

Cisco

Exam Questions 350-201

Performing CyberOps Using Core Security Technologies (CBRCOR)



NEW QUESTION 1

Refer to the exhibit.

Max (K)	Retain	OverflowAction	Entries	Log
15,168	0	OverwriteAsNeeded	20,792	Application
15,168	0	OverwriteAsNeeded	12,559	System
15,360	0	OverwriteAsNeeded	11,173	Windows PowerShell

Which command was executed in PowerShell to generate this log?

- A. Get-EventLog -LogName*
- B. Get-EventLog -List
- C. Get-WinEvent -ListLog* -ComputerName localhost
- D. Get-WinEvent -ListLog*

Answer: A

NEW QUESTION 2

How is a SIEM tool used?

- A. To collect security data from authentication failures and cyber attacks and forward it for analysis
- B. To search and compare security data against acceptance standards and generate reports for analysis
- C. To compare security alerts against configured scenarios and trigger system responses
- D. To collect and analyze security data from network devices and servers and produce alerts

Answer: D

NEW QUESTION 3

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 4

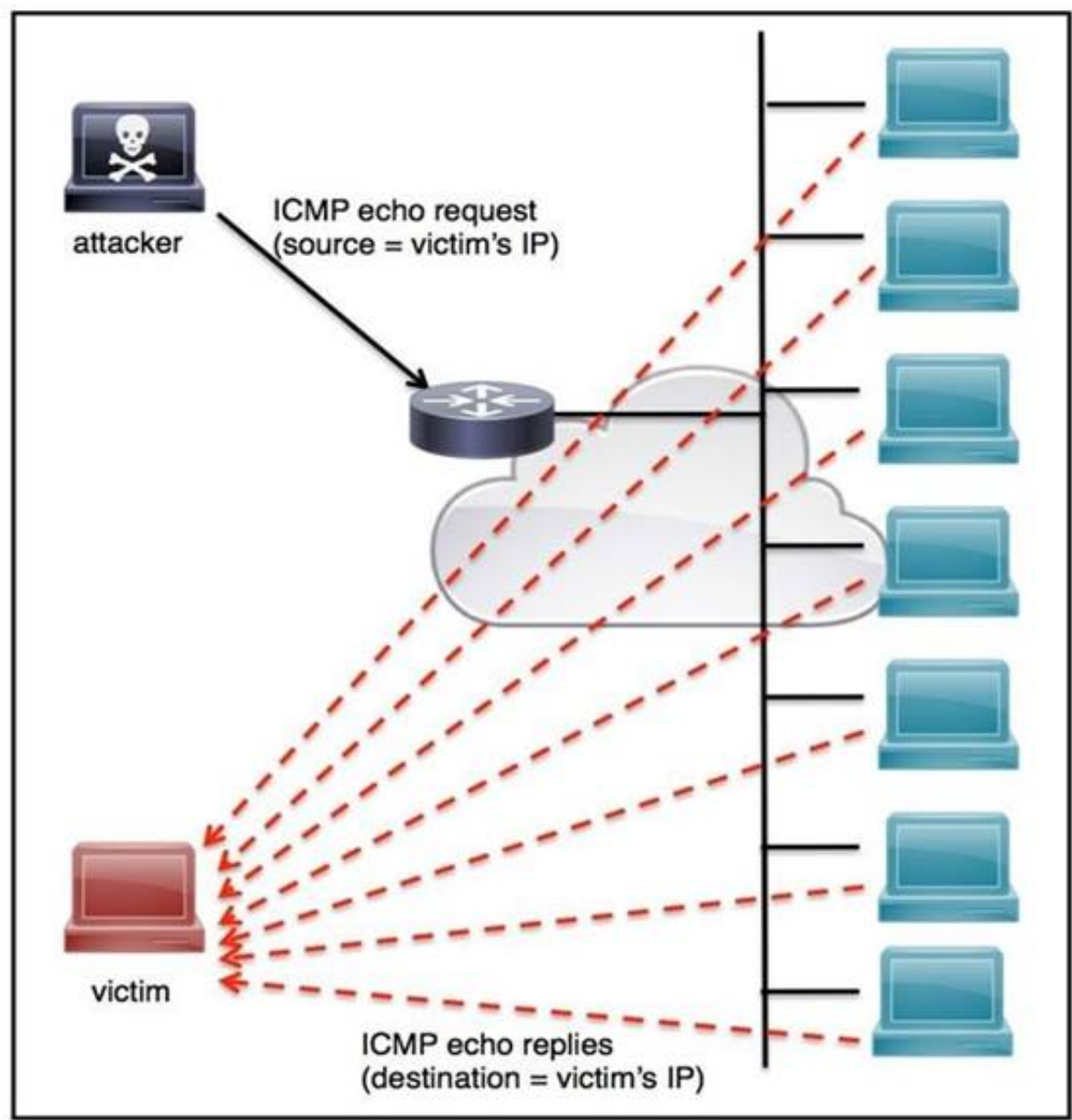
An employee who often travels abroad logs in from a first-seen country during non-working hours. The SIEM tool generates an alert that the user is forwarding an increased amount of emails to an external mail domain and then logs out. The investigation concludes that the external domain belongs to a competitor. Which two behaviors triggered UEBA? (Choose two.)

