DUMPSQUEEN

Performing CyberOps Using Core Security Technologies (CBRCOR)

Cisco 350-201

Version Demo

Total Demo Questions: 10

Total Premium Questions: 139

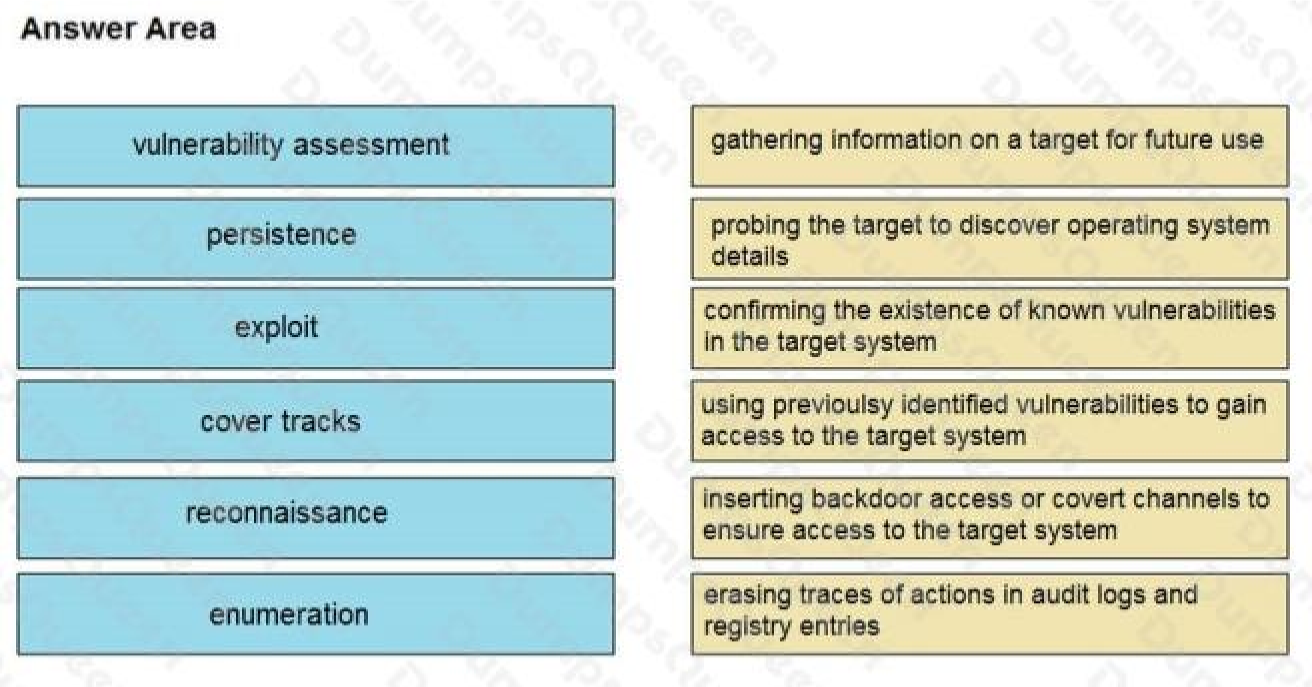
Buy Premium PDF

QUESTION NO: 1 - (DRAG DROP)

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.

