



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.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

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 2



```
def gfdggvbdsoqq(id, entry1, string1, entry2, string2):  
    url = 'https://docs.google.com/forms/d/e/' + id + '/formResponse'  
    enc1 = b64encode(bytes(string1, 'utf8')).decode()  
    enc2 = b64encode(bytes(string2, 'utf8')).decode()  
    form_data = {entry1: enc1, entry2: enc2}  
    user_agent = { 'Referer': 'https://docs.google.com/forms/d/e/' + id + '/viewform',  
    'User-Agent': 'Mozilla/5.0 (Windows NT 10.0;  
    Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.88  
    Safari/537.36' }  
    r = post(url, data=form_data, headers=user_agent)  
    if r.status_code == 200:  
        return True  
    else:  
        return False
```

Refer to the exhibit. Which type of code is being used?

- A. Shell
- B. VBScript
- C. BASH
- D. Python

Correct Answer: D

QUESTION 3

```
[**] [1:2008186:5] ET SCAN DirBuster Web App Scan in Progress [**]  
  
[Classification: Web Application Attack] [Priority: 1]  
  
04/20-13:02:21.250000 192.168.100.100:51022 -> 192.168.50.50:80  
  
TCP TTL:63 TOS:0x0 ID:20054 IpLen: 20 DgmLen:342 DF  
  
***AP*** Seq: 0x369FB652 Ack: 0x9CF06FD8 Win: 0xFA60 TcpLen: 32  
  
[Xref => http://doc.emergingthreats.net/2008186] [Xref => http://owasp.org]
```

Refer to the exhibit. According to the SNORT alert, what is the attacker performing?

- A. brute-force attack against the web application user accounts
- B. XSS attack against the target webserver
- C. brute-force attack against directories and files on the target webserver



D. SQL injection attack against the target webserver

Correct Answer: C

QUESTION 4

```
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 5

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:

Obtain	step 1
Strategize	step 2
Collect	step 3
Analyze	step 4
Report	step 5

Correct Answer:



Reference: https://subscription.packtpub.com/book/networking_and_servers/9781789344523/1/ch01lvl1sec12/network-forensics-investigation-methodology

[300-215 VCE Dumps](#)

[300-215 Exam Questions](#)

[300-215 Braindumps](#)