- A. domain belongs to a competitor
- B. log in during non-working hours
- C. email forwarding to an external domain
- D. log in from a first-seen country
- E. increased number of sent mails

Answer: AB

NEW QUESTION 5

Refer to the exhibit.



An engineer must tune the Cisco IOS device to mitigate an attack that is broadcasting a large number of ICMP packets. The attack is sending the victim's spoofed source IP to a network using an IP broadcast address that causes devices in the network to respond back to the source IP address. Which action does the engineer recommend?

- A. Use command ip verify reverse-path interface
- B. Use global configuration command service tcp-keepalives-out
- C. Use subinterface command no ip directed-broadcast
- D. Use logging trap 6

Answer: A

NEW QUESTION 6

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

Answer Area

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

- A. Mastered
- B. Not Mastered

Answer: A

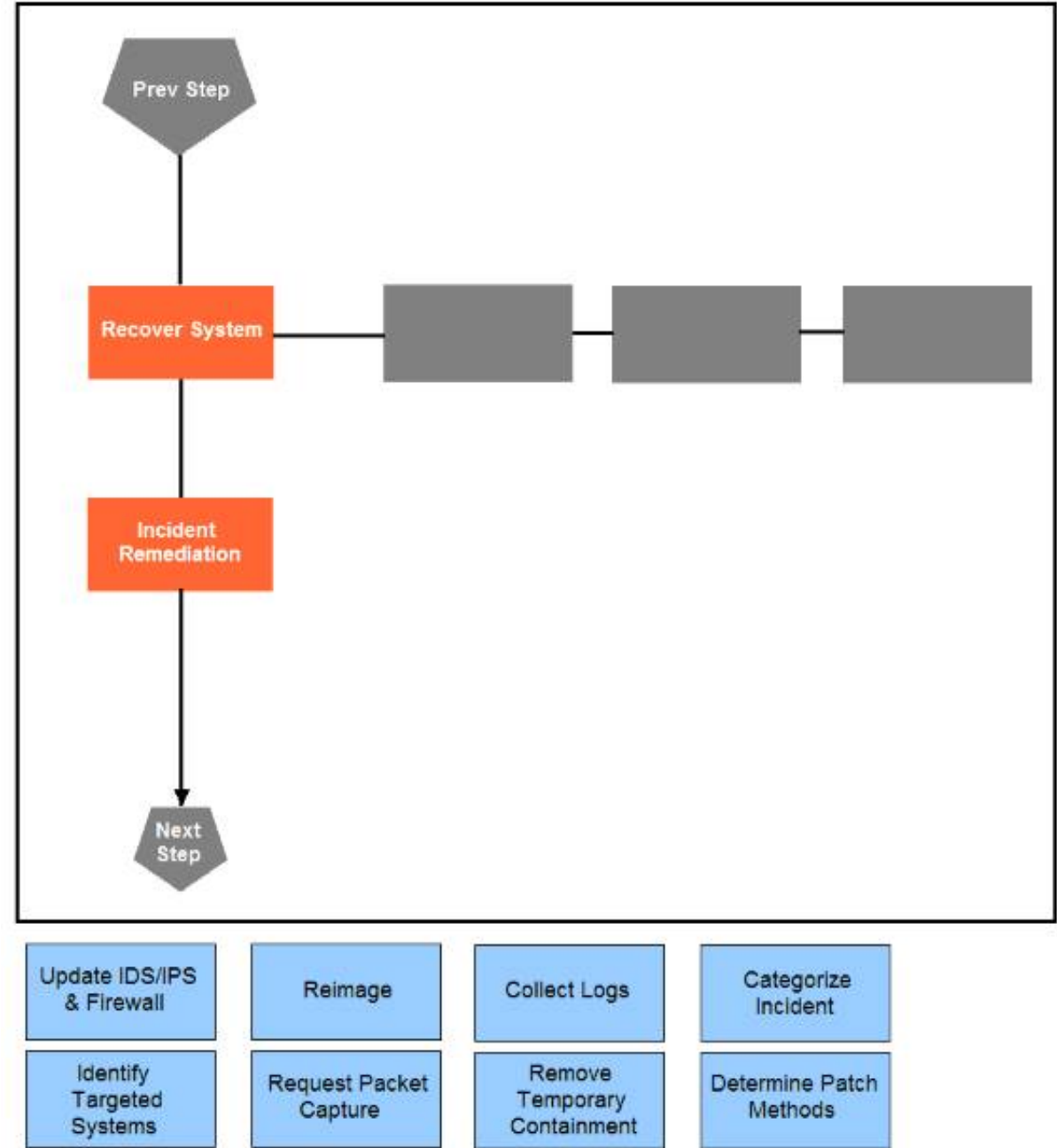
Explanation:

