

Assignment 01 Report

Design

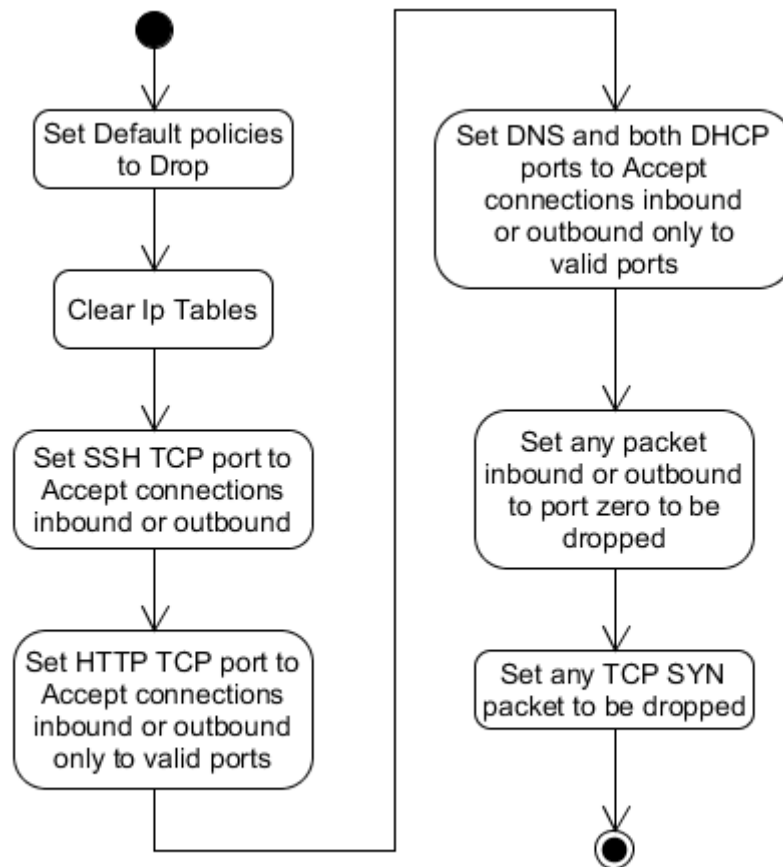


Figure 1 Design work of the shell script

Instructions

How to set the firewall. In the UNIX terminal:

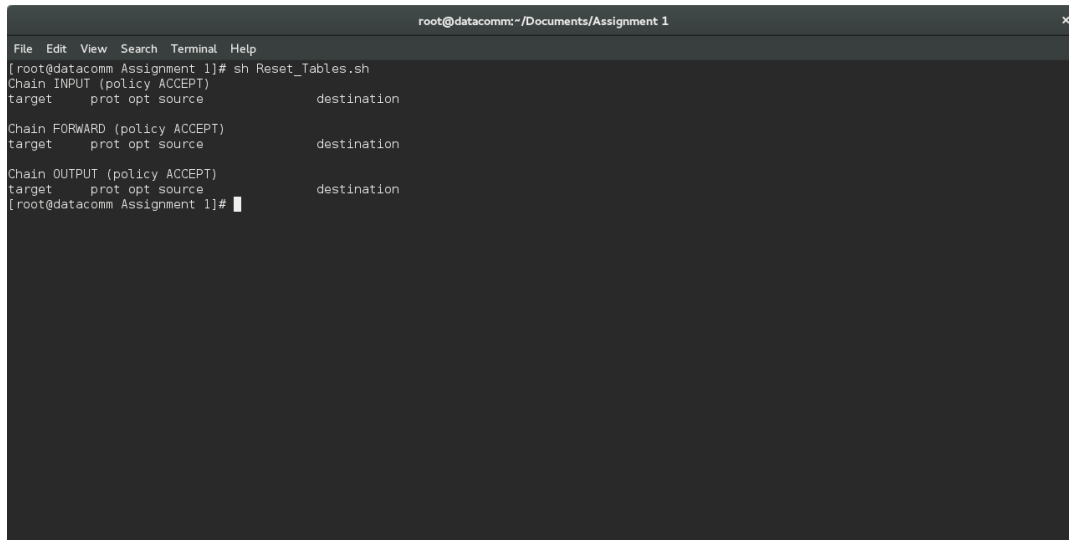
1. Localize the folder which contains the scripts Reset_Tables.sh and C8006_Assignment_1.sh
2. Execute the Reset_Tables.sh script by either:
 - a. sh Reset_Tables.sh
 - b. bash Reset_Tables.sh
3. Execute the firewall script by either:
 - a. sh C8006_Assignment_1.sh
 - b. bash C8006_Assignment_1.sh

Tests

For testing the firewall, I used 2 machines: One machine with the Firewall (192.168.0.16) and the other one without it (192.168.0.15). For the captures I will add a (FW) to the captures of the Firewall Machine and (T) to the one attempting connections with the Firewall Machine.

