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.leads4pass.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

An investigator is analyzing an attack in which malicious files were loaded on the network and were undetected. Several of the images received during the attack include repetitive patterns. Which anti-forensic technique was used?

A. spoofing

B. obfuscation

C. tunneling

D. steganography

Correct Answer: D

Reference: https://doi.org/10.5120/1398-1887 https://www.carbonblack.com/blog/steganography-in-the-modern-attack-landscape/

QUESTION 2

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-sgf-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

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 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

Correct Answer: D

Reference: https://www.forcepoint.com/cyber-edu/incident-response

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).

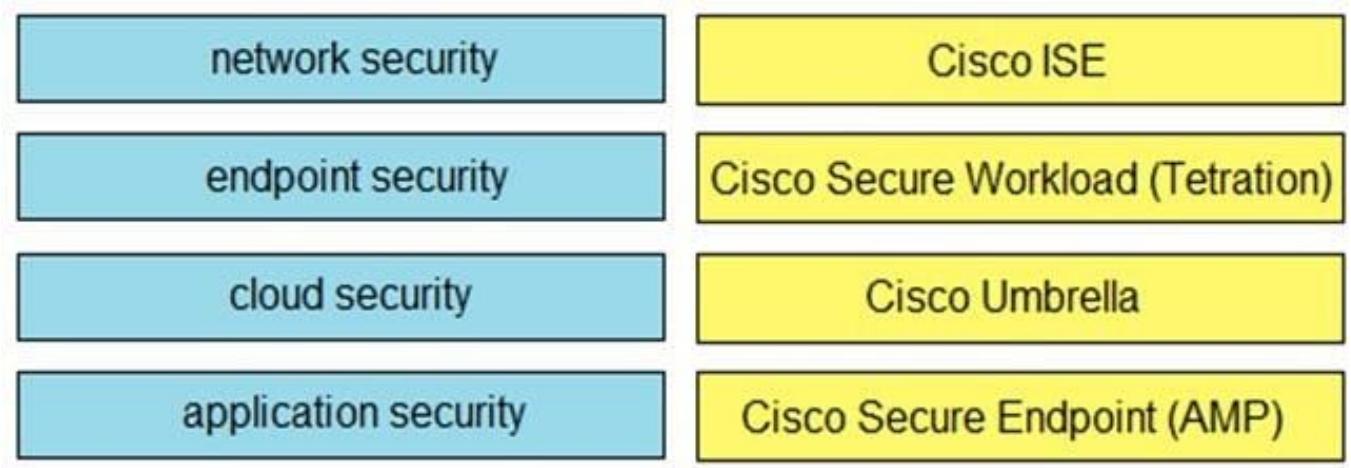
Correct Answer: BC

QUESTION 5

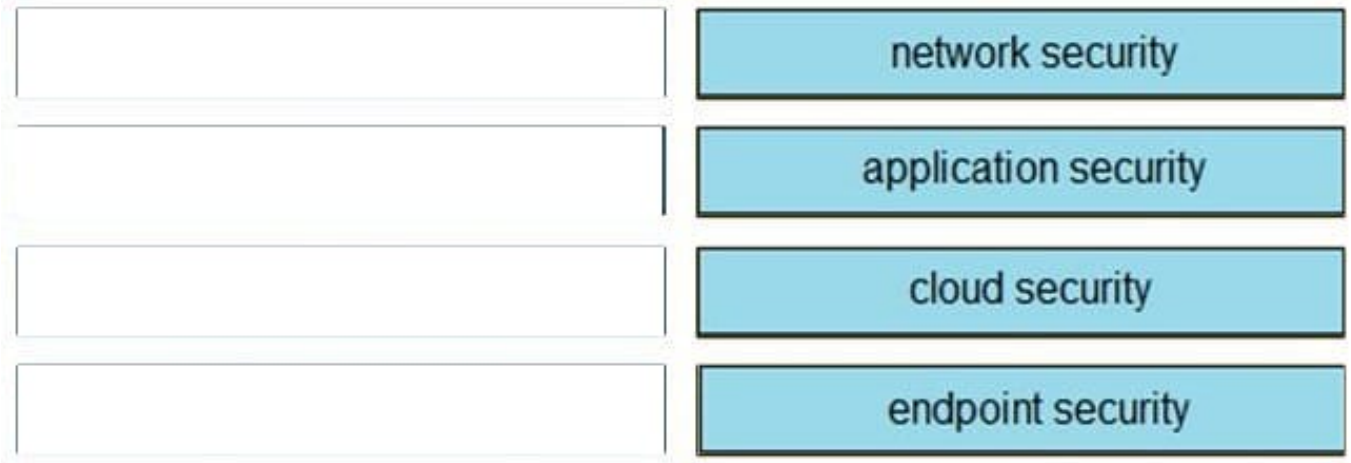
DRAG DROP

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

Select and Place:



Correct Answer:



QUESTION 6

00386078	64	44	45	33	4C	6A	41	34	4C	6A	4D	78	4C	6B	5A	44
00386088	4D	44	59	78	4E	79	34	31	4E	54	41	32	4C	6A	55	31
00386098	4D	44	59	75	4E	6A	67	7A	4E	77	3D	3D	00	AB	AB	AB

Refer to the exhibit. Which encoding technique is represented by this HEX string?