Answer Area

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

NEW QUESTION 7

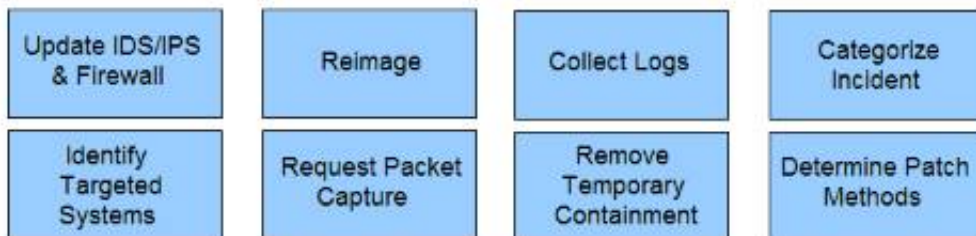
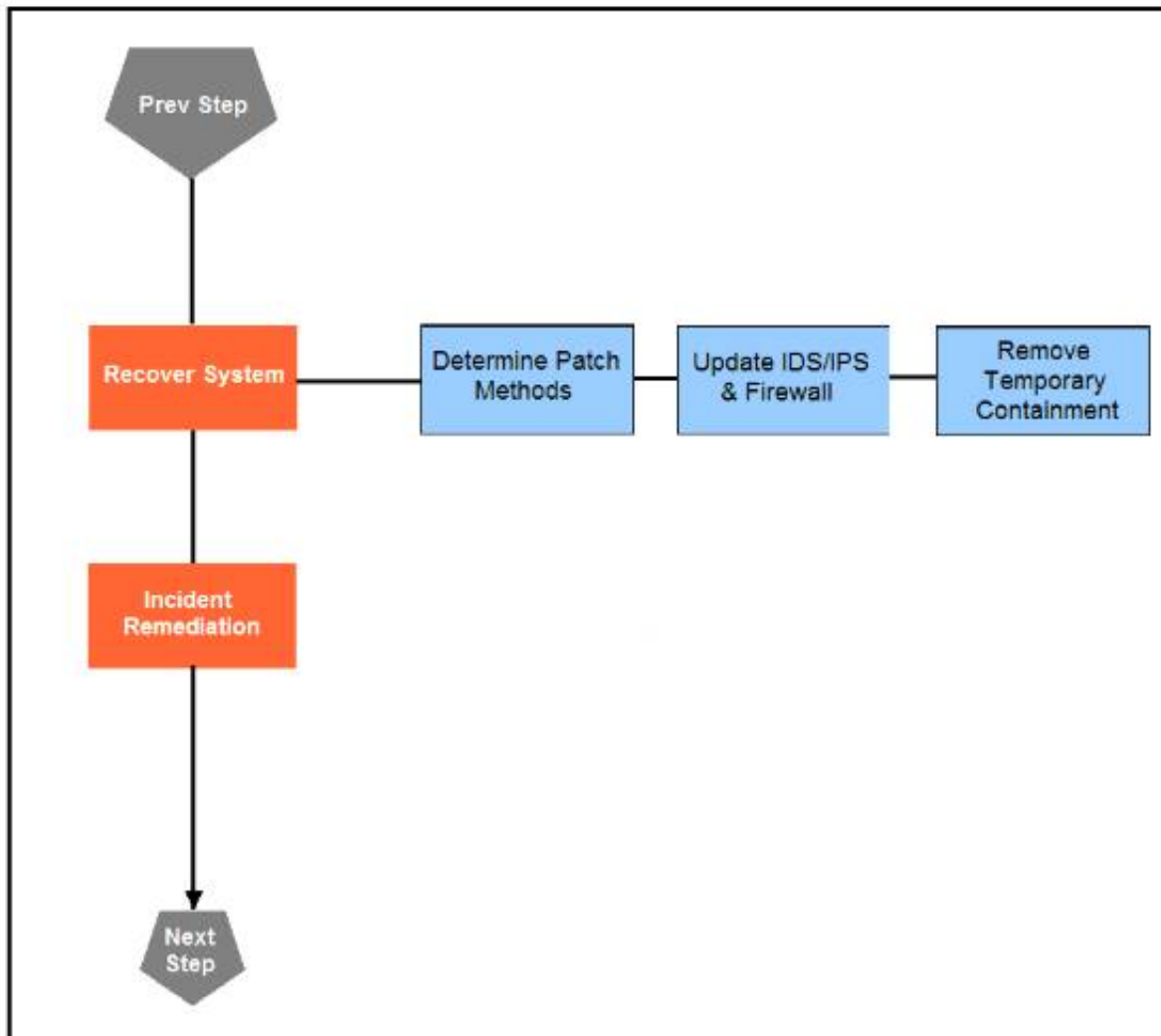
Drag and drop the actions below the image onto the boxes in the image for the actions that should be taken during this playbook step. Not all options are used.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 8

