Exam Questions 350-201

Performing CyberOps Using Core Security Technologies (CBRCOR)

https://www.2passeasy.com/dumps/350-201/

NEW QUESTION 1
Refer to the exhibit.

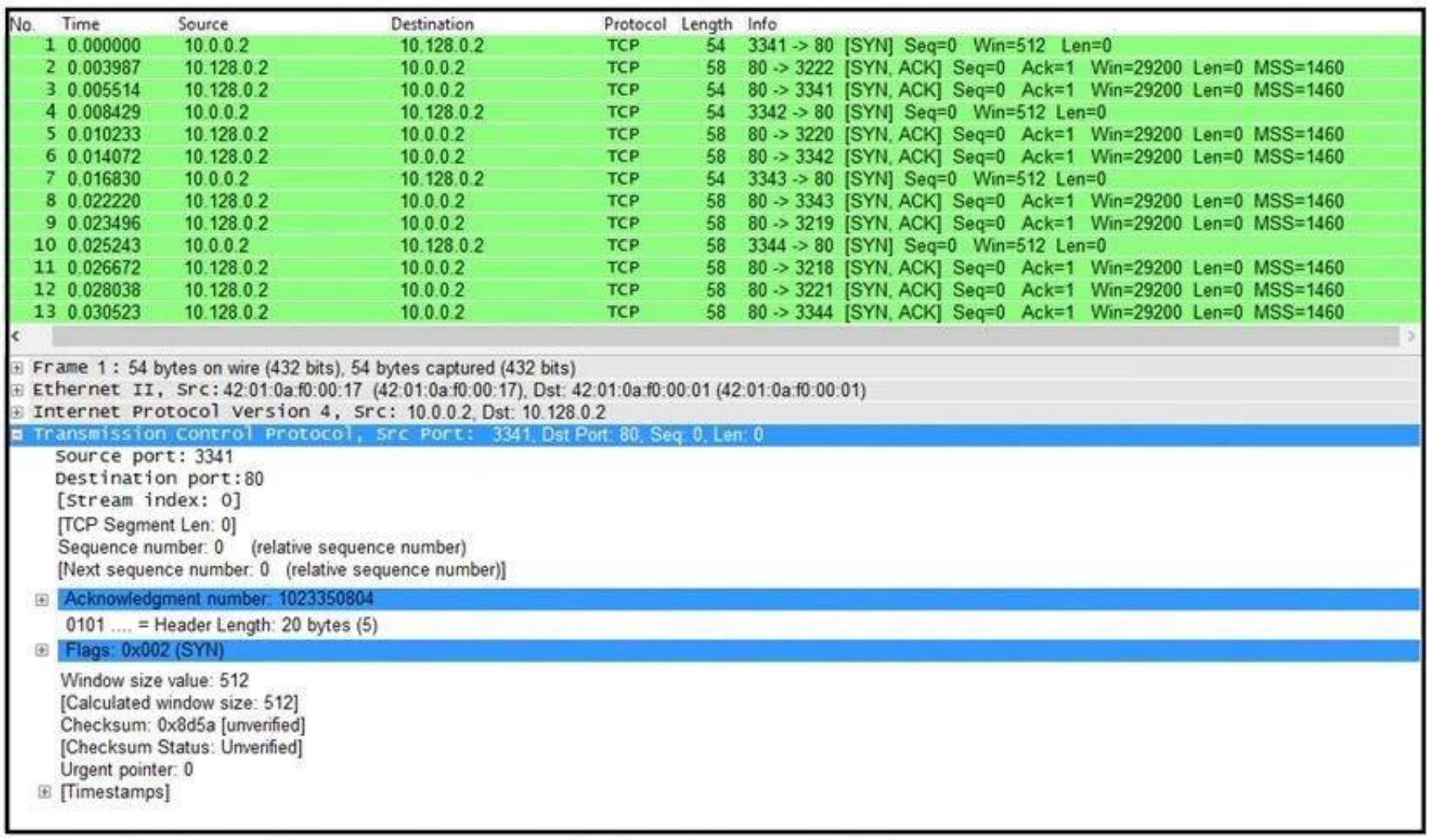
Max (K)	Retain	OverflowAction	Entries	Log
15,168	0	OverwriteAsNeeded	20,792	Application
15,168	0	OverwriteAsNeeded	12,559	System
15,360	0	OverwriteAsNeeded	11,173	Windows PowerShell

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
Refer to the exhibit.



