350-201 Q&As

Performing CyberOps Using Cisco Security Technologies (CBRCOR)

Pass Cisco 350-201 Exam with 100% Guarantee

QUESTION 1

Engineers are working to document, list, and discover all used applications within an organization. During the regular assessment of applications from the HR backup server, an engineer discovered an unknown application. The analysis showed that the application is communicating with external addresses on a non-secure, unencrypted channel. Information gathering revealed that the unknown application does not have an owner and is not being used by a business unit. What are the next two steps the engineers should take in this investigation? (Choose two.)

A. Determine the type of data stored on the affected asset, document the access logs, and engage the incident response team.

B. Identify who installed the application by reviewing the logs and gather a user access log from the HR department.

C. Verify user credentials on the affected asset, modify passwords, and confirm available patches and updates are installed.

D. Initiate a triage meeting with department leads to determine if the application is owned internally or used by any business unit and document the asset owner.

Correct Answer: AD

QUESTION 2

What is the purpose of hardening systems?

A. to securely configure machines to limit the attack surface

B. to create the logic that triggers alerts when anomalies occur

C. to identify vulnerabilities within an operating system

D. to analyze attacks to identify threat actors and points of entry

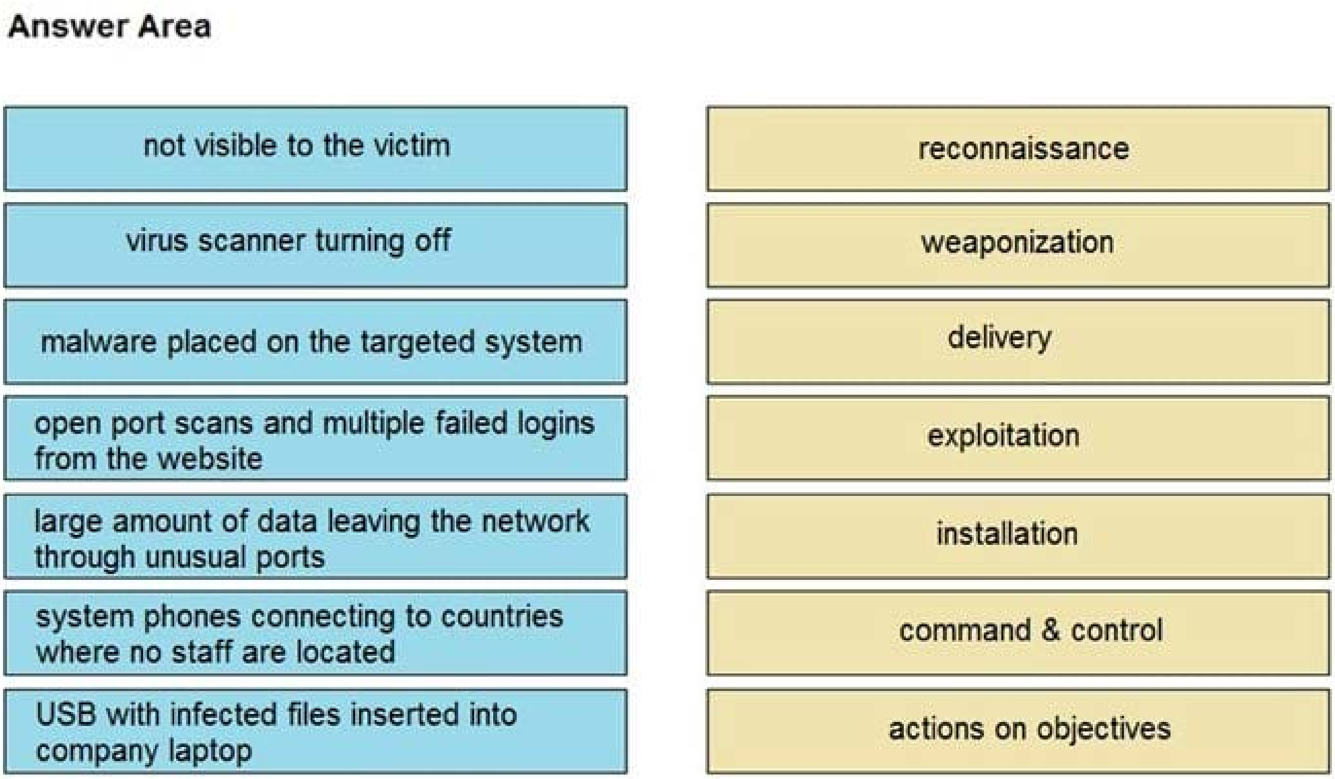
Correct Answer: A

QUESTION 3

DRAG DROP

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.