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 9

An engineer has created a bash script to automate a complicated process. During script execution, this error occurs: permission denied. Which command must be added to execute this script?

- A. chmod +x ex.sh

- B. source ex.sh
- C. chroot ex.sh
- D. sh ex.sh

Answer: A

NEW QUESTION 10

A security analyst receives an escalation regarding an unidentified connection on the Accounting A1 server within a monitored zone. The analyst pulls the logs and discovers that a Powershell process and a WMI tool process were started on the server after the connection was established and that a PE format file was created in the system directory. What is the next step the analyst should take?

- A. Isolate the server and perform forensic analysis of the file to determine the type and vector of a possible attack
- B. Identify the server owner through the CMDB and contact the owner to determine if these were planned and identifiable activities
- C. Review the server backup and identify server content and data criticality to assess the intrusion risk
- D. Perform behavioral analysis of the processes on an isolated workstation and perform cleaning procedures if the file is malicious

Answer: C

NEW QUESTION 10

An engineer is utilizing interactive behavior analysis to test malware in a sandbox environment to see how the malware performs when it is successfully executed. A location is secured to perform reverse engineering on a piece of malware. What is the next step the engineer should take to analyze this malware?

- A. Run the program through a debugger to see the sequential actions
- B. Unpack the file in a sandbox to see how it reacts
- C. Research the malware online to see if there are noted findings
- D. Disassemble the malware to understand how it was constructed

Answer: C

NEW QUESTION 12

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 16

An engineer implemented a SOAR workflow to detect and respond to incorrect login attempts and anomalous user behavior. Since the implementation, the security team has received dozens of false positive alerts and negative feedback from system administrators and privileged users. Several legitimate users were tagged as a threat and their accounts blocked, or credentials reset because of unexpected login times and incorrectly typed credentials. How should the workflow be improved to resolve these issues?

- A. Meet with privileged users to increase awareness and modify the rules for threat tags and anomalous behavior alerts
- B. Change the SOAR configuration flow to remove the automatic remediation that is increasing the false positives and triggering threats
- C. Add a confirmation step through which SOAR informs the affected user and asks them to confirm whether they made the attempts
- D. Increase incorrect login tries and tune anomalous user behavior not to affect privileged accounts


Answer: B

NEW QUESTION 18

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 19

An engineer is developing an application that requires frequent updates to close feedback loops and enable teams to quickly apply patches. The team wants their code updates to get to market as often as possible. Which software development approach should be used to accomplish these goals?

- A. continuous delivery
- B. continuous integration
- C. continuous deployment
- D. continuous monitoring

Answer: A

NEW QUESTION 23

Refer to the exhibit.

