

Cisco

Exam Questions 350-201

Performing CyberOps Using Core Security Technologies (CBRCOR)



NEW QUESTION 1

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.

Answer Area

vulnerability assessment	gathering information on a target for future use
persistence	probing the target to discover operating system details
exploit	confirming the existence of known vulnerabilities in the target system
cover tracks	using previously identified vulnerabilities to gain access to the target system
reconnaissance	inserting backdoor access or covert channels to ensure access to the target system
enumeration	erasing traces of actions in audit logs and registry entries

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

vulnerability assessment	persistence
persistence	reconnaissance
exploit	vulnerability assessment
cover tracks	exploit
reconnaissance	enumeration
enumeration	cover tracks

NEW QUESTION 2

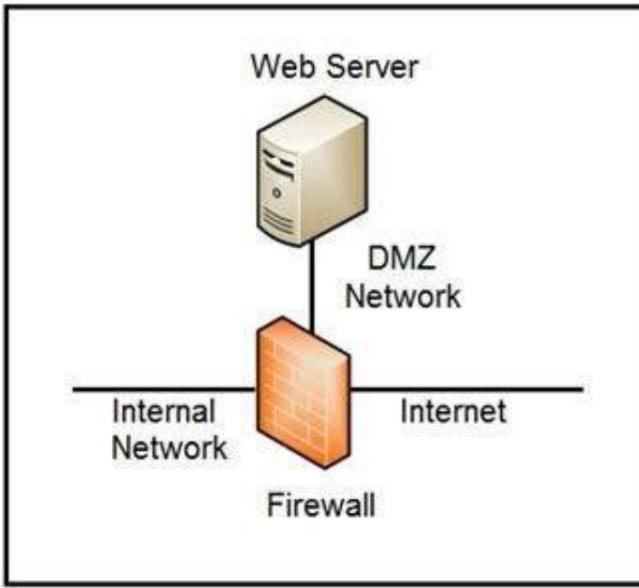
An engineer is investigating several cases of increased incoming spam emails and suspicious emails from the HR and service departments. While checking the event sources, the website monitoring tool showed several web scraping alerts overnight. Which type of compromise is indicated?

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

Answer: C

NEW QUESTION 3

Refer to the exhibit.



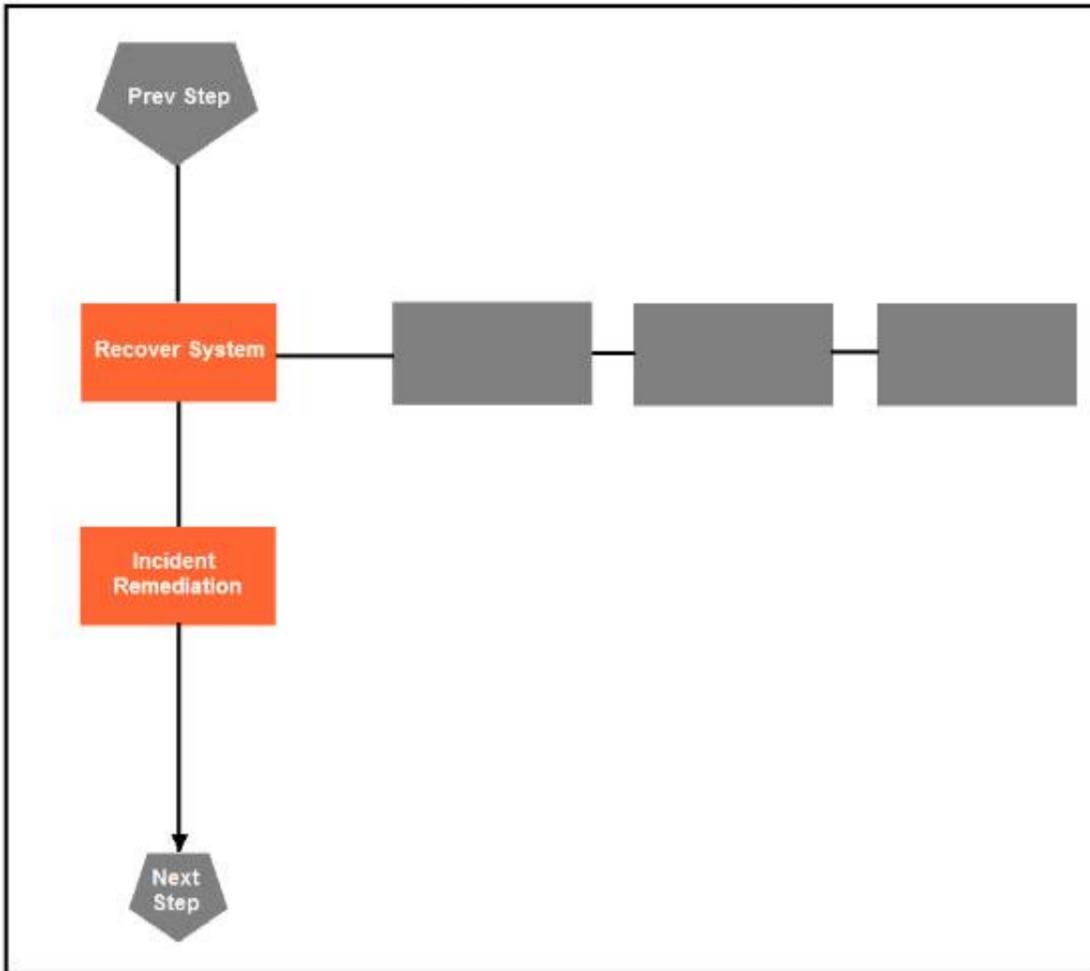
Which two steps mitigate attacks on the webserver from the Internet? (Choose two.)

