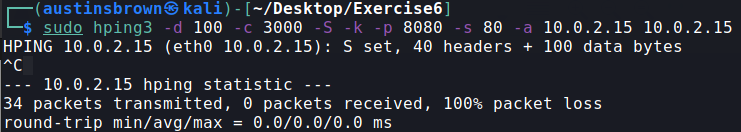
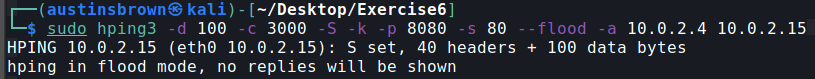
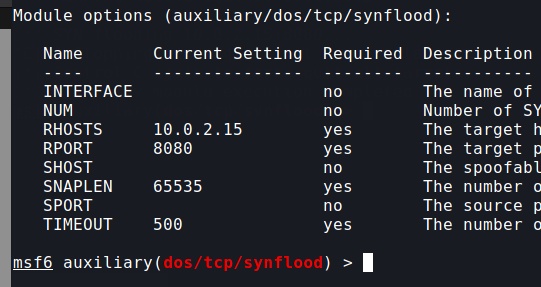
**3.1**

****

**3.2**

****

**4.**

****

**5.1**

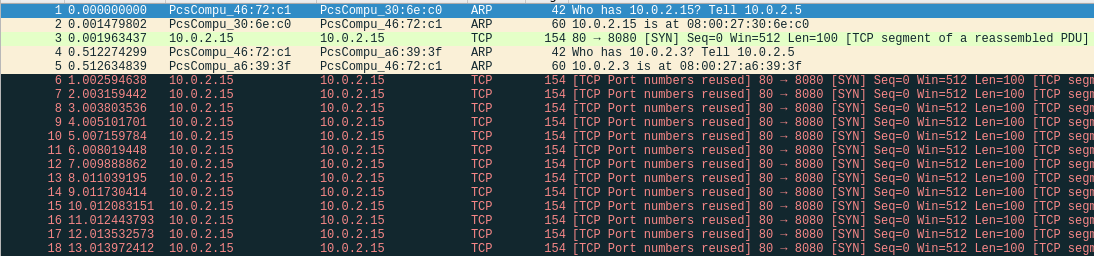
A LAND attack is a type od DOS attack. The goal is to overrun the target with packets. The idea is that the source and destination information are the same. When the machine receives a packet, it tries to reply to itself. This creates a loop, crashing the machine.

**5.2**

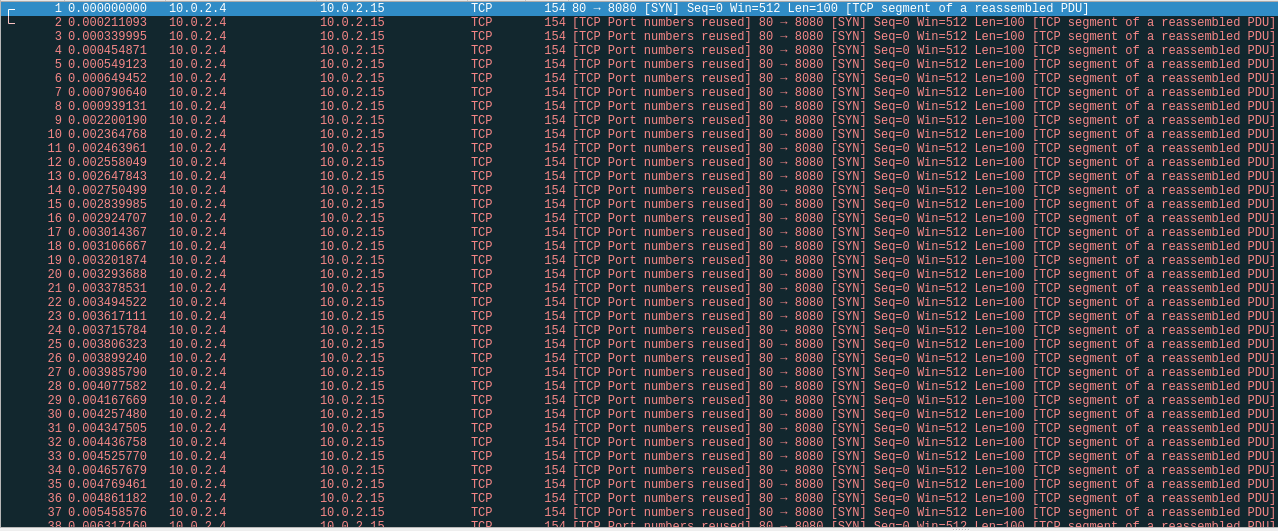
One way to prevent a land attack would be to perform filtering on the packets that are received. If a packet is received that has the same source and destination info, then reject the packet. One way to recover from the attack would be to implement loop detection. That is, the server detects that it is in a loop and resets itself.

**5.3**

In the LAND attack there was a continuous stream of TCP packets sent. The source and destination IP were the same. This is what makes it a LAND attack. Wire shark has detected that something is wrong and has blacklisted the packets.

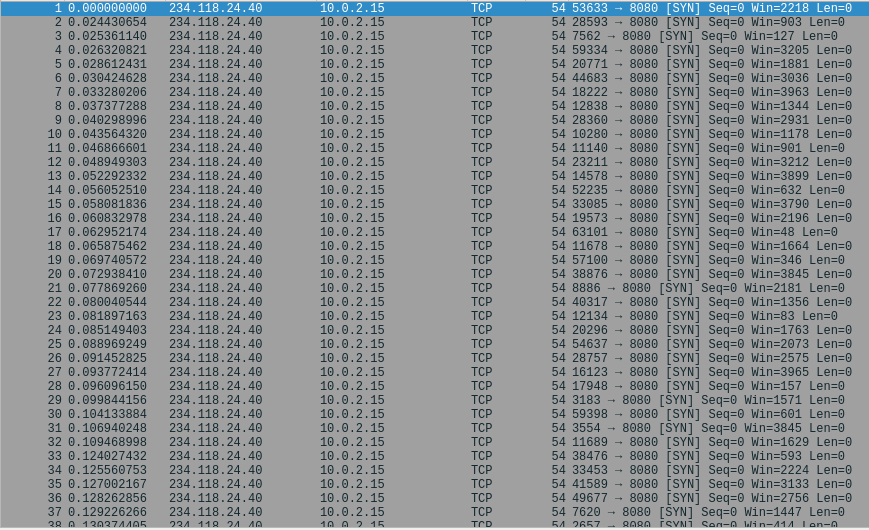


The SYN flood is like the LAND attack. The TCP packets are blacklisted. The difference is that instead of using the same source and destination address, we are spoofing the source to look like the HMI. Many more packets were generated in a short amount of time than the LAND attack. The purpose of this attack is to overwhelm the server.



**5.4**

The results for part 4 are shown below. One difference is that the TCP packets are not blacklisted in part 4. In addition to this, the IP wasn’t spoofed to the IP of the HMI in part 4.

****

**5.5**

SCADABr can keep up because the attacks that we are using have been around for a long time. Security measures have been put into place to keep LAND attacks from causing a loop as well as from keeping SYN flood from totally overwhelming the system. I did notice a small amount of lag when using Metasploit to conduct the attack, but other than that, the firewall prevented a denial of service.