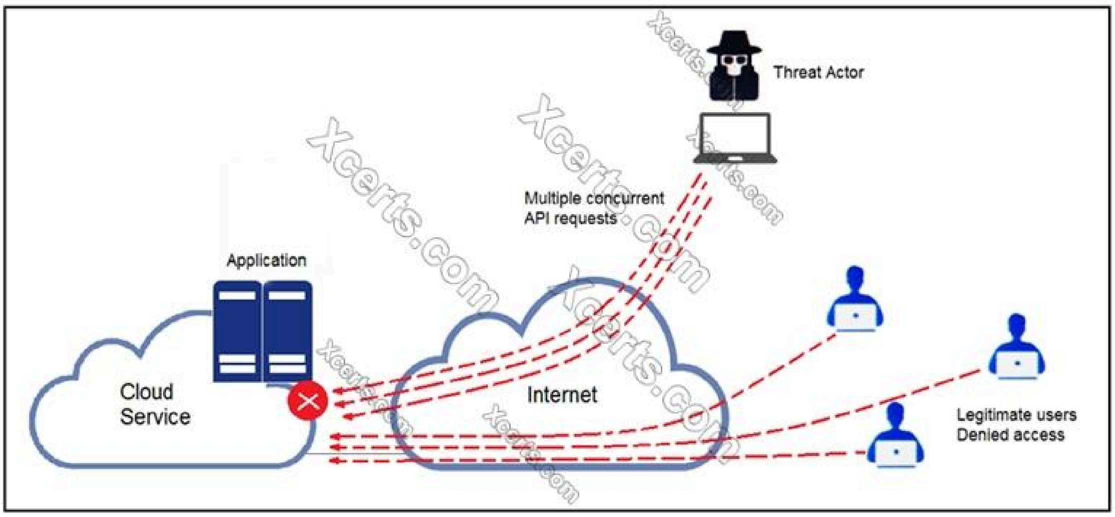
Performing CyberOps Using Core Security Technologies (CBRCOR)

1. Refer to the exhibit. A threat actor behind a single computer exploited a cloud-based application by sending multiple concurrent API requests. These requests made the application unresponsive. Which solution protects the application from being overloaded and ensures more equitable application access across the end-user community?


Threat Actor
Multiple concurrent API requests
Application
Cloud Service
Internet
Legitimate users Denied access

