



300-215^{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

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





QUESTION 1

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 = 'JHB0Z3Q9MHgwMDA1ZTJiZTskdmNxPTB4MDAwNjJzYjY7.'
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, Haslcc
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 2



```
7369808704:error:0D0680A8:asn1 encoding routines:asn1_check_tlen:wrong ag:crypto/asn1/tasn_dec.c:1112:
7369808704:error:0D07803A:asn1 encoding routines:asn1_item_embed_d2i:nested asn1
error:crypto/asn1/tasn_dec.c:274:Type=X509
7369808704:error:0D0680A8:asn1 encoding routines:asn1_check_tlen:wrong tag:crypto/asn1/tasn_dec.c:1112:
7369808704:error:0D08303A:asn1 encoding routines:asn1_template_noexp_d2i:nested asn1
error:crypto/asn1/tasn_dec.c:536:
7369808704:error:0D0680A8:asn1 encoding routines:asn1_check_tlen:wrong tag:crypto/asn1/tasn_dec.c:1112:
7369808704:error:0D07803A:asn1 encoding routines:asn1_item_embed_d2i:nested asn1
error:crypto/asn1/tasn_dec.c:274:Type=RSA
7369808704:error:04093004:rsa routines:old_rsa_priv_decode:RSA lib:crypto/rsa/rsa_ameth.c:72:
7369808704:error:0D0680A8:asn1 encoding routines:asn1_check_tlen:wrong tag:crypto/asn1/tasn_dec.c:1112:
7369808704:error:0D07803A:asn1 encoding routines:asn1_item_embed_d2i:nested asn1
error:crypto/asn1/tasn_dec.c:274:Type=PKCS8_PRIV_KEY_INFO
7369808704:error:2306F041:PKCS12 routines:PKCS12_key_gen_uni:malloc
failure:crypto/pkcs12/p12_key.c:185:
7369808704:error:2307806B:PKCS12 routines:PKCS12_PBE_keyivgen: key gen
error:crypto/pkcs12/p12_crpt.c:55:
7369808704:error:06074078:digital envelope routines:EVP_PBE_CipherInit:keygen
failure:crypto/evp/evp_pbe.c:126:
7369808704:error:23077073:PKCS12 routines:PKCS12_pbe_crypt:pkcs12 algor cipherinit
error:crypto/pkcs12/p12_decr.c:41:
7369808704:error:2306C067:PKCS12 routines:PKCS12_item_i2d_encrypt:encrypt
error:crypto/pkcs12/p12_decr.c:144:
7369808704:error:23073067:PKCS12 routines:PKCS12_pack_p7encdata:encrypt
error:crypto/pkcs12/p12_add.c:119:
```

Refer to the exhibit. What should be determined from this Apache log?

- A. A module named mod_ssl is needed to make SSL connections.
- B. The private key does not match with the SSL certificate.
- C. The certificate file has been maliciously modified
- D. The SSL traffic setup is improper

Correct Answer: D

QUESTION 3

Which technique is used to evade detection from security products by executing arbitrary code in the address space of a separate live operation?

- A. process injection
- B. privilege escalation
- C. GPO modification
- D. token manipulation



Correct Answer: A

Reference: <https://attack.mitre.org/techniques/T1055/>

QUESTION 4

Alert Message

SERVER-WEBAPP LOCK WebDAV Stack Buffer Overflow attempt

Impact:

CVSS base score 7.5

CVSS impact score 6.4

CVSS exploitability score 10.0

Confidentiality Impact PARTIAL

integrity Impact PARTIAL

availability Impact PARTIAL

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 5



```
“pattern”: “[url:value = ‘http://x4z9arb.cn/4712/’]”,
  “pattern_type”: “stix”,
  “valid_from”: “2014-06-29T13:49:37.079Z”
},
{
  “type”: “malware”,
  “spec_version”: “2.1”,
  “id”: “malware--162d917e-766f-4611-b5d6-652791454fca”,
  “created”: “2014-06-30T09:15:17.182Z”,
  “modified”: “2014-06-30T09:15:17.182Z”,
  “name”: “x4z9arb backdoor”,
```

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 6

DRAG DROP

Drag and drop the cloud characteristic from the left onto the challenges presented for gathering evidence on the right.

Select and Place:



broad network access	application details are unavailable to investigators since being deemed private and confidential
rapid Elasticity	obtaining evidence from the cloud service provider
measured service	circumvention of virtual machine isolation techniques via code or bad actor
resource pooling	evidence correlation across one or more cloud providers

Correct Answer:

	rapid Elasticity
	measured service
	resource pooling
	broad network access

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

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 Jun 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 cobblers8@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 2 nd 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 2 nd Day Air®)		0.00				
			Total		\$1,397.11				

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

Card_Refund_186913.xsm

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 9

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 10

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 11

DRAG DROP

Drag and drop the steps from the left into the order to perform forensics analysis of infrastructure networks on the right.

Select and Place:



Correct Answer:



Reference: https://subscription.packtpub.com/book/networking_and_servers/9781789344523/1/ch01lv1sec12/network-forensics-investigation-methodology

QUESTION 12

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 13

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?

- A. /var/log/syslog.log
- B. /var/log/vmksummary.log
- C. var/log/shell.log
- D. var/log/general/log

Correct Answer: A

Reference: <https://docs.vmware.com/en/VMware-vSphere/6.7/com.vmware.vsphere.monitoring.doc/GUID-832A2618-6B11-4A28-9672-93296DA931D0.html>

[300-215 PDF Dumps](#)

[300-215 VCE Dumps](#)

[300-215 Exam Questions](#)