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

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

QUESTION 1

An incident response team is recommending changes after analyzing a recent compromise in which:

a large number of events and logs were involved;

team members were not able to identify the anomalous behavior and escalate it in a timely manner;

several network systems were affected as a result of the latency in detection;

security engineers were able to mitigate the threat and bring systems back to a stable state; and

the issue reoccurred shortly after and systems became unstable again because the correct information was not gathered during the initial identification phase.

Which two recommendations should be made for improving the incident response process? (Choose two.)

A. Formalize reporting requirements and responsibilities to update management and internal stakeholders throughout the incident-handling process effectively.

B. Improve the mitigation phase to ensure causes can be quickly identified, and systems returned to a functioning state.

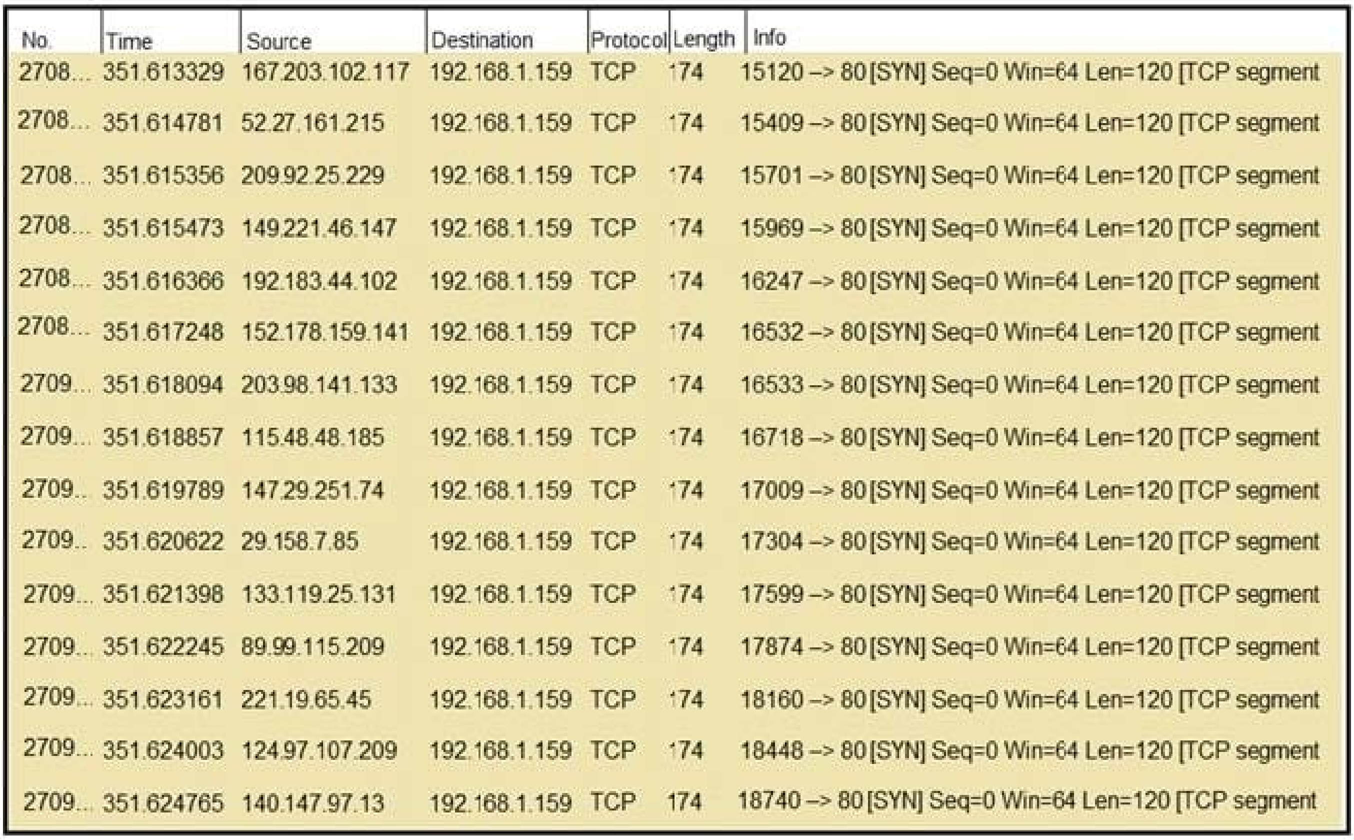
C. Implement an automated operation to pull systems events/logs and bring them into an organizational context.