- 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

Answer: BD

NEW QUESTION 4

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.

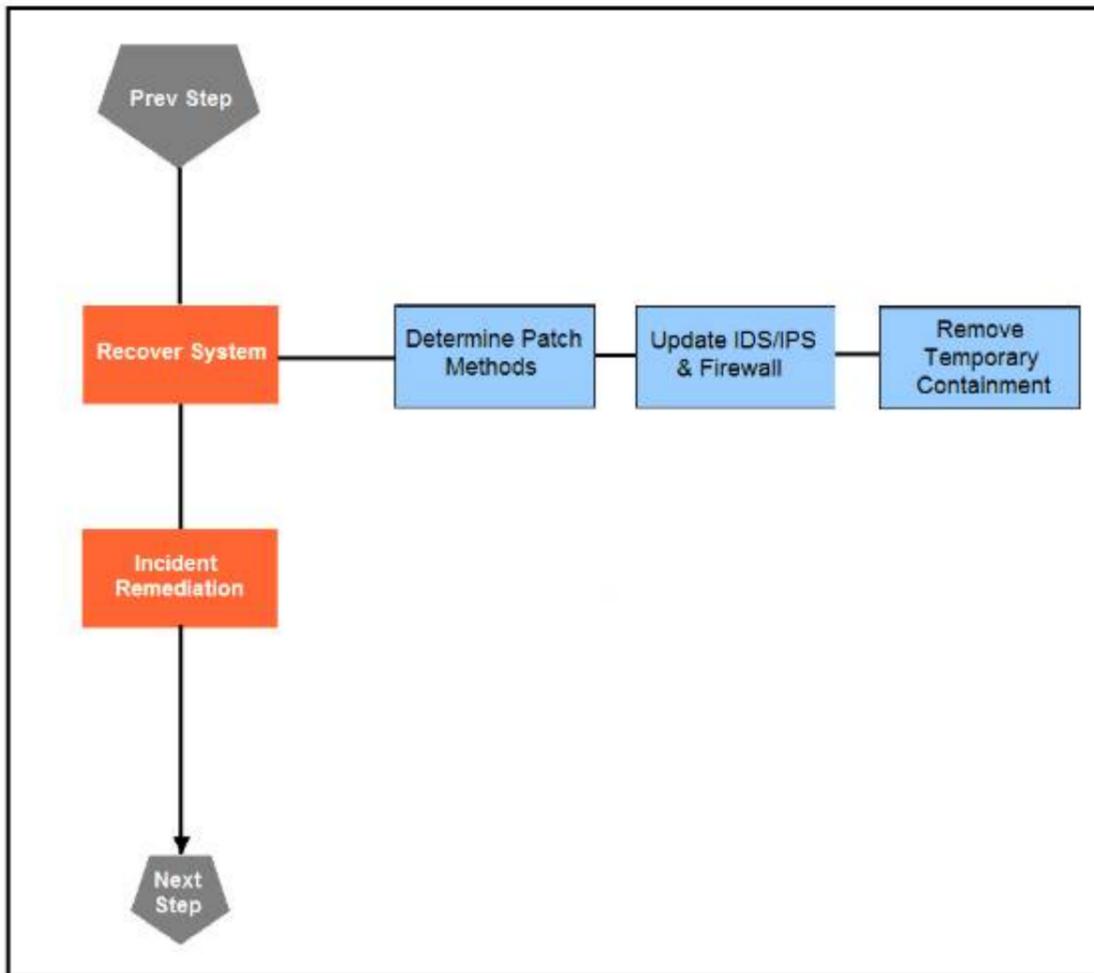


- | | | | |
|---------------------------|------------------------|------------------------------|-------------------------|
| Update IDS/IPS & Firewall | Reimage | Collect Logs | Categorize Incident |
| Identify Targeted Systems | Request Packet Capture | Remove Temporary Containment | Determine Patch Methods |

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:



- | | | | |
|---------------------------|------------------------|------------------------------|-------------------------|
| Update IDS/IPS & Firewall | Reimage | Collect Logs | Categorize Incident |
| Identify Targeted Systems | Request Packet Capture | Remove Temporary Containment | Determine Patch Methods |

NEW QUESTION 5

A security architect is working in a processing center and must implement a DLP solution to detect and prevent any type of copy and paste attempts of sensitive data within unapproved applications and removable devices. Which technical architecture must be used?

- A. DLP for data in motion
- B. DLP for removable data
- C. DLP for data in use
- D. DLP for data at rest

Answer: C

NEW QUESTION 6

Refer to the exhibit.

```

<employees>
  <employee>
    <lastname>Smith</lastname>
    <firstname>Richard</firstname>
  </employee>
  <employee>
    <lastname>Witzel</lastname>
    <firstname>Sevan</firstname>
  </employee>
</employees>
  
```

Which data format is being used?

- A. JSON
- B. HTML
- C. XML
- D. CSV

Answer: B

NEW QUESTION 7

What do 2xx HTTP response codes indicate for REST APIs?

- A. additional action must be taken by the client to complete the request

- B. the server takes responsibility for error status codes
- C. communication of transfer protocol-level information
- D. successful acceptance of the client's request

Answer: D

NEW QUESTION 8

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

Answer: B

NEW QUESTION 9

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 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 organization had a breach due to a phishing attack. An engineer leads a team through the recovery phase of the incident response process. Which action should be taken during this phase?