A. Unicode

B. Binary

C. Base64

D. Charcode

Correct Answer: B

Reference: https://www.suse.com/c/making-sense-hexdump/

QUESTION 7

```
<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

QUESTION 8

A security team receives reports of multiple files causing suspicious activity on users\\' workstations. The file attempted to access highly confidential information in a centralized file server. Which two actions should be taken by a security analyst to evaluate the file in a sandbox? (Choose two.)

A. Inspect registry entries

B. Inspect processes.

C. Inspect file hash.

D. Inspect file type.

E. Inspect PE header.

Correct Answer: BC

Reference: https://medium.com/@Flying_glasses/top-5-ways-to-detect-malicious-file-manually-d02744f7c43a

QUESTION 9

What is a use of TCPdump?

A. to analyze IP and other packets

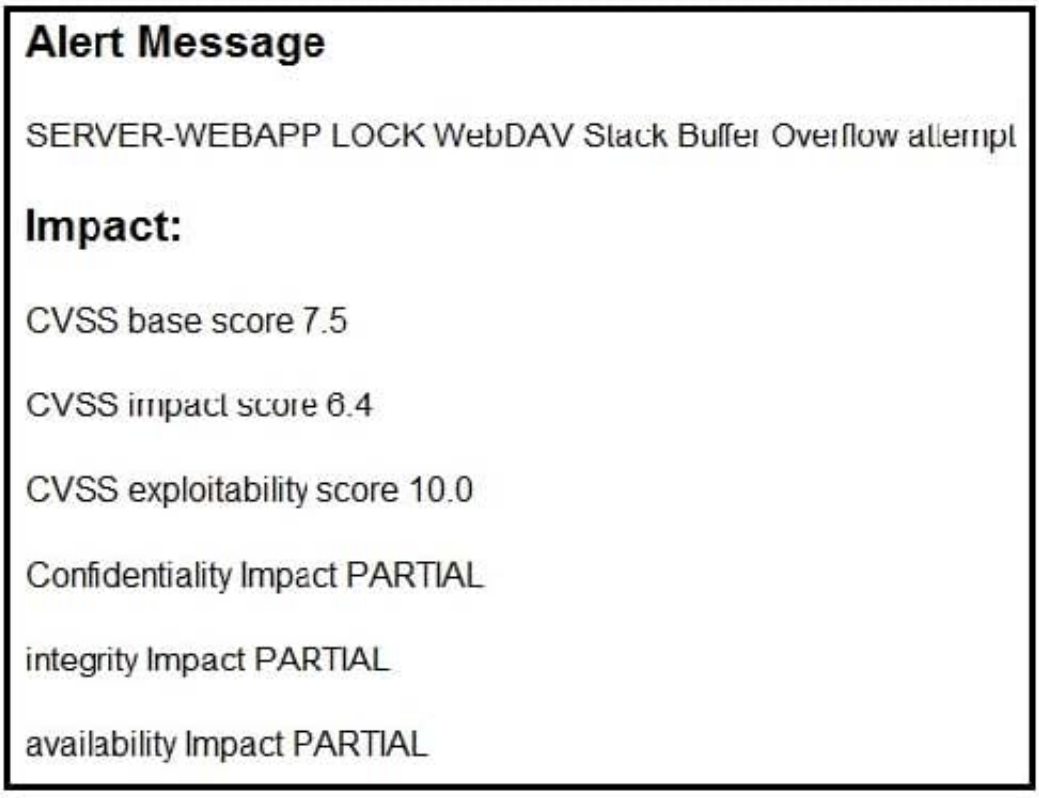
B. to view encrypted data fields

C. to decode user credentials

D. to change IP ports

Correct Answer: A

QUESTION 10



Refer to the exhibit. After a cyber attack, an engineer is analyzing an alert that was missed on the intrusion detection system. The attack exploited a vulnerability in a business critical, web-based application and violated its availability. Which two migration techniques should the engineer recommend? (Choose two.)

A. encapsulation

B. NOP sled technique

C. address space randomization

D. heap-based security

E. data execution prevention

