350-201 Q&As

Performing CyberOps Using Cisco Security Technologies (CBRCOR)

Pass Cisco 350-201 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.leads4pass.com/350-201.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Cisco Official Exam Center

QUESTION 1

The incident response team was notified of detected malware. The team identified the infected hosts, removed the malware, restored the functionality and data of infected systems, and planned a company meeting to improve the incident handling capability.

Which step was missed according to the NIST incident handling guide?

A. Contain the malware

B. Install IPS software

C. Determine the escalation path

D. Perform vulnerability assessment

Correct Answer: D

QUESTION 2

The network operations center has identified malware, created a ticket within their ticketing system, and assigned the case to the SOC with high-level information. A SOC analyst was able to stop the malware from spreading and identified the attacking host. What is the next step in the incident response workflow?

A. eradication and recovery

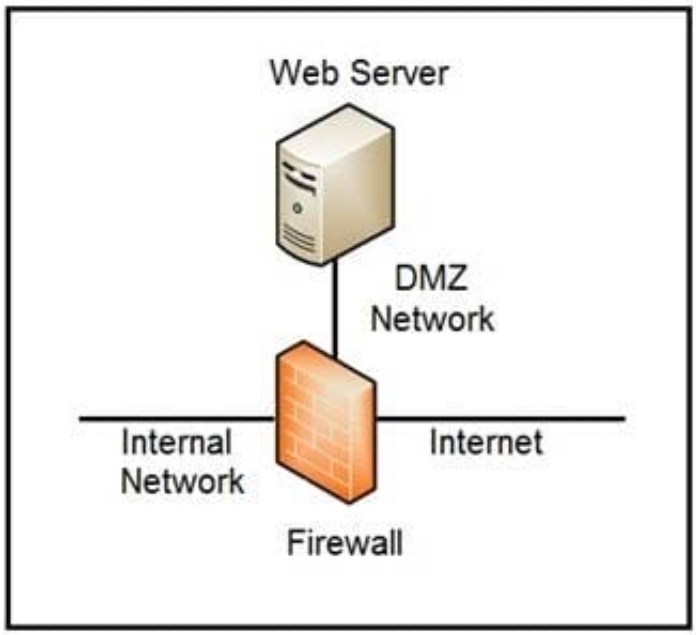
B. post-incident activity

C. containment

D. detection and analysis

Correct Answer: A

QUESTION 3



Refer to the exhibit. Which two steps mitigate attacks on the webserver from the Internet? (Choose two.)

A. Create an ACL on the firewall to allow only TLS 1.3

B. Implement a proxy server in the DMZ network

C. Create an ACL on the firewall to allow only external connections

D. Move the webserver to the internal network

Correct Answer: BD

QUESTION 4

Which bash command will print all lines from the “colors.txt” file containing the non case-sensitive pattern “Yellow”?

A. grep -i “yellow” colors.txt

B. locate “yellow” colors.txt

C. locate -i “Yellow” colors.txt

D. grep “Yellow” colors.txt

Correct Answer: A

QUESTION 5

According to GDPR, what should be done with data to ensure its confidentiality, integrity, and availability?

A. Perform a vulnerability assessment

B. Conduct a data protection impact assessment

C. Conduct penetration testing

D. Perform awareness testing

Correct Answer: B

Reference: https://apdcat.gencat.cat/web/.content/03-documentacio/Reglament_general_de_proteccio_de_dades/documents/DPIA-Guide.pdf

QUESTION 6

A security engineer discovers that a spreadsheet containing confidential information for nine of their employees was fraudulently posted on a competitor\\'s website. The spreadsheet contains names, salaries, and social security numbers. What is the next step the engineer should take in this investigation?