1. Start

First, I set the default policies to a default state of accepting everything by using a shellscript called Reset_Tables.sh



```
root@datacomm:~/Documents/Assignment 1
File Edit View Search Terminal Help
[root@datacomm Assignment 1]# sh Reset_Tables.sh
Chain INPUT (policy ACCEPT)
target    prot opt source                destination

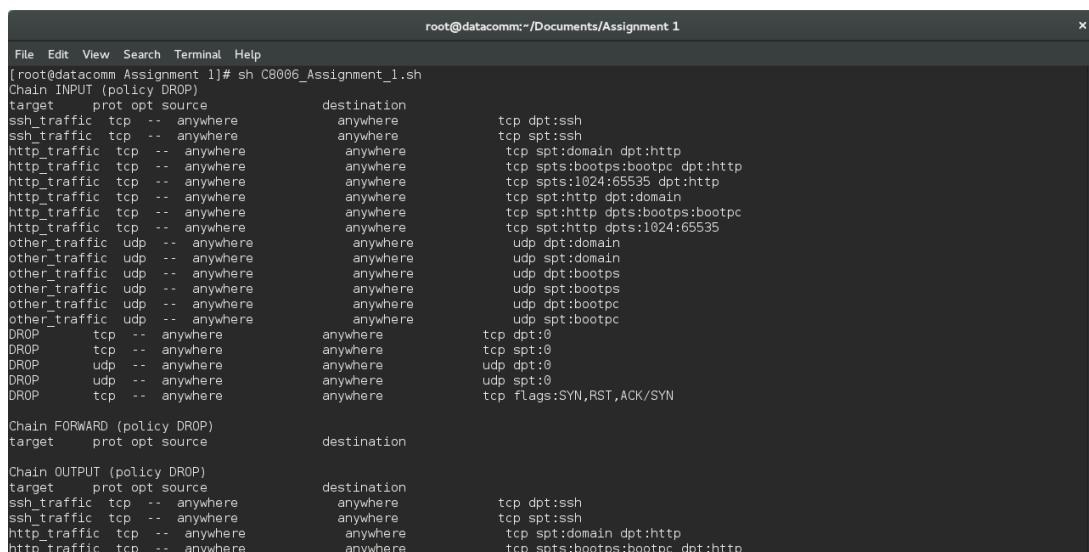
Chain FORWARD (policy ACCEPT)
target    prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target    prot opt source                destination
[root@datacomm Assignment 1]#
```

Figure 2 Reset Tables on firewall Machine (FW)

2. Running the script to set up the firewall

I create the firewall and display the created ip tables.



```
root@datacomm:~/Documents/Assignment 1
File Edit View Search Terminal Help
[root@datacomm Assignment 1]# sh C8006_Assignment_1.sh
Chain INPUT (policy DROP)
target    prot opt source                destination
ssh_traffic tcp -- anywhere             anywhere             tcp dpt:ssh
ssh_traffic tcp -- anywhere             anywhere             tcp spt:ssh
http_traffic tcp -- anywhere             anywhere             tcp spt:domain dpt:http
http_traffic tcp -- anywhere             anywhere             tcp spts:bootps:bootpc dpt:http
http_traffic tcp -- anywhere             anywhere             tcp spts:1024:65535 dpt:http
http_traffic tcp -- anywhere             anywhere             tcp spt:http dpt:domain
http_traffic tcp -- anywhere             anywhere             tcp spt:http dpts:bootps:bootpc
http_traffic tcp -- anywhere             anywhere             tcp spt:http dpts:1024:65535
other_traffic udp -- anywhere             anywhere             udp dpt:domain
other_traffic udp -- anywhere             anywhere             udp spt:domain
other_traffic udp -- anywhere             anywhere             udp dpt:bootps
other_traffic udp -- anywhere             anywhere             udp spt:bootps
other_traffic udp -- anywhere             anywhere             udp dpt:bootpc
other_traffic udp -- anywhere             anywhere             udp spt:bootpc
DROP      tcp -- anywhere             anywhere             tcp dpt:0
DROP      tcp -- anywhere             anywhere             tcp spt:0
DROP      udp -- anywhere             anywhere             udp dpt:0
DROP      udp -- anywhere             anywhere             udp spt:0
DROP      tcp -- anywhere             anywhere             tcp flags:SYN,RST,ACK/SYN

Chain FORWARD (policy DROP)
target    prot opt source                destination

Chain OUTPUT (policy DROP)
target    prot opt source                destination
ssh_traffic tcp -- anywhere             anywhere             tcp dpt:ssh
ssh_traffic tcp -- anywhere             anywhere             tcp spt:ssh
http_traffic tcp -- anywhere             anywhere             tcp spt:domain dpt:http
http_traffic tcp -- anywhere             anywhere             tcp spts:bootps:bootpc dpt:http
```