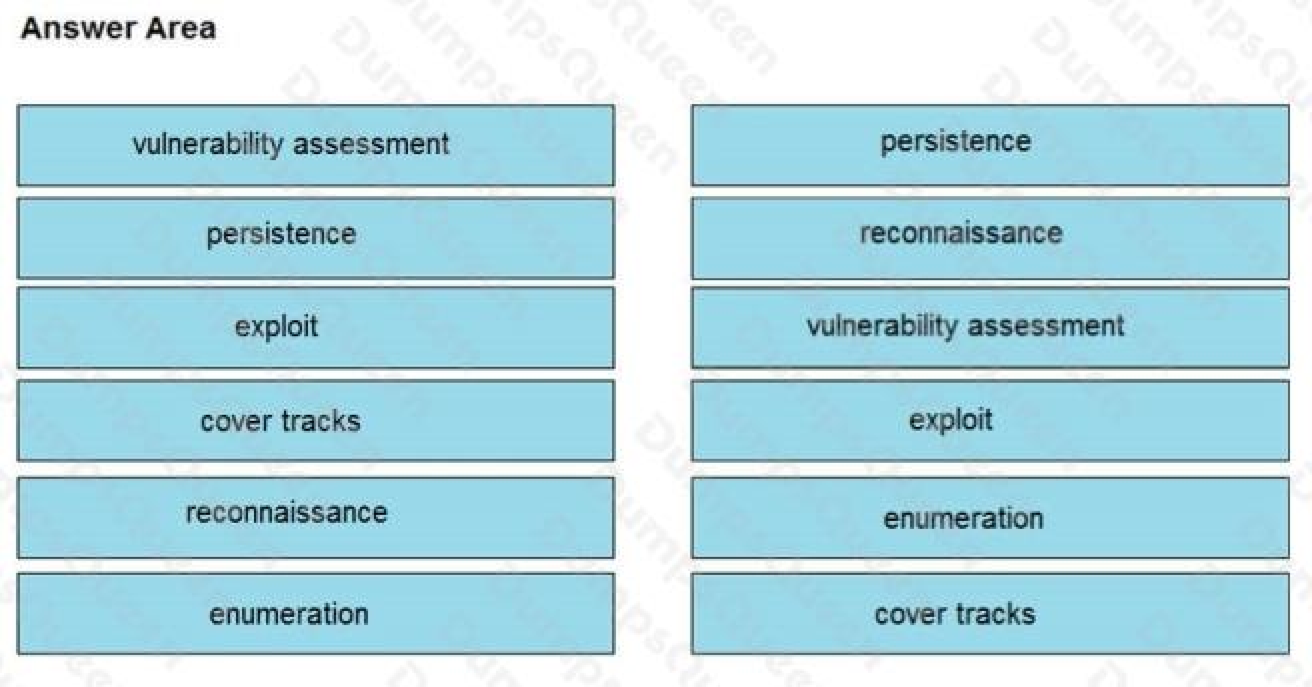
Select and Place:



Answer Area

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

ANSWER:

