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:

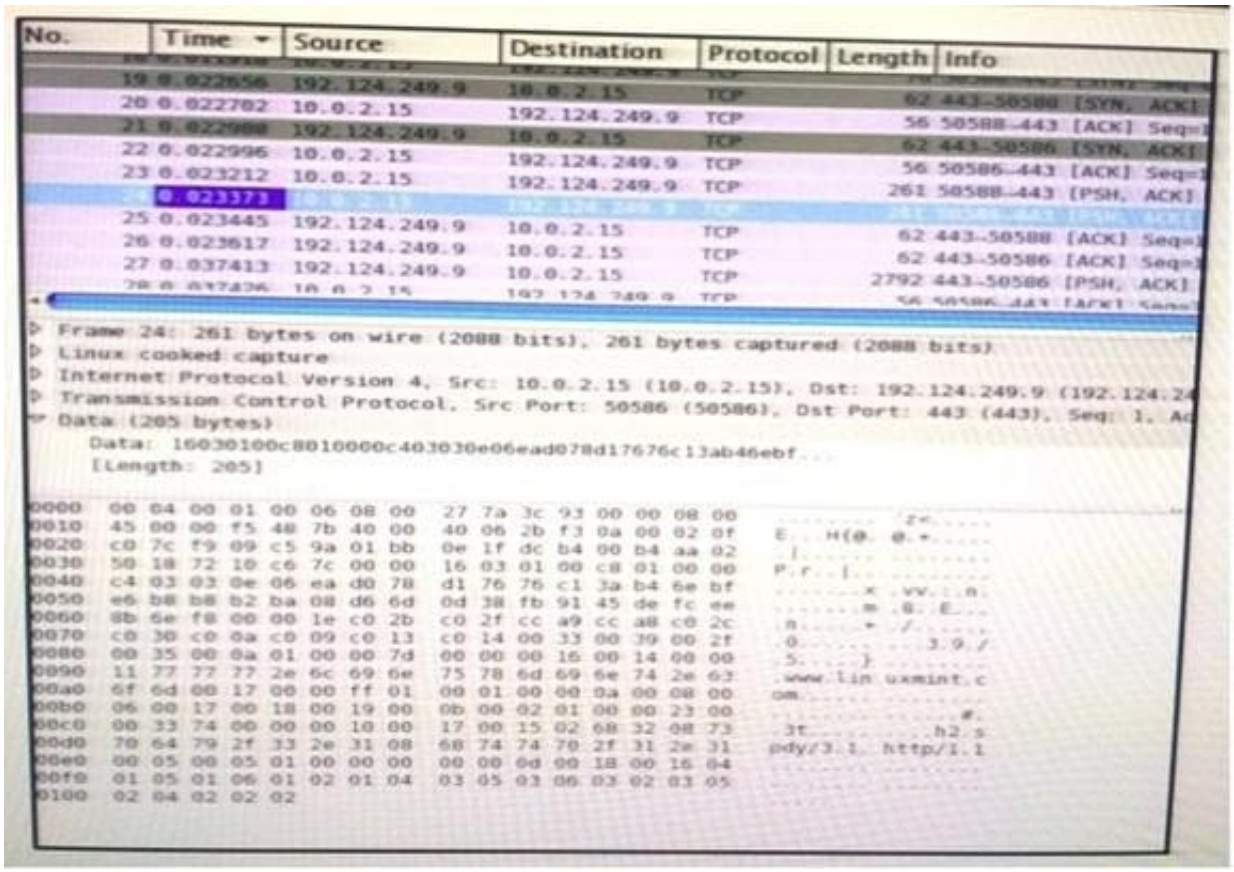
https://www.leads4pass.com/210-255.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Cisco Official Exam Center

QUESTION 1

Refer to the exhibit. Which application protocol is in this PCAP file?



A. TCP

B. SSH

C. HTTP

D. SSL

Correct Answer: D

QUESTION 2

Which option is unnecessary for determining the appropriate containment strategy according to NIST.SP800-61 r2?

A. effectiveness of the strategy

B. time and resource needed to implement the strategy

C. need for evidence preservation

D. attack vector used to compromise the system

Correct Answer: D

QUESTION 3

Which expression creates a filter on a host IP address or name?

A. [src|dst] host

B. [tcp|udp] [src|dst] port

C. ether [src|dst] host

D. gateway host

Correct Answer: A

QUESTION 4

What do the Security Intelligence Events within the FMC allow an administrator to do?

A. See if a host is connecting to a known-bad domain.

B. Check for host-to-server traffic within your network.

C. View any malicious files that a host has downloaded.

D. Verify host-to-host traffic within your network.

Correct Answer: A

QUESTION 5

When evidence is collected, what does NIST SP800-86 specify as a guideline to follow for the order of collection?

A. order of volatility

B. order of importance

C. most difficult to access first

D. least difficult to access first

Correct Answer: B