Packet Count

0

Open the Wireshark program. (Windows: Start->Run, Type in "wireshark") (Linux: From terminal command line or Run, type "wireshark")

Load the pcap file. (File->Open, browse to where you downloaded the pcap file to, select the file, select Open.

Identify the total packet count. This number will be your FLAG.

Field Identification 1

0

Use the provide picture to help identify the different type of fields.

Which field shows the current packet in a more detailed form? (Select a letter.)

A. Packet List B. Packet Details C. Packet Bytes

Field Identification 2

0

Use the provide picture to help identify the different type of fields.

Which field displays all the packets in the current capture file? (Select a letter.)

A. Packet List B. Packet Details C. Packet Bytes

Field Identification 3

0

Use the provide picture to help identify the different type of fields.

Which field displays the data of the current packet in a hexdump style? (Select a letter.)

A. Packet List B. Packet Details C. Packet Bytes

Statistics 1

0

Under the Statistics menu, what provides a tree of all the protocols in a capture with each row containing the statistical values of one protocol? (Select a letter.)

A. Conversations B. Protocol Hierarchy C. IPv4 Statistics D. Endpoints

Statistics 2

0

What is the traffic between two specific endpoints and their respective ports? (Select a letter.)

A. Conversations B. Protocol Hierarchy C. IPv4 Statistics D. Endpoints

Basic 1

0

Refer to the provide picture. What will happen after you select this button? (Select a letter.)

A. Wireshark capture will stop. B. Wireshark capture will pause. C. Wireshark capture will start. D. Wireshark capture will be saved to a file.

Basic 2

0

Refer to the provide picture. What will happen after you select this button? (Select a letter.)

A. Wireshark capture will stop. B. Wireshark capture will pause. C. Wireshark capture will start. D. Wireshark capture will be saved to a file.

Basic 3

0

Refer to the provide picture. What will happen after you select this button? (Select a letter.)

A. Wireshark capture will stop. B. Wireshark capture will pause. C. Wireshark capture will start. D. Wireshark capture will be saved to a file.

Filtering 1

0

Refer to the picture. What is the circled area called and used for? (Select a letter.)

A. Display filter, used to display particular captured packets. B. Capture filter, used to limit packets that are captured. C. Capture filter, used to display particular captured packets. D. Display filter, used to limit packets that are captured.

Filtering 2

0

Refer to the picture. What is the circled area called and used for? (Select a letter.)

A. Display filter, used to display particular captured packets. B. Capture filter, used to limit packets that are captured. C. Capture filter, used to display particular captured packets. D. Display filter, used to limit packets that are captured.

Filtering 3

0

What is the correct display filter to show all traffic for host 192.168.242.216? (Select a letter.)

A. ip address = 192.168.242.216 B. ip addr == 192.168.242.216 C. ip.addr == 192.168.242.216 D. ip.src == 192.168.242.216

Filtering 4

0

What is the correct display filter to show traffic sourced from host 192.168.242.216? (Select a letter.)

A. ip address = 192.168.242.216 B. ip addr == 192.168.242.216 C. ip.addr == 192.168.242.216 D. ip.src == 192.168.242.216

Filtering 5

0

What is the correct display filter to show traffic for tcp port 22 traffic? (Select a letter.)

A. tcp.port == 22 B. tcp port == 22 C. tcp&22 D. tcp.port = 22

Filtering 6

0

What keyboard combination will bring up the find option within your displayed filtered packets? (Select a letter.)

A. SHIFT+A B. SHIFT+F C. CTRL+A D. CTRL+F

Filtering 7

0

Using the Ultimate PCAP file, find the telnet session and follow the tcp stream. What is displayed? (Select a letter.)

A. Username B. Password C. Routing table D. All the above.

Filtering 8

0

Using the Ultimate PCAP file, create a display filter to find all the OSPF Hello Packets. How many OSPF Hello packets are there?

A. 911 B. 411 C. 211 D. 111