



# 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.pass4itsure.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 cloud characteristic from the left onto the challenges presented for gathering evidence on the right.

Select and Place:

broad network access	application details are unavailable to investigators since being deemed private and confidential
rapid Elasticity	obtaining evidence from the cloud service provider
measured service	circumvention of virtual machine isolation techniques via code or bad actor
resource pooling	evidence correlation across one or more cloud providers

Correct Answer:

	rapid Elasticity
	measured service
	resource pooling
	broad network access



QUESTION 2

```

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.....@.....I.LIThis 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 4B u lVP 88 t(u u @ B M v ; s l tV u ; r3
# ^ ) DS @ j P t $ 0 B u $ 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
j 3 t u y N Fu 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 j * 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 3

DRAG DROP

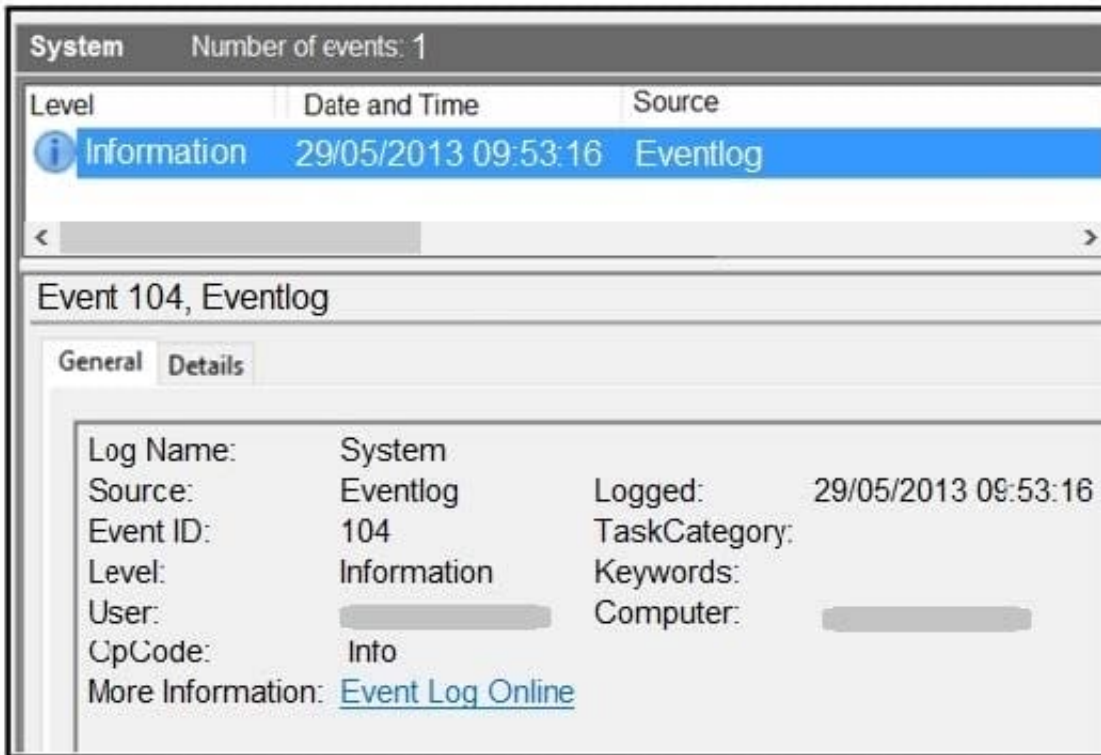
Drag and drop the capabilities on the left onto the Cisco security solutions on the right.

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 4**

Refer to the exhibit. An employee notices unexpected changes and setting modifications on their workstation and creates an incident ticket. A support specialist checks processes and services but does not identify anything suspicious. The ticket was escalated to an analyst who reviewed this event log and also discovered that the workstation had multiple large data dumps on network shares. What should be determined from this information?

- A. data obfuscation
- B. reconnaissance attack
- C. brute-force attack
- D. log tampering

Correct Answer: B

**QUESTION 5**

A scanner detected a malware-infected file on an endpoint that is attempting to beacon to an external site. An analyst has reviewed the IPS and SIEM logs but is unable to identify the file's behavior. Which logs should be reviewed next to evaluate this file further?

- A. email security appliance
- B. DNS server
- C. Antivirus solution
- D. network device



Correct Answer: B

[300-215 PDF Dumps](#)

[300-215 VCE Dumps](#)

[300-215 Exam Questions](#)