D. Allocate additional resources for the containment phase to stabilize systems in a timely manner and reduce an attack\\'s breadth.

E. Modify the incident handling playbook and checklist to ensure alignment and agreement on roles, responsibilities, and steps before an incident occurs.

Correct Answer: CE

QUESTION 2



No.	Time	Source	Destination	Protocol	Length	Info
2708...	351.613329	167.203.102.117	192.168.1.159	TCP	174	15120 –> 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment
2708...	351.614781	52.27.161.215	192.168.1.159	TCP	174	15409 –> 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment
2708...	351.615356	209.92.25.229	192.168.1.159	TCP	174	15701 –> 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment
2708...	351.615473	149.221.46.147	192.168.1.159	TCP	174	15969 –> 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment
2708...	351.616366	192.183.44.102	192.168.1.159	TCP	174	16247 –> 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment
2708...	351.617248	152.178.159.141	192.168.1.159	TCP	174	16532 –> 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment
2709...	351.618094	203.98.141.133	192.168.1.159	TCP	174	16533 –> 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment
2709...	351.618857	115.48.48.185	192.168.1.159	TCP	174	16718 –> 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment
2709...	351.619789	147.29.251.74	192.168.1.159	TCP	174	17009 –> 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment
2709...	351.620622	29.158.7.85	192.168.1.159	TCP	174	17304 –> 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment
2709...	351.621398	133.119.25.131	192.168.1.159	TCP	174	17599 –> 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment
2709...	351.622245	89.99.115.209	192.168.1.159	TCP	174	17874 –> 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment
2709...	351.623161	221.19.65.45	192.168.1.159	TCP	174	18160 –> 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment
2709...	351.624003	124.97.107.209	192.168.1.159	TCP	174	18448 –> 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment
2709...	351.624765	140.147.97.13	192.168.1.159	TCP	174	18740 –> 80 [SYN] Seq=0 Win=64 Len=120 [TCP segment

Refer to the exhibit. What should an engineer determine from this Wireshark capture of suspicious network traffic?

A. There are signs of SYN flood attack, and the engineer should increase the backlog and recycle the oldest half-open TCP connections.

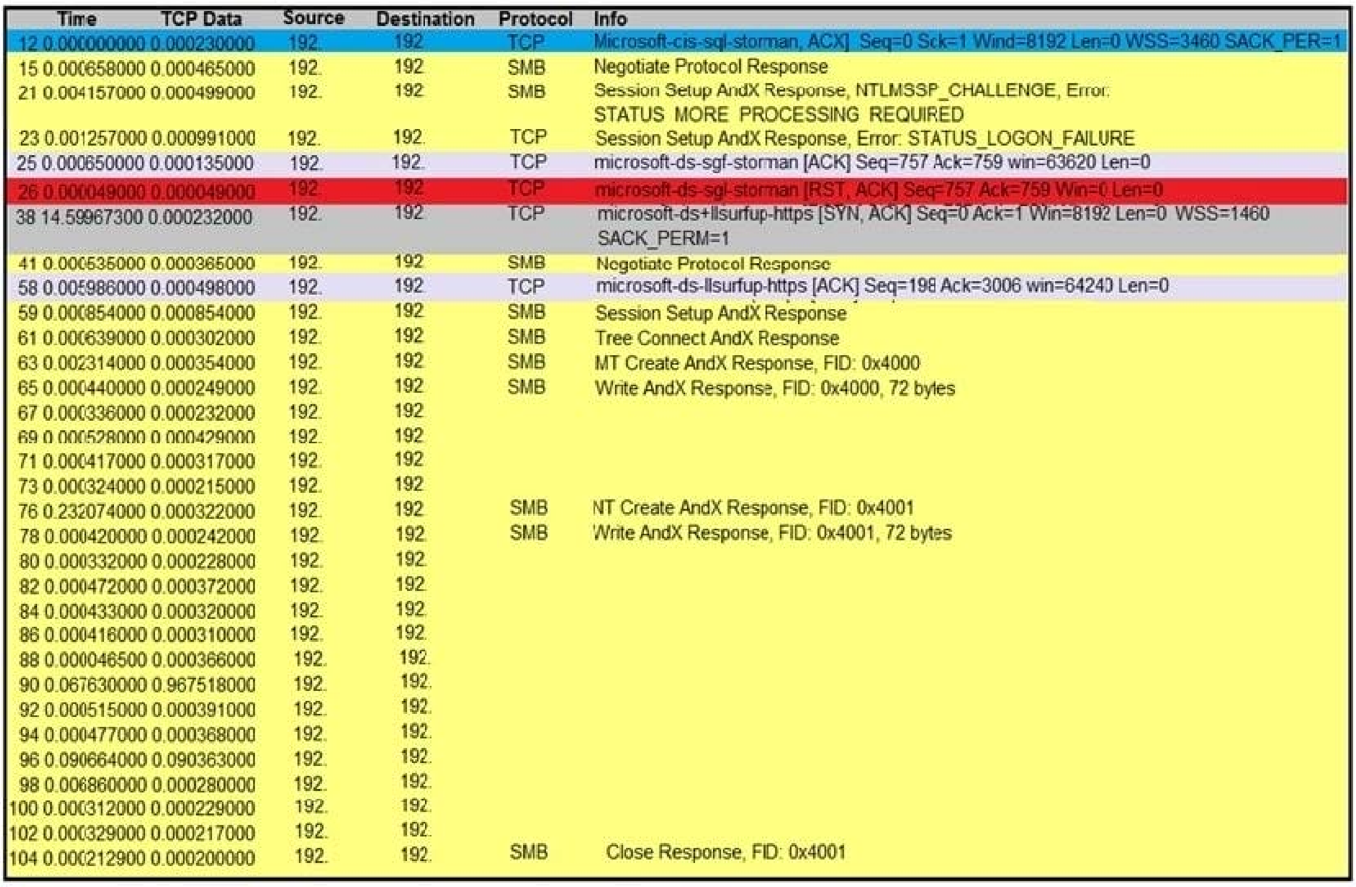
B. There are signs of a malformed packet attack, and the engineer should limit the packet size and set a threshold of bytes as a countermeasure.