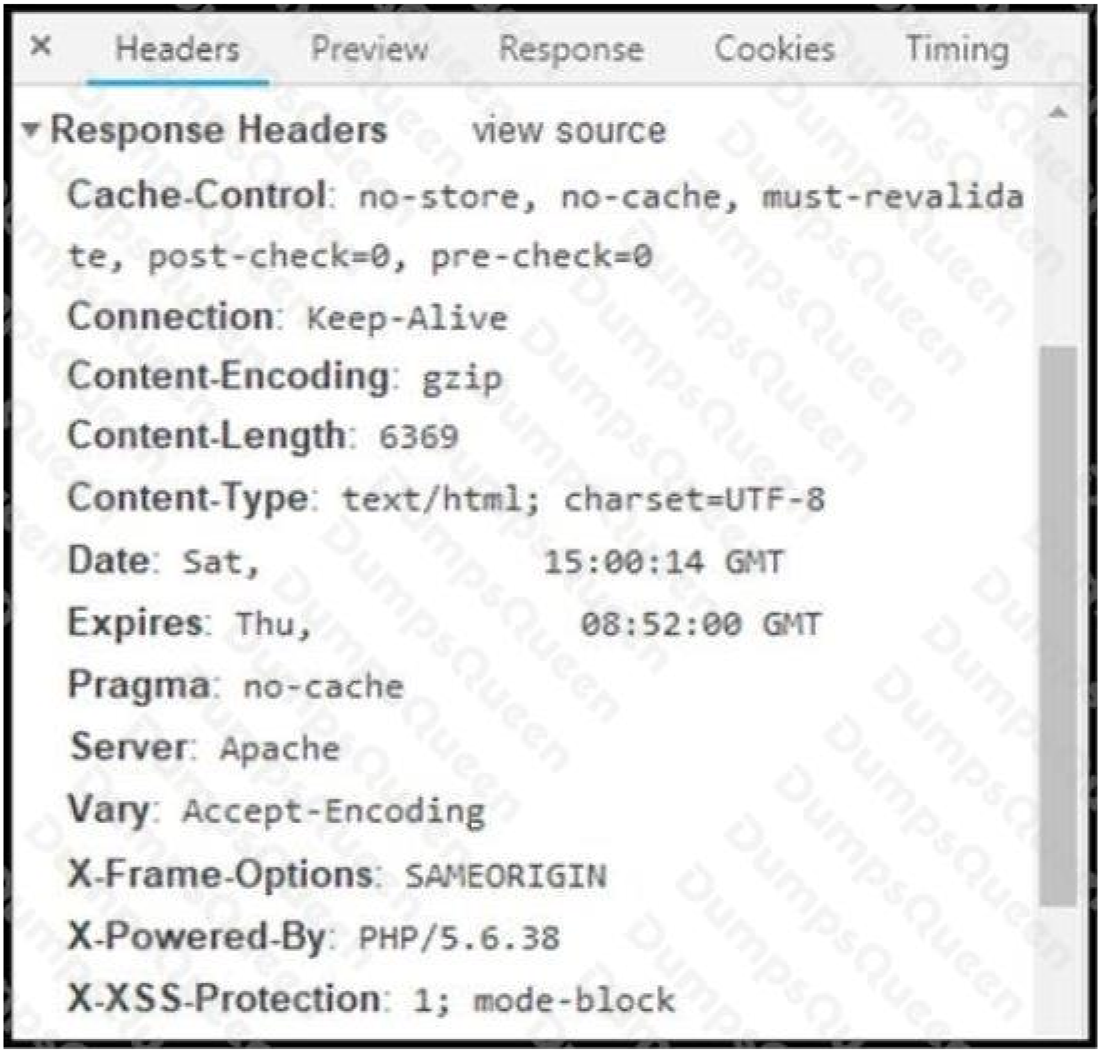


Answer Area

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

Explanation:

QUESTION NO: 2



```
Cache-Control: no-store, no-cache, must-revalida
te, post-check=0, pre-check=0
Connection: Keep-Alive
Content-Encoding: gzip
Content-Length: 6369
Content-Type: text/html; charset=UTF-8
Date: Sat,               15:00:14 GMT
Expires: Thu,               08:52:00 GMT
Pragma: no-cache
Server: Apache
Vary: Accept-Encoding
X-Frame-Options: SAMEORIGIN
X-Powered-By: PHP/5.6.38
X-XSS-Protection: 1; mode-block
```

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

ANSWER: C

QUESTION NO: 3

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.

