CertsDeals

Free Questions for 300-215 by certsdeals

Shared by Hines on 15-04-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

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.)

Options:

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:

B, C

Question 2

Question Type: **MultipleChoice**

What is the goal of an incident response plan?

Options:

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

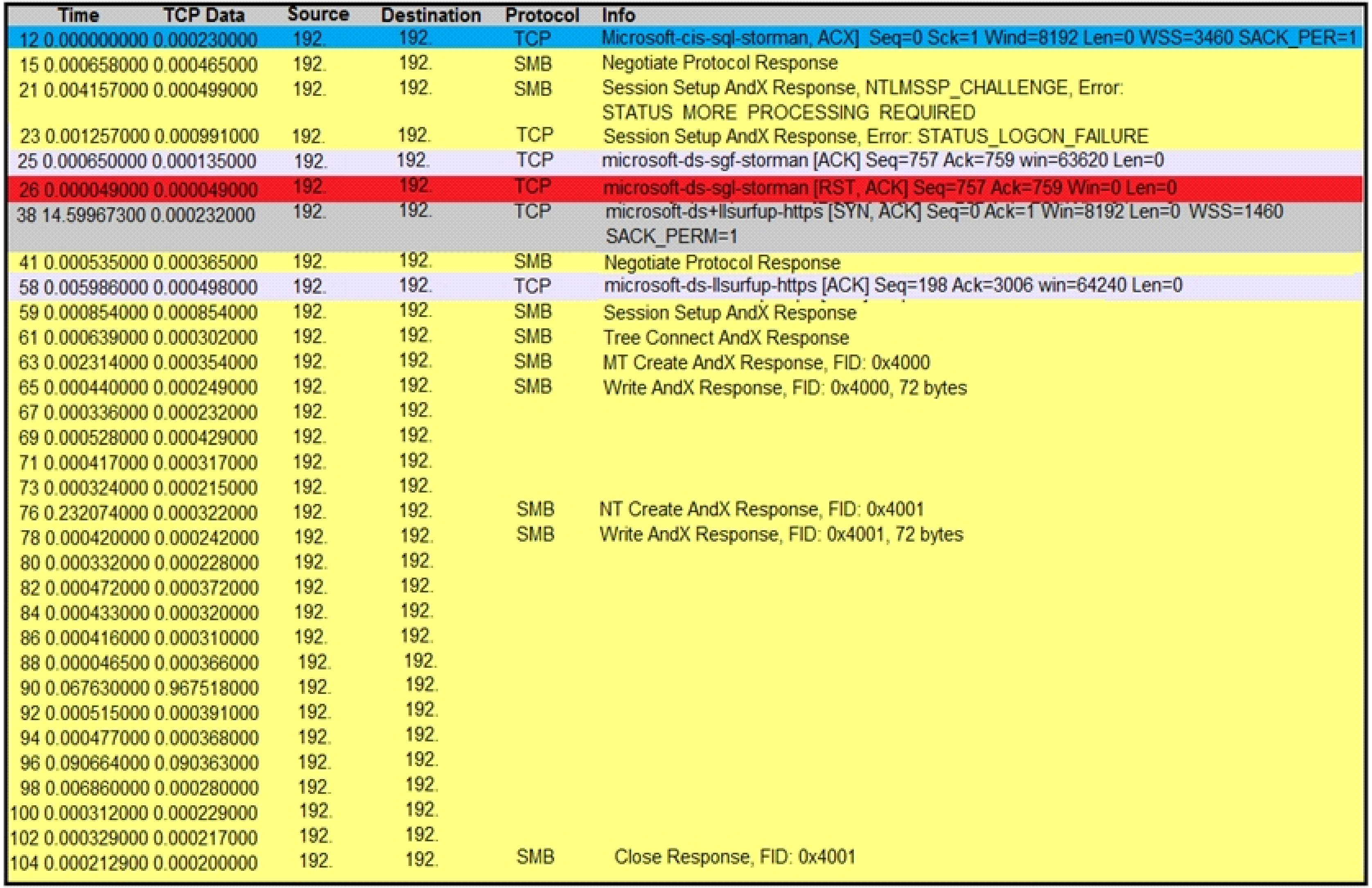
Answer:

D

Question 3

Question Type: **MultipleChoice**

Refer to the exhibit.



	Time	TCP Data	Source	Destination	Protocol	Info
12	0.000000000	0.000230000	192.	192.	TCP	Microsoft-cis-sql-storman, ACX] 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

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?

Options:

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:

B

Question 4

Question Type: MultipleChoice

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?

Options:

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

Question 5

Question Type: **MultipleChoice**

Over the last year, an organization's HR department has accessed data from its legal department on the last day of each month to create a monthly activity report. An engineer is analyzing suspicious activity alerted by a threat intelligence platform that an authorized user in the HR department has accessed legal data daily for the last week. The engineer pulled the network data from the legal department's shared folders and discovered above average-size data dumps. Which threat actor is implied from these artifacts?

Options:

A- privilege escalation

B- internal user errors

C- malicious insider

D- external exfiltration

Answer:

C

Question 6

Question Type: **MultipleChoice**

An "unknown error code" is appearing on an ESXi host during authentication. An engineer checks the authentication logs but is unable to identify the issue. Analysis of the vCenter agent logs shows no connectivity errors. What is the next log file the engineer should check to continue troubleshooting this error?

Options:

A- /var/log/syslog.log

B- /var/log/vmksummary.log

C- var/log/shell.log

D- var/log/general/log

Answer:

A

Question 7

Question Type: **MultipleChoice**

What is the function of a disassembler?

Options:

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

Answer:

A

Explanation:

+analysis&hl=en&as_sdt=0&as_vis=1&oi=scholart