A. Limit the number of API calls that a single client is allowed to make

B. Add restrictions on the edge router on how often a single client can access the API

C. Reduce the amount of data that can be fetched from the total pool of active clients that call the API

D. Increase the application cache of the total pool of active clients that call the API

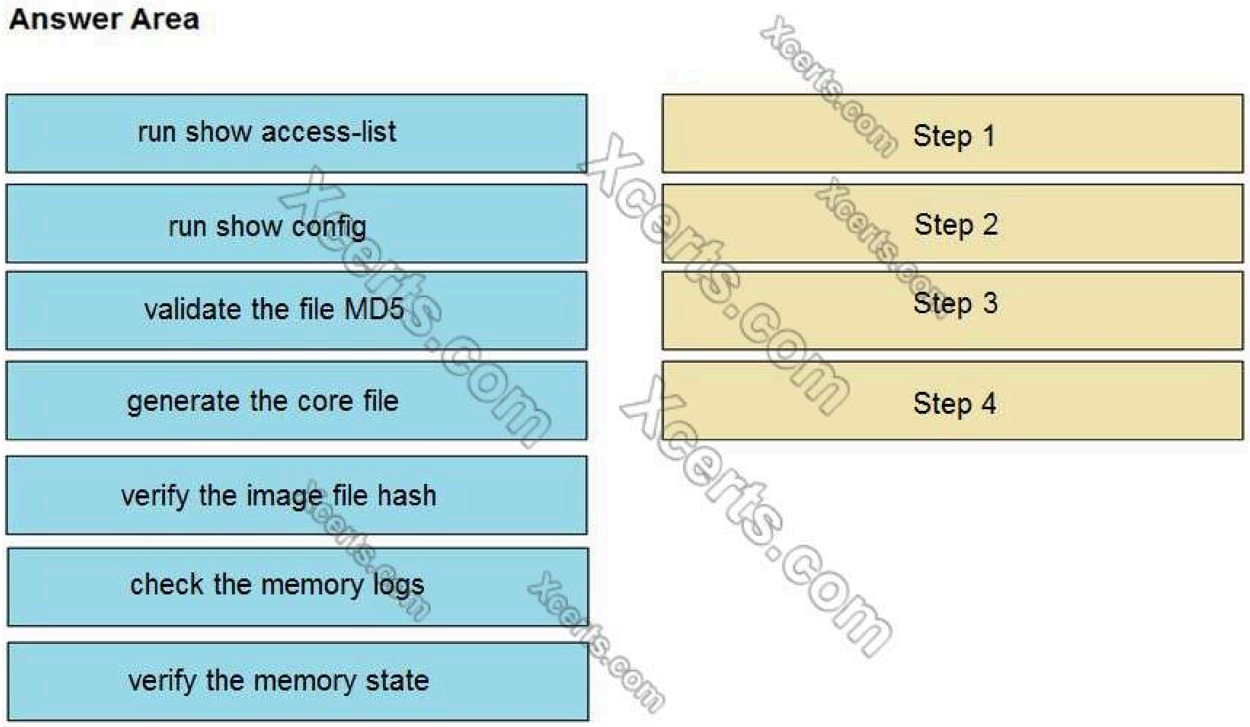
Answer(s): A

---

2. An organization lost connectivity to critical servers, and users cannot access business applications and internal websites. An engineer checks the network devices to investigate the outage and determines that all devices are functioning. Drag and drop the steps from the left into the sequence on the right to continue investigating this issue. Not all options are used.

Select and Place:

Exhibit A:



Answer Area

run show access-list

run show config

validate the file MD5

generate the core file

verify the image file hash

check the memory logs

verify the memory state

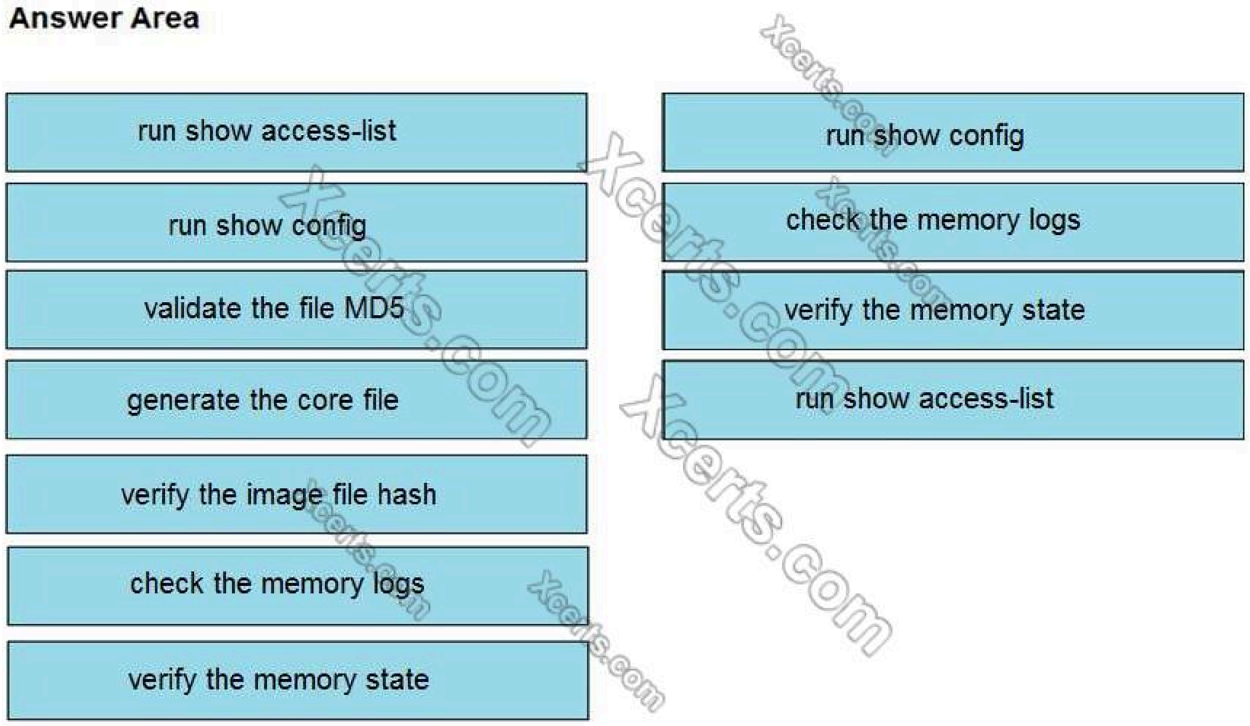
Step 1

Step 2

Step 3

Step 4

Exhibit B:



Answer Area

run show access-list

run show config

validate the file MD5

generate the core file

verify the image file hash

check the memory logs

verify the memory state

run show config

check the memory logs

verify the memory state

run show access-list

A. Please refer to Exhibit B for the answer.

Answer(s): A

---

3. 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

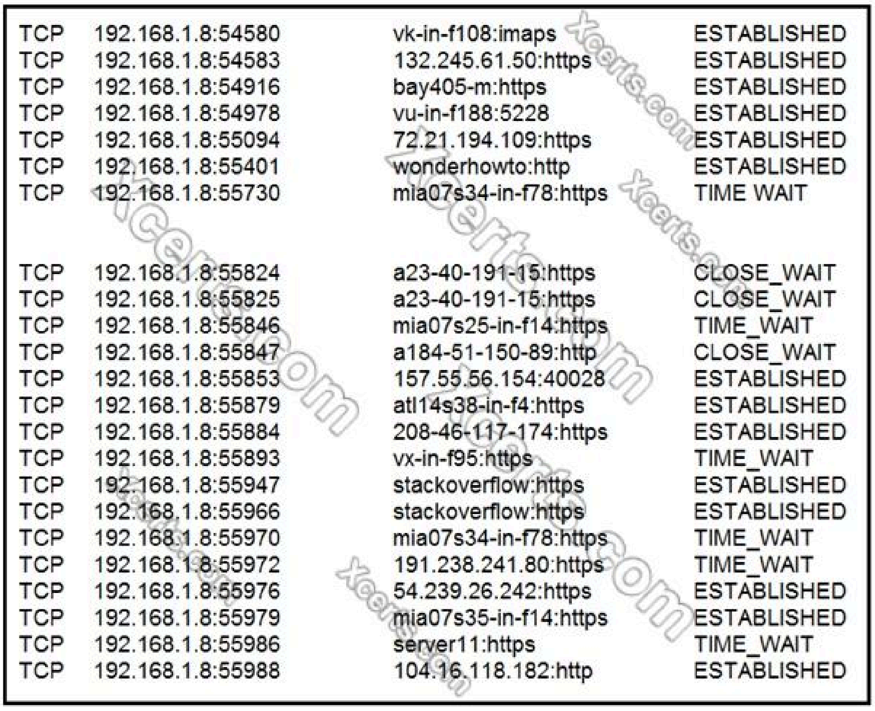
C. accessing multiple servers

D. downloading more than 10 files

Answer(s): C

---

4. Refer to the exhibit. 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?



```
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. packet sniffer

B. malware analysis

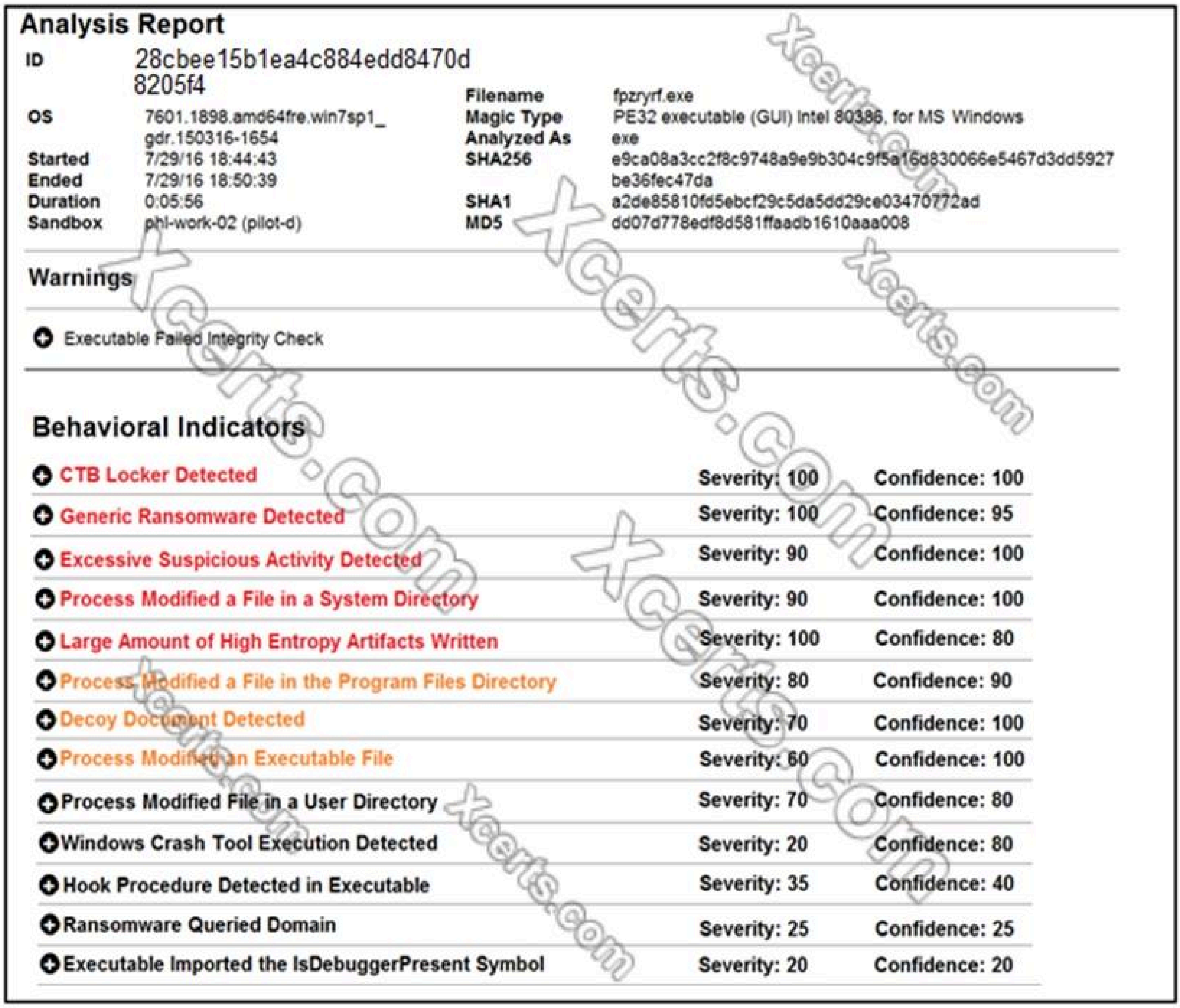
C. SIEM

D. firewall manager

Answer(s): A

---

5. 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?



Analysis Report

ID	28cbee15b1ea4c884edd8470d 8205f4	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	e9ca08a3cc2f8c9748a9e9b304c9f5a16d830066e5467d3dd5927 be36fec47da
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

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(s): C

---

6. The physical security department received a report that an unauthorized person followed an authorized individual to enter a secured premise. The incident was documented and given to a security specialist to analyze. Which step should be taken at this stage?

