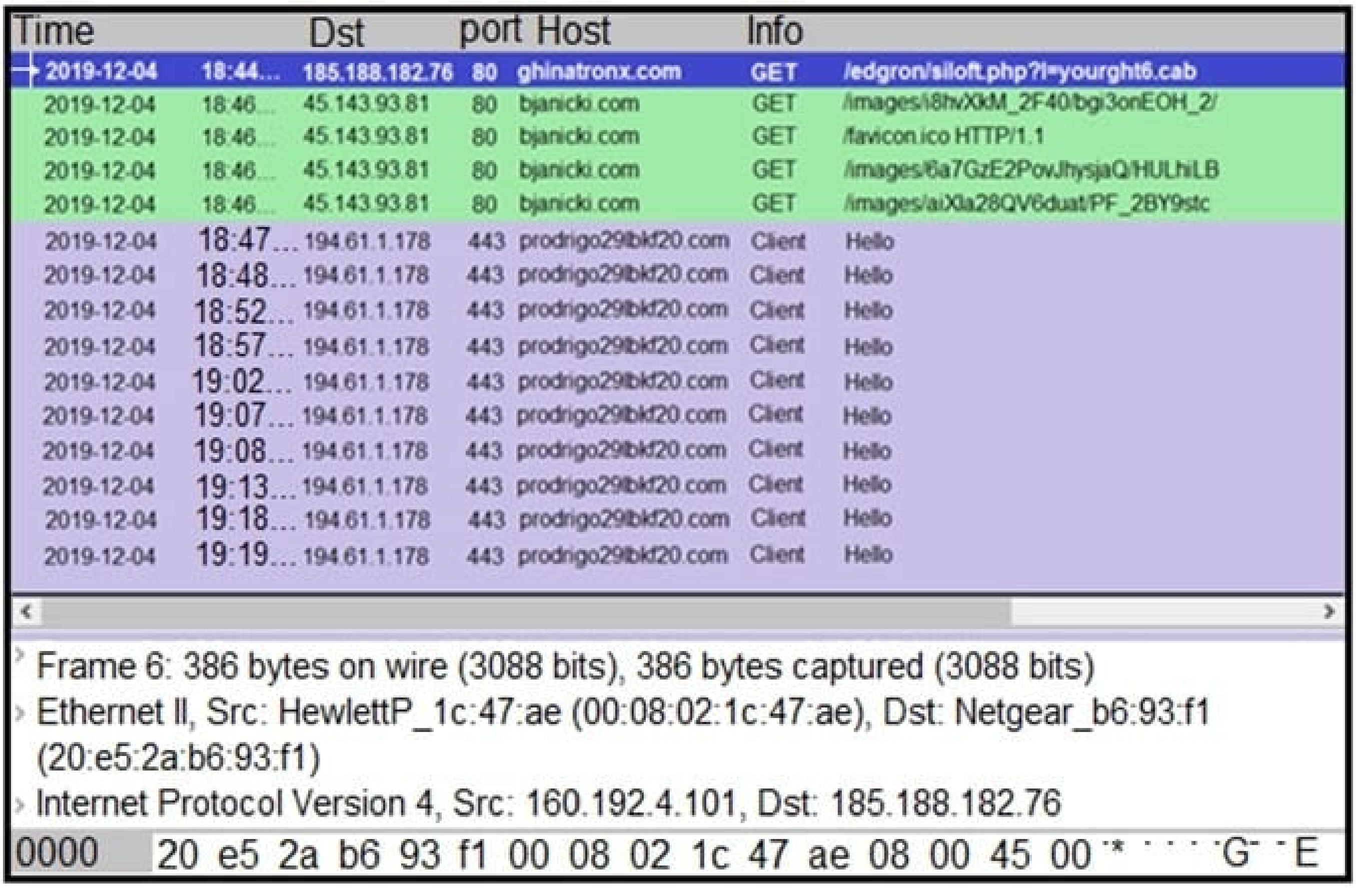
Vendor: Cisco

Exam Code:300-215

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

Version: Demo

QUESTION 1



```
Time                         Dst            port Host                Info
2019-12-04    18:44...    185.188.182.76    80   ghinatronx.com       GET     /edgron/siloft.php?l=yourght6.cab
2019-12-04    18:46...    45.143.93.81      80   bjanicki.com         GET     /images/i8hvXkM_2F40/bgi3onEOH_2/
2019-12-04    18:46...    45.143.93.81      80   bjanicki.com         GET     /favicon.ico HTTP/1.1
2019-12-04    18:46...    45.143.93.81      80   bjanicki.com         GET     /images/6a7GzE2PovJhysjaQ/HULhiLB
2019-12-04    18:46...    45.143.93.81      80   bjanicki.com         GET     /images/aiXla28QV6duat/PF_2BY9stc
2019-12-04    18:47...    194.61.1.178      443  prodrigo29lbkf20.com  Client  Hello
2019-12-04    18:48...    194.61.1.178      443  prodrigo29lbkf20.com  Client  Hello
2019-12-04    18:52...    194.61.1.178      443  prodrigo29lbkf20.com  Client  Hello
2019-12-04    18:57...    194.61.1.178      443  prodrigo29lbkf20.com  Client  Hello
2019-12-04    19:02...    194.61.1.178      443  prodrigo29lbkf20.com  Client  Hello
2019-12-04    19:07...    194.61.1.178      443  prodrigo29lbkf20.com  Client  Hello
2019-12-04    19:08...    194.61.1.178      443  prodrigo29lbkf20.com  Client  Hello
2019-12-04    19:13...    194.61.1.178      443  prodrigo29lbkf20.com  Client  Hello
2019-12-04    19:18...    194.61.1.178      443  prodrigo29lbkf20.com  Client  Hello
2019-12-04    19:19...    194.61.1.178      443  prodrigo29lbkf20.com  Client  Hello

Frame 6: 386 bytes on wire (3088 bits), 386 bytes captured (3088 bits)
Ethernet II, Src: HewlettP_1c:47:ae (00:08:02:1c:47:ae), Dst: Netgear_b6:93:f1
(20:e5:2a:b6:93:f1)
Internet Protocol Version 4, Src: 160.192.4.101, Dst: 185.188.182.76
0000   20 e5 2a b6 93 f1 00 08 02 1c 47 ae 08 00 45 00  .*.....G..E
```

Refer to the exhibit. A network engineer is analyzing a Wireshark file to determine the HTTP request that caused the initial Ursnif banking Trojan binary to download. Which filter did the engineer apply to sort the Wireshark traffic logs?

A. http.request.un matches