C. There are signs of a DNS attack, and the engineer should hide the BIND version and restrict zone transfers as a countermeasure.

D. There are signs of ARP spoofing, and the engineer should use Static ARP entries and IP address-to-MAC address mappings as a countermeasure.

Correct Answer: A

QUESTION 3



	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-sql-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 byles
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

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?

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.

Correct Answer: B

QUESTION 4

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

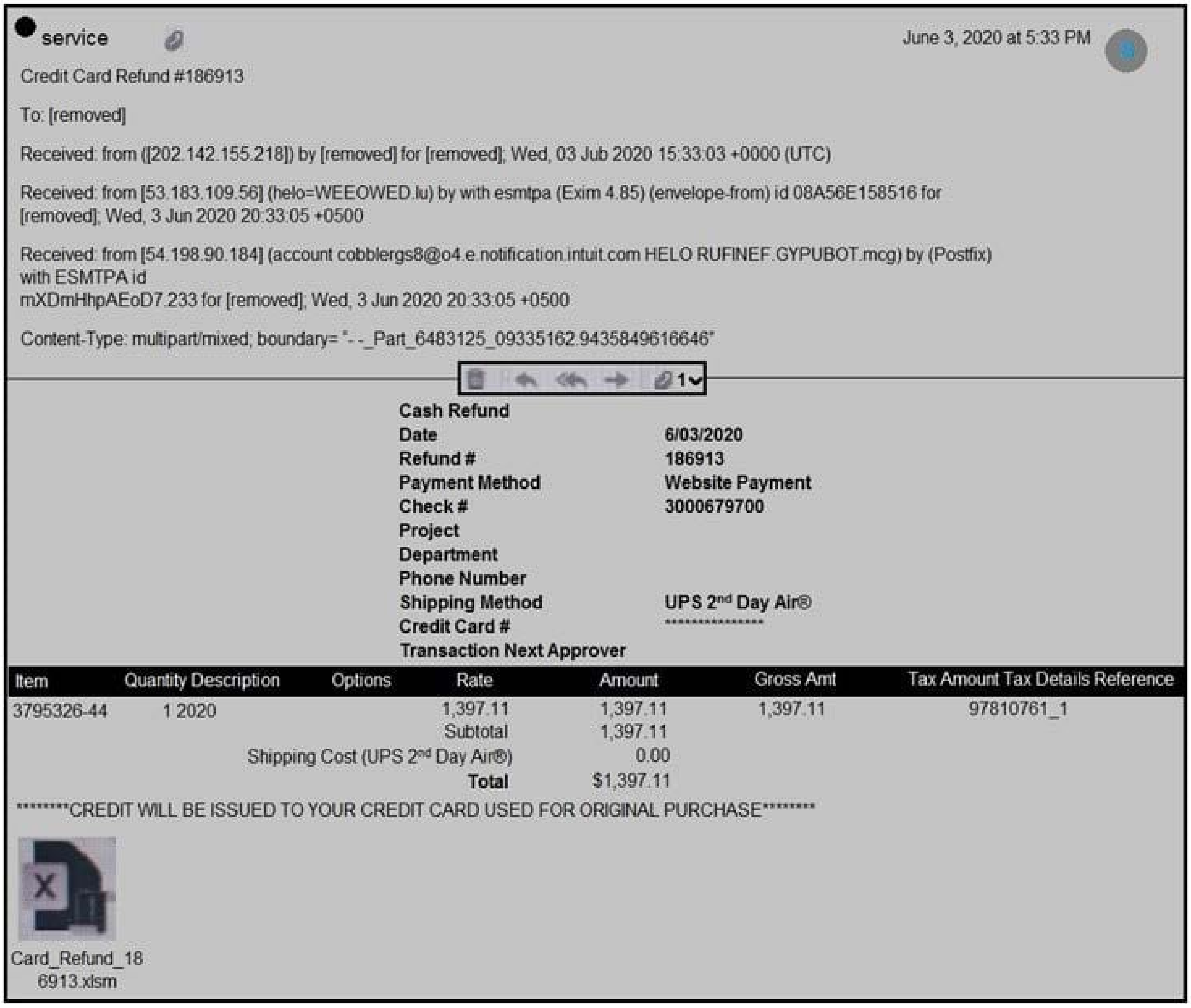
C. HKEY_CURRENT_USER\Software\Classes\Winlog