A. Determine if there is internal knowledge of this incident.

B. Check incoming and outgoing communications to identify spoofed emails.

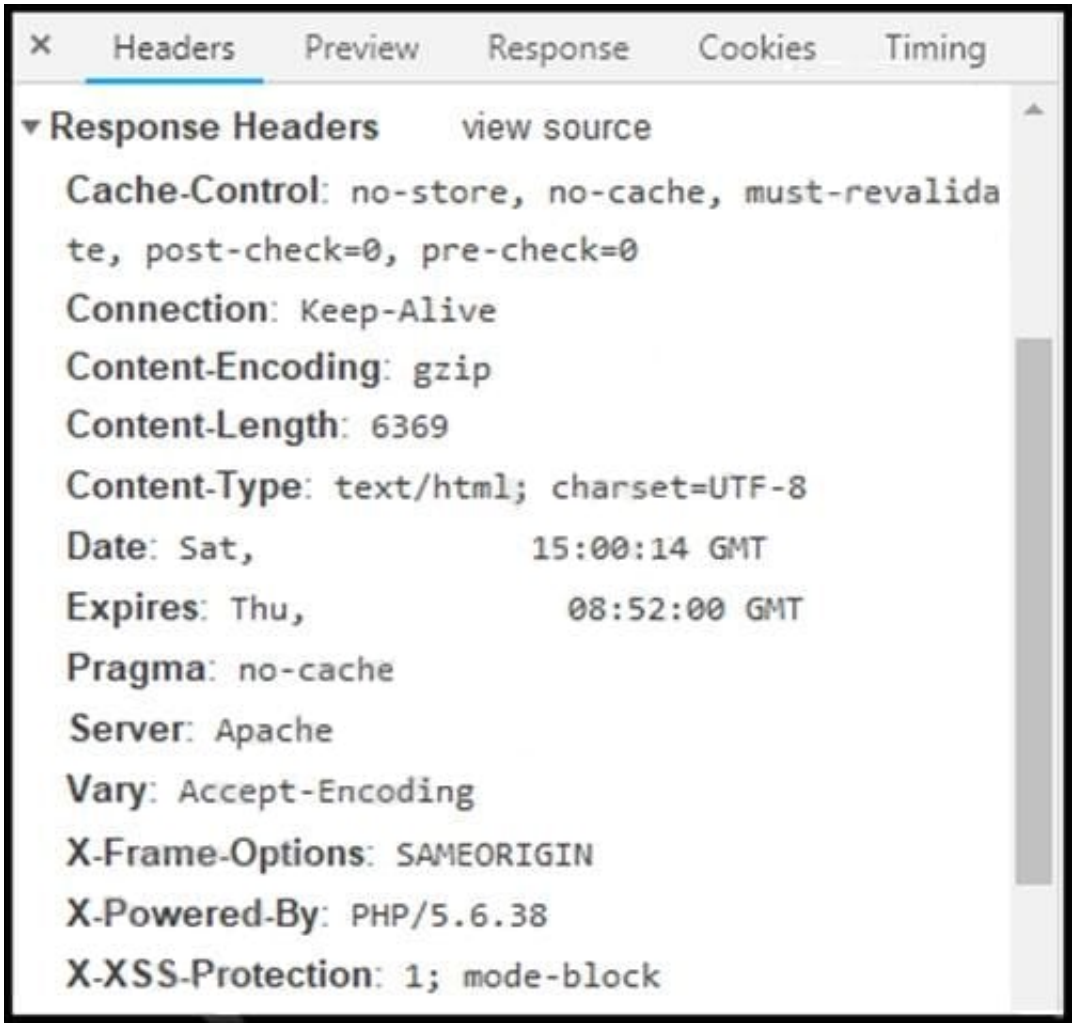
C. Disconnect the network from Internet access to stop the phishing threats and regain control.

D. Engage the legal department to explore action against the competitor that posted the spreadsheet.

Correct Answer: D

QUESTION 7

Refer to the exhibit. Where are the browser page rendering permissions displayed?