Analysis Report			
ID	12cbeee21b1ea4	Filename	fpzryrf.exe
OS	7601.1898.amd64fre.win7sp1_gdr.150316-1654	Magic Type	PE32 executable (GUI) Intel 80386, for MS Windows
Started	7/29/16 18:44:43	Analyzed As	exe
Ended	7/29/16 18:50:39	SHA256	e9ca08a3cc2f8c9748a9e9b304c9f5a16d830066e5467d3dd5927be36fec47da
Duration	0:05:56	SHA1	a2de85810fd5ebcf29c5da5dd29ce03470772ad
Sandbox	phl-work-02 (pilot-d)	MD5	dd07d778edf8d581ffaadb1610aaa008
Warnings			
+ Executable Failed Integrity Check			
Behavioral Indicators			
+ CTB Locker Detected	Severity: 100	Confidence: 100	
+ Generic Ransomware Detected	Severity: 100	Confidence: 95	
+ Excessive Suspicious Activity Detected	Severity: 90	Confidence: 100	
+ Process Modified a File in a System Directory	Severity: 90	Confidence: 100	
+ Large Amount of High Entropy Artifacts Written	Severity: 100	Confidence: 80	
+ Process Modified a File in the Program Files Directory	Severity: 80	Confidence: 90	
+ Decoy Document Detected	Severity: 70	Confidence: 100	
+ Process Modified an Executable File	Severity: 60	Confidence: 100	
+ Process Modified File in a User Directory	Severity: 70	Confidence: 80	
+ Windows Crash Tool Execution Detected	Severity: 20	Confidence: 80	
+ Hook Procedure Detected in Executable	Severity: 35	Confidence: 40	
+ Ransomware Queried Domain	Severity: 25	Confidence: 25	
+ Executable Imported the IsDebuggerPresent Symbol	Severity: 20	Confidence: 20	

Cisco Advanced Malware Protection installed on an end-user desktop has automatically submitted a low prevalence file to the Threat Grid analysis engine for further analysis. What should be concluded from this report?

- A. The prioritized behavioral indicators of compromise do not justify the execution of the “ransomware” because the scores do not indicate the likelihood of

- malicious ransomware.
- B. The prioritized behavioral indicators of compromise do not justify the execution of the “ransomware” because the scores are high and do not indicate the likelihood of malicious ransomware.
- C. The prioritized behavioral indicators of compromise justify the execution of the “ransomware” because the scores are high and indicate the likelihood that malicious ransomware has been detected.
- D. The prioritized behavioral indicators of compromise justify the execution of the “ransomware” because the scores are low and indicate the likelihood that malicious ransomware has been detected.

Answer: C

NEW QUESTION 27

Refer to the exhibit.

Max (K)	Retain	OverflowAction	Entries	Log
-----	-----	-----	-----	---
15,168	0	OverwriteAsNeeded	20,792	Application
15,168	0	OverwriteAsNeeded	12,559	System
15,360	0	OverwriteAsNeeded	11,173	Windows PowerShell

An employee is a victim of a social engineering phone call and installs remote access software to allow an “MS Support” technician to check his machine for malware. The employee becomes suspicious after the remote technician requests payment in the form of gift cards. The employee has copies of multiple, unencrypted database files, over 400 MB each, on his system and is worried that the scammer copied the files off but has no proof of it. The remote technician was connected sometime between 2:00 pm and 3:00 pm over https. What should be determined regarding data loss between the employee’s laptop and the remote technician’s system?

- A. No database files were disclosed
- B. The database files were disclosed
- C. The database files integrity was violated
- D. The database files were intentionally corrupted, and encryption is possible

Answer: C

NEW QUESTION 30

An engineer is moving data from NAS servers in different departments to a combined storage database so that the data can be accessed and analyzed by the organization on-demand. Which data management process is being used?

- A. data clustering
- B. data regression
- C. data ingestion
- D. data obfuscation

Answer: A

NEW QUESTION 33

A threat actor has crafted and sent a spear-phishing email with what appears to be a trustworthy link to the site of a conference that an employee recently attended. The employee clicked the link and was redirected to a malicious site through which the employee downloaded a PDF attachment infected with ransomware. The employee opened the attachment, which exploited vulnerabilities on the desktop. The ransomware is now installed and is calling back to its command and control server. Which security solution is needed at this stage to mitigate the attack?

