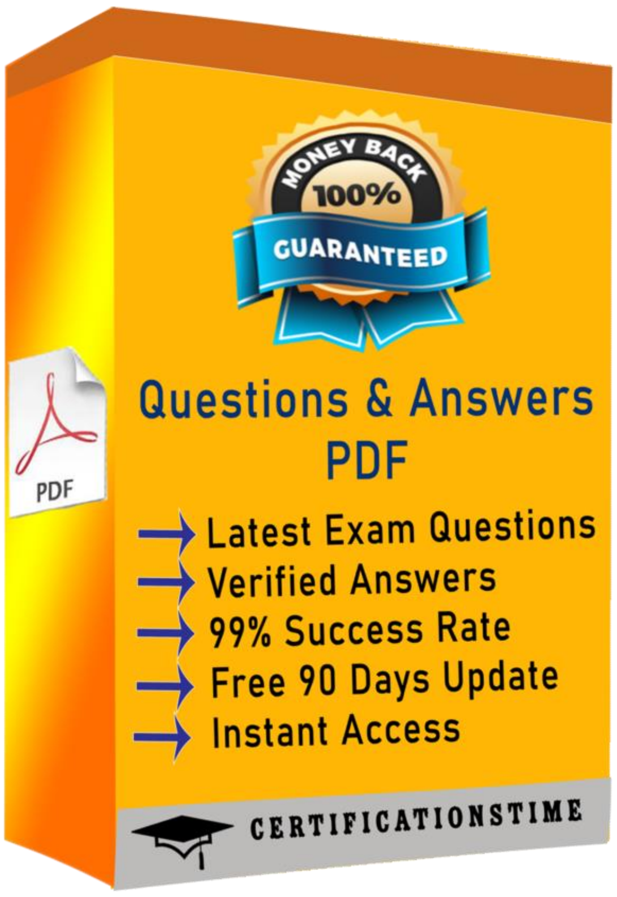
Cisco

Exam Questions 350-201

Performing CyberOps Using Core Security Technologies (CBRCOR)

https://certificationstime.com/



Question: 1

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

Question: 2

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 assetsthe attacker handled or acquired
C. Change access controlsto high risk assets in the enterprise
D. Identify movement of the attacker in the enterprise
Answer: D

Question: 3

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 ofstaff members with asset relations
D. key assets and executives
E. malware analysisreport
Answer: BE

QUESTION 4

A security analyst receives an escalation regarding an unidentified connection on the Accounting A1 server within a monitored zone. The analyst pulls the logs and discovers that a Powershell process and a WMI tool process were started on the server after the connection was established and that a PE format file was created in the system directory. What is the next step the analyst should take?

A. Isolate the server and perform forensic analysis of the file to determine the type and vector of a possible attack
B. Identify the server owner through the CMDB and contact the owner to determine if these were planned and identifiable activities
C. Review the server backup and identify server content and data criticality to assess the intrusion risk
D. Perform behavioral analysis of the processes on an isolated workstation and perform cleaning procedures if the file is malicious
Answer: C

QUESTION 5

Refer to the exhibit.
350-201 dumps 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?

A. exploitation
B. actions on objectives
C. delivery
D. reconnaissance
Answer: C

QUESTION 6

The incident response team was notified of detected malware. The team identified the infected hosts, removed the malware, restored the functionality and data of infected systems, and planned a company meeting to improve the incident handling capability. Which step was missed according to the NIST incident handling guide?

A. Contain the malware
B. Install IPS software
C. Determine the escalation path
D. Perform vulnerability assessment
Answer: D

QUESTION 7

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.
350-201 dumps exhibit

Solution:
350-201 dumps exhibit

Does this meet the goal?
A. Yes
B. Not Mastered
Answer: A

Full Access

https://certificationstime.com/updated/350-201-exam-dumps-pdf/