- A. Host a discovery meeting and define configuration and policy updates
- B. Update the IDS/IPS signatures and reimagine the affected hosts
- C. Identify the systems that have been affected and tools used to detect the attack
- D. Identify the traffic with data capture using Wireshark and review email filters

Answer: C

NEW QUESTION 14

A payroll administrator noticed unexpected changes within a piece of software and reported the incident to the incident response team. Which actions should be taken at this step in the incident response workflow?

- A. Classify the criticality of the information, research the attacker's motives, and identify missing patches
- B. Determine the damage to the business, extract reports, and save evidence according to a chain of custody
- C. Classify the attack vector, understand the scope of the event, and identify the vulnerabilities being exploited
- D. Determine the attack surface, evaluate the risks involved, and communicate the incident according to the escalation plan

Answer: B

NEW QUESTION 18

An engineer is going through vulnerability triage with company management because of a recent malware outbreak from which 21 affected assets need to be patched or remediated. Management decides not to prioritize fixing the assets and accepts the vulnerabilities. What is the next step the engineer should take?

- A. Investigate the vulnerability to prevent further spread
- B. Acknowledge the vulnerabilities and document the risk
- C. Apply vendor patches or available hot fixes
- D. Isolate the assets affected in a separate network

Answer: D

NEW QUESTION 23

An organization had several cyberattacks over the last 6 months and has tasked an engineer with looking for patterns or trends that will help the organization anticipate future attacks and mitigate them. Which data analytic technique should the engineer use to accomplish this task?

- A. diagnostic
- B. qualitative
- C. predictive
- D. statistical

Answer: C

NEW QUESTION 26

Refer to the exhibit.

```
pragma: no-cache
server: Apache
status: 200
strict-transport-security: max-age=31536000
vary: Accept-Encoding
x-content-type-options: nosniff
x-frame-options: SAMEORIGIN
x-test-debug: nURL=www.cisco.com, realm=0, isRealm=0, realDomain=0, shortrealm=0
x-xss-protection: 1; mode=block
```

Where are the browser page rendering permissions displayed?