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 3
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 4
Drag and drop the mitigation steps from the left onto the vulnerabilities they mitigate on the right.

Answer Area

Restrict administrative access to operating systems and applications in accordance with job duties	End-user desktops allow the execution of non-approved applications that include malicious code
Use multifactor authentication for remote access or accessing sensitive information	Application security vulnerabilities can be used to execute malicious code
Change backup and store software and configuration settings for at least three months	Privilege accounts have full rights to information systems
Patch applications including flash, web browsers, and PDF viewers	User verification is weak and based on a single factor
Utilize application control to stop malware delivery and execution	Data or access loss occurs due to cybersecurity incidents

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Restrict administrative access to operating systems and applications in accordance with job duties	Utilize application control to stop malware delivery and execution
Use multifactor authentication for remote access or accessing sensitive information	Patch applications including flash, web browsers, and PDF viewers
Change backup and store software and configuration settings for at least three months	Restrict administrative access to operating systems and applications in accordance with job duties
Patch applications including flash, web browsers, and PDF viewers	Use multifactor authentication for remote access or accessing sensitive information
Utilize application control to stop malware delivery and execution	Change backup and store software and configuration settings for at least three months

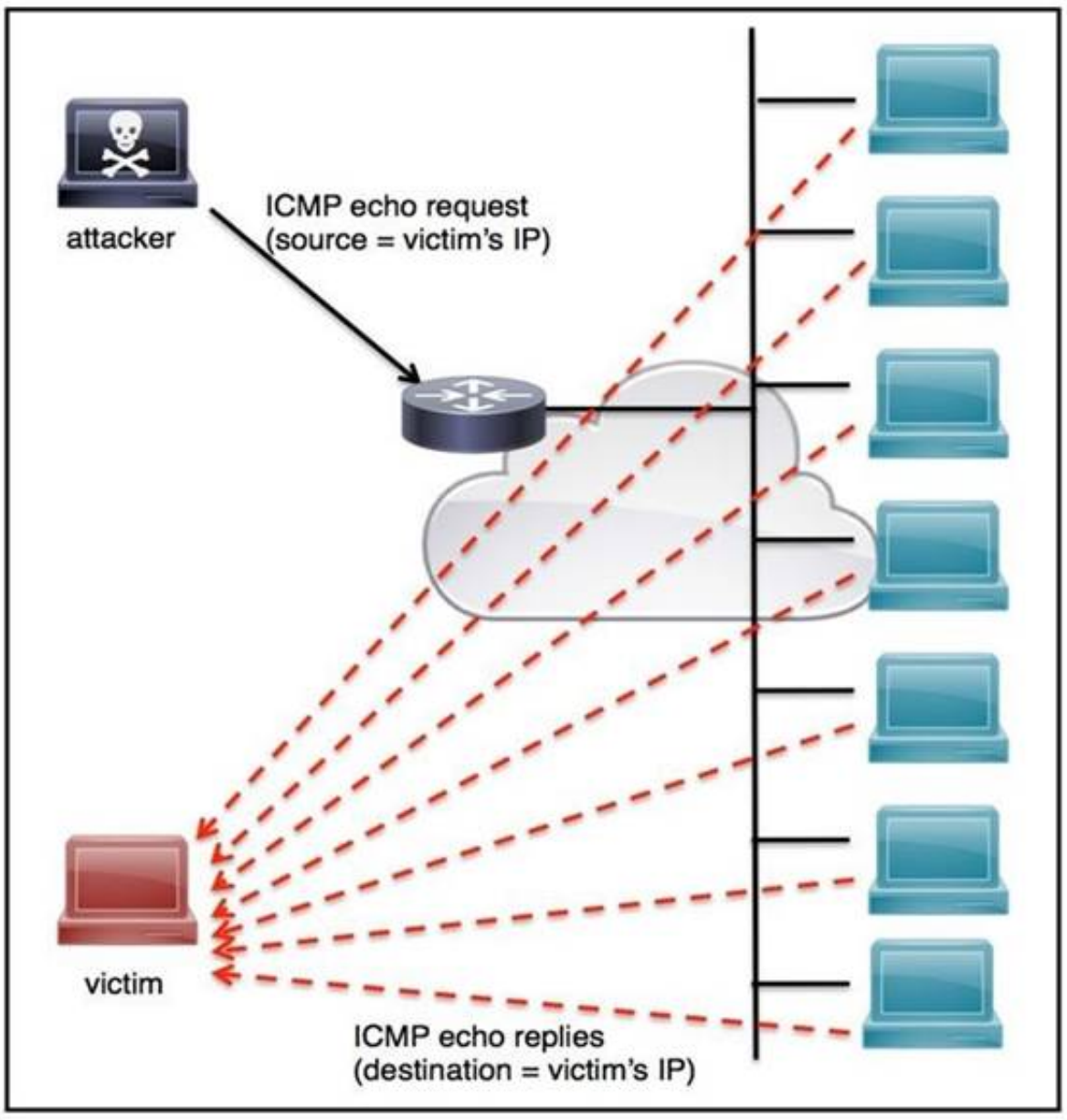
NEW QUESTION 5
An employee who often travels abroad logs in from a first-seen country during non-working hours. The SIEM tool generates an alert that the user is forwarding an increased amount of emails to an external mail domain and then logs out. The investigation concludes that the external domain 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 6
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