Correct Answer: CE

QUESTION 11

Which tool conducts memory analysis?

A. MemDump

B. Sysinternals Autoruns

C. Volatility

D. Memoryze

Correct Answer: C

Reference: https://resources.infosecinstitute.com/topic/memory-forensics-and-analysis-using-volatility/

QUESTION 12

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

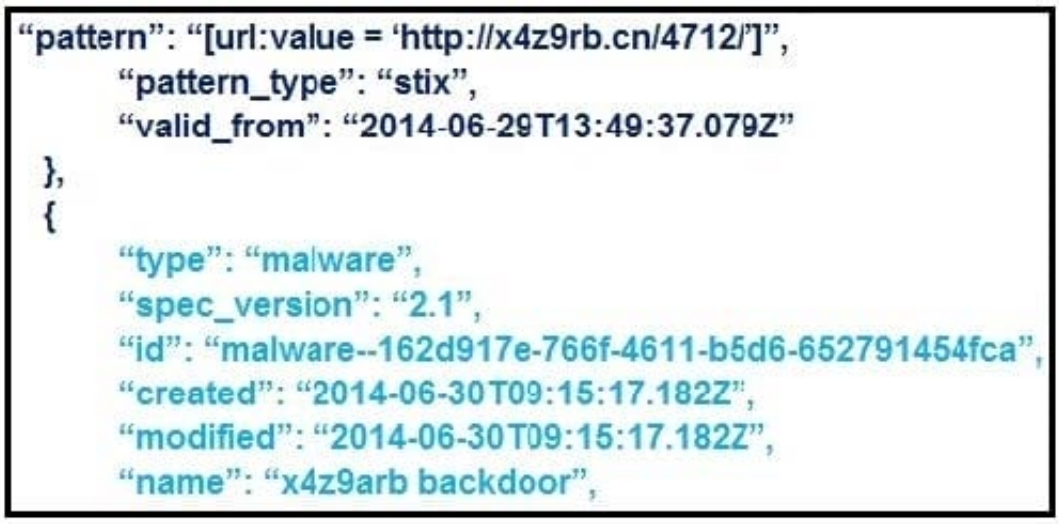
B. alarm raised by the SIEM

C. information from the email header

D. alert identified by the cybersecurity team

Correct Answer: B

QUESTION 13



Refer to the exhibit. What is the IOC threat and URL in this STIX JSON snippet?

A. malware; `http://x4z9arb.cn/4712/\\'

B. malware; x4z9arb backdoor

C. x4z9arb backdoor; http://x4z9arb.cn/4712/

D. malware; malware--162d917e-766f-4611-b5d6-652791454fca

E. stix; `http://x4z9arb.cn/4712/\\'

Correct Answer: D

QUESTION 14

A security team detected an above-average amount of inbound tcp/135 connection attempts from unidentified senders. The security team is responding based on their incident response playbook. Which two elements are part of the eradication phase for this incident? (Choose two.)

A. anti-malware software

B. data and workload isolation

C. centralized user management

D. intrusion prevention system

E. enterprise block listing solution

Correct Answer: CD

QUESTION 15

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

Latest 300-215 Dumps 300-215 Exam Questions 300-215 Braindumps