- A. web security solution
- B. email security solution
- C. endpoint security solution
- D. network security solution

Answer: D

NEW QUESTION 36

Refer to the exhibit.


```
def map_to_lowercase_letter(s):
    return ord('a') + ((s-ord('a')) % 26)
def next_domain(domain):
    dl = [ord(x) for x in list(domain)]
    dl[0] = map_to_lowercase_letter(dl[0] + dl[3])
    dl[1] = map_to_lowercase_letter(dl[0] + 2*dl[1])
    dl[2] = map_to_lowercase_letter(dl[0] + dl[2] - 1)
    dl[3] = map_to_lowercase_letter(dl[1] + dl[2] + dl[3])
    return ''.join([chr(x) for x in dl])
def isBanjoriTail(seed):
    for c0 in xrange(97,123):
        for c1 in xrange(97, 123):
            for c2 in xrange(97,123):
                for c3 in xrange(97,123):
                    domain = chr(c0)+chr(c1)+chr(c2)+chr(c3)
                    domain = next_domain(domain)
                    if seed.startswith(domain):
                        return False
    return True
seeds = {
    "nhcisatformatisticirekb.com",
    "egfesatformatisticirekb.com",
    "qwfusatformatisticirekb.com",
    "eijhsatformatisticirekb.com",
    "siowsatformatisticirekb.com",
    "dhansatformatisticirekb.com",
    "zvogsatformatisticirekb.com",
    "yaewsatformatisticirekb.com",
    "wgxfusatformatisticirekb.com",
    "vfxlsatformatisticirekb.com",
    "usjssatformatisticirekb.com",
    "selzsatformatisticirekb.com",
    "nzjqsatformatisticirekb.com",
    "kencsatformatisticirekb.com",
    "fzkxsatformatisticirekb.com",
    "babysatformatisticirekb.com",
}
for seed in seeds:
    print seed,isBanjoriTail(seed)
```

What results from this script?

- A. Seeds for existing domains are checked
- B. A search is conducted for additional seeds
- C. Domains are compared to seed rules
- D. A list of domains as seeds is blocked

Answer: B

NEW QUESTION 40

A company launched an e-commerce website with multiple points of sale through internal and external e- stores. Customers access the stores from the public website, and employees access the stores from the intranet with an SSO. Which action is needed to comply with PCI standards for hardening the systems?

- A. Mask PAN numbers
- B. Encrypt personal data
- C. Encrypt access
- D. Mask sales details

Answer: B

NEW QUESTION 42

Drag and drop the type of attacks from the left onto the cyber kill chain stages at which the attacks are seen on the right.

Answer Area

- not visible to the victim
- virus scanner turning off
- malware placed on the targeted system
- open port scans and multiple failed logins from the website
- large amount of data leaving the network through unusual ports
- system phones connecting to countries where no staff are located
- USB with infected files inserted into company laptop

- reconnaissance
- weaponization
- delivery
- exploitation
- installation
- command & control
- actions on objectives

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

- not visible to the victim
- virus scanner turning off
- malware placed on the targeted system
- open port scans and multiple failed logins from the website
- large amount of data leaving the network through unusual ports
- system phones connecting to countries where no staff are located
- USB with infected files inserted into company laptop

- system phones connecting to countries where no staff are located
- malware placed on the targeted system
- not visible to the victim
- large amount of data leaving the network through unusual ports
- USB with infected files inserted into company laptop
- virus scanner turning off
- open port scans and multiple failed logins from the website

NEW QUESTION 46

Where do threat intelligence tools search for data to identify potential malicious IP addresses, domain names, and URLs?

- A. customer data
- B. internal database
- C. internal cloud
- D. Internet

Answer: D

NEW QUESTION 48

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 49

A threat actor attacked an organization's Active Directory server from a remote location, and in a thirty-minute timeframe, stole the password for the administrator account and attempted to access 3 company servers. The threat actor successfully accessed the first server that contained sales data, but no files were downloaded. A second server was also accessed that contained marketing information and 11 files were downloaded. When the threat actor accessed the third server that contained corporate financial data, the session was disconnected, and the administrator's account was disabled. Which activity triggered the behavior analytics tool?

- A. accessing the Active Directory server
- B. accessing the server with financial data
- C. accessing multiple servers
- D. downloading more than 10 files

Answer: C

NEW QUESTION 54

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

350-201 Practice Exam Features:

- * 350-201 Questions and Answers Updated Frequently
- * 350-201 Practice Questions Verified by Expert Senior Certified Staff
- * 350-201 Most Realistic Questions that Guarantee you a Pass on Your First Try
- * 350-201 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The 350-201 Practice Test Here](#)