Vendor: Cisco

Exam Code: 300-215

Exam Name: Conducting Forensic Analysis and Incident Response Using Cisco CyberOps Technologies

Version: DEMO

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”

Answer: D
Explanation:
The PowerShell cmdlet Get-Content reads content line-by-line from a file and is commonly used for processing logs or large text files. When combined with Select-String, it can search for specific patterns (such as "ERROR" or "SUCCESS") within those lines and return a collection of matching objects, including metadata like line number and line content.
Get-Content -Path: Correct syntax to read the log file from a UNC path. Select-String "ERROR", "SUCCESS": Searches for these terms in each line and returns matching lines as structured output.

QUESTION 2
Refer to the exhibit. An engineer is analyzing a TCP stream in a Wireshark after a suspicious email with a URL. What should be determined about the SMB traffic from this stream?

Time	TCP Data	Source	Destination	Protocol	Info
12 0.000000000	0.000230000	192.	192.	TCP	Microsoft-cis-sql-storman, ACK] Seq=0 Sck=1 Wind=8192 Len=0 WSS=3460 SACK_PER=1
15 0.000658000	0.000465000	192.	192.	SMB	Negotiate Protocol Response
21 0.004157000	0.000499000	192.	192.	SMB	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
23 0.001257000	0.000991000	192.	192.	TCP	Session Setup AndX Response, Error: STATUS_LOGON_FAILURE
25 0.000650000	0.000135000	192.	192.	TCP	microsoft-ds-sgf-storman [ACK] Seq=757 Ack=759 win=63620 Len=0
26 0.000049000	0.000049000	192.	192.	TCP	microsoft-ds-sgl-storman [RST, ACK] Seq=757 Ack=759 Win=0 Len=0
38 14.59967300	0.000232000	192.	192.	TCP	microsoft-ds+llsurfup-https [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 WSS=1460 SACK_PERM=1
41 0.000535000	0.000365000	192.	192.	SMB	Negotiate Protocol Response
58 0.005986000	0.000498000	192.	192.	TCP	microsoft-ds-llsurfup-https [ACK] Seq=198 Ack=3006 win=64240 Len=0
59 0.000854000	0.000854000	192.	192.	SMB	Session Setup AndX Response
61 0.000639000	0.000302000	192.	192.	SMB	Tree Connect AndX Response
63 0.002314000	0.000354000	192.	192.	SMB	MT Create AndX Response, FID: 0x4000
65 0.000440000	0.000249000	192.	192.	SMB	Write AndX Response, FID: 0x4000, 72 bytes
67 0.000336000	0.000232000	192.	192.		
69 0.000528000	0.000429000	192.	192.		
71 0.000417000	0.000317000	192.	192.		
73 0.000324000	0.000215000	192.	192.		
76 0.232074000	0.000322000	192.	192.	SMB	NT Create AndX Response, FID: 0x4001
78 0.000420000	0.000242000	192.	192.	SMB	Write AndX Response, FID: 0x4001, 72 bytes
80 0.000332000	0.000228000	192.	192.		
82 0.000472000	0.000372000	192.	192.		
84 0.000433000	0.000320000	192.	192.		
86 0.000416000	0.000310000	192.	192.		
88 0.000046500	0.000366000	192.	192.		
90 0.067630000	0.967518000	192.	192.		
92 0.000515000	0.000391000	192.	192.		
94 0.000477000	0.000368000	192.	192.		
96 0.090664000	0.090363000	192.	192.		
98 0.006860000	0.000280000	192.	192.		
100 0.000312000	0.000229000	192.	192.		
102 0.000329000	0.000217000	192.	192.		
104 0.000212900	0.000200000	192.	192.	SMB	Close Response, FID: 0x4001

A. It is redirecting to a malicious phishing website
B. It is exploiting redirect vulnerability
C. It is requesting authentication on the user site.
D. It is sharing access to files and printers.

Answer: D
Explanation:
The Wireshark output shows SMB protocol transactions, including NT Create AndX Response and Write AndX Response, indicating the transfer of files or objects. SMB (Server Message Block) is a protocol used for file sharing and printer access in Windows networks. The log does not indicate phishing or redirection behavior but rather normal SMB communication such as accessing files or shared resources.

QUESTION 3
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

Answer: D
Explanation:
The goal of an incident response plan (IRP) is to provide structured procedures for responding to cybersecurity incidents in a way that limits damage, contains the threat, and ensures business continuity.

QUESTION 4
A security team received an alert of suspicious activity on a user's Internet browser. The user's anti- virus software indicated that the file attempted to create a fake recycle bin folder and connect to an external IP address. Which two actions should be taken by the security analyst with the executable file for further analysis? (Choose two.)