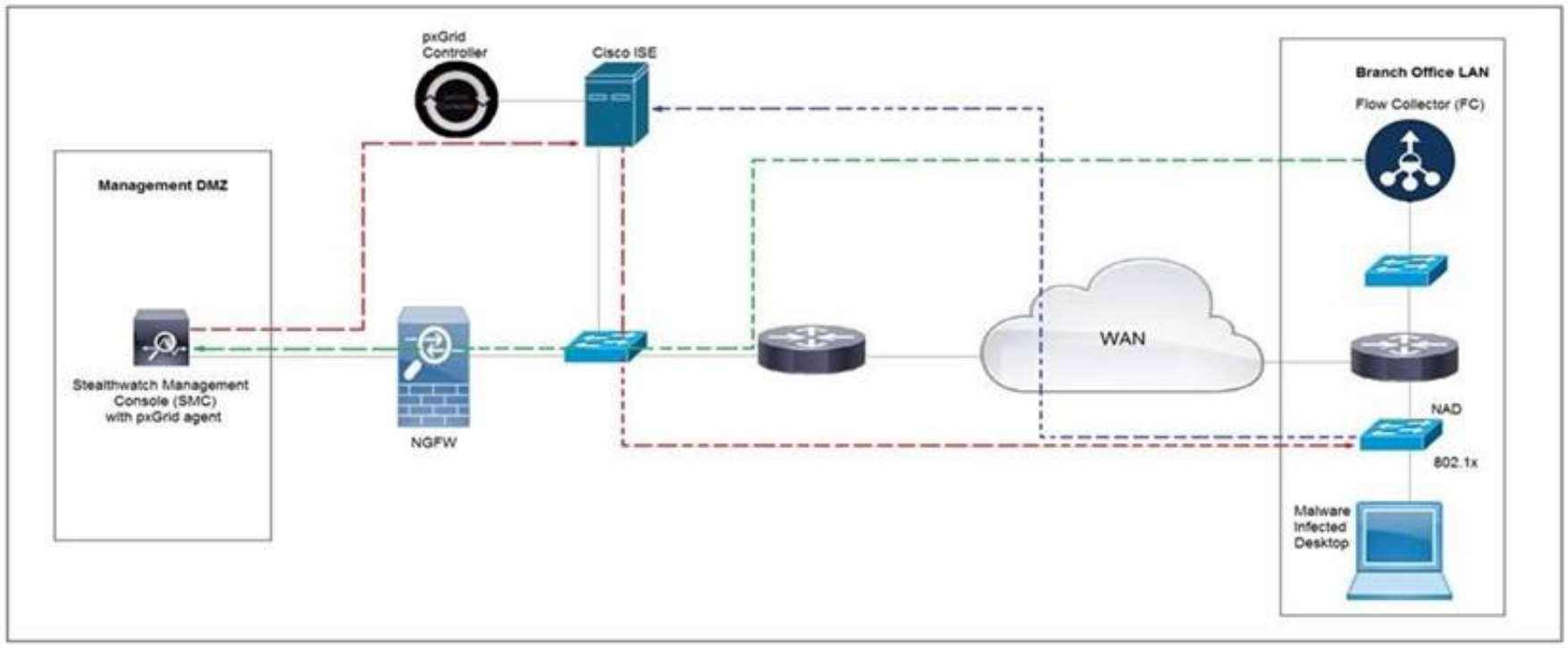
Answer: A

NEW QUESTION 7
A SOC analyst is investigating a recent email delivered to a high-value user for a customer whose network their organization monitors. The email includes a suspicious attachment titled "Invoice RE: 0004489". The hash of the file is gathered from the Cisco Email Security Appliance. After searching Open Source Intelligence, no available history of this hash is found anywhere on the web. What is the next step in analyzing this attachment to allow the analyst to gather indicators of compromise?

A. Run and analyze the DLP Incident Summary Report from the Email Security Appliance
B. Ask the company to execute the payload for real time analysis
C. Investigate further in open source repositories using YARA to find matches
D. Obtain a copy of the file for detonation in a sandbox

Answer: D

NEW QUESTION 8
Refer to the exhibit.



Cisco Rapid Threat Containment using Cisco Secure Network Analytics (Stealthwatch) and ISE detects the threat of malware-infected 802.1x authenticated endpoints and places that endpoint into a Quarantine VLAN using Adaptive Network Control policy. Which telemetry feeds were correlated with SMC to identify the malware?

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

Answer: B

NEW QUESTION 9
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

Answer: D

NEW QUESTION 10
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 10
An organization installed a new application server for IP phones. An automated process fetched user credentials from the Active Directory server, and the application will have access to on-premises and cloud services. Which security threat should be mitigated first?

A. aligning access control policies
B. exfiltration during data transfer
C. attack using default accounts
D. data exposure from backups

Answer: B

NEW QUESTION 14
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 19
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 23
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 26
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

