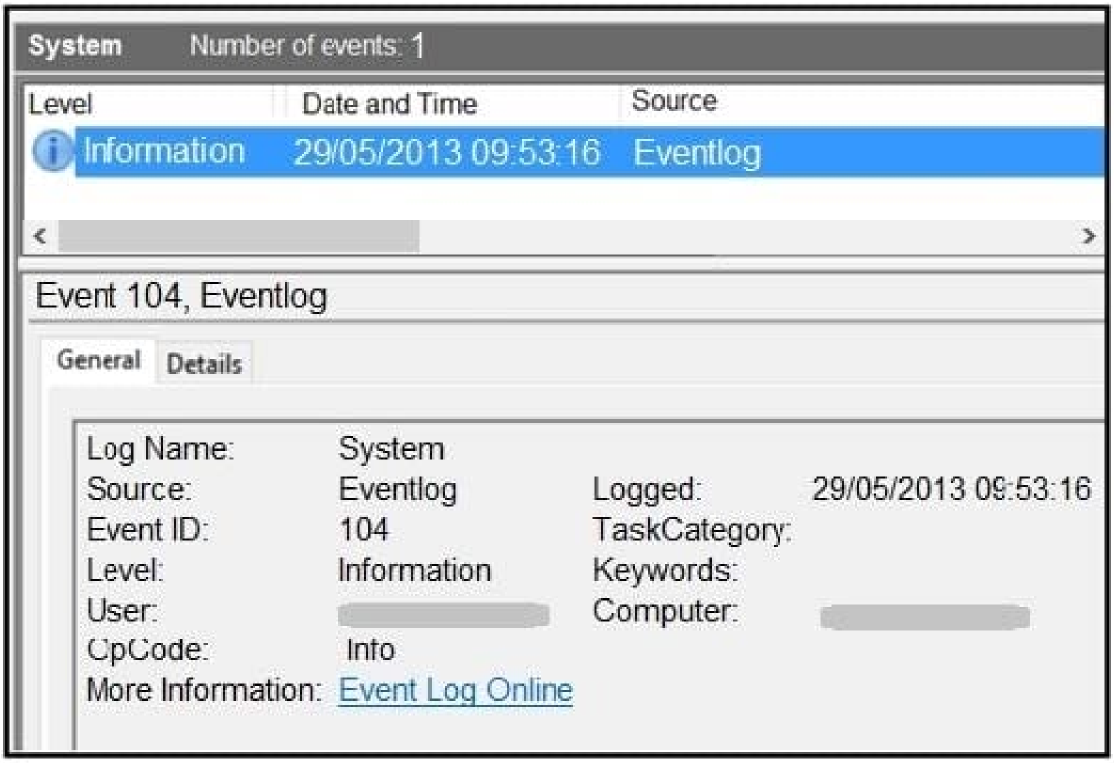
300-215$^{\text{Q\&As}}$

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

Pass Cisco 300-215 Exam with 100% Guarantee

QUESTION 1



System Number of events: 1

Level	Date and Time	Source
Information	29/05/2013 09:53:16	Eventlog

Event 104, Eventlog

Log Name: System
Source: Eventlog Logged: 29/05/2013 09:53:16
Event ID: 104 TaskCategory:
Level: Information Keywords:
User: [redacted] Computer: [redacted]
CpCode: Info
More Information: Event Log Online

Refer to the exhibit. An employee notices unexpected changes and setting modifications on their workstation and creates an incident ticket. A support specialist checks processes and services but does not identify anything suspicious. The ticket was escalated to an analyst who reviewed this event log and also discovered that the workstation had multiple large data dumps on network shares. What should be determined from this information?

A. data obfuscation

B. reconnaissance attack

C. brute-force attack

D. log tampering

Correct Answer: B

QUESTION 2

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 3

An organization uses a Windows 7 workstation for access tracking in one of their physical data centers on which a guard documents entrance/exit activities of all personnel. A server shut down unexpectedly in this data center, and a security specialist is analyzing the case. Initial checks show that the previous two days of entrance/exit logs are missing, and the guard is confident that the logs were entered on the workstation. Where should the security specialist look next to continue investigating this case?

A. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon

B. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\ProfileList

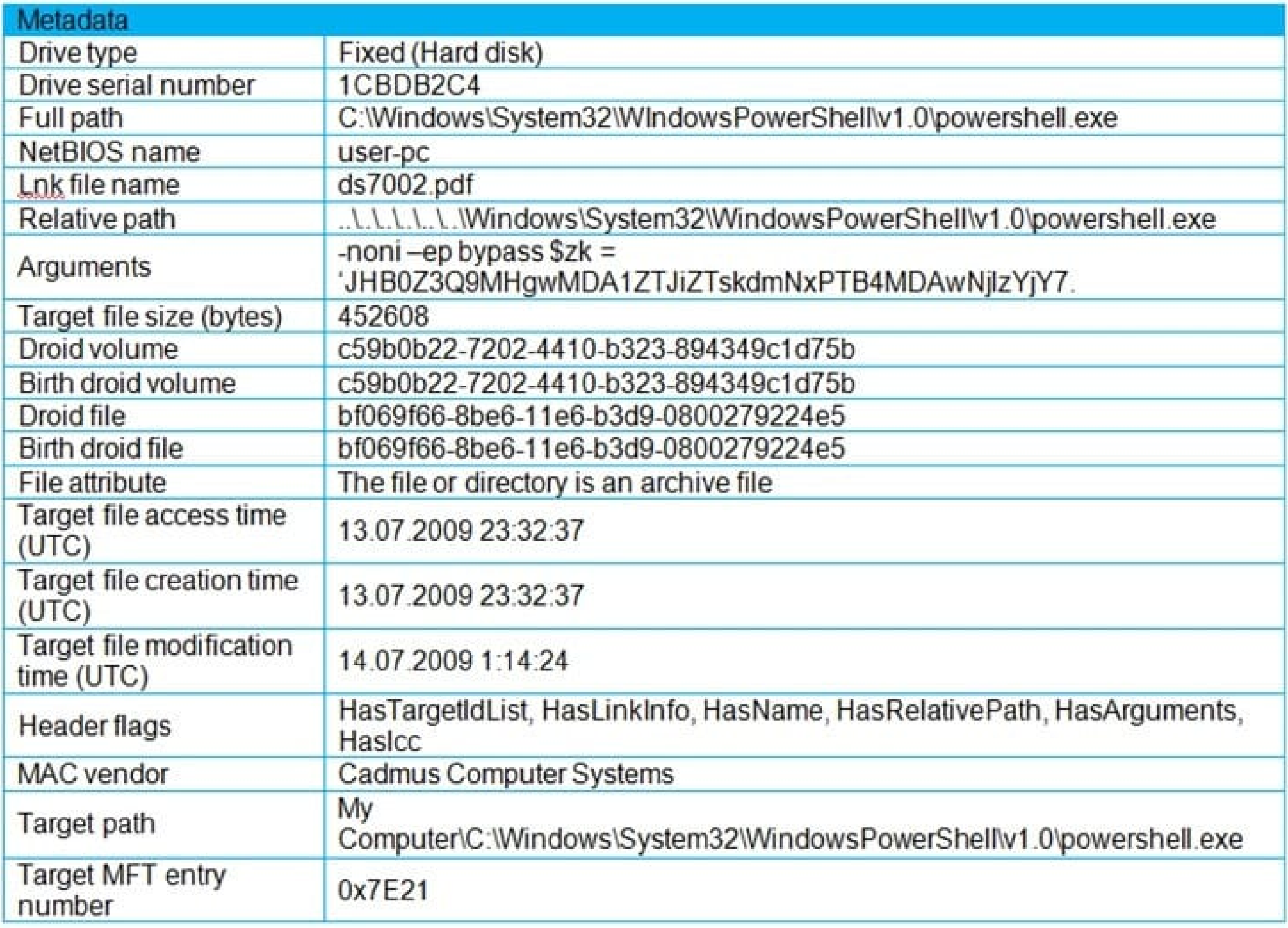
C. HKEY_CURRENT_USER\Software\Classes\Winlog

D. HKEY_LOCAL_MACHINES\SOFTWARE\Microsoft\WindowsNT\CurrentUser

Correct Answer: A

Reference: https://www.sciencedirect.com/topics/computer-science/window-event-log

QUESTION 4



Metadata	
Drive type	Fixed (Hard disk)
Drive serial number	1CBDB2C4
Full path	C:\Windows\System32\WIndowsPowerShell\v1.0\powershell.exe
NetBIOS name	user-pc
Lnk file name	ds7002.pdf
Relative path	..\..\..\..\..\..\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Arguments	-noni –ep bypass $zk = 'JHB0Z3Q9MHgwMDA1ZTJiZTskdmNxPTB4MDAwNjlzYjY7.
Target file size (bytes)	452608
Droid volume	c59b0b22-7202-4410-b323-894349c1d75b
Birth droid volume	c59b0b22-7202-4410-b323-894349c1d75b
Droid file	bf069f66-8be6-11e6-b3d9-0800279224e5
Birth droid file	bf069f66-8be6-11e6-b3d9-0800279224e5
File attribute	The file or directory is an archive file
Target file access time (UTC)	13.07.2009 23:32:37
Target file creation time (UTC)	13.07.2009 23:32:37
Target file modification time (UTC)	14.07.2009 1:14:24
Header flags	HasTargetIdList, HasLinkInfo, HasName, HasRelativePath, HasArguments, HasIcc
MAC vendor	Cadmus Computer Systems
Target path	My Computer\C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Target MFT entry number	0x7E21

Refer to the exhibit. An engineer is analyzing a .LNK (shortcut) file recently received as an email attachment and blocked by email security as suspicious. What is the next step an engineer should take?

A. Delete the suspicious email with the attachment as the file is a shortcut extension and does not represent any threat.

B. Upload the file to a virus checking engine to compare with well-known viruses as the file is a virus disguised as a legitimate extension.

C. Quarantine the file within the endpoint antivirus solution as the file is a ransomware which will encrypt the documents of a victim.

D. Open the file in a sandbox environment for further behavioral analysis as the file contains a malicious script that runs on execution.

Correct Answer: D

QUESTION 5

A security team receives reports of multiple files causing suspicious activity on users\\' workstations. The file attempted to access highly confidential information in a centralized file server. Which two actions should be taken by a security analyst to evaluate the file in a sandbox? (Choose two.)

A. Inspect registry entries

B. Inspect processes.

C. Inspect file hash.

D. Inspect file type.

E. Inspect PE header.

Correct Answer: BC

Reference: https://medium.com/@Flying_glasses/top-5-ways-to-detect-malicious-file-manually-d02744f7c43a