A. Evaluate the process activity in Cisco Umbrella.
B. Analyze the TCP/IP Streams in Cisco Secure Malware Analytics (Threat Grid).
C. Evaluate the behavioral indicators in Cisco Secure Malware Analytics (Threat Grid).
D. Analyze the Magic File type in Cisco Umbrella.
E. Network Exit Localization in Cisco Secure Malware Analytics (Threat Grid).

Answer: BC
Explanation:
Cisco Secure Malware Analytics (formerly Threat Grid) enables deep file behavior analysis, including TCP/IP stream analysis and behavioral indicators such as file system activity, process injection, registry changes, and command and control communication. These are essential in understanding what the suspicious file does post-execution, especially given the described behavior of creating a fake folder and outbound connection attempts.

QUESTION 5
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

Answer: A
Explanation:
The root cause analysis in incident response focuses on identifying the initial trigger or root cause of the incident to understand how it started and how to prevent recurrence. In this scenario, the phishing email sent to the victim (A) is the initial trigger that led to the employee's action of clicking the malvertising link, resulting in the malware download. The other options represent later stages in the incident response cycle, such as detection (SIEM alert, cybersecurity team's alert) or supporting evidence (email header information), but they do not address the root cause, which is the phishing email itself.

QUESTION 6
Refer to the exhibit. Which two actions should be taken based on the intelligence information? (Choose two.)

```
<stix:Indicator id= "CISA:Indicator-18559cbf-57ce-49ba-bb73-2bdf5426744c" timestamp= "2020-04-
08T00:44:39.970278+00:00" xsi:type= "indicator:IndicatorType">
<indicator:Title>Malicious FQDN Indicator</indicator:Title>
<indicator:Observable id= "CISA:Observable-dd7a25ea-830f-46cd-9d2a-d7b5aa354f89">
<cybox:Object id= "CISA:Object-a2169ad2-5273-41cb-9491-48c69b22da74">
<cybox:Properties xsi:type= "DomainNameObj:DomainNameObjectType" type= "FQDN">
<DomainNameObj:Value condition= "Equals" >Fightcovid19.shop</DomainNameObj:Value>
</cybox:Properties>
</cybox:Object>
</indicator:Observable>
</stix:Indicator>
<stix:Indicator id= "CISA:Indicator-2035a032-6b8d-4dd9-8752-7316af76e702" timestamp= "2020-04-
08T00:44:39.970417+00:00" xsi:type= "indicator:IndicatorType">
<indicator:Title>Malicious FQDN Indicator</indicator:Title>
<indicator:Observable id= "CISA:Observable-463472d3-e45e-46c1-bf05-da7458cb943c">
<cybox:Object id= "CISA:Object-7728bd69-e724-4917-9550-9ae853becf28">
<cybox:Properties xsi:type= "DomainNameObj:DomainNameObjectType" type= "FQDN">
<DomainNameObj:Value condition= "Equals">nocovid19.shop</DomainNameObj:Value>
</cybox:Properties>
</cybox:Object>
</indicator:Observable>
</stix:Indicator>
<stix:Indicator id= "CISA:Indicator-8b56999b-a015-4399-ab80-cca9bcaf7ebf" timestamp= "2020-04-
08T00:44:39.970554+00:00" xsi:type= "indicator:IndicatorType">
<indicator:Title>Malicious FQDN Indicator</indicator:Title>
<indicator:Observable id= "CISA:Observable-0648e1db-aa4e-4aca-914e-ea0ccd445254">
<cybox:Object id= "CISA:Object-db21b6ca-0c1b-474d-8bf7-950ead2d9760">
<cybox:Properties xsi:type= "DomainNameObj:DomainNameObjectType" type= "FQDN">
<DomainNameObj:Value condition= "Equals">stopcovid19.shop</DomainNameObj:Value>
</cybox:Properties>
</cybox:Object>
</indicator:Observable>
</stix:Indicator>
```

A. Block network access to all .shop domains
B. Add a SIEM rule to alert on connections to identified domains.
C. Use the DNS server to block hole all .shop requests.
D. Block network access to identified domains.
E. Route traffic from identified domains to block hole.

Answer: BD
Explanation:
The STIX intelligence feed in the exhibit identifies specific malicious domains, such as:
fightcovid19.shop
nocovid19.shop
stopcovid19.shop
These are categorized as "Malicious FQDN Indicator."
The recommended cybersecurity actions when such threat intelligence is received are:

Block network access to identified domains: This directly prevents users or systems from communicating with known malicious infrastructure and is a critical first step in threat mitigation.

Add a SIEM rule to alert on connections to identified domains: This ensures that any attempted communication with these domains is flagged for immediate review and action,

enabling real-time threat detection and incident response.

