300-215 Q&As

Conducting Forensic Analysis and Incident Response Using Cisco Technologies for CyberOps (CBRFIR)

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

QUESTION 1

A website administrator has an output of an FTP session that runs nightly to download and unzip files to a local staging server. The download includes thousands of files, and the manual process used to find how many files failed to download is time-consuming. The administrator is working on a PowerShell script that will parse a log file and summarize how many files were successfully downloaded versus ones that failed. Which script will read the contents of the file one line at a time and return a collection of objects?

A. Get-Content-Folder \\Server\FTPFolder\Logfiles\ftpfiles.log | Show-From "ERROR", "SUCCESS"

B. Get-Content –ifmatch \\Server\FTPFolder\Logfiles\ftpfiles.log | Copy-Marked “ERROR”, “SUCCESS”

C. Get-Content –Directory \\Server\FTPFolder\Logfiles\ftpfiles.log | Export-Result “ERROR”, “SUCCESS”

D. Get-Content –Path \\Server\FTPFolder\Logfiles\ftpfiles.log | Select-String “ERROR”, “SUCCESS”

Correct Answer: D

QUESTION 2

What is the function of a disassembler?

A. aids performing static malware analysis

B. aids viewing and changing the running state

C. aids transforming symbolic language into machine code

D. aids defining breakpoints in program execution

Correct Answer: A

Reference: https://scholar.google.co.in/scholar?q=disassembler+aids+performing+static+malware+analysisandhl=enandas_sdt=0andas_vis=1andoi=scholart

QUESTION 3

An engineer received a report of a suspicious email from an employee. The employee had already opened the attachment, which was an empty Word document. The engineer cannot identify any clear signs of compromise but while reviewing running processes, observes that PowerShell.exe was spawned by cmd.exe with a grandparent winword.exe process. What is the recommended action the engineer should take?

A. Upload the file signature to threat intelligence tools to determine if the file is malicious.

B. Monitor processes as this a standard behavior of Word macro embedded documents.

C. Contain the threat for further analysis as this is an indication of suspicious activity.

D. Investigate the sender of the email and communicate with the employee to determine the motives.

Correct Answer: A

QUESTION 4

An employee receives an email from a "trusted" person containing a hyperlink that is malvertising. The employee clicks the link and the malware downloads. An information analyst observes an alert at the SIEM and engages the cybersecurity team to conduct an analysis of this incident in accordance with the incident response plan. Which event detail should be included in this root cause analysis?

A. phishing email sent to the victim

B. alarm raised by the SIEM

C. information from the email header

D. alert identified by the cybersecurity team

Correct Answer: B

QUESTION 5

A network host is infected with malware by an attacker who uses the host to make calls for files and shuttle traffic to bots. This attack went undetected and resulted in a significant loss. The organization wants to ensure this does not happen in the future and needs a security solution that will generate alerts when command and control communication from an infected device is detected. Which network security solution should be recommended?

A. Cisco Secure Firewall ASA

B. Cisco Secure Firewall Threat Defense (Firepower)

C. Cisco Secure Email Gateway (ESA)

D. Cisco Secure Web Appliance (WSA)

Correct Answer: B

Latest 300-215 Dumps   300-215 VCE Dumps   300-215 Exam Questions