I) Exercise One: Good old telnet

`File: telnet.pcap`

Work: reconstruct the telnet session

Questions

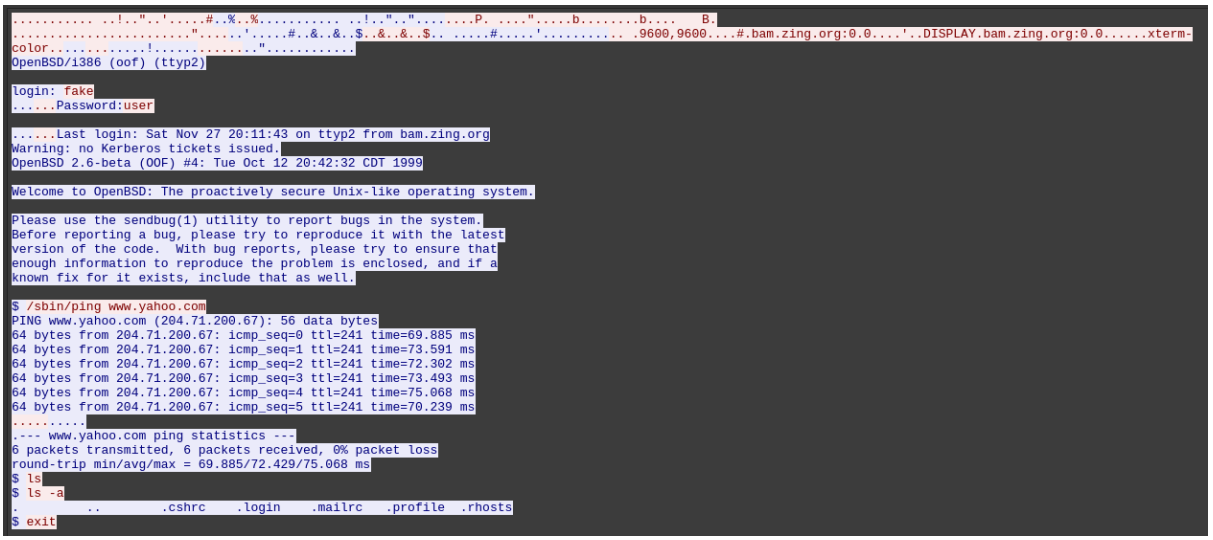
1. Who logged into 192.168.0.1?
   Username:_____ Password: _____
2. After logged what the user do?

TIP: telnet traffic is not secure

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

TIP: pay attention to source IP

1. **massivesyn1.pcap is a SYN flood attempt.**

SYN flood attacks are common DoS (Denial of Service) attacks where multiple SYN packets are sent to overwhelm a target by exhausting resources, typically with no intention of completing the TCP handshake.

2. **massivesyn2.pcap is a SYN flood attempt.**

Given the naming and context, it's likely that both captures involve SYN flood attempts. Analyzing both could reveal variations in the attack pattern, volume, or IP sources but would still likely show signs of a SYN flood attack.

III) Exercise three: compare traffic

`Files: student1.pcap and student2.pcap`

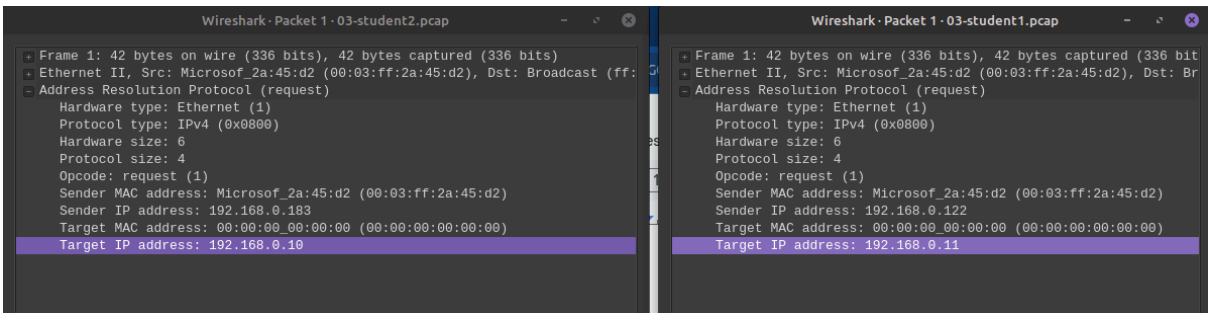
Scenario: You are an IT admin in UCR, you had reported that *student1* (a new student) cannot browse or mail with its laptop. After some research, *student2*, sitting next to *student1*, can browse with any problems.

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



Solution

1. **Student 1 should set their IP address to match the correct network configuration, targeting `192.168.0.10`** instead of `192.168.0.11`.
2. This can involve:
    - **Changing the IP address manually** (if using a static IP).
    - **Renewing the DHCP lease** (if the network is configured to assign IP addresses automatically).

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

1. **What kind of protocol is used?**
    - The protocol used here is **MSN Messenger Service Protocol** (`MSNMS`), which runs over **TCP**. Specifically, the communication is occurring over **TCP port 1863**, which is used by the MSN Messenger service for messaging.
2. **Who are the chatters?**
    - The chatters in this capture are two MSN Messenger users with the following email addresses:
        - `tesla_brian@hotmail.com`
        - `tesla_thomas@hotmail.com`
3. **What do they say about you (sysadmin)?**
    - From the packet capture provided, we don't have the specific message content that directly reveals what is said about the sysadmin. However, the presence of **MSG** packets between these two users (e.g., `MSG tesla_thomas@hotmail.com Thomas 97`) indicates a conversation exchange. If accessible in the full packet data, the actual message payload could reveal details of their conversation, which might mention the sysadmin if there are comments about network monitoring or other admin-related topics.