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.geekcert.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

A company\\'s web server availability was breached by a DDoS attack and was offline for 3 hours because it was not deemed a critical asset in the incident response playbook. Leadership has requested a risk assessment of the asset. An analyst conducted the risk assessment using the threat sources, events, and vulnerabilities.

Which additional element is needed to calculate the risk?

A. assessment scope

B. event severity and likelihood

C. incident response playbook

D. risk model framework

Correct Answer: D

QUESTION 2

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 3

Refer to the exhibit. Which command was executed in PowerShell to generate this log?

Max (K)	Retain	OverflowAction	Entries	Log
15,168	0	OverwriteAsNeeded	20,792	Application
15,168	0	OverwriteAsNeeded	12,559	System
15,360	0	OverwriteAsNeeded	11,173	Windows PowerShell

A. Get-EventLog -LogName*

B. Get-EventLog -List

C. Get-WinEvent -ListLog* -ComputerName localhost

D. Get-WinEvent -ListLog*

Correct Answer: A

Reference: https://lists.xymon.com/archive/2019-March/046125.html

QUESTION 4

A SOC team is informed that a UK-based user will be traveling between three countries over the next 60 days. Having the names of the 3 destination countries and the user\\'s working hours, what must the analyst do next to detect an abnormal behavior?

A. Create a rule triggered by 3 failed VPN connection attempts in an 8-hour period

B. Create a rule triggered by 1 successful VPN connection from any nondestination country

C. Create a rule triggered by multiple successful VPN connections from the destination countries

D. Analyze the logs from all countries related to this user during the traveling period

Correct Answer: D

QUESTION 5

A security engineer discovers that a spreadsheet containing confidential information for nine of their employees was fraudulently posted on a competitor\\'s website. The spreadsheet contains names, salaries, and social security numbers. What is the next step the engineer should take in this investigation?

A. Determine if there is internal knowledge of this incident.

B. Check incoming and outgoing communications to identify spoofed emails.

C. Disconnect the network from Internet access to stop the phishing threats and regain control.

D. Engage the legal department to explore action against the competitor that posted the spreadsheet.

Correct Answer: D