



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

```
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>
<cyboxCommn:Simple_Hash_Value>cf2b3ad32a8a4cfb05e9dfc45875bd70</cyboxCommon:Simple_Ha
sh_Value>
</cyboxCommon:Hash>
</FileObj:Hashes>
</cybox:Properties>
<cybox:Relationship xsi:type= "cyboxVocabs:ObjectRelatiobshipVocab-
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

QUESTION 2



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 3



```

GET /wp-content/rm1q_q6x4_15/ HTTP/1.1
Host: iraniansk.com
Connection: Keep-Alive

HTTP/1.1 200 OK
Server: nginx
Date: Mon, 10 Aug 2020 20:16:17 GMT
Content-Type: application/octet-stream
Transfer-Encoding: chunked
Connection: keep-alive
Cache-Control: no-cache, must-revalidate
Pragma: no-cache
Expires: Mon, 10 Aug 2020 20:16:17 GMT
Content-Disposition: attachment; filename="Fy.exe"
Content-Transfer-Encoding: binary
Set-Cookie: 5f31ab113af08=1597090577; expires=Mon, 10-Aug-2020 20:17:17 GMT; Max-Age=60; path=/
Last-Modified: Mon, 10 Aug 2020 20:16:17 GMT
Vary: Accept-Encoding, User-Agent

6000
MZ.....@.....!L!This program cannot be run in DOS mode

$ N3 'JM' J[ 'l'0' - 'Rich
PE L fl_ t J @
f
0 @ < L @ text s t
^ rdata x @ @data _ 0 $ @ rsrc
8 @
@
8
Vj 6 B ^ A J
Q R $ I Y V DS tV Y^ V Nt ^ B j r8 % j x e x F
I M x
3 Vj d AB B ^ A 'B B V B DS tV 0 Y^ U u u u u C E | U u u u u E
] $ u $ U u u 4 B u l V P 8 8 t ( u u @ B M v ; s l t V u ; r 3
# ^ ] DS @ j P t $ 0 B u t $ T $ z 0 d 0 $ SY DS T $ k @ T s u DS DS T s k |
@@ T $ u DS VW @ x 5 0 C v 0 U YP Y ; D $ t 6 ; u 3 ^ F U Sp < C 3 e S w
3
A D
| 3 t u y N F u S @ = | e ~ y + M U @ y H
@ U y J B U y l A
U 2 : G M u ^ 3 ] U SC e e u 3 = SC t M V M M 0 j M Q @ V E
E | * E P E u V SC | E t M E ^ A x D S V I D ( t H + ^ I D ( t M +
$ V t q A r 9 T $ t r l L S v 2 ^ U M w 3 Q | Y
3 s e E P M h B E P E B < V t s k B ^ t $ t $ t $ q l 8 t $ q 8 j q 8 j q
8 D $ t $ P F c L $ @ O P B D $ | B B h w 3 P P t $ t $ t $ P j B

```

1 client pkt, 231 server pkts, 1 turn

Entire conversation (290kB) Show and save data as ASCII Stream 2

Refer to the exhibit. According to the Wireshark output, what are two indicators of compromise for detecting an Emotet malware download? (Choose two.)

- A. Domain name:iraniansk.com
- B. Server: nginx



C. Hash value: 5f31ab113af08=1597090577

D. filename= "Fy.exe"

E. Content-Type: application/octet-stream

Correct Answer: CE

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

An engineer received a call to assist with an ongoing DDoS attack. The Apache server is being targeted, and availability is compromised. Which step should be taken to identify the origin of the threat?

- A. An engineer should check the list of usernames currently logged in by running the command `$ who | cut -d ' ' -f1 | sort | uniq`
- B. An engineer should check the server's processes by running commands `ps -aux` and `sudo ps -a`.
- C. An engineer should check the services on the machine by running the command `service -status-all`.
- D. An engineer should check the last hundred entries of a web server with the command `sudo tail -100 /var/log/apache2/access.log`.



Correct Answer: D

[Latest 300-215 Dumps](#)

[300-215 PDF Dumps](#)

[300-215 Practice Test](#)