- A. x-frame-options
- B. x-xss-protection
- C. x-content-type-options
- D. x-test-debug

Answer: C

NEW QUESTION 29

An engineer notices that unauthorized software was installed on the network and discovers that it was installed by a dormant user account. The engineer suspects an escalation of privilege attack and responds to the incident. Drag and drop the activities from the left into the order for the response on the right.

Answer Area

Identify systems to be taken offline	Step 1
Conduct content scans	Step 2
Collect log data	Step 3
Request system patch	Step 4
Reimage	Step 5

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Identify systems to be taken offline	Conduct content scans
Conduct content scans	Collect log data
Collect log data	Identify systems to be taken offline
Request system patch	Reimage
Reimage	Request system patch

NEW QUESTION 30

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 35

Drag and drop the threat from the left onto the scenario that introduces the threat on the right. Not all options are used.

Answer Area

spoofing attack	installing network devices
broken authentication attack	developing new code
injection attack	implementing a new application
man-in-the-middle attack	changing configuration settings
privilege escalation attack	
default credential attack	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

spoofing attack	man-in-the-middle attack
broken authentication attack	injection attack
injection attack	privilege escalation attack
man-in-the-middle attack	default credential attack
privilege escalation attack	
default credential attack	

NEW QUESTION 37

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?

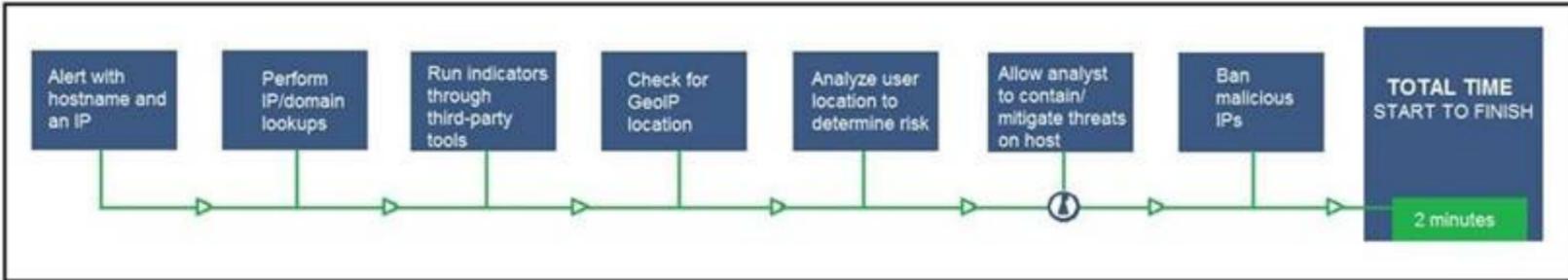
- A. continuous delivery
- B. continuous integration

- C. continuous deployment
- D. continuous monitoring

Answer: A

NEW QUESTION 40

Refer to the exhibit.



An engineer configured this SOAR solution workflow to identify account theft threats and privilege escalation, evaluate risk, and respond by resolving the threat. This solution is handling more threats than Security analysts have time to analyze. Without this analysis, the team cannot be proactive and anticipate attacks. Which action will accomplish this goal?

- A. Exclude the step “BAN malicious IP” to allow analysts to conduct and track the remediation
- B. Include a step “Take a Snapshot” to capture the endpoint state to contain the threat for analysis
- C. Exclude the step “Check for GeolP location” to allow analysts to analyze the location and the associated risk based on asset criticality
- D. Include a step “Reporting” to alert the security department of threats identified by the SOAR reporting engine

Answer: A

NEW QUESTION 41

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.

Answer: C

NEW QUESTION 45

Refer to the exhibit.

Analysis Report

ID	12cbbee21b1ea4	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 48

An audit is assessing a small business that is selling automotive parts and diagnostic services. Due to increased customer demands, the company recently started to accept credit card payments and acquired a POS terminal. Which compliance regulations must the audit apply to the company?

