Assignment 12: Firewalls

Jesse Russell

Step 3:

```
Chain FWDI_public_allow (0 references)
 pkts bytes target     prot opt in     out     source               destination

Chain FWDI_public_deny (0 references)
 pkts bytes target     prot opt in     out     source               destination

Chain FWDI_public_log (0 references)
 pkts bytes target     prot opt in     out     source               destination

Chain FWDO_public (0 references)
 pkts bytes target     prot opt in     out     source               destination

Chain FWDO_public_allow (0 references)
 pkts bytes target     prot opt in     out     source               destination

Chain FWDO_public_deny (0 references)
 pkts bytes target     prot opt in     out     source               destination

Chain FWDO_public_log (0 references)
 pkts bytes target     prot opt in     out     source               destination

Chain INPUT_ZONES (0 references)
 pkts bytes target     prot opt in     out     source               destination

Chain INPUT_ZONES_SOURCE (0 references)
 pkts bytes target     prot opt in     out     source               destination

Chain INPUT_direct (0 references)
 pkts bytes target     prot opt in     out     source               destination

Chain IN_public (0 references)
 pkts bytes target     prot opt in     out     source               destination

Chain IN_public_allow (0 references)
 pkts bytes target     prot opt in     out     source               destination

Chain IN_public_deny (0 references)
 pkts bytes target     prot opt in     out     source               destination

Chain IN_public_log (0 references)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT_direct (0 references)
 pkts bytes target     prot opt in     out     source               destination
[root@localhost ~]#
```

The firewall's current rules have been flushed with iptables -vnL

Step 4:

```
[root@localhost ~]# iptables -P INPUT DROP
[root@localhost ~]# iptables -vnL
Chain INPUT (policy DROP 1 packets, 67 bytes)
 pkts bytes target     prot opt in     out     source
```

The input chain was set to reject all.

Step 5:

```
[root@localhost ~]# iptables -P INPUT ACCEPT
[root@localhost ~]# iptables -A INPUT -s 192.168.100.100 -j DROP
[root@localhost ~]# iptables -vnL
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 DROP       all  --  *      *       192.168.100.100      0.0.0.0/0
```

The input chain was set back to accept. Then the chain was set to drop all packets from 192.168.100.100.

Step 7:

```
[root@localhost ~]# nmap -sT 127.0.0.1

Starting Nmap 6.40 ( http://nmap.org ) at 2019-12-06 14:48 EST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0010s latency).
Not shown: 994 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
25/tcp   open  smtp
80/tcp   open  http
111/tcp  open  rpcbind
631/tcp  open  ipp
6000/tcp open  X11

Nmap done: 1 IP address (1 host up) scanned in 0.12 seconds
[root@localhost ~]#
```

The result of the nmap scan. Ports 22, 25, 80, 111, 631, 6000 have apps running on them.