A. X-Frame-Options

B. X-XSS-Protection

C. Content-Type

D. Cache-Control

Correct Answer: C

QUESTION 8

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

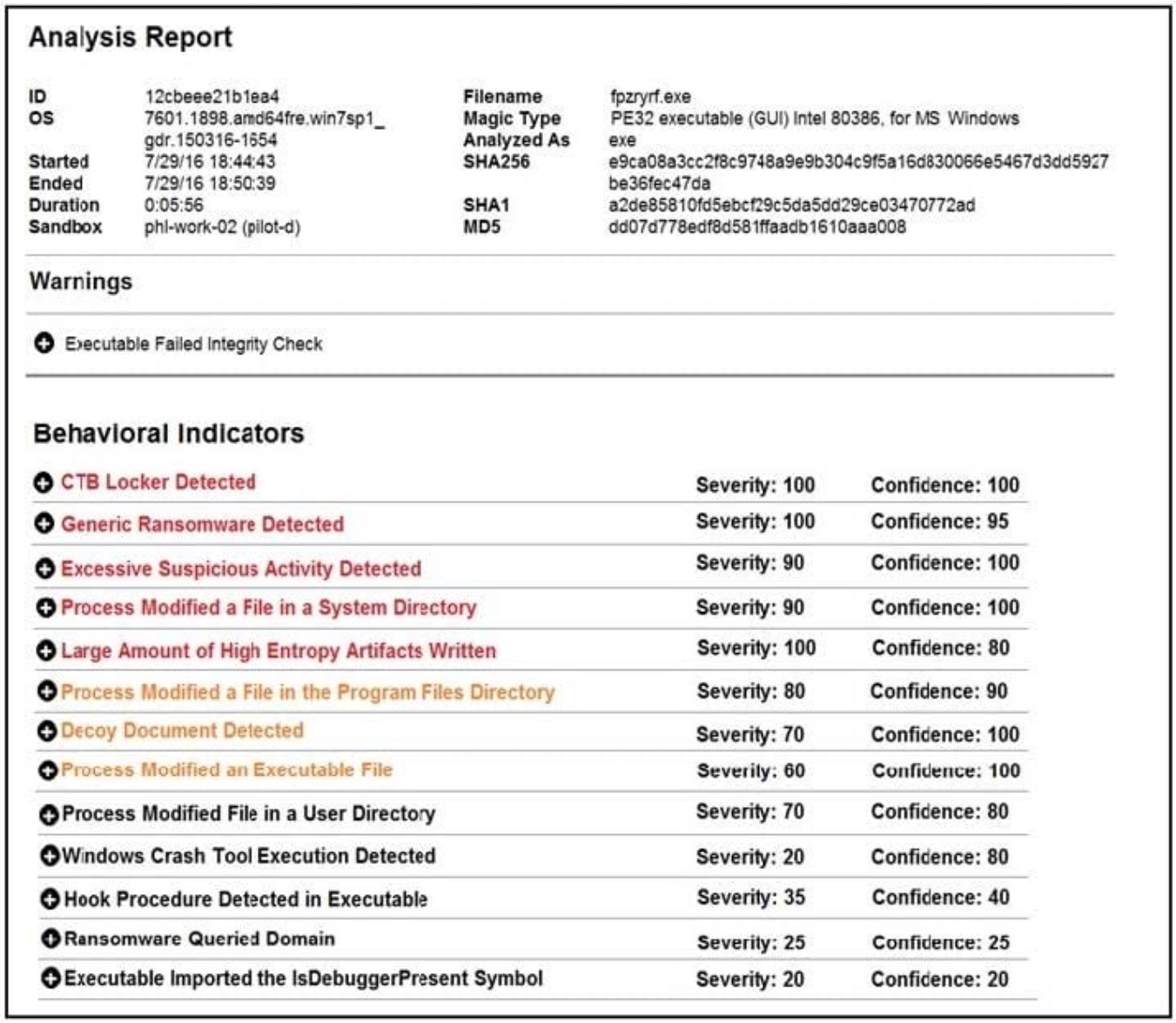
B. event severity and likelihood

C. incident response playbook

D. risk model framework

Correct Answer: D

QUESTION 9



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
		Analyzed As	exe
Started	7/29/16 18:44:43	SHA256	e9ca08a3cc2f8c9748a9e9b304c9f5a16d830066e5467d3dd5927be36fec47da
Ended	7/29/16 18:50:39		
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

Refer to the exhibit. 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.

Correct Answer: C

QUESTION 10

What is the difference between process orchestration and automation?

A. Orchestration combines a set of automated tools, while automation is focused on the tools to automate process flows.

B. Orchestration arranges the tasks, while automation arranges processes.

C. Orchestration minimizes redundancies, while automation decreases the time to recover from redundancies.

D. Automation optimizes the individual tasks to execute the process, while orchestration optimizes frequent and repeatable processes.

