350-201$^{\text{Q\&As}}$

Performing CyberOps Using Cisco Security Technologies (CBRCOR)

Pass Cisco 350-201 Exam with 100% Guarantee

Following Questions and Answers are all new published by Cisco Official Exam Center

QUESTION 1

An analyst is alerted for a malicious file hash. After analysis, the analyst determined that an internal workstation is communicating over port 80 with an external server and that the file hash is associated with Duqu malware. Which tactics, techniques, and procedures align with this analysis?

A. Command and Control, Application Layer Protocol, Duqu

B. Discovery, Remote Services: SMB/Windows Admin Shares, Duqu

C. Lateral Movement, Remote Services: SMB/Windows Admin Shares, Duqu

D. Discovery, System Network Configuration Discovery, Duqu

Correct Answer: A

QUESTION 2

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.

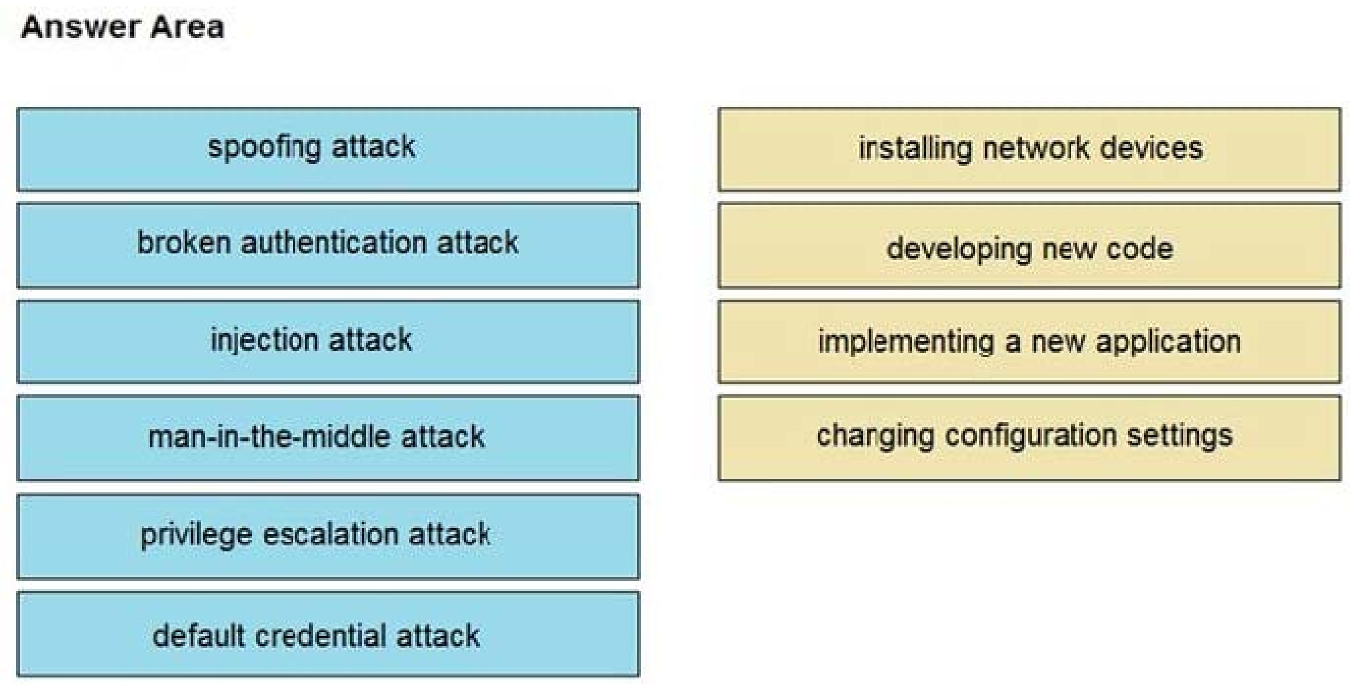
Correct Answer: A

QUESTION 3

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.

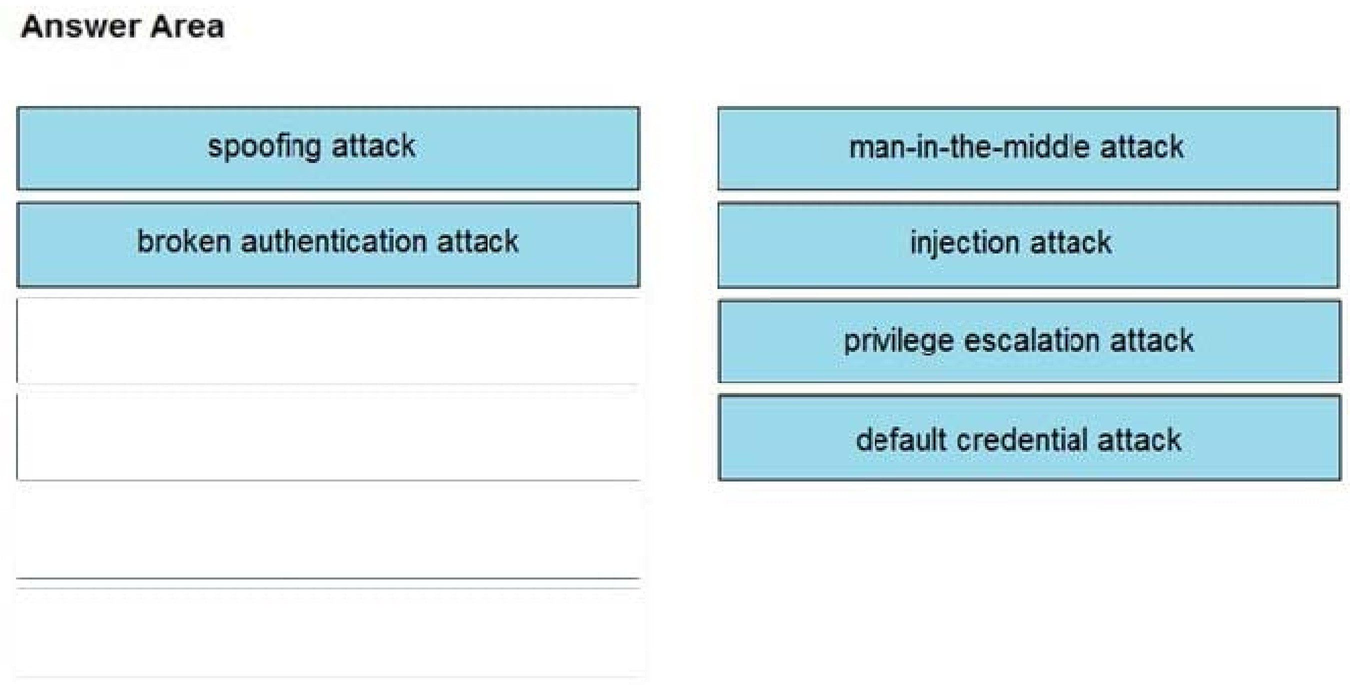
Select and Place:



Answer Area

spoofing attack	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	

Correct Answer:



Answer Area

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

QUESTION 4

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

QUESTION 5

A malware outbreak is detected by the SIEM and is confirmed as a true positive. The incident response team follows the playbook to mitigate the threat. What is the first action for the incident response team?

A. Assess the network for unexpected behavior

B. Isolate critical hosts from the network

C. Patch detected vulnerabilities from critical hosts

D. Perform analysis based on the established risk factors

Correct Answer: B