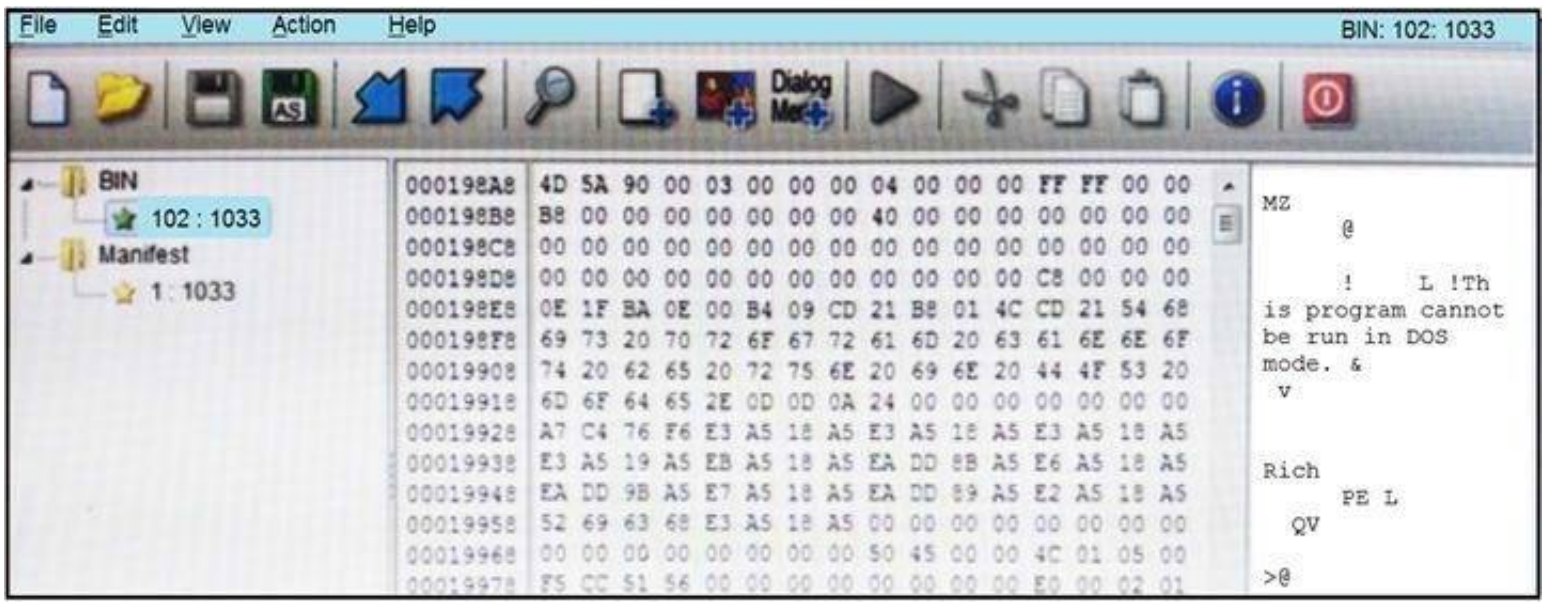
Answer: D

NEW QUESTION 31
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 32
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 33
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	reconnaissance
virus scanner turning off	weaponization
malware placed on the targeted system	delivery
open port scans and multiple failed logins from the website	exploitation