QUESTION 7
Refer to the exhibit. Which two determinations should be made about the attack from the Apache access logs? (Choose two.)

```
84.55.41.57 - -[17/Apr/2016:06:57:24 +0100] "GET/wordpress/wp-login.php HTTP/1.1" 200 1568 "-"
84.55.41.57 - -[17/Apr/2016:06:57:31 +0100] "POST/wordpress/wp-login.php HTTP/1.1" 302 1150
"http://www.example.com/wordpress/wp-login.php"

84.55.41.57 - -[17/Apr/2016:06:57:31 +0100] "GET/wordpress/wp-admin/ HTTP/1.1" 200 12905
"http://www.example.com/wordpress/wp-login.php"
84.55.41.57 - -[17/Apr/2016:07:00:32 +0100] "POST/wordpress/wp-admin/admin-ajax.php HTTP/1.1"
200 454 "http://www.example.com/wordpress/wp-admin/"

84.55.41.57 - -[17/Apr/2016:07:11:48 +0100 "GET/wordpress/wp-admin/plugin-install.php HTTP/1.1"
200 12459 "http://www.example.com/wordpress/wp-admin/plugin-install.php?tab=upload"
 84.55.41.57 - -[17/Apr/2016:07:16:06 +0100] "GET /wordpress/wp-admin/update.php? action=install-
plugin&plugin=file-manager&_wpnonce=3c6c8a7fca HTTP/1.1" 200 5698

"http://www.example.com/wordpress/wp-admin/plugin install.php?tab=search&s=file+permission"
 84.55.41.57 - -[17/Apr/2016:07:18:19 +0100] "GET /wordpress/wp-
admin/plugins.php?action=activat&plugin=file-manager%2Ffile-manager.php&_wpnonce=bf932ee530
HTTP/1.1" 302.451 "http://www.example.com/wordpress/wp-admin/update.php?action=install-
plugin&plugin=file-manager&_wpnonce=3c6c8a7fca"

84.55.41.57 - -[17/Apr/2016:07:21:46 +0100] "GET /wordpress/wp-admin/admin-ajax.php?
action=connector&cmd=upload&target=l1_d3AtY29udGVudA&name%5B%5D=r57.php&FILES
=&_=1460873968131 HTTP/1.1" 200 731 "http://www.example.com/wordpress/wp-admin/admin.php?
page=fie-manager_settings"

84.55.41.57 - -[17/Apr/2016:07:22:53+0100] "GET /wordpress/wp-content/r57.php HTTP/1.1" 200 9036 "-"
84.55.41.57- -[17/Apr/2016:07:32:24 +0100] "POST /wordpress/wp-content/r57.php?14 HTTP/1.1" 200
8030 "http://www.example.com/wordpress/wp-content/r57.php?14"
84.55.41.57 - -[17/Apr/2016:07:29:21 +0100] "GET /wordpress/wp-content/r57.php?29 HTTP/1.1" 200
8391 "http://www.example.com/wordpress/wp-content/r57.php?28"
```

A. The attacker used r57 exploit to elevate their privilege.
B. The attacker uploaded the WordPress file manager trojan.
C. The attacker performed a brute force attack against WordPress and used SQL injection against the backend database.
D. The attacker used the WordPress file manager plugin to upload r57.php.
E. The attacker logged on normally to WordPress admin page.

Answer: BD
Explanation:
The Apache access logs in the exhibit show a sequence of HTTP requests and responses indicative of a malicious upload via WordPress:

A POST to:
/wp-admin/admin-ajax.php with parameters that include uploading r57.php (a known PHP web shell).
The uploaded file name appears as r57.php in:
&name=%5B%5D=r57.php&FILES...
There are plugin installation and activation attempts, specifically for:
file-manager plugin:
plugin=file-manager&...
Which is known to be vulnerable and exploited for file uploads.
GET requests to:
/wp-content/57.php and variations such as 57.php?28 -- This suggests that r57.php was successfully uploaded and is being accessed.
These logs reveal that:
The attacker used the WordPress file manager plugin to upload r57.php -- confirmed by plugin activity and file uploads.
The attacker uploaded the WordPress file manager trojan -- as evidenced by the direct access to /wp-content/57.php (r57 shell variant).

QUESTION 8
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

Answer: C
Explanation:
This scenario describes a substitution cipher, where data is made unreadable or less recognizable without altering its functionality. According to the Cisco CyberOps Associate guide, obfuscation includes techniques such as shifting, encoding, and symbol manipulation to mask the true nature of data or code:
"A very well-known cipher, the Caesar cipher... shifts the letter of the alphabet by a fixed number... This technique is a form of data obfuscation used to bypass detection mechanisms.".