- A. HIPAA
- B. FISMA
- C. COBIT
- D. PCI DSS

Answer: D

NEW QUESTION 51

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 52

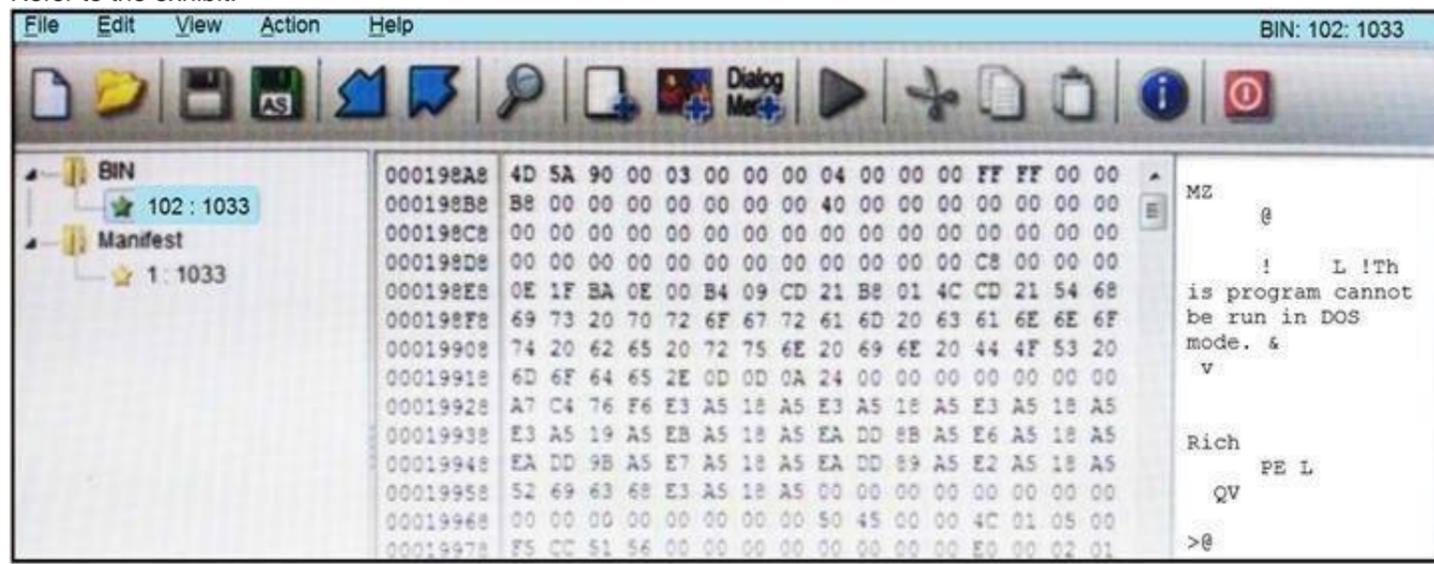
A threat actor has crafted and sent a spear-phishing email with what appears to be a trustworthy link to the site of a conference that an employee recently attended. The employee clicked the link and was redirected to a malicious site through which the employee downloaded a PDF attachment infected with 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 54

Refer to the exhibit.



An engineer is reverse engineering a suspicious file by examining its resources. What does this file indicate?

- A. a DOS MZ executable format
- B. a MS-DOS executable archive
- C. an archived malware
- D. a Windows executable file

Answer: D

NEW QUESTION 55

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 58

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 63

Refer to the exhibit.

Host Address	Host Name	First Sent	Last Sent	CI	TI	RC	C&C	EP	DS	DT	DH	EX	PV	AN	Location	Host Groups
128.107.78.8		12/15/16 5:26 PM	1/27/17 9:13 PM												United States	United States

The Cisco Secure Network Analytics (Stealthwatch) console alerted with “New Malware Server Discovered” and the IOC indicates communication from an end-user desktop to a Zeus C&C Server. Drag and drop the actions that the analyst should take from the left into the order on the right to investigate and remediate this IOC.

Answer Area

- Execute rapid threat containment
- Investigate and classify the exposure
- Investigate infected hosts
- Search for infected hosts
- Examine returned results

- Step 1
- Step 2
- Step 3
- Step 4
- Step 5

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

- Execute rapid threat containment
- Investigate and classify the exposure
- Investigate infected hosts
- Search for infected hosts
- Examine returned results

- Search for infected hosts
- Investigate infected hosts
- Investigate and classify the exposure
- Examine returned results
- Execute rapid threat containment

