



# 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.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



## Alert Message

SERVER-WEBAPP LOCK WebDAV Stack 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 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 4

Which tool is used for reverse engineering malware?

- A. Ghidra
- B. SNORT
- C. Wireshark
- D. NMAP

Correct Answer: A

Reference: <https://www.nsa.gov/resources/everyone/ghidra/#:~:text=Ghidra%20is%20a%20software%20reverse,in%20their%20networks%20and%20systems.>

#### QUESTION 5

No.	Time	Source	Destination	Protocol	Length	Info
7	5.616434	Dell_a3:0d:10	09:c2:50	ARP	42	192.168.51.105 is at 00:24:e8:a3:0d:10
8	5.616583	Dell_a3:0d:10	Intel_53:f2:7c	ARP	42	192.168.51.1 is at 00:24:e8:a3:0d:10 (duplicate use of 192.168.51.105 detected!
9	5.626711	Dell_a3:0d:10	09:c2:50	ARP	42	192.168.51.201 is at 00:24:e8:a3:0d:10
21	15.647788	Dell_a3:0d:10	7c:05:07:ad:43:67	ARP	42	192.168.51.1 is at 00:24:e8:a3:0d:10 (duplicate use of 192.168.51.201 detected!
18	15.637271	Dell_a3:0d:10	Sonicwal_09:c2:50	ARP	42	192.168.51.105 is at 00:24:e8:a3:0d:10
19	15.637486	Dell_a3:0d:10	Intel_53:f2:7c	ARP	42	192.168.51.1 is at 00:24:e8:a3:0d:10 (duplicate use of 192.168.51.105 detected!
20	15.647656	Dell_a3:0d:10	Sonicwal_09:c2:50	ARP	42	192.168.51.201 is at 00:24:e8:a3:0d:10
21	15.647788	Dell_a3:0d:10	7c:05:07:ad:43:67	ARP	42	192.168.51.1 is at 00:24:e8:a3:0d:10 (duplicate use of 192.168.51.201 detected!
34	25.658359	Dell_a3:0d:10	Sonicwal_09:c2:50	ARP	42	192.168.51.105 is at 00:24:e8:a3:0d:10
35	25.658429	Dell_a3:0d:10	Intel_53:f2:7c	ARP	42	192.168.51.1 is at 00:24:e8:a3:0d:10
▶ Frame 10: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)						
▶ Ethernet II, Src: Dell_a3:0d:10 (00:24:e8:a3:0d:10), Dst: 7c:05:07:ad:43:67 (7c:05:07:ad:43:67)						
▶ Address Resolution Protocol (reply)						

Refer to the exhibit. A security analyst notices unusual connections while monitoring traffic. What is the attack vector, and which action should be taken to prevent this type of event?

- A. DNS spoofing; encrypt communication protocols
- B. SYN flooding; block malicious packets
- C. ARP spoofing; configure port security
- D. MAC flooding; assign static entries

Correct Answer: C

[Latest 300-215 Dumps](#)

[300-215 VCE Dumps](#)

[300-215 Practice Test](#)