350-201 Q&As

Performing CyberOps Using Cisco Security Technologies (CBRCOR)

Pass Cisco 350-201 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass2lead.com/350-201.html

100% Passing Guarantee
100% Money Back Assurance

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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

An organization suffered a security breach in which the attacker exploited a Netlogon Remote Protocol vulnerability for further privilege escalation. Which two actions should the incident response team take to prevent this type of attack from reoccurring? (Choose two.)

A. Implement a patch management process.

B. Scan the company server files for known viruses.

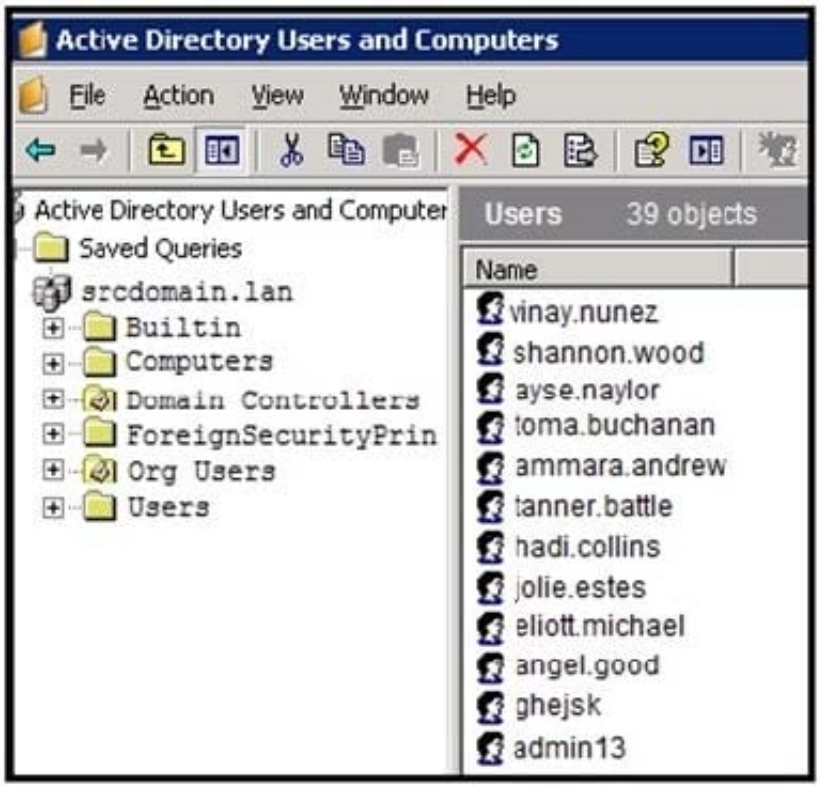
C. Apply existing patches to the company servers.

D. Automate antivirus scans of the company servers.

E. Define roles and responsibilities in the incident response playbook.

Correct Answer: DE

QUESTION 2



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 3

A security manager received an email from an anomaly detection service, that one of their contractors has downloaded 50 documents from the company\\'s confidential document management folder using a company-owned asset al039-ice4ce687TL0500. A security manager reviewed the content of downloaded documents and noticed that the data affected is from different departments. What are the actions a security manager should take?

A. Measure confidentiality level of downloaded documents.

B. Report to the incident response team.

C. Escalate to contractor\\'s manager.

D. Communicate with the contractor to identify the motives.

Correct Answer: B

QUESTION 4

What is a benefit of key risk indicators?

A. clear perspective into the risk position of an organization

B. improved visibility on quantifiable information

C. improved mitigation techniques for unknown threats

D. clear procedures and processes for organizational risk

Correct Answer: C

Reference: https://www.metricstream.com/insights/Key-Risk-indicators-ERM.htm#:~:text=Risk%20Management%20(ERM)-,Overview,and%20mitigate%20them%20in%20time.

QUESTION 5

A SOC team is investigating a recent, targeted social engineering attack on multiple employees. Cross-correlated log

analysis revealed that two hours before the attack, multiple assets received requests on TCP port 79. Which action should be taken by the SOC team to mitigate this attack?

A. Disable BIND forwarding from the DNS server to avoid reconnaissance.

B. Disable affected assets and isolate them for further investigation.

C. Configure affected devices to disable NETRJS protocol.

D. Configure affected devices to disable the Finger service.

Correct Answer: D