A. Determine the assets to which the attacker has access

B. Identify assets the attacker handled or acquired

C. Change access controls to high risk assets in the enterprise

D. Identify movement of the attacker in the enterprise

Answer(s): D

---

7. 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

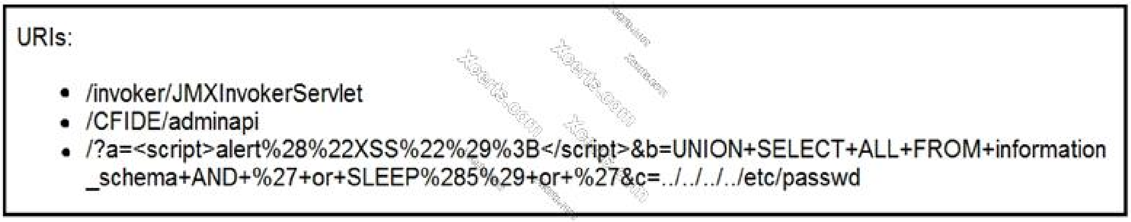
□ D. key assets and executives

□ E. malware analysis report

Answer(s): B E

---

8. Refer to the exhibit. At which stage of the threat kill chain is an attacker, based on these URIs of inbound web requests from known malicious Internet scanners?



URIs:

- /invoker/JMXInvokerServlet
- /CFIDE/adminapi
- /?a=<script>alert%28%22XSS%22%29%3B</script>&b=UNION+SELECT+ALL+FROM+information_schema+AND+%27+or+SLEEP%285%29+or+%27&c=../../../../etc/passwd

A. exploitation

B. actions on objectives

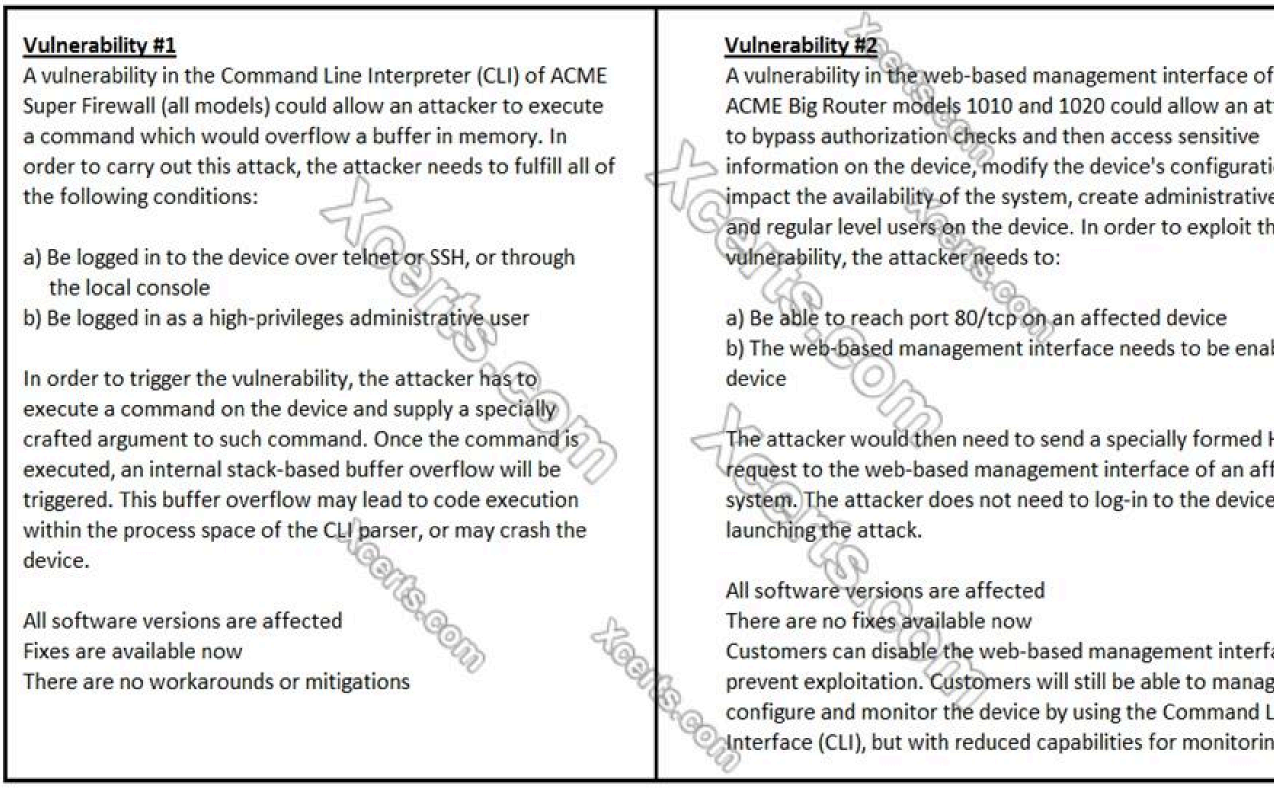
C. delivery

D. reconnaissance

Answer(s): C

---

9. Refer to the exhibit. How must these advisories be prioritized for handling?



Vulnerability #1

A vulnerability in the Command Line Interpreter (CLI) of ACME Super Firewall (all models) could allow an attacker to execute a command which would overflow a buffer in memory. In order to carry out this attack, the attacker needs to fulfill all of the following conditions:

