



# 300-215<sup>Q&As</sup>

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.geekcert.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

```
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 2

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

Uf = rypted
sJs = "" '!!!
wWLu = ""
FETw = 1
    for i=1 to len(Uf)
if ( asc(mid(Uf, i, 1)) > 47 and asc(mid(Uf, i, 1)) < 58) then
sJs = sJs + mid(Uf, 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 3

Which magic byte indicates that an analyzed file is a pdf file?

A. cGRmZmlsZQ

B. 706466666

C. 255044462d

D. 0a0ah4cg

Correct Answer: C

---

### QUESTION 4

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 5



No.	Time	Source	Destination	Protocol	Length	Info
7	5.616434	Dell_a3:0d:10	_09:c2:50	ARP	42	192.168.51.105 is at 00:24:e8:a3:0d:10
8	5.616583	Dell_a3:0d:10	Intel_53:f2:7c	ARP	42	192.168.51.1 is at 00:24:e8:a3:0d:10 (duplicate use of 192.168.51.105 detected!
9	5.626711	Dell_a3:0d:10	_09:c2:50	ARP	42	192.168.51.201 is at 00:24:e8:a3:0d:10
21	15.647788	Dell_a3:0d:10	7c:05:07:ad:43:67	ARP	42	192.168.51.1 is at 00:24:e8:a3:0d:10 (duplicate use of 192.168.51.201 detected!
18	15.637271	Dell_a3:0d:10	Sonicwal_09:c2:50	ARP	42	192.168.51.105 is at 00:24:e8:a3:0d:10
19	15.637486	Dell_a3:0d:10	Intel_53:f2:7c	ARP	42	192.168.51.1 is at 00:24:e8:a3:0d:10 (duplicate use of 192.168.51.105 detected!
20	15.647656	Dell_a3:0d:10	Sonicwal_09:c2:50	ARP	42	192.168.51.201 is at 00:24:e8:a3:0d:10
21	15.647788	Dell_a3:0d:10	7c:05:07:ad:43:67	ARP	42	192.168.51.1 is at 00:24:e8:a3:0d:10 (duplicate use of 192.168.51.201 detected!
34	25.658359	Dell_a3:0d:10	Sonicwal_09:c2:50	ARP	42	192.168.51.105 is at 00:24:e8:a3:0d:10
35	25.658429	Dell_a3:0d:10	Intel_53:f2:7c	ARP	42	192.168.51.1 is at 00:24:e8:a3:0d:10
▶ Frame 10: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)						
▶ Ethernet II, Src: Dell_a3:0d:10 (00:24:e8:a3:0d:10), Dst: 7c:05:07:ad:43:67 (7c:05:07:ad:43:67)						
▶ Address Resolution Protocol (reply)						

Refer to the exhibit. A security analyst notices unusual connections while monitoring traffic. What is the attack vector, and which action should be taken to prevent this type of event?

- A. DNS spoofing; encrypt communication protocols
- B. SYN flooding; block malicious packets
- C. ARP spoofing; configure port security
- D. MAC flooding; assign static entries

Correct Answer: C

[300-215 VCE Dumps](#)

[300-215 Practice Test](#)

[300-215 Braindumps](#)