Figure 3 Setting up the Firewall (FW)

3. Review the current state of the accounting chains

```
root@datacomm:~/Documents/Assignment 1
File Edit View Search Terminal Help
4 2416 other_traffic udp -- any any anywhere anywhere udp dpt:bootps
1 328 other_traffic udp -- any any anywhere anywhere udp spt:bootps
0 0 other_traffic udp -- any any anywhere anywhere udp dpt:bootpc
0 0 other_traffic udp -- any any anywhere anywhere udp spt:bootpc
0 0 DROP tcp -- any any anywhere anywhere tcp dpt:0
0 0 DROP tcp -- any any anywhere anywhere tcp spt:0
0 0 DROP udp -- any any anywhere anywhere udp dpt:0
0 0 DROP udp -- any any anywhere anywhere udp spt:0
0 0 DROP tcp -- any any anywhere anywhere tcp flags:SYN,RST,ACK/SYN

Chain FORWARD (policy DROP 0 packets, 0 bytes)
pkts bytes target prot opt in out source destination

Chain OUTPUT (policy DROP 0 packets, 0 bytes)
pkts bytes target prot opt in out source destination
0 0 ssh_traffic tcp -- any any anywhere anywhere tcp dpt:ssh
0 0 ssh_traffic tcp -- any any anywhere anywhere tcp spt:ssh
0 0 http_traffic tcp -- any any anywhere anywhere tcp spt:domain dpt:http
0 0 http_traffic tcp -- any any anywhere anywhere tcp spts:bootps:bootpc dpt:http
0 0 http_traffic tcp -- any any anywhere anywhere tcp spts:1024:65535 dpt:http
0 0 http_traffic tcp -- any any anywhere anywhere tcp spt:http dpt:domain
0 0 http_traffic tcp -- any any anywhere anywhere tcp spt:http dpts:bootps:bootpc
0 0 http_traffic tcp -- any any anywhere anywhere tcp spt:http dpts:1024:65535
0 0 other_traffic udp -- any any anywhere anywhere udp dpt:domain
0 0 other_traffic udp -- any any anywhere anywhere udp spt:domain
1 328 other_traffic udp -- any any anywhere anywhere udp dpt:bootps
0 0 other_traffic udp -- any any anywhere anywhere udp spt:bootps
0 0 other_traffic udp -- any any anywhere anywhere udp dpt:bootpc
0 0 other_traffic udp -- any any anywhere anywhere udp spt:bootpc
0 0 DROP tcp -- any any anywhere anywhere tcp dpt:0
0 0 DROP tcp -- any any anywhere anywhere tcp spt:0
0 0 DROP udp -- any any anywhere anywhere udp dpt:0
0 0 DROP udp -- any any anywhere anywhere udp spt:0
0 0 DROP tcp -- any any anywhere anywhere tcp flags:SYN,RST,ACK/SYN

Chain http_traffic (12 references)
pkts bytes target prot opt in out source destination
0 0 ACCEPT all -- any any anywhere anywhere

Chain other_traffic (12 references)
pkts bytes target prot opt in out source destination
6 3072 ACCEPT all -- any any anywhere anywhere
```

Figure 4 Checking the State of the Chains (FW)

