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.passapply.com/350-201.html

100% Passing Guarantee
100% Money Back Assurance

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

An engineer has created a bash script to automate a complicated process. During script execution, this error occurs: permission denied. Which command must be added to execute this script?

A. chmod +x ex.sh

B. source ex.sh

C. chroot ex.sh

D. sh ex.sh

Correct Answer: A

Reference: https://www.redhat.com/sysadmin/exit-codes-demystified

QUESTION 3

A threat actor has crafted and sent a spear-phishing email with what appears to be a trustworthy link to the site of a conference that an employee recently attended. The employee clicked the link and was redirected to a malicious site through which the employee downloaded a PDF attachment infected with ransomware. The employee opened the attachment, which exploited vulnerabilities on the desktop. The ransomware is now installed and is calling back to its command and control server.

Which security solution is needed at this stage to mitigate the attack?

A. web security solution

B. email security solution

C. endpoint security solution

D. network security solution

Correct Answer: D

QUESTION 4

A patient views information that is not theirs when they sign in to the hospital\\'s online portal. The patient calls the support center at the hospital but continues to be put on hold because other patients are experiencing the same issue. An incident has been declared, and an engineer is now on the incident bridge as the CyberOps Tier 3 Analyst. There is a concern about the disclosure of PII occurring in real-time.

What is the first step the analyst should take to address this incident?

A. Evaluate visibility tools to determine if external access resulted in tampering

B. Contact the third-party handling provider to respond to the incident as critical

C. Turn off all access to the patient portal to secure patient records

D. Review system and application logs to identify errors in the portal code

Correct Answer: C

QUESTION 5

A security expert is investigating a breach that resulted in a $32 million loss from customer accounts. Hackers were able to steal API keys and two-factor codes due to a vulnerability that was introduced in a new code a few weeks before the attack.

Which step was missed that would have prevented this breach?

A. use of the Nmap tool to identify the vulnerability when the new code was deployed

B. implementation of a firewall and intrusion detection system

C. implementation of an endpoint protection system

D. use of SecDevOps to detect the vulnerability during development

Correct Answer: D

Reference: https://securityintelligence.com/how-to-prioritize-security-vulnerabilities-in-secdevops/