D. HKEY_LOCAL_MACHINES\SOFTWARE\Microsoft\WindowsNT\CurrentUser

Correct Answer: A

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

QUESTION 5



● service

June 3, 2020 at 5:33 PM

Credit Card Refund #186913

To: [removed]

Received: from ([202.142.155.218]) by [removed] for [removed]; Wed, 03 Jub 2020 15:33:03 +0000 (UTC)

Received: from [53.183.109.56] (helo=WEEOWED.lu) by with esmtpa (Exim 4.85) (envelope-from) id 08A56E158516 for [removed]; Wed, 3 Jun 2020 20:33:05 +0500

Received: from [54.198.90.184] (account cobblergs8@o4.e.notification.intuit.com HELO RUFINEF.GYPUBOT.mcg) by (Postfix) with ESMTPA id mXDmHhpAEoD7.233 for [removed]; Wed, 3 Jun 2020 20:33:05 +0500

Content-Type: multipart/mixed; boundary= "- -_Part_6483125_09335162.9435849616646"

Cash Refund

Date	**6/03/2020**
Refund #	**186913**
Payment Method	**Website Payment**
Check #	**3000679700**
Project	
Department	
Phone Number	
Shipping Method	**UPS 2nd Day Air®**
Credit Card #	***************
Transaction Next Approver	

Item	Quantity Description	Options	Rate	Amount	Gross Amt	Tax Amount Tax Details Reference
3795326-44	1 2020		1,397.11	1,397.11	1,397.11	97810761_1
			Subtotal	1,397.11		
			Shipping Cost (UPS 2nd Day Air®)	0.00		
			Total	$1,397.11		

********CREDIT WILL BE ISSUED TO YOUR CREDIT CARD USED FOR ORIGINAL PURCHASE********

Card_Refund_186913.xlsm

Refer to the exhibit. Which element in this email is an indicator of attack?

A. IP Address: 202.142.155.218

B. content-Type: multipart/mixed

C. attachment: "Card-Refund"

D. subject: "Service Credit Card"

Correct Answer: C

QUESTION 6

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 7

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 8

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 9

An engineer is analyzing a ticket for an unexpected server shutdown and discovers that the web-server ran out of useable memory and crashed.

Which data is needed for further investigation?

A. /var/log/access.log

B. /var/log/messages.log

C. /var/log/httpd/messages.log

D. /var/log/httpd/access.log

Correct Answer: B

QUESTION 10

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

Correct Answer: B