limitation of cyber security risk insurance?

- A. It does not cover the costs to restore stolen identities as a result of a cyber attack
- B. It does not cover the costs to hire forensics experts to analyze the cyber attack
- C. It does not cover the costs of damage done by third parties as a result of a cyber attack
- D. It does not cover the costs to hire a public relations company to help deal with a cyber attack

Answer: A

NEW QUESTION 9

Refer to the exhibit.



An engineer is investigating a case with suspicious usernames within the active directory. After the engineer investigates and cross-correlates events from other sources, it appears that the 2 users are privileged, and their creation date matches suspicious network traffic that was initiated from the internal network 2 days prior. Which type of compromise is occurring?

- A. compromised insider
- B. compromised root access
- C. compromised database tables
- D. compromised network

Answer: D

NEW QUESTION 10

A new malware variant is discovered hidden in pirated software that is distributed on the Internet. Executives have asked for an organizational risk assessment. The security officer is given a list of all assets. According to NIST, which two elements are missing to calculate the risk assessment? (Choose two.)

- A. incident response playbooks
- B. asset vulnerability assessment
- C. report of staff members with asset relations
- D. key assets and executives
- E. malware analysis report

Answer: BE

NEW QUESTION 10

An engineer returned to work and realized that payments that were received over the weekend were sent to the wrong recipient. The engineer discovered that the SaaS tool that processes these payments was down over the weekend. Which step should the engineer take first?

- A. Utilize the SaaS tool team to gather more information on the potential breach
- B. Contact the incident response team to inform them of a potential breach
- C. Organize a meeting to discuss the services that may be affected
- D. Request that the purchasing department creates and sends the payments manually

Answer: A

NEW QUESTION 13

What is the HTTP response code when the REST API information requested by the authenticated user cannot be found?

- A. 401B.-402C.403D.404E.405

Answer: A

NEW QUESTION 18

A SIEM tool fires an alert about a VPN connection attempt from an unusual location. The incident response team validates that an attacker has installed a remote access tool on a user's laptop while traveling. The attacker has the user's credentials and is attempting to connect to the network. What is the next step in handling the incident?

- A. Block the source IP from the firewall
- B. Perform an antivirus scan on the laptop
- C. Identify systems or services at risk
- D. Identify lateral movement

Answer: C

NEW QUESTION 21

A company's web server availability was breached by a DDoS attack and was offline for 3 hours because it was not deemed a critical asset in the incident response playbook. Leadership has requested a risk assessment of the asset. An analyst conducted the risk assessment using the threat sources, events, and vulnerabilities. Which additional element is needed to calculate the risk?

- A. assessment scope
- B. event severity and likelihood
- C. incident response playbook
- D. risk model framework

Answer: D

NEW QUESTION 25

A threat actor used a phishing email to deliver a file with an embedded macro. The file was opened, and a remote code execution attack occurred in a company's infrastructure. Which steps should an engineer take at the recovery stage?

- A. Determine the systems involved and deploy available patches
- B. Analyze event logs and restrict network access
- C. Review access lists and require users to increase password complexity
- D. Identify the attack vector and update the IDS signature list

Answer: B

NEW QUESTION 27

Refer to the exhibit.

```
def get_umbrella_dispos(domains):
    # put in right format to pass as argument in POST request
    values = str(json.dumps(domains))
    req = requests.post(investigate_url, data=values, headers=headers)
    # time for timestamp of verdict domain
    time = datetime.now().isoformat()
    # error handling if true then the request was HTTP 200, so successful
    if(req.status_code == 200):
        print("SUCCESS: request has the following code: 200\n")
        output = req.json()

        if(domain_status == -1):
            print("The domain %(domain)s is found MALICIOUS at %(time)s\n" % {'domain': domain, 'time': time})
        elif(domain_status == 1):
            print("The domain %(domain)s is found CLEAN at %(time)s\n" % {'domain': domain, 'time': time})
        else:
            print("The domain %(domain)s is found UNDEFINED / RISKY at %(time)s\n" % {'domain': domain, 'time': time})
    else:
        print("An error has occurred with the following code %(error)s, please consult the following link: https://docs.umbrella.com/investigate-api/" % {'error': req.status_code})
```

Which code snippet will parse the response to identify the status of the domain as malicious, clean or undefined?

- A.

```
for domain in domains[:]:
    domain_status = domain_output["status"]
```
- B.

```
while domain in domains:
    domain_status = domain_output["status"]
```
- C.

```
for domain in domains:
    domain_output = output[domain]
    domain_status = domain_output["status"]
```
- D.

```
while domains in domains:
    domain_output = output[domain]
    domain_status = domain_output["status"]
```

- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: C

NEW QUESTION 32

An API developer is improving an application code to prevent DDoS attacks. The solution needs to accommodate instances of a large number of API requests coming for legitimate purposes from trustworthy services. Which solution should be implemented?

