DUMPSARENA

Performing CyberOps Using Core Security Technologies (CBRCOR)

Cisco 350-201

Version Demo

Total Demo Questions: 10

Total Premium Questions: 139

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

QUESTION NO: 1

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

QUESTION NO: 2

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 averages. If the limit is exceeded, temporarily block access from the IP address and return a 402 HTTP error code.

B. Implement REST API Security Essentials solution to automatically mitigate limit exhaustion. If the limit is exceeded, temporarily block access from the service and return a 409 HTTP error code.

C. Increase a limit of replies in a given interval for each API. If the limit is exceeded, block access from the API key permanently and return a 450 HTTP error code.

D. Apply a limit to the number of requests in a given time interval for each API. If the rate is exceeded, block access from the API key temporarily and return a 429 HTTP error code.

ANSWER: D

Explanation:

Reference: https://www.whoishostingthis.com/resources/http-status-codes/

QUESTION NO: 3 - (DRAG DROP)

DRAG DROP

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.

Select and Place:

ANSWER:

Answer Area

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

Explanation:

QUESTION NO: 4 - (DRAG DROP)

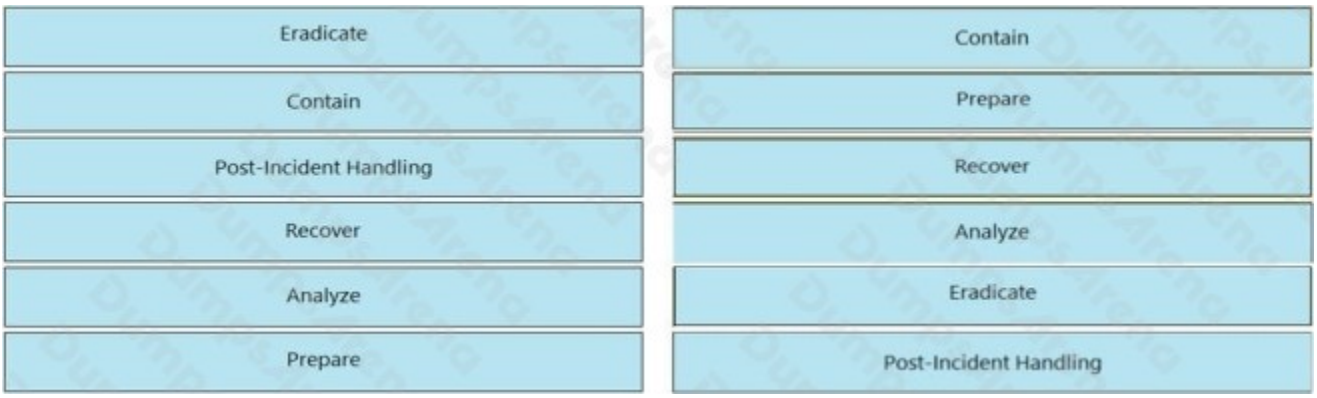
DRAG DROP

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

Select and Place:

Eradicate	Review 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.

ANSWER:



Explanation:

Reference:

https://www.securitymetrics.com/blog/6-phases-incident-response-plan

QUESTION NO: 5

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: B E

Explanation:

Reference: https://cloudogre.com/risk-assessment/

QUESTION NO: 6

A SOC engineer discovers that the organization had three DDOS attacks overnight. Four servers are reported offline, even though the hardware seems to be working as expected. One of the offline servers is affecting the pay system reporting times. Three employees, including executive management, have reported ransomware on their laptops. Which steps help the engineer understand a comprehensive overview of the incident?

A. Run and evaluate a full packet capture on the workloads, review SIEM logs, and define a root cause.

B. Run and evaluate a full packet capture on the workloads, review SIEM logs, and plan mitigation steps.

C. Check SOAR to learn what the security systems are reporting about the overnight events, research the attacks, and plan mitigation step.

D. Check SOAR to know what the security systems are reporting about the overnight events, review the threat vectors, and define a root cause.

ANSWER: D

QUESTION NO: 7

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

Explanation:

Reference: https://www.pluralsight.com/blog/it-ops/linux-file-permissions

QUESTION NO: 8

An organization suffered a security breach in which the attacker exploited a Netlogon Remote Protocol vulnerability for further privilege escalation. Which two actions should the incident response team take to prevent this type of attack from reoccurring? (Choose two.)

A. Implement a patch management process.

B. Scan the company server files for known viruses.

C. Apply existing patches to the company servers.

D. Automate antivirus scans of the company servers.

E. Define roles and responsibilities in the incident response playbook.

ANSWER: D E

QUESTION NO: 9

Employees receive an email from an executive within the organization that summarizes a recent security breach and requests that employees verify their credentials through a provided link. Several employees report the email as suspicious, and a security analyst is investigating the reports. Which two steps should the analyst take to begin this investigation? (Choose two.)

A. Evaluate the intrusion detection system alerts to determine the threat source and attack surface.

B. Communicate with employees to determine who opened the link and isolate the affected assets.

C. Examine the firewall and HIPS configuration to identify the exploited vulnerabilities and apply recommended mitigation.

D. Review the mail server and proxy logs to identify the impact of a potential breach.

E. Check the email header to identify the sender and analyze the link in an isolated environment.

ANSWER: C E

QUESTION NO: 10

Engineers are working to document, list, and discover all used applications within an organization. During the regular assessment of applications from the HR backup server, an engineer discovered an unknown application. The analysis showed that the application is communicating with external addresses on a non-secure, unencrypted channel. Information gathering revealed that the unknown application does not have an owner and is not being used by a business unit. What are the next two steps the engineers should take in this investigation? (Choose two.)

A. Determine the type of data stored on the affected asset, document the access logs, and engage the incident response team.

B. Identify who installed the application by reviewing the logs and gather a user access log from the HR department.

C. Verify user credentials on the affected asset, modify passwords, and confirm available patches and updates are installed.

D. Initiate a triage meeting with department leads to determine if the application is owned internally or used by any business unit and document the asset owner.

ANSWER: A D