300-215Q&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.pass2lead.com/300-215.html

100% Passing Guarantee
100% Money Back Assurance

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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

Which information is provided bout the object file by the "-h" option in the objdump line command objdump ? oasys ? vax ? fu.o?

A. bfdname

B. debugging

C. help

D. headers

Correct Answer: D

Reference: https://sourceware.org/binutils/docs/binutils/objdump.html

QUESTION 2

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

QUESTION 3

An attacker embedded a macro within a word processing file opened by a user in an organization\\'s legal department. The attacker used this technique to gain access to confidential financial data. Which two recommendations should a security expert make to mitigate this type of attack? (Choose two.)

A. controlled folder access

B. removable device restrictions

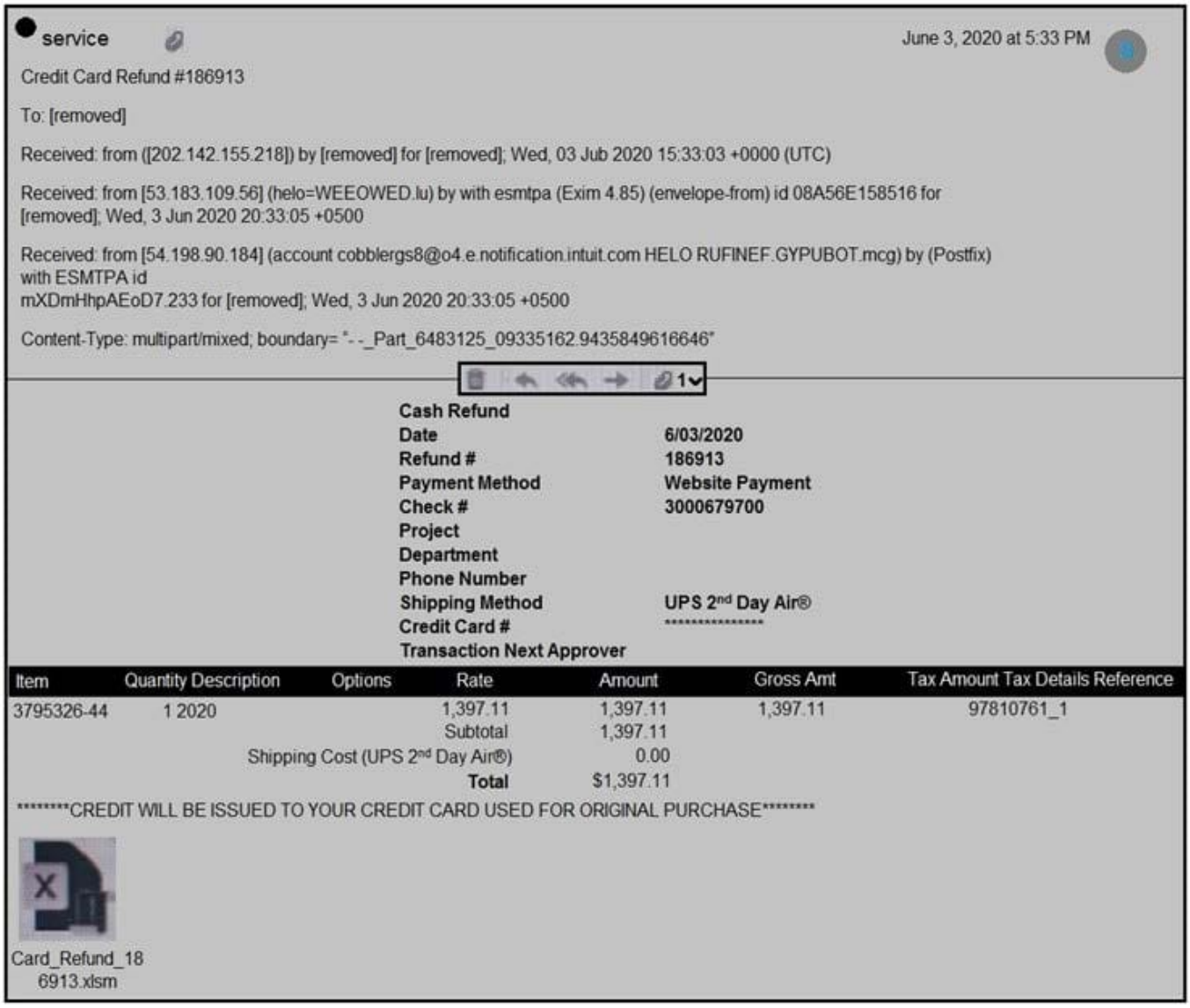
C. signed macro requirements

D. firewall rules creation

E. network access control

Correct Answer: AC

QUESTION 4


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"

1

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 5

```
<indicator:Observable id= "example:Observable-9c9869a2-f822-4682-bda4-e89d31b18704">
        <cybox:Object id= "example:EmailMessage-9d56af8e-5588-4ed3-affd-bd769ddd7fe2">
          <cybox:Properties xsi:type= "EmailMessageObj:EmailMessageObjectType">
            <EmailMessageObj:Attachments>
                <EmailMessageObj:File object_reference= "example:File-c182bcb6-8023-44a8-b340-157295abc8a6"/>
            </EmailMessageObj:Attachments>
      </cybox:Properties>
      <cybox:Related_Objects>
        <cybox:Related_Object id= "example:File-c182bcb6-8023-44a8-b340-157295abc8a6"
          <cybox:Properties xsi:type= "FileObj:FileObjectType">
                <FileObj:File_Name condition= "StartsWith">Final Report</FileObj:File_Name>
                <FileObj:File_Extension condition= "Equals">doc.exe</FileObj:File_Extension>
          </cybox:Properties>
        <cybox:Relationship xsi:type= "cyboxVocabs:ObjectRelationshipVocab-1.1">Contains</cybox:Relationship>
      </cybox:Related_Object>
    </cybox:Related_Objects>
  </cybox:Object>
</indicator:Observable>
```

Refer to the exhibit. Which determination should be made by a security analyst?

A. An email was sent with an attachment named "Grades.doc.exe".

B. An email was sent with an attachment named "Grades.doc".

C. An email was sent with an attachment named "Final Report.doc".

D. An email was sent with an attachment named "Final Report.doc.exe".

Correct Answer: D