- A. Restrict the number of requests based on a calculation of daily average
- B. If the limit is exceeded, temporarily block access from the IP address and return a 402 HTTP error code.
- C. Implement REST API Security Essentials solution to automatically mitigate limit exhaustio
- D. If the limit is exceeded, temporarily block access from the service and return a 409 HTTP error code.
- E. Increase a limit of replies in a given interval for each AP
- F. If the limit is exceeded, block access from the API key permanently and return a 450 HTTP error code.
- G. Apply a limit to the number of requests in a given time interval for each AP
- H. If the rate is exceeded, block access from the API key temporarily and return a 429 HTTP error code.

Answer: D

NEW QUESTION 35

A customer is using a central device to manage network devices over SNMPv2. A remote attacker caused a denial of service condition and can trigger this vulnerability by issuing a GET request for the ciscoFlashMIB OID on an affected device. Which should be disabled to resolve the issue?

- A. SNMPv2
- B. TCP small services
- C. port UDP 161 and 162
- D. UDP small services

Answer: A

NEW QUESTION 36

An engineer receives an incident ticket with hundreds of intrusion alerts that require investigation. An analysis of the incident log shows that the alerts are from

trusted IP addresses and internal devices. The final incident report stated that these alerts were false positives and that no intrusions were detected. What action should be taken to harden the network?

- A. Move the IPS to after the firewall facing the internal network
- B. Move the IPS to before the firewall facing the outside network
- C. Configure the proxy service on the IPS
- D. Configure reverse port forwarding on the IPS

Answer: C

NEW QUESTION 39

Refer to the exhibit.

<p>Vulnerability #1</p> <p>A vulnerability in the Command Line Interpreter (CLI) of ACME Super Firewall (all models) could allow an attacker to execute a command which would overflow a buffer in memory. In order to carry out this attack, the attacker needs to fulfill all of the following conditions:</p> <ul style="list-style-type: none"> a) Be logged in to the device over telnet or SSH, or through the local console b) Be logged in as a high-privileges administrative user <p>In order to trigger the vulnerability, the attacker has to execute a command on the device and supply a specially crafted argument to such command. Once the command is executed, an internal stack-based buffer overflow will be triggered. This buffer overflow may lead to code execution within the process space of the CLI parser, or may crash the device.</p> <p>All software versions are affected Fixes are available now There are no workarounds or mitigations</p>	<p>Vulnerability #2</p> <p>A vulnerability in the web-based management interface of the ACME Big Router models 1010 and 1020 could allow an attacker to bypass authorization checks and then access sensitive information on the device, modify the device's configuration, impact the availability of the system, create administrative level and regular level users on the device. In order to exploit this vulnerability, the attacker needs to:</p> <ul style="list-style-type: none"> a) Be able to reach port 80/tcp on an affected device b) The web-based management interface needs to be enabled on the device <p>The attacker would then need to send a specially formed HTTP request to the web-based management interface of an affected system. The attacker does not need to log-in to the device before launching the attack.</p> <p>All software versions are affected There are no fixes available now Customers can disable the web-based management interface to prevent exploitation. Customers will still be able to manage, configure and monitor the device by using the Command Line Interface (CLI), but with reduced capabilities for monitoring.</p>
---	--

How must these advisories be prioritized for handling?

- A. The highest priority for handling depends on the type of institution deploying the devices
- B. Vulnerability #2 is the highest priority for every type of institution
- C. Vulnerability #1 and vulnerability #2 have the same priority
- D. Vulnerability #1 is the highest priority for every type of institution

Answer: D

NEW QUESTION 42

Refer to the exhibit.

```
#!/usr/bin/env python3

import re

def (username, minlen):
    if type(username) != str:
        raise TypeError
    if minlen < 3:
        raise ValueError
    if len(username) < minlen:
        return False
    if not re.match('[a-z0-9._]*$', username):
        return False
    if username[0].isnumeric():
        return False
    return True
```

An organization is using an internal application for printing documents that requires a separate registration on the website. The application allows format-free user creation, and users must match these required conditions to comply with the company's user creation policy:

- minimum length: 3
- usernames can only use letters, numbers, dots, and underscores
- usernames cannot begin with a number

The application administrator has to manually change and track these daily to ensure compliance. An engineer is tasked to implement a script to automate the

process according to the company user creation policy. The engineer implemented this piece of code within the application, but users are still able to create format-free usernames. Which change is needed to apply the restrictions?

- A. modify code to return error on restrictions `def return_false_user(username, minlen)`
- B. automate the restrictions `def automate_user(username, minlen)`
- C. validate the restrictions, `def validate_user(username, minlen)`
- D. modify code to force the restrictions, `def force_user(username, minlen)`

Answer: B

NEW QUESTION 45

What is a benefit of key risk indicators?