a) Be logged in to the device over telnet or SSH, or through the local console

b) Be logged in as a high-privileges administrative user

In order to trigger the vulnerability, the attacker has to execute a command on the device and supply a specially crafted argument to such command. Once the command is executed, an internal stack-based buffer overflow will be triggered. This buffer overflow may lead to code execution within the process space of the CLI parser, or may crash the device.

All software versions are affected

Fixes are available now

There are no workarounds or mitigations

Vulnerability #2

A vulnerability in the web-based management interface of ACME Big Router models 1010 and 1020 could allow an at to bypass authorization checks and then access sensitive information on the device, modify the device's configurati impact the availability of the system, create administrative and regular level users on the device. In order to exploit th vulnerability, the attacker needs to:

a) Be able to reach port 80/tcp on an affected device

b) The web-based management interface needs to be enal device

The attacker would then need to send a specially formed I request to the web-based management interface of an aff system. The attacker does not need to log-in to the device launching the attack.

All software versions are affected

There are no fixes available now

Customers can disable the web-based management interf prevent exploitation. Customers will still be able to manag configure and monitor the device by using the Command L Interface (CLI), but with reduced capabilities for monitorin

A. The highest priority for handling depends on the type of institution deploying the devices

B. Vulnerability #2 is the highest priority for every type of institution

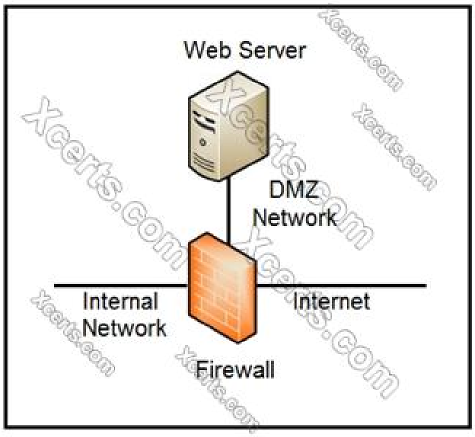
C. Vulnerability #1 and vulnerability #2 have the same priority

D. Vulnerability #1 is the highest priority for every type of institution

Answer(s): D

---

10. 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

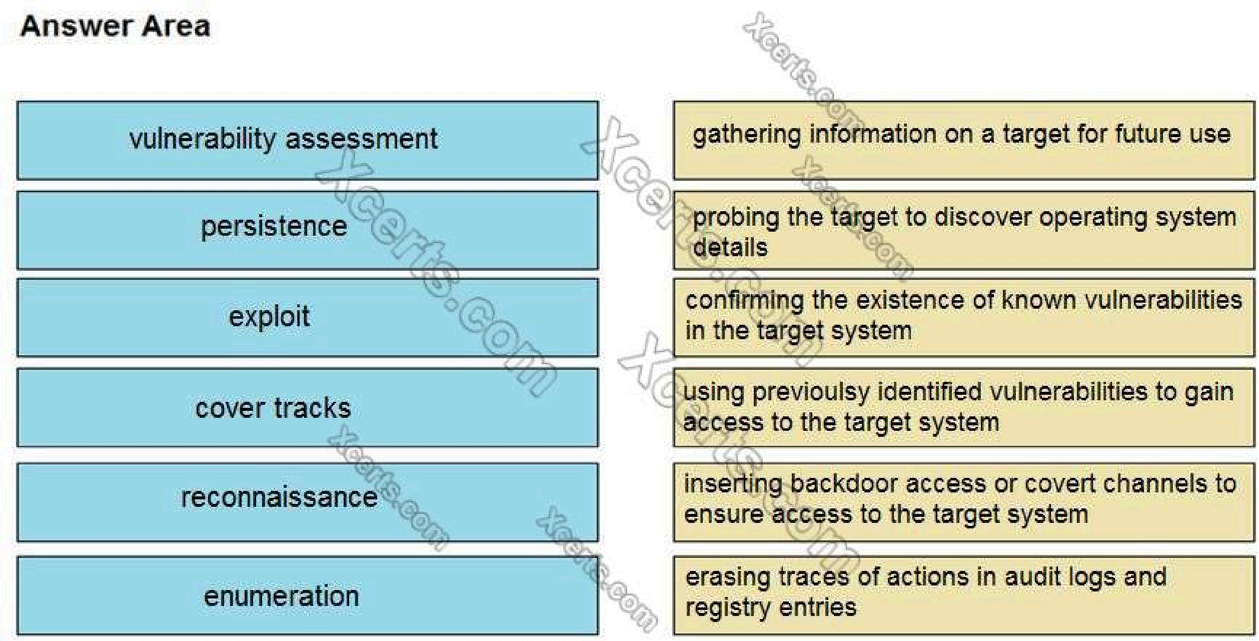
☐ D. Move the webserver to the internal network

☐ E. Move the webserver to the external network

Answer(s): B D

---

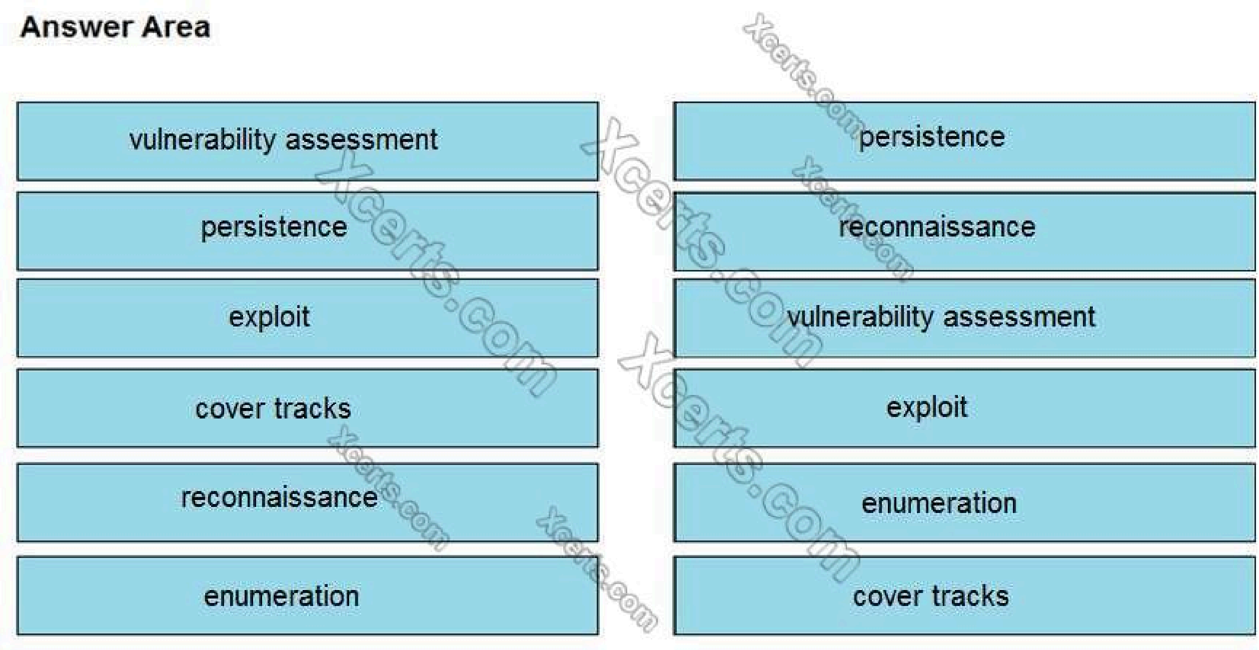
11. Drag and drop the phases to evaluate the security posture of an asset from the left onto the activity that happens during the phases on the right.
Select and Place:
Exhibit A:



