



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

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

QUESTION 2

00386078	64	44	45	33	4C	6A	41	34	4C	6A	4D	78	4C	6B	5A	44
00386088	4D	44	59	78	4E	79	34	31	4E	54	41	32	4C	6A	55	31
00386098	4D	44	59	75	4E	6A	67	7A	4E	77	3D	3D	00	AB	AB	AB

Refer to the exhibit. Which encoding technique is represented by this HEX string?

- A. Unicode
- B. Binary
- C. Base64
- D. Charcode

Correct Answer: B

Reference: <https://www.suse.com/c/making-sense-hexdump/>



QUESTION 3

Time	Dst	port	Host	Info
2019-12-04 18:44...	185.188.182.76	80	ghinatronx.com	GET /edgron/siloft.php?i=yourght6.cab
2019-12-04 18:46...	45.143.93.81	80	bjanicki.com	GET /images/i8hvXXM_2F40bg3onEOH_2/
2019-12-04 18:46...	45.143.93.81	80	bjanicki.com	GET /favicon.ico HTTP/1.1
2019-12-04 18:46...	45.143.93.81	80	bjanicki.com	GET /images/6a7GzE2PowJhysjaQ/HULhLB
2019-12-04 18:46...	45.143.93.81	80	bjanicki.com	GET /images/aiXla28QV6duat/PF_28Y9stc
2019-12-04 18:47...	194.61.1.178	443	prodrigo29bkd20.com	Client Hello
2019-12-04 18:48...	194.61.1.178	443	prodrigo29bkd20.com	Client Hello
2019-12-04 18:52...	194.61.1.178	443	prodrigo29bkd20.com	Client Hello
2019-12-04 18:57...	194.61.1.178	443	prodrigo29bkd20.com	Client Hello
2019-12-04 19:02...	194.61.1.178	443	prodrigo29bkd20.com	Client Hello
2019-12-04 19:07...	194.61.1.178	443	prodrigo29bkd20.com	Client Hello
2019-12-04 19:08...	194.61.1.178	443	prodrigo29bkd20.com	Client Hello
2019-12-04 19:13...	194.61.1.178	443	prodrigo29bkd20.com	Client Hello
2019-12-04 19:18...	194.61.1.178	443	prodrigo29bkd20.com	Client Hello
2019-12-04 19:19...	194.61.1.178	443	prodrigo29bkd20.com	Client Hello


```

> Frame 6: 386 bytes on wire (3088 bits), 386 bytes captured (3088 bits)
> Ethernet II, Src: HewlettP_1c:47:ae (00:08:02:1c:47:ae), Dst: Netgear_b6:93:f1 (20:e5:2a:b6:93:f1)
> Internet Protocol Version 4, Src: 160.192.4.101, Dst: 185.188.182.76
0000  20 e5 2a b6 93 f1 00 08 02 1c 47 ae 08 00 45 00 * . . . G E
  
```

Refer to the exhibit. A network engineer is analyzing a Wireshark file to determine the HTTP request that caused the initial Ursnif banking Trojan binary to download. Which filter did the engineer apply to sort the Wireshark traffic logs?

- A. http.request.un matches
- B. tls.handshake.type ==1
- C. tcp.port eq 25
- D. tcp.window_size ==0

Correct Answer: B

Reference:

<https://www.malware-traffic-analysis.net/2018/11/08/index.html>

<https://unit42.paloaltonetworks.com/wireshark-tutorial-examining-ursnif-infections/>

QUESTION 4

A security team receives reports of multiple files causing suspicious activity on users\' workstations. The file attempted to access highly confidential information in a centralized file server. Which two actions should be taken by a security analyst to evaluate the file in a sandbox? (Choose two.)



- A. Inspect registry entries
- B. Inspect processes.
- C. Inspect file hash.
- D. Inspect file type.
- E. Inspect PE header.

Correct Answer: BC

Reference: https://medium.com/@Flying_glasses/top-5-ways-to-detect-malicious-file-manually-d02744f7c43a

QUESTION 5

Artifact 32: http-syracusecoffee.com-80-10-1

Src: network (GUI) Intel 80386, for MS Windows	Imports: 100 Type: EXE – PE32 executable	SHA256: 54065f8e84ea846e319408b23e65ad371cd09e0580c4980a199674034a3ab09
Size: 270848	Exports: 1 AV Sigs: 0	MD5: f4a49b3e4aa82e1fc63adf48d133ae2a

Path http-syracusecoffee.com-80-10-1	SHA1 446e86e8d3b556afabe414bff4c250776e196c82
Mime Type application/x-dosexec; charset=binary	Created At +142.693s
Magic Type PF32 executable (GUI) Intel 80386, for MS Windows	Related to stream 10

PE Sections

Headers

Imported/Exported Symbols

Artifact 33: http-qstride.com-80-8-1

Src: network ASCII text	Imports: 0 Type: HTMLS – HTML document,	SHA256: boc7e6712ecbf97a1e3a14f19e3aed5dbd655321a2852565bfc5518925713db
Size: 318	Exports: 0 AV Sigs: 0	MD5: fa172c77abd7b03605d33cd1ae373657

Path http-qstride.com-80-8-1	SHA1 9785fb3254695c25c621eb4cd81cf7a2a3c8258f
Mime Type text/html; charset=us-ascii	Created At +141.865s
Magic Type HTML document, ASCII text	Related to stream 8

Refer to the exhibit. What do these artifacts indicate?

- A. An executable file is requesting an application download.
- B. A malicious file is redirecting users to different domains.
- C. The MD5 of a file is identified as a virus and is being blocked.
- D. A forged DNS request is forwarding users to malicious websites.

Correct Answer: A



VCE & PDF

PassApply.com

<https://www.passapply.com/300-215.html>

2024 Latest passapply 300-215 PDF and VCE dumps Download

[300-215 Practice Test](#)

[300-215 Study Guide](#)

[300-215 Braindumps](#)