- A. clear perspective into the risk position of an organization
- B. improved visibility on quantifiable information
- C. improved mitigation techniques for unknown threats
- D. clear procedures and processes for organizational risk

Answer: C

NEW QUESTION 48

Drag and drop the components from the left onto the phases of the CI/CD pipeline on the right.

Answer Area

build	Phase 1
release	Phase 2
deploy	Phase 3
operate	Phase 4
monitor	Phase 5
test	Phase 6
plan	Phase 7
develop	Phase 8

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

build	plan
release	develop
deploy	build
operate	test
monitor	release
test	deploy
plan	operate
develop	monitor

NEW QUESTION 52

Refer to the exhibit.

TCP	192.168.1.8:54580	vk-in-f108:imaps	ESTABLISHED
TCP	192.168.1.8:54583	132.245.61.50:https	ESTABLISHED
TCP	192.168.1.8:54916	bay405-m:https	ESTABLISHED
TCP	192.168.1.8:54978	vu-in-f188:5228	ESTABLISHED
TCP	192.168.1.8:55094	72.21.194.109:https	ESTABLISHED
TCP	192.168.1.8:55401	wonderhowto:http	ESTABLISHED
TCP	192.168.1.8:55730	mia07s34-in-f78:https	TIME_WAIT
TCP	192.168.1.8:55824	a23-40-191-15:https	CLOSE_WAIT
TCP	192.168.1.8:55825	a23-40-191-15:https	CLOSE_WAIT
TCP	192.168.1.8:55846	mia07s25-in-f14:https	TIME_WAIT
TCP	192.168.1.8:55847	a184-51-150-89:http	CLOSE_WAIT
TCP	192.168.1.8:55853	157.55.56.154:40028	ESTABLISHED
TCP	192.168.1.8:55879	atl14s38-in-f4:https	ESTABLISHED
TCP	192.168.1.8:55884	208-46-117-174:https	ESTABLISHED
TCP	192.168.1.8:55893	vx-in-f95:https	TIME_WAIT
TCP	192.168.1.8:55947	stackoverflow:https	ESTABLISHED
TCP	192.168.1.8:55966	stackoverflow:https	ESTABLISHED
TCP	192.168.1.8:55970	mia07s34-in-f78:https	TIME_WAIT
TCP	192.168.1.8:55972	191.238.241.80:https	TIME_WAIT
TCP	192.168.1.8:55976	54.239.26.242:https	ESTABLISHED
TCP	192.168.1.8:55979	mia07s35-in-f14:https	ESTABLISHED
TCP	192.168.1.8:55986	server11:https	TIME_WAIT
TCP	192.168.1.8:55988	104.16.118.182:http	ESTABLISHED

A security analyst needs to investigate a security incident involving several suspicious connections with a possible attacker. Which tool should the analyst use to identify the source IP of the offender?

- A. packet sniffer
- B. malware analysis
- C. SIEM
- D. firewall manager

Answer: A

NEW QUESTION 56

An engineer received an alert of a zero-day vulnerability affecting desktop phones through which an attacker sends a crafted packet to a device, resets the credentials, makes the device unavailable, and allows a default administrator account login. Which step should an engineer take after receiving this alert?

- A. Initiate a triage meeting to acknowledge the vulnerability and its potential impact
- B. Determine company usage of the affected products
- C. Search for a patch to install from the vendor
- D. Implement restrictions within the VoIP VLANs

Answer: C

NEW QUESTION 57

A security expert is investigating a breach that resulted in a \$32 million loss from customer accounts. Hackers were able to steal API keys and two-factor codes due to a vulnerability that was introduced in a new code a few weeks before the attack. Which step was missed that would have prevented this breach?

- A. use of the Nmap tool to identify the vulnerability when the new code was deployed
- B. implementation of a firewall and intrusion detection system
- C. implementation of an endpoint protection system
- D. use of SecDevOps to detect the vulnerability during development

Answer: D

NEW QUESTION 58

Refer to the exhibit.

Asset	Threat	Vulnerability	Likelihood (1-10)	Impact (1-10)
Servers	Natural Disasters – Flooding	Server Room is on the zero floor	3	10
Secretary Workstation	Usage of illegitimate software	Inadequate control of software	7	6
Payment Process	Eavesdropping, Misrouting/re-routing of messages	Unencrypted communications	5	10
Website	Website Intrusion	No IDS/IPS usage	6	8

Which asset has the highest risk value?

- A. servers
- B. website
- C. payment process
- D. secretary workstation

Answer: C

NEW QUESTION 62

.....

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 350-201 Exam with Our Prep Materials Via below:

<https://www.certleader.com/350-201-dumps.html>