



210-255^{Q&As}

Cisco Cybersecurity Operations

Pass Cisco 210-255 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.geekcert.com/210-255.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

Which two options can be used by a threat actor to determine the role of a server? (Choose two.)

- A. PCAP
- B. tracer
- C. running processes
- D. hard drive configuration
- E. applications

Correct Answer: CE

QUESTION 2

The screenshot shows a Wireshark capture of network traffic. The main pane displays a list of packets, with packet 4 selected. The packet list table is as follows:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	6.131.174.107	106.153.244.155	TCP	62	wfremoterm > http [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
2	1.000000	106.153.244.155	6.131.174.107	TCP	58	http > wfremoterm [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
3	2.000000	6.131.174.107	106.153.244.155	TCP	60	wfremoterm > http [ACK] Seq=1 Ack=1 Win=64240 Len=0
4	3.000000	6.131.174.107	106.153.244.155	HTTP	793	GET /png.php?034780E086125BA1FCC75FA73B09FE9C377E066692F812728F1C1C88EF26E67FA44A41C1E3B8854073FA2D098435FE97B1C337A1113FE0B781F80688768E326AF5DEC1AC0FF255A48
5	4.000000	106.153.244.155	6.131.174.107	TCP	54	http > wfremoterm [ACK] Seq=1 Ack=640 Win=65535 Len=0
6	5.000000	106.153.244.155	6.131.174.107	HTTP	482	HTTP/1.1 200 OK (text/html)
7	6.000000	6.131.174.107	106.153.244.155	TCP	60	wfremoterm > http [ACK] Seq=640 Ack=429 Win=63812 Len=0
8	7.000000	106.153.244.155	6.131.174.107	TCP	54	http > wfremoterm [FIN, ACK] Seq=429 Ack=640 Win=65535 Len=0
9	8.000000	6.131.174.107	106.153.244.155	TCP	60	wfremoterm > http [ACK] Seq=640 Ack=438 Win=63812 Len=0

The details pane for the selected packet (4) shows the following information:

- Checksum: 0xe330 [validation disabled]
- Sequence/ACK analysis
- Hypertext Transfer Protocol
 - [truncated] GET /png.php?034780E086125BA1FCC75FA73B09FE9C377E066692F812728F1C1C88EF26E67FA44A41C1E3B8854073FA2D098435FE97B1C337A1113FE0B781F80688768E326AF5DEC1AC0FF255A48
 - [truncated] Expert Info (Chat/Sequence): GET /png.php?034780E086125BA1FCC75FA73B09FE9C377E066692F812728F1C1C88EF26E67FA44A41C1E3B8854073FA2D098435FE97B1C337A1113FE0B781F80688768E326AF5DEC1AC0FF255A48
 - Request Method: GET
 - Request URI: [truncated] http://fdsa1re367hs64a.ase4wrfdfg9.com/png.php?034780E086125BA1FCC75FA73B09FE9C377E066692F812728F1C1C88EF26E67FA44A41C1E3B8854073FA2D098435FE97B1C337A1113FE0B781F80688768E326AF5DEC1AC0FF255A48
 - Request Version: HTTP/1.1
 - User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729)\r\n
 - Host: fdsa1re367hs64a.ase4wrfdfg9.com\r\n
 - Connection: Keep-Alive\r\n
 - \r\n
 - [full request URI [truncated]: http://fdsa1re367hs64a.ase4wrfdfg9.com/png.php?034780E086125BA1FCC75FA73B09FE9C377E066692F812728F1C1C88EF26E67FA44A41C1E3B8854073FA2D098435FE97B1C337A1113FE0B781F80688768E326AF5DEC1AC0FF255A48

Refer to the exhibit. Which information is interesting about the HTTP GET shown?

- A. The User-Agent is Mozilla/4.0



- B. The HTTP GET is encoded
- C. timestamps
- D. The protocol is TCP

Correct Answer: B

QUESTION 3

A CMS plugin creates two files that are accessible from the Internet myplugin.html and exploitable.php. A newly discovered exploit takes advantage of an injection vulnerability in exploitable.php. To exploit the vulnerability, one must send an HTTP POST with specific variables to exploitable.php. You see traffic to your webserver that consists of only HTTP GET requests to myplugin.html. Which category best describes this activity?

- A. weaponization
- B. exploitation
- C. installation
- D. reconnaissance

Correct Answer: B

QUESTION 4

What is the common artifact that is used to uniquely identify a detected file?

- A. Hash
- B. Timestamp
- C. File size

Correct Answer: A

QUESTION 5

How do you verify that one of your hosts is potentially compromised based on their communication destinations?

- A. Search the communication destinations of the host in the Talos IP and Domain Reputation Center.
- B. Analyze how much traffic the host sent and received from each IP address or domain.
- C. See if any Stealthwatch alarms were triggered for the host communicating with internal hosts.
- D. Check the Firepower appliance to see if malicious files were downloaded.



Correct Answer: A

[210-255 VCE Dumps](#)

[210-255 Study Guide](#)

[210-255 Braindumps](#)