

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.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

```
function decrypt(rypted, key)
On Error Resume Next

UUF = rypted
sJs = "" '!!!
wWLu = ""
FETw = 1
    for i=1 to len(UUF)
if ( asc(mid(UUF, i, 1)) > 47 and asc(mid(UUF, i, 1)) < 58) then
sJs = sJs + mid(UUF, i, 1) '!!!
FETw = 1
else
if FETw = 1 then
NEL = CInt(sJs) '!!!
VlxJ = XOR_Func(NEL, key) '!!!
wWLu = wWLu + Chr(VlxJ) '!!!
end if
sJs = ""
FETw = 0
end if
vkB = bEBk or CFc
next
decrypt = wWLu
end function

function XOR_Func(qit, ANF)
On Error Resume Next
sCLx = qit xor ANF
XOR_Func = sCLx

end function
```

Refer to the exhibit. Which type of code created the snippet?

- A. VB Script
- B. Python
- C. PowerShell
- D. Bash Script

Correct Answer: A

QUESTION 2

What is a concern for gathering forensics evidence in public cloud environments?

- A. High Cost: Cloud service providers typically charge high fees for allowing cloud forensics.
- B. Configuration: Implementing security zones and proper network segmentation.
- C. Timeliness: Gathering forensics evidence from cloud service providers typically requires substantial time.
- D. Multitenancy: Evidence gathering must avoid exposure of data from other tenants.

Correct Answer: D

Reference: https://www.researchgate.net/publication/307871954_About_Cloud_Forensics_Challenges_and_Solutions

QUESTION 3

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 4

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 5

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 6

What is the function of a disassembler?

- A. aids performing static malware analysis
- B. aids viewing and changing the running state
- C. aids transforming symbolic language into machine code
- D. aids defining breakpoints in program execution

Correct Answer: A

Reference: https://scholar.google.co.in/scholar?q=disassembler+aids+performing+static+malware+analysis&hl=en&das_sdt=0&das_vis=1&doi=scholar

QUESTION 7

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 8

A security team is discussing lessons learned and suggesting process changes after a security breach incident. During the incident, members of the security team failed to report the abnormal system activity due to a high project workload. Additionally, when the incident was identified, the response took six hours due to management being unavailable to provide the approvals needed. Which two steps will prevent these issues from occurring in the future? (Choose two.)

- A. Introduce a priority rating for incident response workloads.
- B. Provide phishing awareness training for the fill security team.
- C. Conduct a risk audit of the incident response workflow.
- D. Create an executive team delegation plan.
- E. Automate security alert timeframes with escalation triggers.

Correct Answer: AE

QUESTION 9

```
84.55.41.57 - [17/Apr/2016:06:57:24 +0100] "GET/wordpress/wp-login.php HTTP/1.1" 200 1568 "-"
84.55.41.57 - [17/Apr/2016:06:57:31 +0100] "POST/wordpress/wp-login.php HTTP/1.1" 302 1150
"http://www.example.com/wordpress/wp-login.php"

84.55.41.57 - [17/Apr/2016:06:57:31 +0100] "GET/wordpress/wp-admin/ HTTP/1.1" 200 12905
"http://www.example.com/wordpress/wp-login.php"
84.55.41.57 - [17/Apr/2016:07:00:32 +0100] "POST/wordpress/wp-admin/admin-ajax.php HTTP/1.1"
200 454 "http://www.example.com/wordpress/wp-admin/"

84.55.41.57 - [17/Apr/2016:07:11:48 +0100] "GET/wordpress/wp-admin/plugin-install.php HTTP/1.1"
200 12459 "http://www.example.com/wordpress/wp-admin/plugin-install.php?tab=upload"
84.55.41.57 - [17/Apr/2016:07:16:06 +0100] "GET /wordpress/wp-admin/update.php? action=install-
plugin&plugin=file-manager&_wpnonce=3c6c8a7fca HTTP/1.1" 200 5698

"http://www.example.com/wordpress/wp-admin/plugin install.php?tab=search&s=file+permission"
84.55.41.57 - [17/Apr/2016:07:18:19 +0100] "GET /wordpress/wp-
admin/plugins.php?action=activat&plugin=file-manager%2Ffile-manager.php&_wpnonce=bf932ee530
HTTP/1.1" 302.451 "http://www.example.com/wordpress/wp-admin/update.php?action=install-
plugin&plugin=file-manager&_wpnonce=3c6c8a7fca"

84.55.41.57 - [17/Apr/2016:07:21:46 +0100] "GET /wordpress/wp-admin/admin-ajax.php?
action=connector&cmd=upload&target=l1_d3AtY29udGVudA&name%5B%5D=r57.php&FILES
=&_1460873968131 HTTP/1.1" 200 731 "http://www.example.com/wordpress/wp-admin/admin.php?
page=file-manager_settings"

84.55.41.57 - [17/Apr/2016:07:22:53+0100] "GET /wordpress/wp-content/r57.php HTTP/1.1" 200 9036 "-"
84.55.41.57 - [17/Apr/2016:07:32:24 +0100] "POST /wordpress/wp-content/r57.php?14 HTTP/1.1" 200
8030 "http://www.example.com/wordpress/wp-content/r57.php?14"
84.55.41.57 - [17/Apr/2016:07:29:21 +0100] "GET /wordpress/wp-content/r57.php?29 HTTP/1.1" 200
8391 "http://www.example.com/wordpress/wp-content/r57.php?28"
```

Refer to the exhibit. Which two determinations should be made about the attack from the Apache access logs? (Choose two.)

- A. The attacker used r57 exploit to elevate their privilege.
- B. The attacker uploaded the word press file manager trojan.
- C. The attacker performed a brute force attack against word press and used sql injection against the backend database.
- D. The attacker used the word press file manager plugin to upoad r57.php.
- E. The attacker logged on normally to word press admin page.

Correct Answer: CD

QUESTION 10

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

[300-215 VCE Dumps](#)

[300-215 Practice Test](#)

[300-215 Exam Questions](#)