4. SSH port Test

For this test I try to connect from the machine that has the firewall on to the machine without the firewall. It Succeeds as it lets me connect to the other machine.

```
root@datacomm:~
File Edit View Search Terminal Help
Chain OUTPUT (policy DROP 0 packets, 0 bytes)
pkts bytes target prot opt in out source destination
0 0 ssh_traffic tcp -- any any anywhere anywhere tcp dpt:ssh
0 0 ssh_traffic tcp -- any any anywhere anywhere tcp spt:ssh
0 0 http_traffic tcp -- any any anywhere anywhere tcp spt:domain dpt:http
0 0 http_traffic tcp -- any any anywhere anywhere tcp spts:bootps:bootpc dpt:http
0 0 http_traffic tcp -- any any anywhere anywhere tcp spts:1024:65535 dpt:http
0 0 http_traffic tcp -- any any anywhere anywhere tcp spt:http dpt:domain
0 0 http_traffic tcp -- any any anywhere anywhere tcp spt:http dpts:bootps:bootpc
0 0 http_traffic tcp -- any any anywhere anywhere tcp spt:http dpts:1024:65535
0 0 other_traffic udp -- any any anywhere anywhere udp dpt:domain
0 0 other_traffic udp -- any any anywhere anywhere udp spt:domain
1 328 other_traffic udp -- any any anywhere anywhere udp dpt:bootps
0 0 other_traffic udp -- any any anywhere anywhere udp spt:bootps
0 0 other_traffic udp -- any any anywhere anywhere udp dpt:bootpc
0 0 other_traffic udp -- any any anywhere anywhere udp spt:bootpc
0 0 DROP tcp -- any any anywhere anywhere tcp dpt:0
0 0 DROP tcp -- any any anywhere anywhere tcp spt:0
0 0 DROP udp -- any any anywhere anywhere udp dpt:0
0 0 DROP udp -- any any anywhere anywhere udp spt:0
0 0 DROP tcp -- any any anywhere anywhere tcp flags:SYN,RST,ACK/SYN

Chain http_traffic (12 references)
pkts bytes target prot opt in out source destination
0 0 ACCEPT all -- any any anywhere anywhere

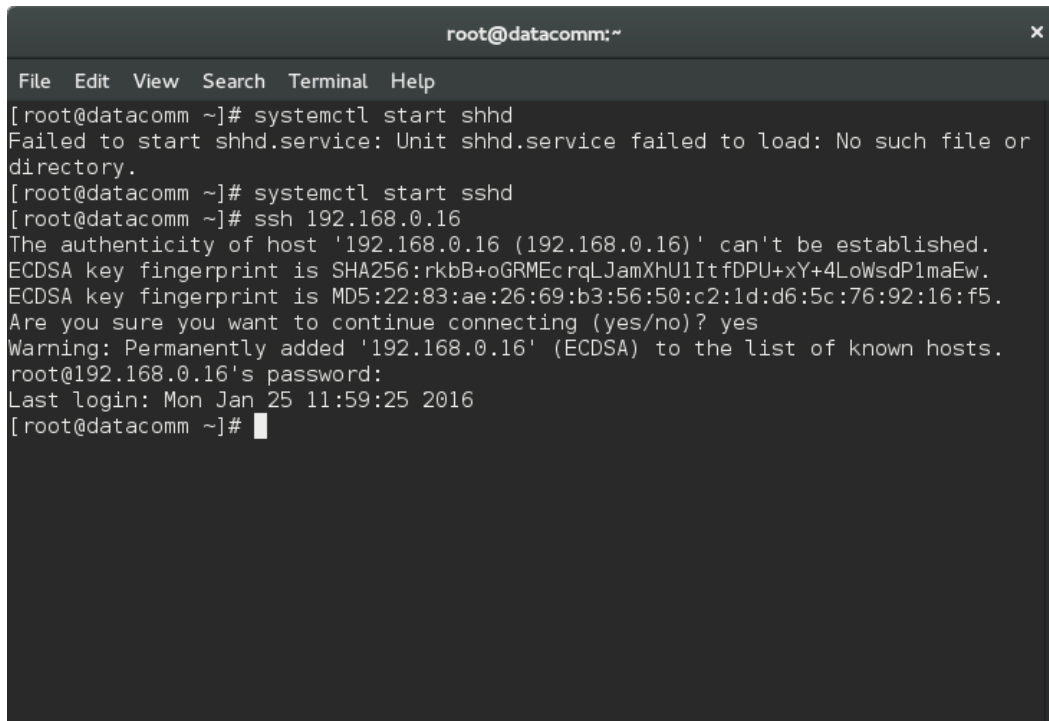
Chain other_traffic (12 references)
pkts bytes target prot opt in out source destination
6 3072 ACCEPT all -- any any anywhere anywhere

Chain ssh_traffic (4 references)
pkts bytes target prot opt in out source destination
0 0 ACCEPT all -- any any anywhere anywhere

root@datacomm Assignment 1# ssh 192.168.0.15
[root@datacomm Assignment 1]# ssh 192.168.0.15
The authenticity of host '192.168.0.15 (192.168.0.15)' can't be established.
ECDSA key fingerprint is SHA256:veCWBV29cXZ0/WbE3LT8oh260SSyflVdBR9WjTpIX00.
ECDSA key fingerprint is MD5:0e:ed:ea:96:53:54:ed:81:3d:8d:e2:3c:f6e:ac:b2:fe.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.0.15' (ECDSA) to the list of known hosts.
root@192.168.0.15's password:
Last login: Mon Jan 25 12:38:53 2016
[root@datacomm ~]#
```