B. tls.handshake.type ==1

C. tcp.port eq 25

D. tcp.window_size ==0

Correct Answer: B

Reference:

https://www.malware-traffic-analysis.net/2018/11/08/index.html

https://unit42.paloaltonetworks.com/wireshark-tutorial-examining-ursnif-infections/

QUESTION 2

An investigator is analyzing an attack in which malicious files were loaded on the network and were undetected. Several of the images received during the attack include repetitive patterns. Which anti-forensic technique was used?

A. spoofing

B. obfuscation

C. tunneling

D. steganography

Correct Answer: D

Reference: https://doi.org/10.5120/1398-1887 https://www.carbonblack.com/blog/steganography-in-the-modern-attack-landscape/

QUESTION 3

A threat actor attempts to avoid detection by turning data into a code that shifts numbers to the right four times. Which anti-forensics technique is being used?

A. encryption

B. tunneling

C. obfuscation

D. poisoning

Correct Answer: C

Reference: https://www.vadesecure.com/en/malware-analysis-understanding-code-obfuscation-techniques/#:~:text=Obfuscation%20of%20character%20strings%20is,data%20when%20the%20code%20executes.

QUESTION 4

Which technique is used to evade detection from security products by executing arbitrary code in the address space of a separate live operation?

A. process injection

B. privilege escalation

C. GPO modification

D. token manipulation

Correct Answer: A

Reference: https://attack.mitre.org/techniques/T1055/

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

QUESTION 6

What is the goal of an incident response plan?

A. to identify critical systems and resources in an organization

B. to ensure systems are in place to prevent an attack

C. to determine security weaknesses and recommend solutions

D. to contain an attack and prevent it from spreading

Correct Answer: D

Reference: https://www.forcepoint.com/cyber-edu/incident-response

---

QUESTION 7

A scanner detected a malware-infected file on an endpoint that is attempting to beacon to an external site. An analyst has reviewed the IPS and SIEM logs but is unable to identify the file\\'s behavior. Which logs should be reviewed next to evaluate this file further?