NEW QUESTION 66

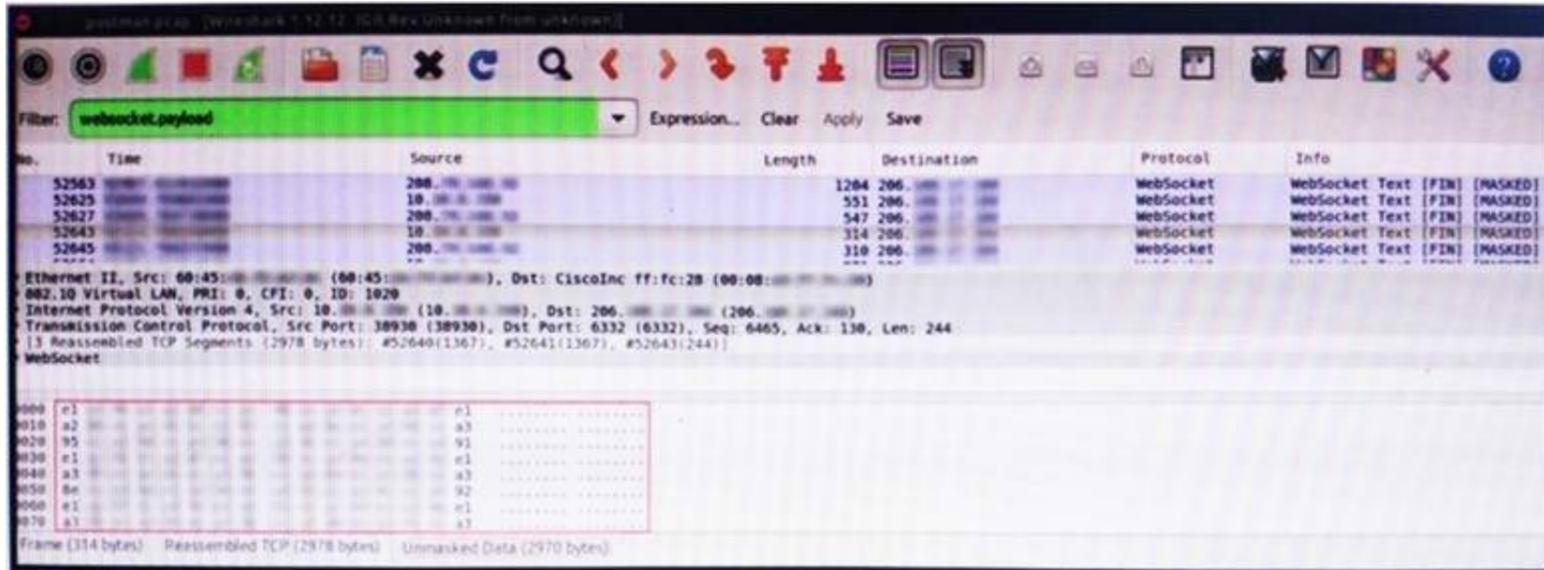
Where do threat intelligence tools search for data to identify potential malicious IP addresses, domain names, and URLs?

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

Answer: D

NEW QUESTION 67

Refer to the exhibit.



An engineer is analyzing this Vlan0386-int12-117.pcap file in Wireshark after detecting a suspicious network activity. The origin header for the direct IP connections in the packets was initiated by a google chrome extension on a WebSocket protocol. The engineer checked message payloads to determine what information was being sent off-site but the payloads are obfuscated and unreadable. What does this STIX indicate?

- A. The extension is not performing as intended because of restrictions since ports 80 and 443 should be accessible
- B. The traffic is legitimate as the google chrome extension is reaching out to check for updates and fetches this information
- C. There is a possible data leak because payloads should be encoded as UTF-8 text
- D. There is a malware that is communicating via encrypted channels to the command and control server

Answer: C

NEW QUESTION 70

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 75

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 76

An engineer wants to review the packet overviews of SNORT alerts. When printing the SNORT alerts, all the packet headers are included, and the file is too large to utilize. Which action is needed to correct this problem?

- A. Modify the alert rule to "output alert_syslog: output log"
- B. Modify the output module rule to "output alert_quick: output filename"
- C. Modify the alert rule to "output alert_syslog: output header"
- D. Modify the output module rule to "output alert_fast: output filename"

Answer: A

NEW QUESTION 81

A Mac laptop user notices that several files have disappeared from their laptop documents folder. While looking for the files, the user notices that the browser history was recently cleared. The user raises a case, and an analyst reviews the network usage and discovers that it is abnormally high. Which step should be taken to continue the investigation?

- A. Run the sudo sysdiagnose command
- B. Run the sh command
- C. Run the w command
- D. Run the who command

Answer: A

NEW QUESTION 86

.....

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](#)