300-215Q&As

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

Pass Cisco 300-215 Exam with 100% Guarantee

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

https://www.leads4pass.com/300-215.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

What is the transmogrify anti-forensics technique?

A. hiding a section of a malicious file in unused areas of a file

B. sending malicious files over a public network by encapsulation

C. concealing malicious files in ordinary or unsuspecting places

D. changing the file header of a malicious file to another file type

Correct Answer: D

Reference: https://www.csoonline.com/article/2122329/the-rise-of-anti-forensics.html#:~:text=Transmogrify%20is%20similarly%20wise%20to,a%20file%20from%2C%20say%2C%20.

QUESTION 2

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"

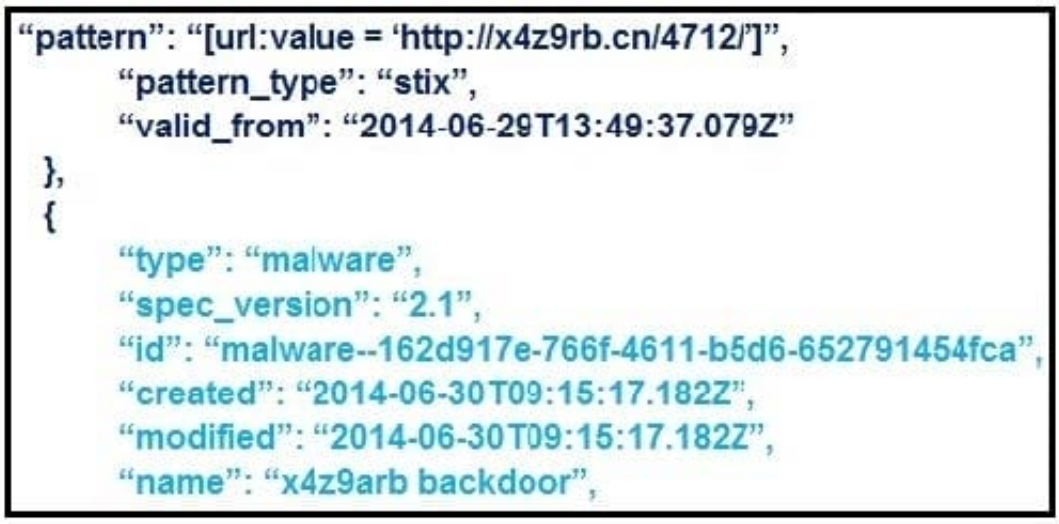
B. Get-Content –ifmatch \\Server\FTPFolder\Logfiles\ftpfiles.log | Copy-Marked “ERROR”, “SUCCESS”

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 3



Refer to the exhibit. What is the IOC threat and URL in this STIX JSON snippet?

A. malware; `http://x4z9arb.cn/4712/\\'

B. malware; x4z9arb backdoor

C. x4z9arb backdoor; http://x4z9arb.cn/4712/

D. malware; malware--162d917e-766f-4611-b5d6-652791454fca

E. stix; `http://x4z9arb.cn/4712/\\'

Correct Answer: D

QUESTION 4

An engineer received a call to assist with an ongoing DDoS attack. The Apache server is being targeted, and availability is compromised. Which step should be taken to identify the origin of the threat?

A. An engineer should check the list of usernames currently logged in by running the command $ who | cut –d' ' -f1| sort | uniq

B. An engineer should check the server\\'s processes by running commands ps -aux and sudo ps -a.

C. An engineer should check the services on the machine by running the command service -status-all.

D. An engineer should check the last hundred entries of a web server with the command sudo tail -100 /var/log/apache2/access.log.

Correct Answer: D

QUESTION 5

What is the steganography anti-forensics technique?

A. hiding a section of a malicious file in unused areas of a file

B. changing the file header of a malicious file to another file type

C. sending malicious files over a public network by encapsulation

D. concealing malicious files in ordinary or unsuspecting places

Correct Answer: A

https://blog.eccouncil.org/6-anti-forensic-techniques-that-every-cyber-investigator-dreads/