A. email security appliance

B. DNS server

C. Antivirus solution

D. network device

Correct Answer: B

QUESTION 8

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"

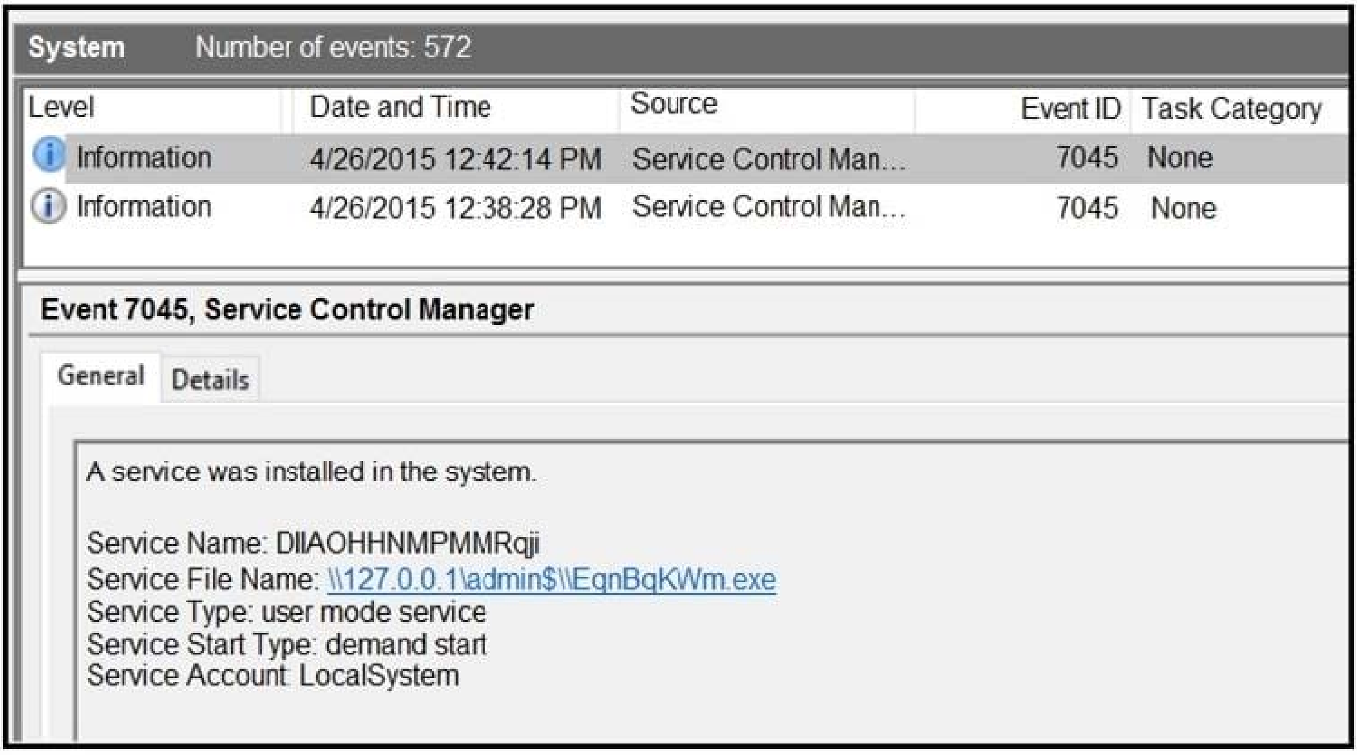
B. Get-Content –ifmatch \\Server\FTPFolder\Logfiles\ftpfiles.log | Copy-Marked “ERROR”, “SUCCESS”

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 9



System Number of events: 572

Level	Date and Time	Source	Event ID	Task Category
Information	4/26/2015 12:42:14 PM	Service Control Man...	7045	None
Information	4/26/2015 12:38:28 PM	Service Control Man...	7045	None

Event 7045, Service Control Manager

A service was installed in the system.

Service Name: DllAOHHNMPMMRqji
Service File Name: \\127.0.0.1\admin$\\EqnBqKWm.exe
Service Type: user mode service
Service Start Type: demand start
Service Account: LocalSystem

Refer to the exhibit. An HR department submitted a ticket to the IT helpdesk indicating slow performance on an internal share server. The helpdesk engineer checked the server with a real-time monitoring tool and did not notice anything suspicious. After checking the event logs, the engineer noticed an event that occurred 48 hour prior. Which two indicators of compromise should be determined from this information? (Choose two.)

