# 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. tracert

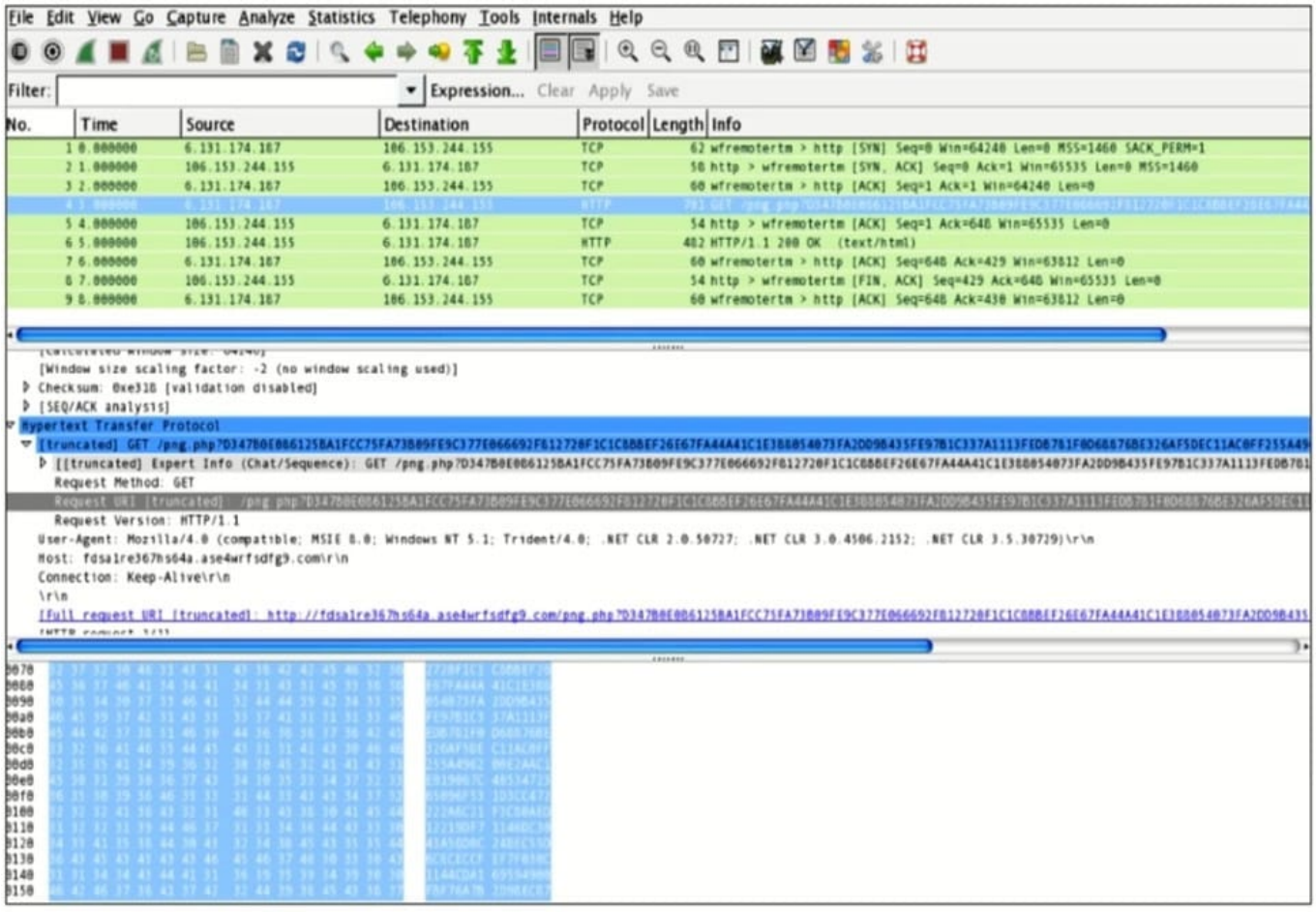
C. running processes

D. hard drive configuration

E. applications

Correct Answer: CE

**QUESTION 2**




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