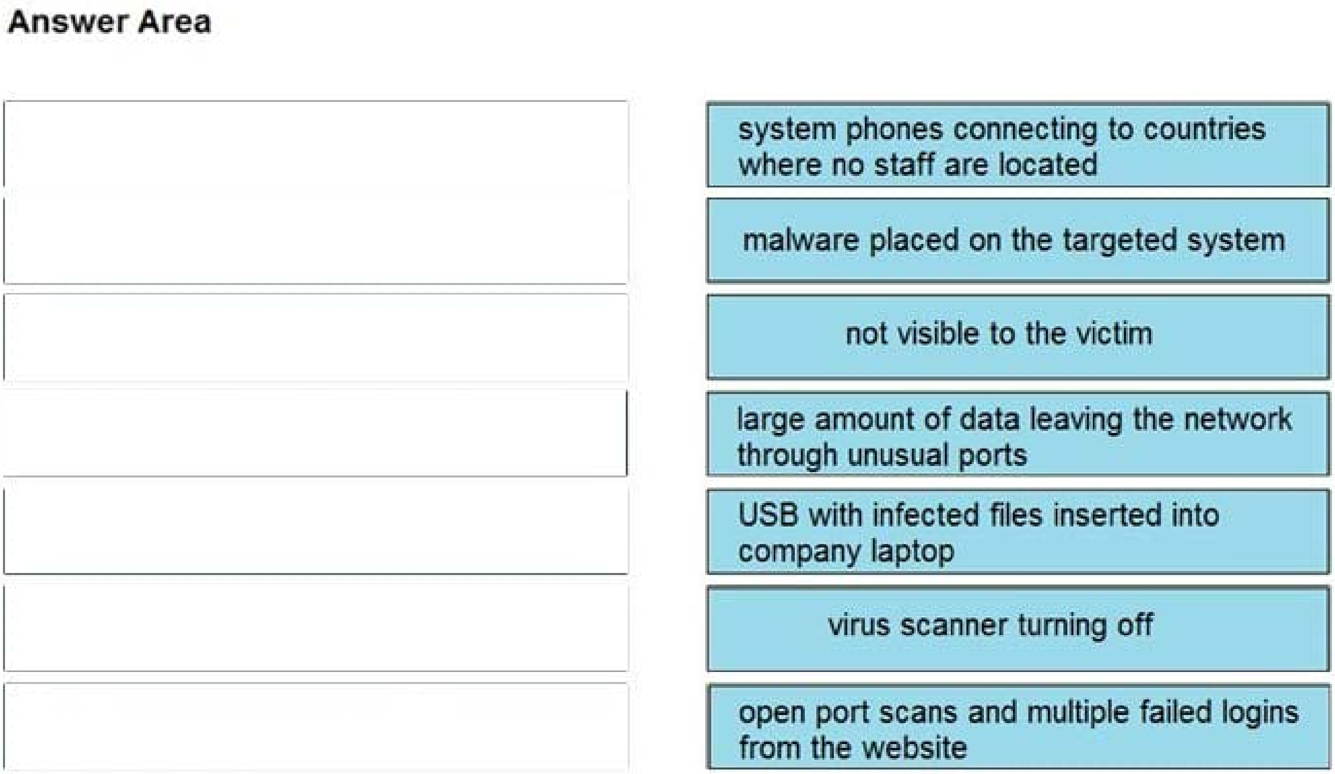
Select and Place:



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

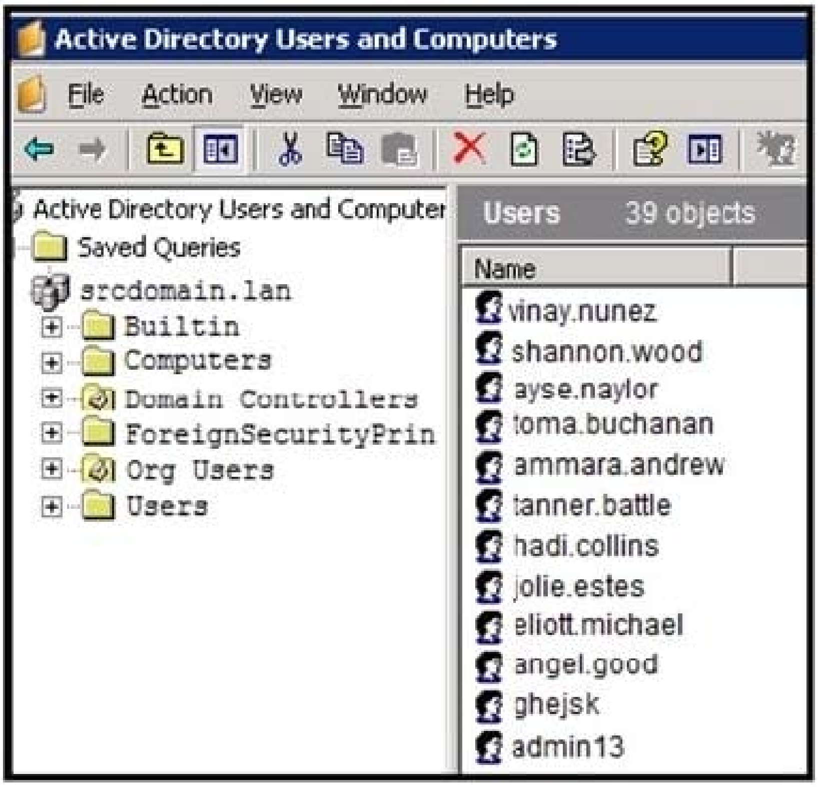
Correct Answer:



Answer Area

	system phones connecting to countries where no staff are located
	malware placed on the targeted system
	not visible to the victim
	large amount of data leaving the network through unusual ports
	USB with infected files inserted into company laptop
	virus scanner turning off
	open port scans and multiple failed logins from the website

QUESTION 4


Active Directory Users and Computers
File Action View Window Help

Active Directory Users and Computer
- Saved Queries
- srcdomain.lan
  - Builtin
  - Computers
  - Domain Controllers
  - ForeignSecurityPrin
  - Org Users
  - Users

Users 39 objects

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

Correct Answer: D

QUESTION 5

A security architect in an automotive factory is working on the Cyber Security Management System and is implementing procedures and creating policies to prevent attacks. Which standard must the architect apply?

A. IEC62446

B. IEC62443

C. IEC62439-3

D. IEC62439-2

Correct Answer: B