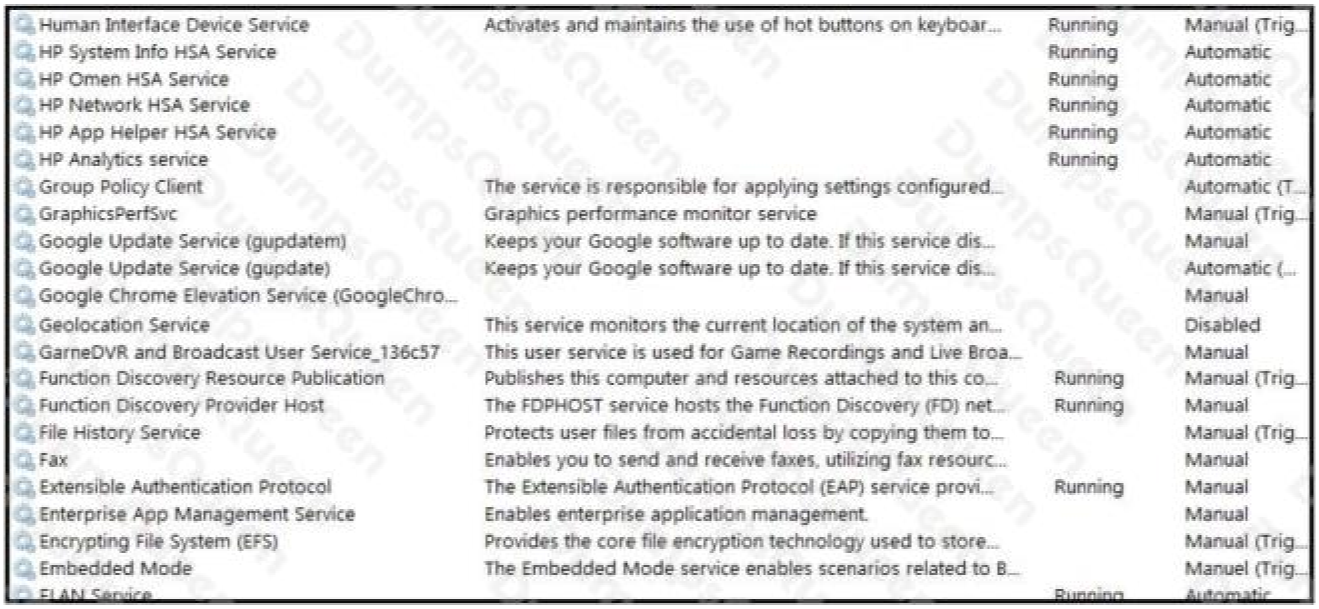
B. Orchestration arranges the tasks, while automation arranges processes.

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.

ANSWER: A

QUESTION NO: 4



Human Interface Device Service	Activates and maintains the use of hot buttons on keyboar...	Running	Manual (Trig...
HP System Info HSA Service		Running	Automatic
HP Omen HSA Service		Running	Automatic
HP Network HSA Service		Running	Automatic
HP App Helper HSA Service		Running	Automatic
HP Analytics service		Running	Automatic
Group Policy Client	The service is responsible for applying settings configured...		Automatic (T...
GraphicsPerfSvc	Graphics performance monitor service		Manual (Trig...
Google Update Service (gupdatem)	Keeps your Google software up to date. If this service dis...		Manual
Google Update Service (gupdate)	Keeps your Google software up to date. If this service dis...		Automatic (...
Google Chrome Elevation Service (GoogleChro...			Manual
Geolocation Service	This service monitors the current location of the system an...		Disabled
GarneDVR and Broadcast User Service_136c57	This user service is used for Game Recordings and Live Broa...		Manual
Function Discovery Resource Publication	Publishes this computer and resources attached to this co...	Running	Manual (Trig...
Function Discovery Provider Host	The FDPHOST service hosts the Function Discovery (FD) net...	Running	Manual
File History Service	Protects user files from accidental loss by copying them to...		Manual (Trig...
Fax	Enables you to send and receive faxes, utilizing fax resourc...		Manual
Extensible Authentication Protocol	The Extensible Authentication Protocol (EAP) service provi...	Running	Manual
Enterprise App Management Service	Enables enterprise application management.		Manual
Encrypting File System (EFS)	Provides the core file encryption technology used to store...		Manual (Trig...
Embedded Mode	The Embedded Mode service enables scenarios related to B...		Manuel (Trig...
ELAN Service		Running	Automatic

Refer to the exhibit. An engineer received multiple reports from employees unable to log into systems with the error: The Group Policy Client service failed to logon – Access is denied. Through further analysis, the engineer discovered several unexpected modifications to system settings. Which type of breach is occurring?

