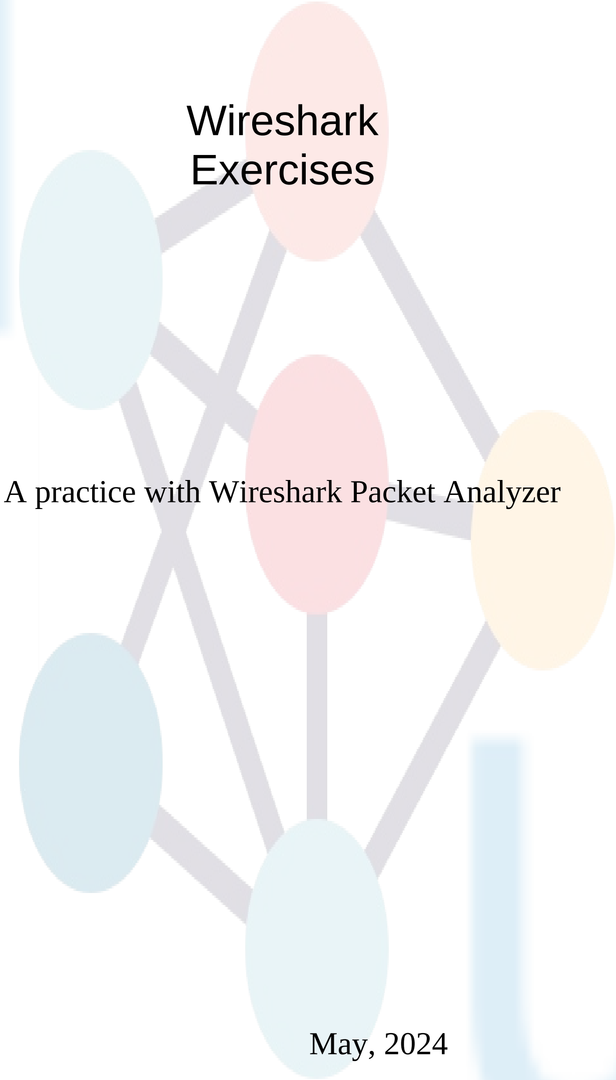

Wireshark Exercises

A practice with Wireshark Packet Analyzer

May, 2024

Table of Contents

I) Exercise One: Good old telnet

`File: telnet.pcap`

Work: reconstruct the telnet session

Questions

1. Who logged into 192.168.0.1?
   Username:____________________ Password: ______________

2. After logged what the user do?

TIP: telnet traffic is not secure

II) Exercise two: massive TCP SYN

`File: massivesyn1.pcap and massivesyn2.pcap`

Work: Find files differences

Questions

1. massivesyn1.pcap is a __________________ attempt

1. massivesyn2.pcap is a __________________ attempt

TIP: pay attention to source IP

III) Exercise three: compare traffic

`Files: student1.pcap and student2.pcap`

Scenario: You are an IT admin in UCR, you had reported that *student1* (a new student) cannot browse or mail with its laptop. After some research, *student2*, sitting next to *student1*, can browse with any problems.

Work: compare these two capture files and state why *student1*'s machine is not online

Solution

1. *student1* must ____________________________

TIP: pay attention to first ARP package

IV) Exercise four: chatty employees

`File: chat.pcap`

Work: compare these two capture files and state why *student1*'s machine is not online

Question

1. What kind of protocol is used?
2. Who are the chatters?
3. What do they say about you (sysadmin)?

TIP: your chat can be monitored by network admin