Figure 5 SSH Connection (FW)

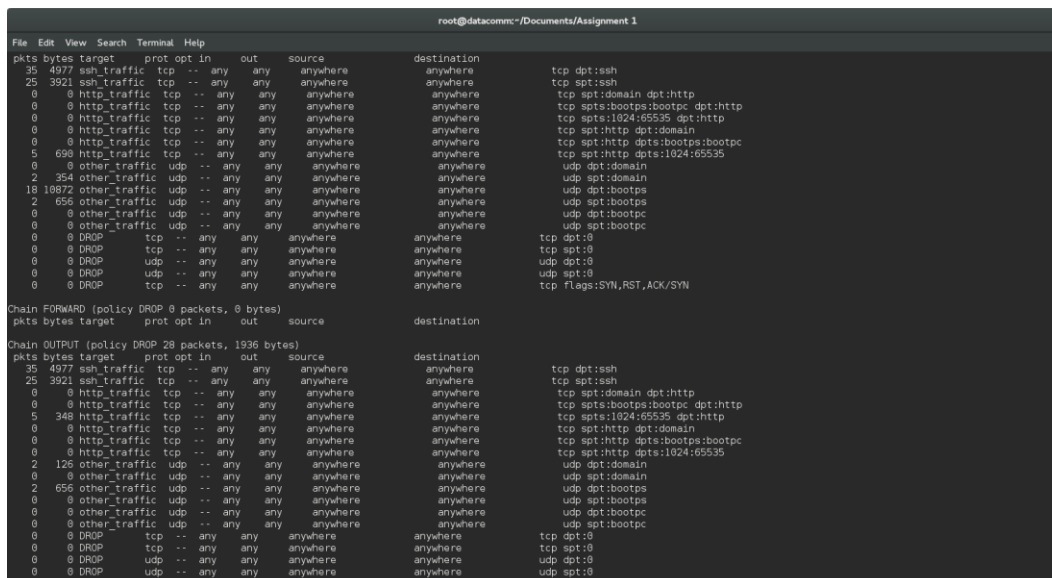
Now I try to connect to the machine with the firewall using the machine without a firewall. It lets me connect to it meaning that the port is open.



```
root@datacomm:~  
File Edit View Search Terminal Help  
[root@datacomm ~]# systemctl start sshd  
Failed to start sshd.service: Unit sshd.service failed to load: No such file or directory.  
[root@datacomm ~]# systemctl start sshd  
[root@datacomm ~]# ssh 192.168.0.16  
The authenticity of host '192.168.0.16 (192.168.0.16)' can't be established.  
ECDSA key fingerprint is SHA256:rkB+oGRMEcrqLJamXhU1ItfDPU+xY+4LowsdP1maEw.  
ECDSA key fingerprint is MD5:22:83:ae:26:69:b3:56:50:c2:1d:d6:5c:76:92:16:f5.  
Are you sure you want to continue connecting (yes/no)? yes  
Warning: Permanently added '192.168.0.16' (ECDSA) to the list of known hosts.  
root@192.168.0.16's password:  
Last login: Mon Jan 25 11:59:25 2016  
[root@datacomm ~]#
```

Figure 6 SSH Connection to the Firewall Machine (T)