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 previoulsy 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

Exhibit B:



Answer Area

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

A. Please refer to Exhibit B for the answer.

Answer(s): A

---

12. 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(s): B

---

13. 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(s): B

---

14. 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(s): D

---

15. An engineer is analyzing a possible compromise that happened a week ago when the company database servers unexpectedly went down. The analysis reveals that attackers tampered with Microsoft SQL Server Resolution Protocol and launched a DDoS attack. The engineer must act quickly to ensure that all systems are protected. Which two tools should be used to detect and mitigate this type of future attack? (Choose two.)

□ A. firewall

□ B. Wireshark

□ C. autopsy

□ D. SHA512

□ E. IPS

Answer(s): A B

---

16. A European-based advertisement company collects tracking information from partner websites and stores it on a local server to provide tailored ads. Which standard must the company follow to safeguard the resting data?

A. HIPAA

B. PCI-DSS

C. Sarbanes-Oxley

D. GDPR

Answer(s): D

---

17. 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 reimage 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(s): C

---

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(s): D

---

19. The incident response team receives information about the abnormal behavior of a host. A malicious file is found being executed from an external USB flash drive. The team collects and documents all the necessary evidence from the computing resource. What is the next step?

A. Conduct a risk assessment of systems and applications

B. Isolate the infected host from the rest of the subnet

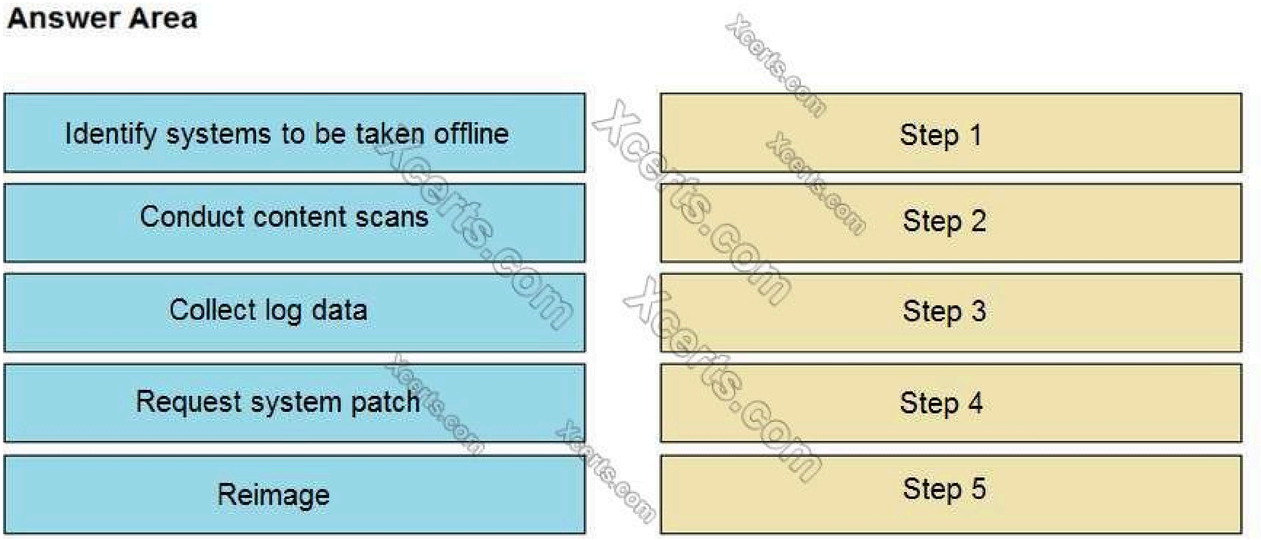
C. Install malware prevention software on the host

D. Analyze network traffic on the host’s subnet

Answer(s): B

---

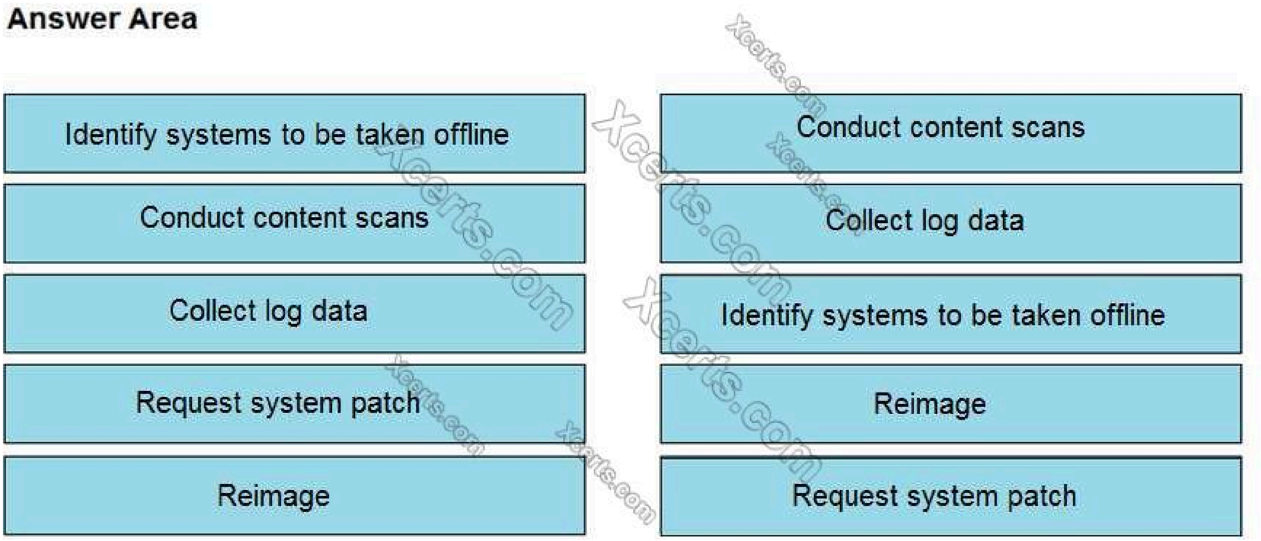
20. An engineer notices that unauthorized software was installed on the network and discovers that it was installed by a dormant user account. The engineer suspects an escalation of privilege attack and responds to the incident. Drag and drop the activities from the left into the order for the response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



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

Exhibit B:



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

A. Please refer to Exhibit B for the answer.

Answer(s): A