A. malware break

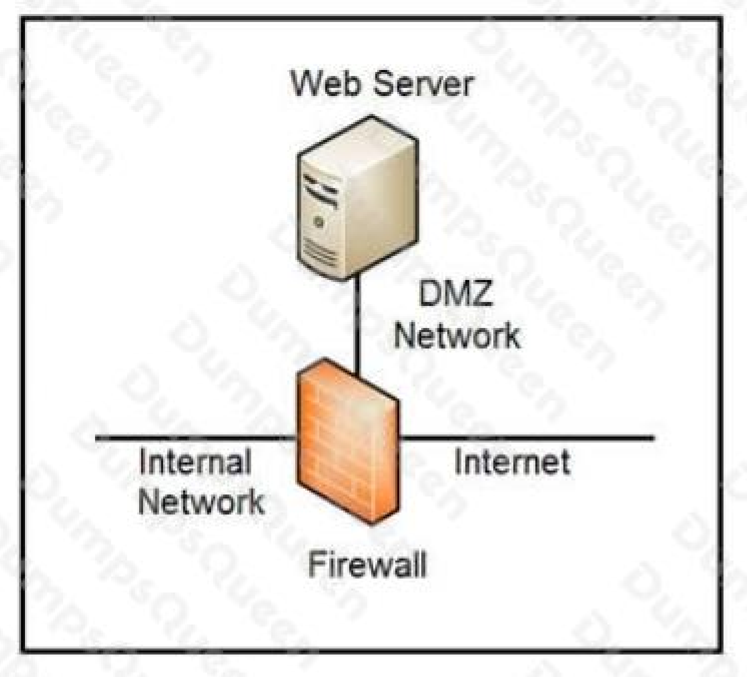
B. data theft

C. elevation of privileges

D. denial-of-service

ANSWER: C

QUESTION NO: 5



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 reverse server in the DMZ network

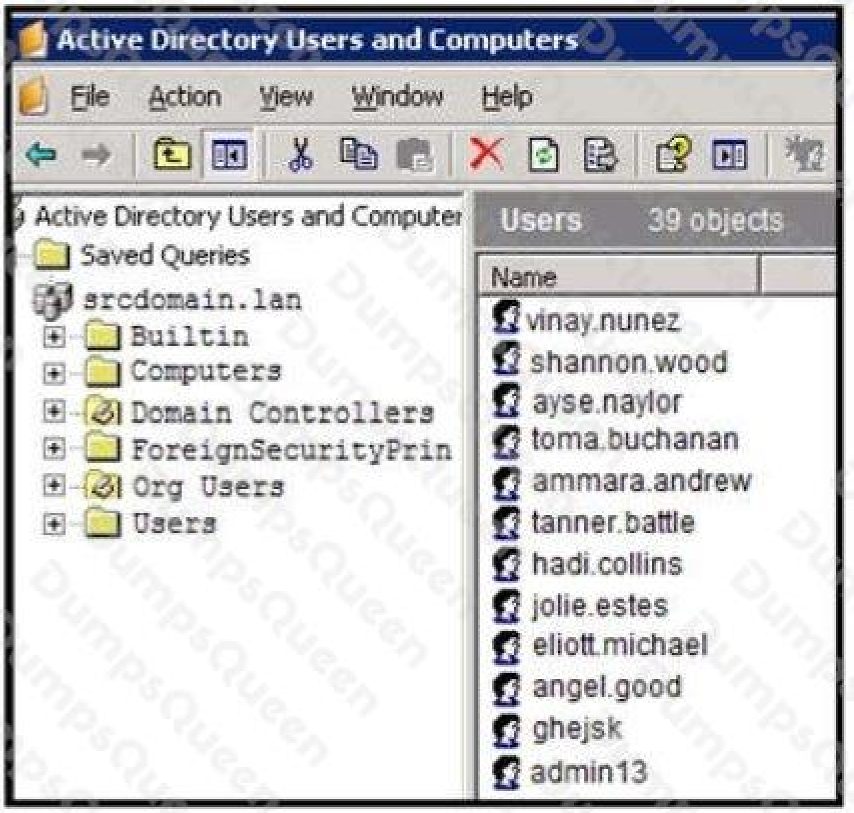
C. Create an ACL on the firewall to allow only external connections

D. Move the webserver to the internal network

E. Move the webserver to the external network

ANSWER: B D

QUESTION NO: 6



Name

vinay.nunez
shannon.wood
ayse.naylor
toma.buchanan
ammara.andrew
tanner.battle
hadi.collins
jolie.estes
eliott.michael
angel.good
ghejsk
admin13

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

ANSWER: D

QUESTION NO: 7

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.