Then I check the accounting chains to review that it got added to the chain. And we can see that the ssh operations right now got added to the chain.



```
root@datacomm:~/Documents/Assignment 1  
File Edit View Search Terminal Help  
pkts bytes target prot opt in out source destination  
35 4977 ssh_traffic tcp -- any any anywhere anywhere tcp dpt:ssh  
25 3921 ssh_traffic tcp -- any any anywhere anywhere tcp spt:ssh  
0 0 http_traffic tcp -- any any anywhere anywhere tcp spt:domain dpt:http  
0 0 http_traffic tcp -- any any anywhere anywhere tcp spts:bootps:bootpc dpt:http  
0 0 http_traffic tcp -- any any anywhere anywhere tcp spts:1024:65535 dpt:http  
0 0 http_traffic tcp -- any any anywhere anywhere tcp spt:http dpt:domain  
0 0 http_traffic tcp -- any any anywhere anywhere tcp spt:http dpts:bootps:bootpc  
5 698 http_traffic tcp -- any any anywhere anywhere tcp spt:http dpts:1024:65535  
0 0 other_traffic udp -- any any anywhere anywhere udp dpt:domain  
2 354 other_traffic udp -- any any anywhere anywhere udp spt:domain  
18 18872 other_traffic udp -- any any anywhere anywhere udp dpt:bootps  
2 656 other_traffic udp -- any any anywhere anywhere udp spt:bootps  
0 0 other_traffic udp -- any any anywhere anywhere udp dpt:bootpc  
0 0 other_traffic udp -- any any anywhere anywhere udp spt:bootpc  
0 0 DROP tcp -- any any anywhere anywhere tcp dpt:0  
0 0 DROP tcp -- any any anywhere anywhere tcp spt:0  
0 0 DROP udp -- any any anywhere anywhere udp dpt:0  
0 0 DROP udp -- any any anywhere anywhere udp spt:0  
0 0 DROP tcp -- any any anywhere anywhere tcp flags:SYN,RST,ACK/SYN  
  
Chain FORWARD (policy DROP 0 packets, 0 bytes)  
pkts bytes target prot opt in out source destination  
35 4977 ssh_traffic tcp -- any any anywhere anywhere tcp dpt:ssh  
25 3921 ssh_traffic tcp -- any any anywhere anywhere tcp spt:ssh  
0 0 http_traffic tcp -- any any anywhere anywhere tcp spt:domain dpt:http  
0 0 http_traffic tcp -- any any anywhere anywhere tcp spts:bootps:bootpc dpt:http  
0 0 http_traffic tcp -- any any anywhere anywhere tcp spts:1024:65535 dpt:http  
0 0 http_traffic tcp -- any any anywhere anywhere tcp spt:http dpt:domain  
0 0 http_traffic tcp -- any any anywhere anywhere tcp spt:http dpts:bootps:bootpc  
5 698 http_traffic tcp -- any any anywhere anywhere tcp spt:http dpts:1024:65535  
0 0 other_traffic udp -- any any anywhere anywhere udp dpt:domain  
2 354 other_traffic udp -- any any anywhere anywhere udp spt:domain  
18 18872 other_traffic udp -- any any anywhere anywhere udp dpt:bootps  
2 656 other_traffic udp -- any any anywhere anywhere udp spt:bootps  
0 0 other_traffic udp -- any any anywhere anywhere udp dpt:bootpc  
0 0 other_traffic udp -- any any anywhere anywhere udp spt:bootpc  
0 0 DROP tcp -- any any anywhere anywhere tcp dpt:0  
0 0 DROP tcp -- any any anywhere anywhere tcp spt:0  
0 0 DROP udp -- any any anywhere anywhere udp dpt:0  
0 0 DROP udp -- any any anywhere anywhere udp spt:0
```