large amount of data leaving the network through unusual ports	installation
system phones connecting to countries where no staff are located	command & control
USB with infected files inserted into company laptop	actions on objectives

A. Mastered
B. Not Mastered

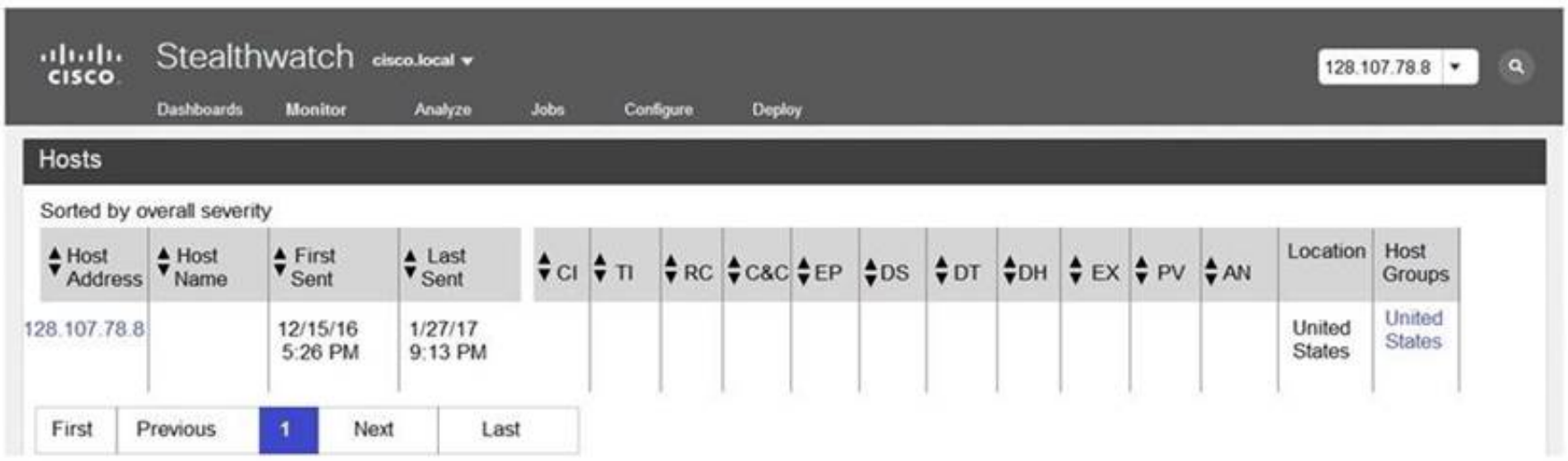
Answer: A

Explanation:

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

NEW QUESTION 37
Refer to the exhibit.