Correct Answer: A

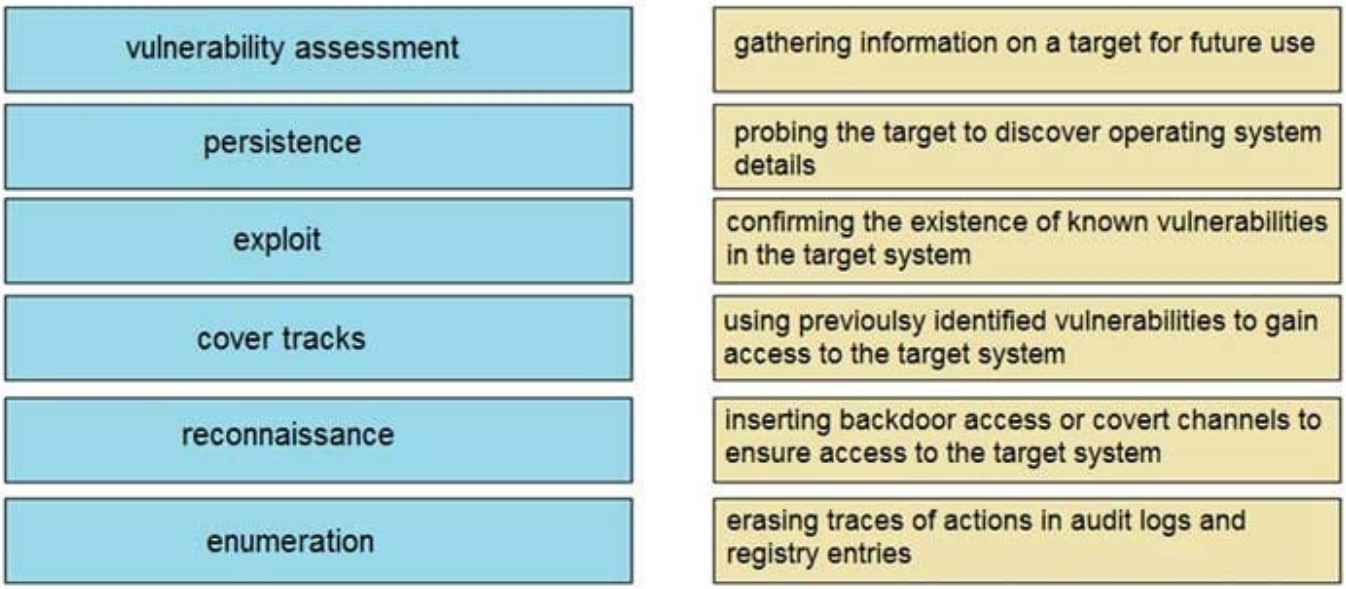
QUESTION 11

DRAG DROP

Drag and drop the phases to evaluate the security posture of an asset from the left onto the activity that happens during the phases on the right.

Select and Place:

Answer Area



Correct Answer:

Answer Area

QUESTION 12

An organization is using a PKI management server and a SOAR platform to manage the certificate lifecycle. The SOAR platform queries a certificate management tool to check all endpoints for SSL certificates that have either expired or are nearing expiration. Engineers are struggling to manage problematic certificates outside of PKI management since

deploying certificates and tracking them requires searching server owners manually.

Which action will improve workflow automation?

A. Implement a new workflow within SOAR to create tickets in the incident response system, assign problematic certificate update requests to server owners, and register change requests.

B. Integrate a PKI solution within SOAR to create certificates within the SOAR engines to track, update, and monitor problematic certificates.

C. Implement a new workflow for SOAR to fetch a report of assets that are outside of the PKI zone, sort assets by certification management leads and automate alerts that updates are needed.

D. Integrate a SOAR solution with Active Directory to pull server owner details from the AD and send an automated email for problematic certificates requesting updates.

Correct Answer: C

QUESTION 13

A company recently completed an internal audit and discovered that there is CSRF vulnerability in 20 of its hosted applications. Based on the audit, which recommendation should an engineer make for patching?

A. Identify the business applications running on the assets

B. Update software to patch third-party software

C. Validate CSRF by executing exploits within Metasploit

D. Fix applications according to the risk scores

Correct Answer: D

QUESTION 14

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

Correct Answer: D

Reference: https://www.varonis.com/blog/what-is-siem/

QUESTION 15

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

Correct Answer: D