



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.passapply.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

```
[**] [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 2

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 3

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 4

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 5



System Number of events: 572				
Level	Date and Time	Source	Event ID	Task Category
Information	4/26/2015 12:42:14 PM	Service Control Man...	7045	None
Information	4/26/2015 12:38:28 PM	Service Control Man...	7045	None
Event 7045, Service Control Manager				
General Details				
A service was installed in the system.				
Service Name: DIIAHHNMPMMRqji				
Service File Name: \\127.0.0.1\admin\$\EgnBqKWm.exe				
Service Type: user mode service				
Service Start Type: demand start				
Service Account: LocalSystem				

Refer to the exhibit. An HR department submitted a ticket to the IT helpdesk indicating slow performance on an internal share server. The helpdesk engineer checked the server with a real-time monitoring tool and did not notice anything suspicious. After checking the event logs, the engineer noticed an event that occurred 48 hour prior. Which two indicators of compromise should be determined from this information? (Choose two.)

- A. unauthorized system modification
- B. privilege escalation
- C. denial of service attack
- D. compromised root access
- E. malware outbreak

Correct Answer: AD

[Latest 300-215 Dumps](#)

[300-215 Study Guide](#)

[300-215 Braindumps](#)