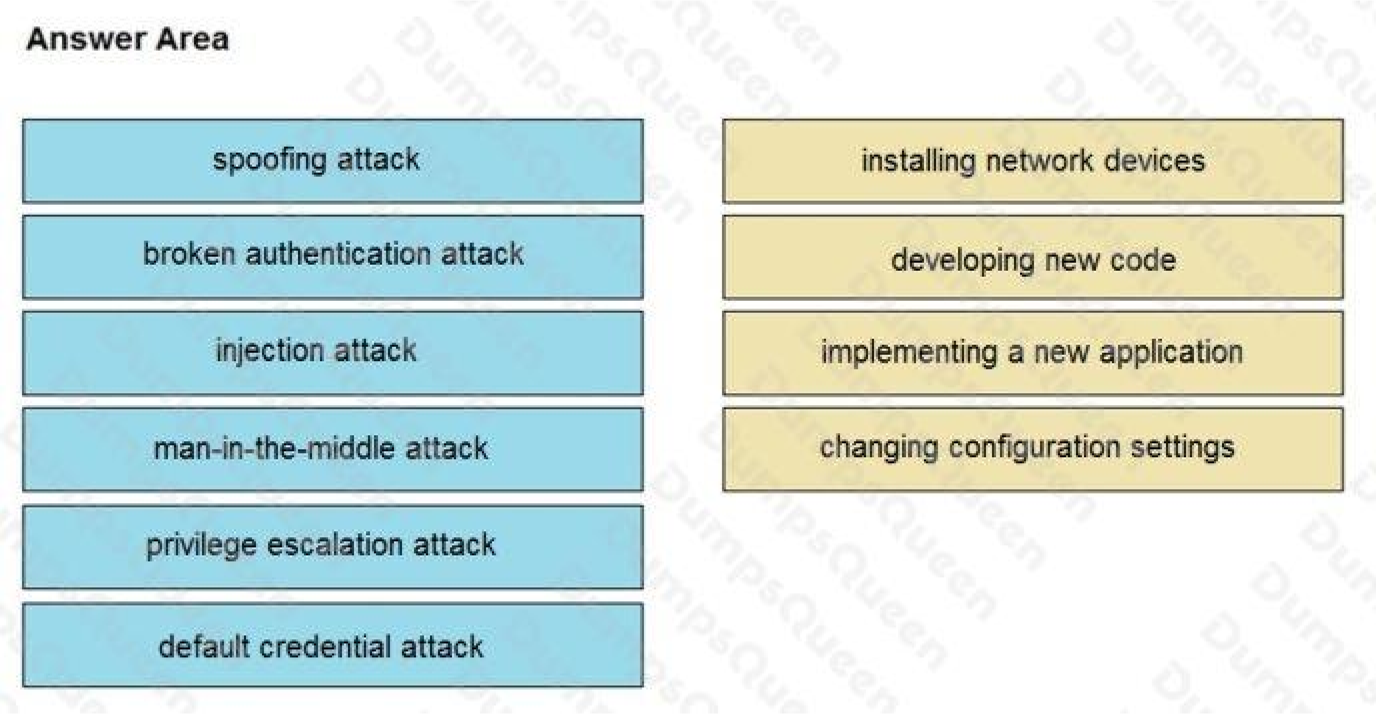
ANSWER: C E

QUESTION NO: 8 - (DRAG DROP)

DRAG DROP

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

Select and Place:



Answer Area

spoofing attack

broken authentication attack

injection attack

man-in-the-middle attack

privilege escalation attack

default credential attack

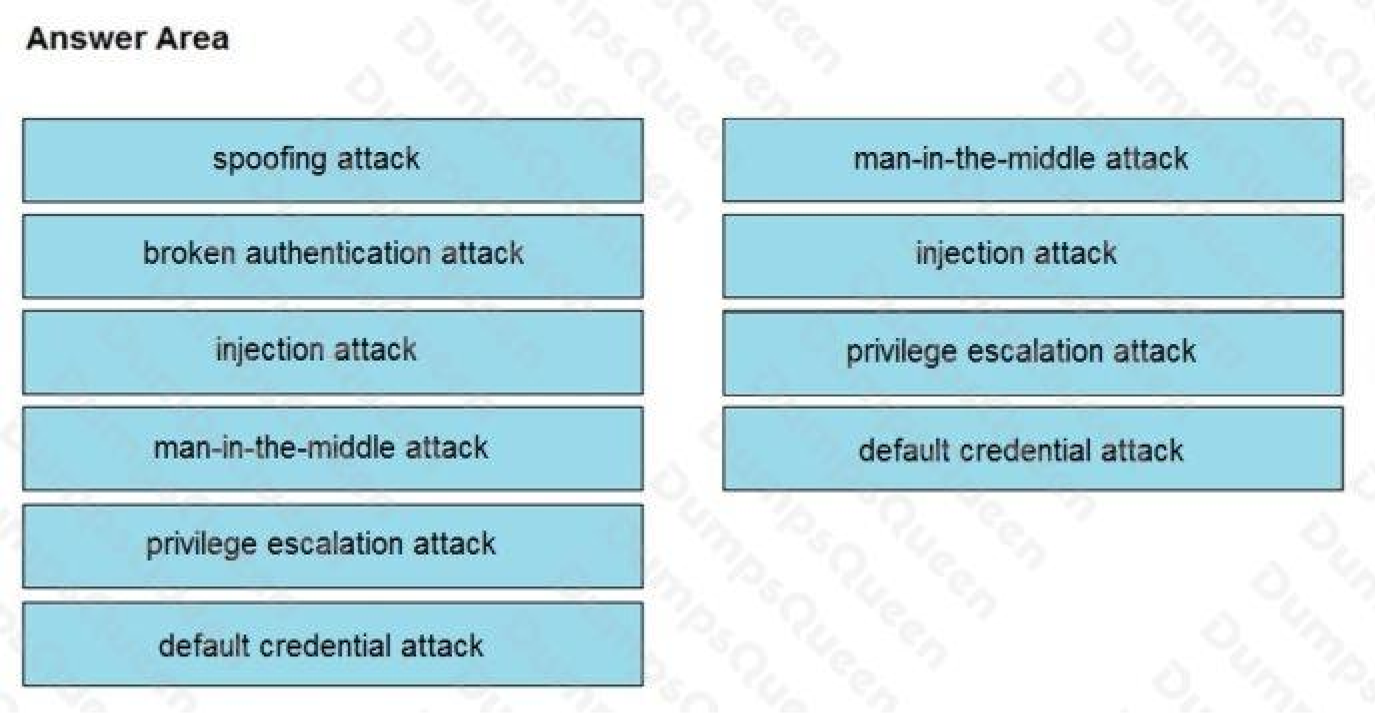
installing network devices

developing new code

implementing a new application

changing configuration settings

ANSWER:



Answer Area

spoofing attack

broken authentication attack

injection attack

man-in-the-middle attack

privilege escalation attack

default credential attack

man-in-the-middle attack

injection attack

privilege escalation attack

default credential attack

Explanation:

QUESTION NO: 9

A security incident affected an organization's critical business services, and the customer-side web API became unresponsive and crashed. An investigation revealed a spike of API call requests and a high number of inactive sessions during the incident. Which two recommendations should the engineers make to prevent similar incidents in the future? (Choose two.)

A. Configure shorter timeout periods.

B. Determine API rate-limiting requirements.

C. Implement API key maintenance.

D. Automate server-side error reporting for customers.

E. Decrease simultaneous API responses.

ANSWER: B D

QUESTION NO: 10

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: A B