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	Step 1
Investigate and classify the exposure	Step 2
Investigate infected hosts	Step 3
Search for infected hosts	Step 4
Examine returned results	Step 5

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

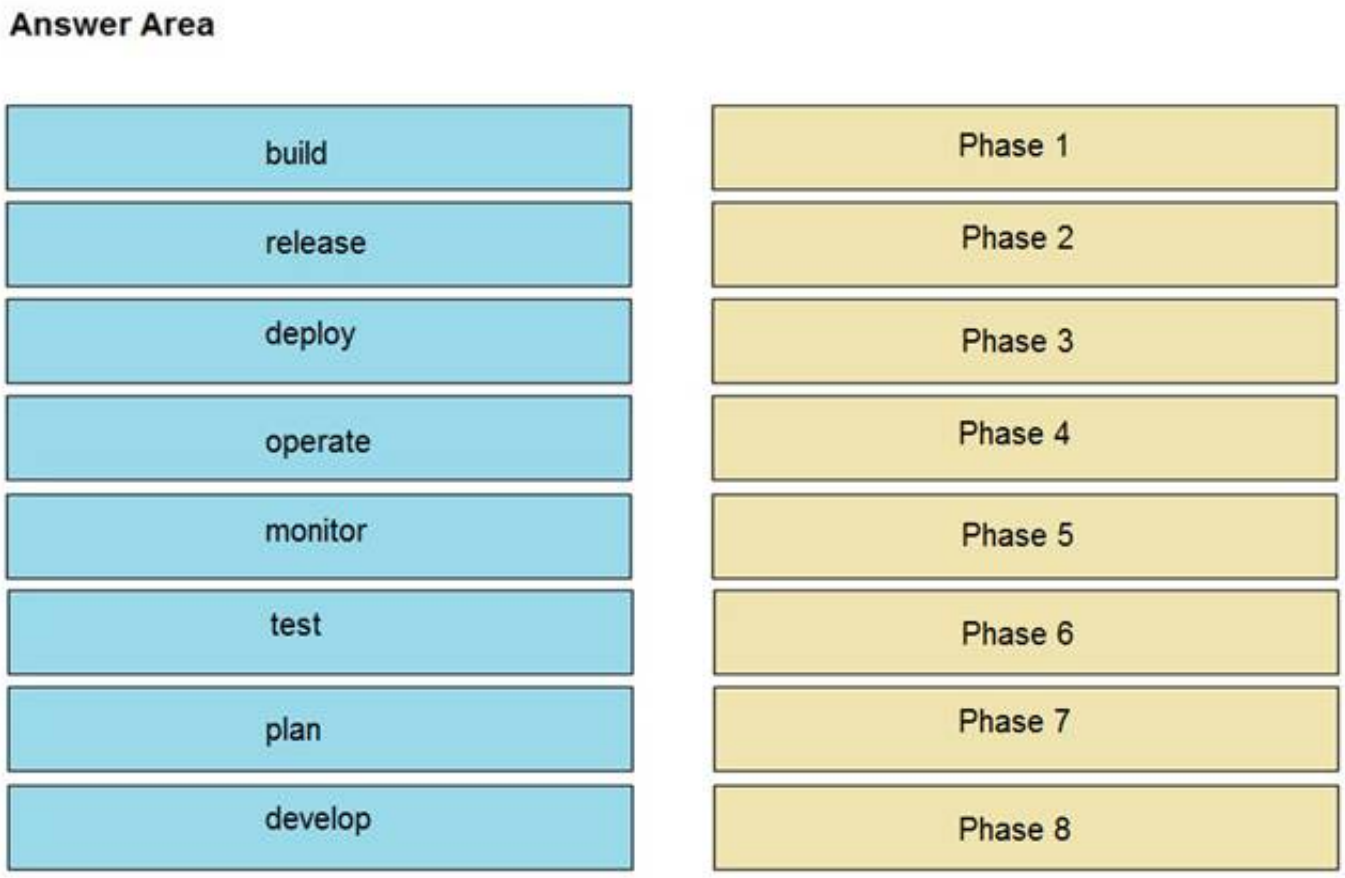
Execute rapid threat containment	Search for infected hosts
Investigate and classify the exposure	Investigate infected hosts
Investigate infected hosts	Investigate and classify the exposure
Search for infected hosts	Examine returned results
Examine returned results	Execute rapid threat containment

NEW QUESTION 40
An engineer is analyzing a possible compromise that happened a week ago when the company ? (Choose two.)

