Semana 9 WireShark
Christopher Zúñiga C28730

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?

1. **Username:** fake **Password:** user
2. **$**/sbin/ping www.yahoo.com

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

1. **SYN** flood attempt
2. **SYN** flood attempt

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 _____

1. **Student 1 has to match his IP address with the correct network configuration which is 192.168.0.10**

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)?

1. **MSNMS (TCP)**
2. **tesla_brian@hotmail.com, tesla_thomas@hotmail.com**
3. **Captured packets do not contain information in regard of sysadmin**