A. unauthorized system modification

B. privilege escalation

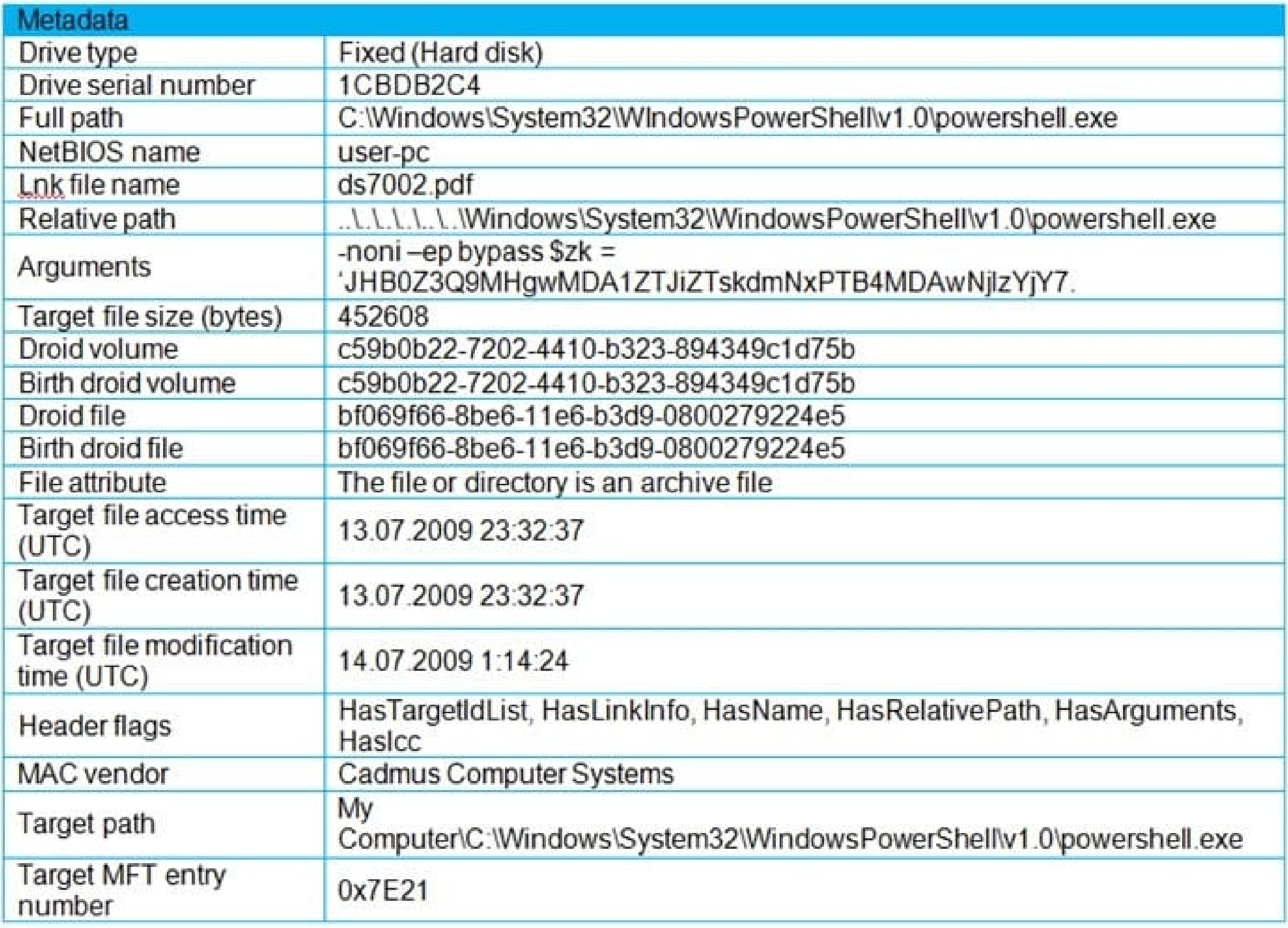
C. denial of service attack

D. compromised root access

E. malware outbreak

Correct Answer: AD

QUESTION 10



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 11

What is a use of TCPdump?

A. to analyze IP and other packets

B. to view encrypted data fields

C. to decode user credentials

D. to change IP ports

Correct Answer: A

QUESTION 12

Which tool is used for reverse engineering malware?

A. Ghidra

B. SNORT

C. Wireshark

D. NMAP

Correct Answer: A

Reference: https://www.nsa.gov/resources/everyone/ghidra/#:~:text=Ghidra%20is%20a%20software%20reverse,in%20their%20networks%20and%20systems.