A. firewall
B. Wireshark
C. autopsy
D. SHA512
E. IPS

Answer: AB

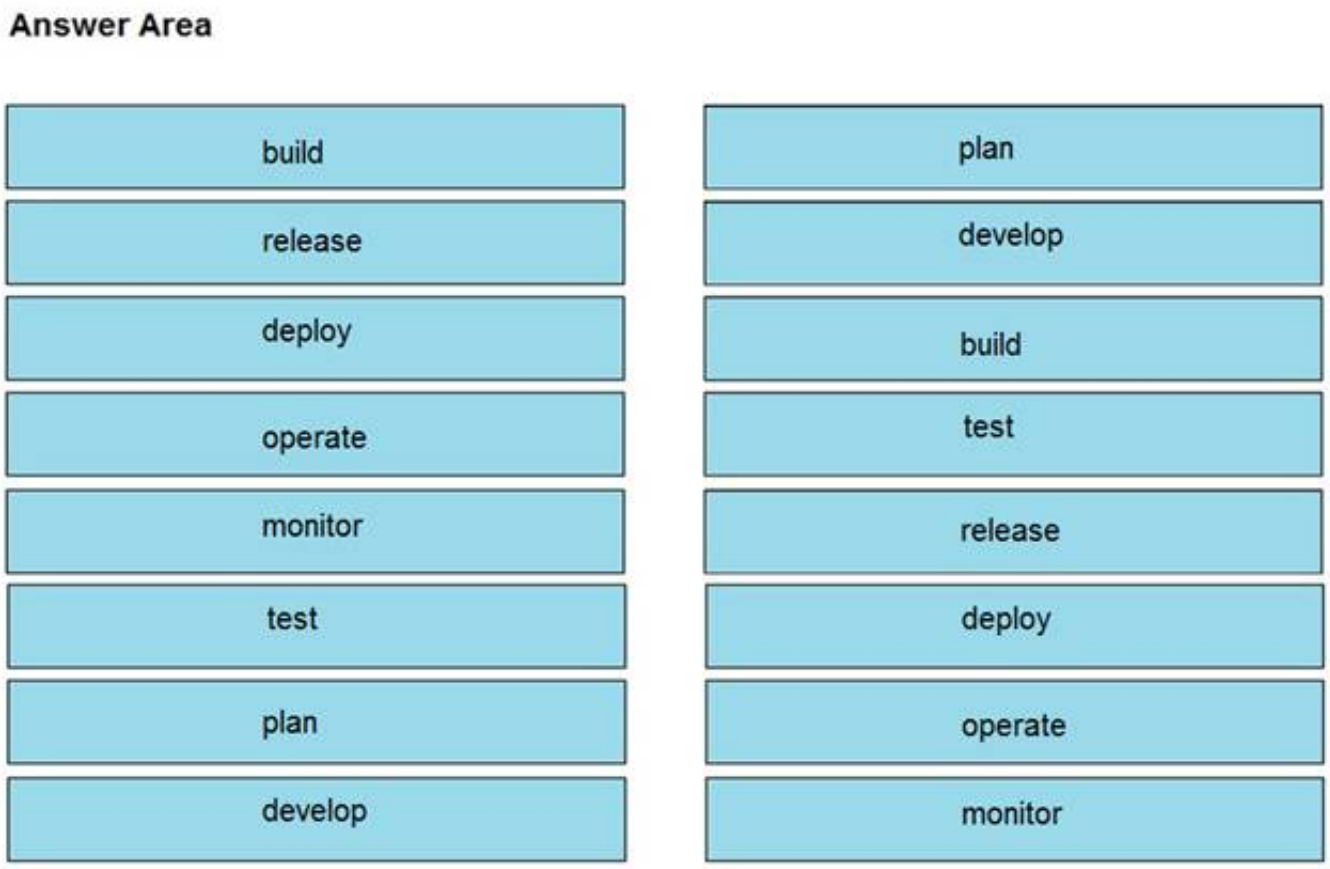
NEW QUESTION 43
Drag and drop the components from the left onto the phases of the CI/CD pipeline on the right.



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 47
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 48
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, realmDomain=0, shortrealm=0
x-xss-protection: 1; mode=block
```

Where does it signify that a page will be stopped from loading when a scripting attack is detected?

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

Answer: C

NEW QUESTION 52
.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual 350-201 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the 350-201 Product From:

https://www.2passeasy.com/dumps/350-201/

Money Back Guarantee

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 FirstTry

* 350-201 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year