



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

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 2

Alert Message

SERVER-WEBAPP LOCK WebDAV Slack 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 3

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 4

```
[**] [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 5

```
indicator:Observable id= "example:Observable-Pattern-5f1dedd3-ece3-4007-94cd-7d52784c1474">
<cybox:Object id= "example:Object-3a7aa9db-d082-447c-a422-293b78e24238">
<cybox:Properties xsi:type= "EmailMessageObj:EmailMessageObjectType">
<EmailMessageObj:Header>
<EmailMessageObj:From category= "e-mail">
<AddressObj:Address_Value condition= "Contains">@state.gov</AddressObj:Address_Value>
</EmailMessageObj:From>
</EmailMessageObj:Header>
</cybox:Properties>
<cybox:Related_Objects>
<cybox:Related_Object>
<cybox:Properties xsi:type= "FileObj:FileObjectType">
<FileObj:File_Extension>pdf</FileObj:File_Extension>
<FileObj:Size_In_Bytes>87022</FileObj:Size_In_Bytes>
<FileObj:Hashes>
<cyboxCommon:Hash>
<cyboxCommon:Type xsi:type= "cyboxVocabs:HashNameVocab- 1.0">MD5</cyboxCommon:Type>
<cyboxCommon:Simple_Hash_Value>cf2b3ad32a8a4cfb05e9dfc45875bd70</cyboxCommon:Simple_Ha
sh_Value>
</cyboxCommon:Hash>
</FileObj:Hashes>
</cybox:Properties>
<cybox:Relationship xsi:type= "cyboxVocabs:ObjectRelationshipVocab-
1.0">Contains</cybox:Relationship>
</cybox:Related_Object>|
</cybox:Related_Objects>
</cybox:Object>
</indicator:Observable>
```

Refer to the exhibit. Which two actions should be taken as a result of this information? (Choose two.)

- A. Update the AV to block any file with hash "cf2b3ad32a8a4cfb05e9dfc45875bd70".
- B. Block all emails sent from an @state.gov address.
- C. Block all emails with pdf attachments.
- D. Block emails sent from Admin@state.net with an attached pdf file with md5 hash "cf2b3ad32a8a4cfb05e9dfc45875bd70".
- E. Block all emails with subject containing "cf2b3ad32a8a4cfb05e9dfc45875bd70".

Correct Answer: AB