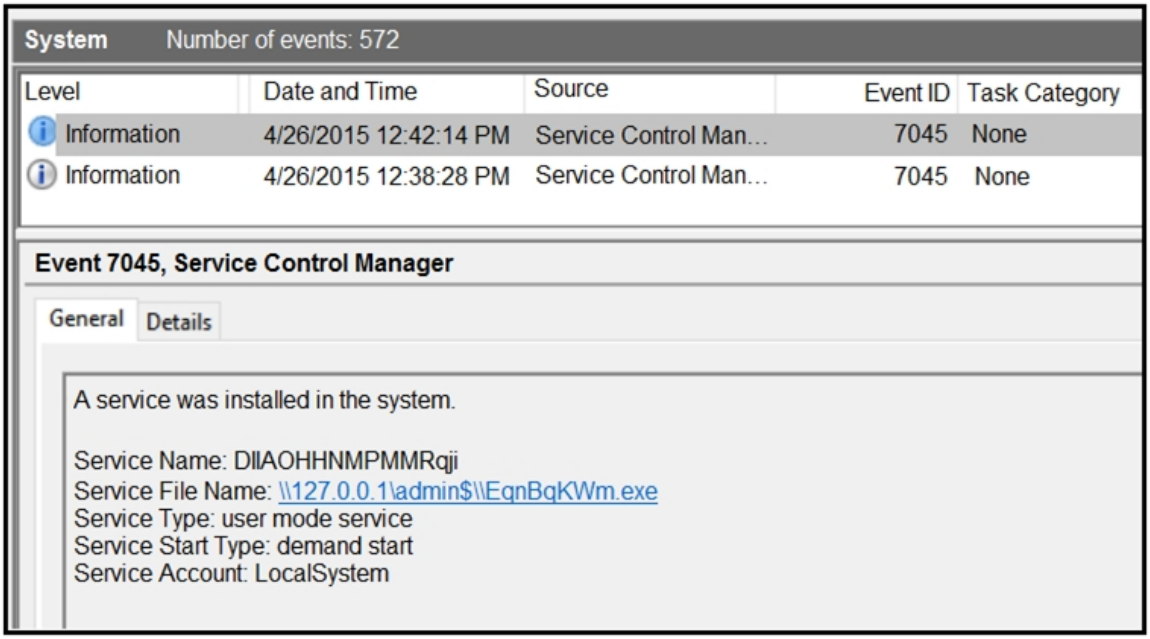
QUESTION 9
Which technique is used to evade detection from security products by executing arbitrary code in the address space of a separate live operation?

A. process injection
B. privilege escalation
C. GPO modification
D. token manipulation

Answer: A
Explanation:
Process injection is a tactic where malicious code is inserted into the memory space of another process, enabling it to run with the privileges and context of a legitimate application. The Cisco study guide explains that this method allows malware to "hide in plain sight" within trusted processes and evade endpoint detection and response (EDR) tools.
It specifically notes: "Process injection techniques allow malware to execute within the memory space of a legitimate process, avoiding detection and taking advantage of the process's

permissions.".

QUESTION 10
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

Answer: AE
Explanation:
According to the event log, a suspicious service was installed (DIAOHHNMPMMRgji) with a service file pointing to a remote share (\\127.0.0.1\admin$\EqnBqKWm.exe). This type of activity strongly suggests:

Unauthorized system modification: Installation of a service without proper authorization, especially with a random or obfuscated name, directly fits the description of system modification. The use of admin$ (administrative share) further implies this wasn't part of standard operations.

Malware outbreak: The use of a service that points to an executable with a seemingly random name and the demand start configuration indicate a potential backdoor or remote-controlled malware.

As stated in the Cisco CyberOps Associate guide, event ID 7045 with unusual service names or file paths is a strong Indicator of Compromise (IoC) for malware or persistence mechanisms. Options like privilege escalation or DoS are not directly evidenced in the event log shown. There's

no indication that the LocalSystem account was elevated beyond its default, nor that system resources were overwhelmed (as would be typical in DoS).

QUESTION 11
Which magic byte indicates that an analyzed file is a pdf file?

A. cGRmZmlsZQ
B. 706466666
C. 255044462d
D. 0a0ah4cg

Answer: C
Explanation:
The magic number (also known as a magic byte) is a sequence of bytes used to identify the format of a file. For PDF files, the standard magic number is: 25 50 44 46, which translates to %PDF in ASCII.
Option C (255044462d) begins with 25 50 44 46, confirming it's a PDF file signature.
This is a key forensic detail when performing file type identification and validation of potentially obfuscated or renamed files.

QUESTION 12
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

Answer: D
Explanation:
The best immediate step during a DDoS attack against an Apache web server is to inspect the access logs, which will show which IP addresses are making requests, their frequency, and potential patterns of abuse. As covered in the Cisco CyberOps material, "Apache logs can reveal the IPs responsible for flooding the service with requests". The command sudo tail -100 /var/log/apache2/access.log allows quick review of recent activity.

Thank You for Trying Our Product

Passleader Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.passleader.com/all-products.html

10% Discount Coupon Code: **ASTR14**