Figure 7 State of the chains after the SSH Connection part 1 (FW)

```

root@datacomm:~/Documents/Assignment 1
File Edit View Search Terminal Help
0 0 other_traffic udp -- any any anywhere anywhere udp spt:bootpc
0 0 DROP tcp -- any any anywhere anywhere tcp dpt:0
0 0 DROP tcp -- any any anywhere anywhere tcp spt:0
0 0 DROP udp -- any any anywhere anywhere udp dpt:0
0 0 DROP udp -- any any anywhere anywhere udp spt:0
0 0 DROP tcp -- any any anywhere anywhere tcp flags:SYN,RST,ACK/SYN

Chain FORWARD (policy DROP 0 packets, 0 bytes)
pkts bytes target prot opt in out source destination
Chain OUTPUT (policy DROP 28 packets, 1936 bytes)
pkts bytes target prot opt in out source destination
35 4977 ssh_traffic tcp -- any any anywhere anywhere tcp dpt:ssh
25 3921 ssh_traffic tcp -- any any anywhere anywhere tcp spt:ssh
0 0 http_traffic tcp -- any any anywhere anywhere tcp spt:domain dpt:http
0 0 http_traffic tcp -- any any anywhere anywhere tcp spts:bootps:bootpc dpt:http
5 348 http_traffic tcp -- any any anywhere anywhere tcp spts:1024:65535 dpt:http
0 0 http_traffic tcp -- any any anywhere anywhere tcp spt:http dpt:domain
0 0 http_traffic tcp -- any any anywhere anywhere tcp spt:http dpts:bootps:bootpc
0 0 http_traffic tcp -- any any anywhere anywhere tcp spt:http dpts:1024:65535
2 126 other_traffic udp -- any any anywhere anywhere udp dpt:domain
0 0 other_traffic udp -- any any anywhere anywhere udp spt:domain
2 656 other_traffic udp -- any any anywhere anywhere udp dpt:bootps
0 0 other_traffic udp -- any any anywhere anywhere udp spt:bootps
0 0 other_traffic udp -- any any anywhere anywhere udp dpt:bootpc
0 0 other_traffic udp -- any any anywhere anywhere udp spt:bootpc
0 0 DROP tcp -- any any anywhere anywhere tcp dpt:0
0 0 DROP tcp -- any any anywhere anywhere tcp spt:0
0 0 DROP udp -- any any anywhere anywhere udp dpt:0
0 0 DROP udp -- any any anywhere anywhere udp spt:0
0 0 DROP tcp -- any any anywhere anywhere tcp flags:SYN,RST,ACK/SYN

Chain http_traffic (12 references)
pkts bytes target prot opt in out source destination
10 1038 ACCEPT all -- any any anywhere anywhere

Chain other_traffic (12 references)
pkts bytes target prot opt in out source destination
26 12664 ACCEPT all -- any any anywhere anywhere

Chain ssh_traffic (4 references)
pkts bytes target prot opt in out source destination
120 17796 ACCEPT all -- any any anywhere anywhere

[root@datacomm Assignment 1]#

```

Figure 8 State of the chains after the SSH Connection part 2 (FW)

Now I use hping3 to test the SSH connection between both machines. It works as it shows a 0% loss, reconfirming the previously done test.

```

root@datacomm:~/Documents/Assignment 1
File Edit View Search Terminal Help
pkts bytes target prot opt in out source destination
35 4977 ssh_traffic tcp -- any any anywhere anywhere tcp dpt:ssh
83 13329 ssh_traffic tcp -- any any anywhere anywhere tcp spt:ssh
0 0 http_traffic tcp -- any any anywhere anywhere tcp spt:domain dpt:http
0 0 http_traffic tcp -- any any anywhere anywhere tcp spts:bootps:bootpc dpt:http
5 348 http_traffic tcp -- any any anywhere anywhere tcp spts:1024:65535 dpt:http
0 0 http_traffic tcp -- any any anywhere anywhere tcp spt:http dpt:domain
0 0 http_traffic tcp -- any any anywhere anywhere tcp spt:http dpts:bootps:bootpc
7 280 http_traffic tcp -- any any anywhere anywhere tcp spt:http dpts:1024:65535
2 126 other_traffic udp -- any any anywhere anywhere udp dpt:domain
0 0 other_traffic udp -- any any anywhere anywhere udp spt:domain
3 984 other_traffic udp -- any any anywhere anywhere udp dpt:bootps
0 0 other_traffic udp -- any any anywhere anywhere udp spt:bootps
0 0 other_traffic udp -- any any anywhere anywhere udp dpt:bootpc
0 0 other_traffic udp -- any any anywhere anywhere udp spt:bootpc
0 0 DROP tcp -- any any anywhere anywhere tcp dpt:0
0 0 DROP tcp -- any any anywhere anywhere tcp spt:0
0 0 DROP udp -- any any anywhere anywhere udp dpt:0
0 0 DROP udp -- any any anywhere anywhere udp spt:0
0 0 DROP tcp -- any any anywhere anywhere tcp flags:SYN,RST,ACK/SYN

Chain http_traffic (12 references)
pkts bytes target prot opt in out source destination
24 1674 ACCEPT all -- any any anywhere anywhere

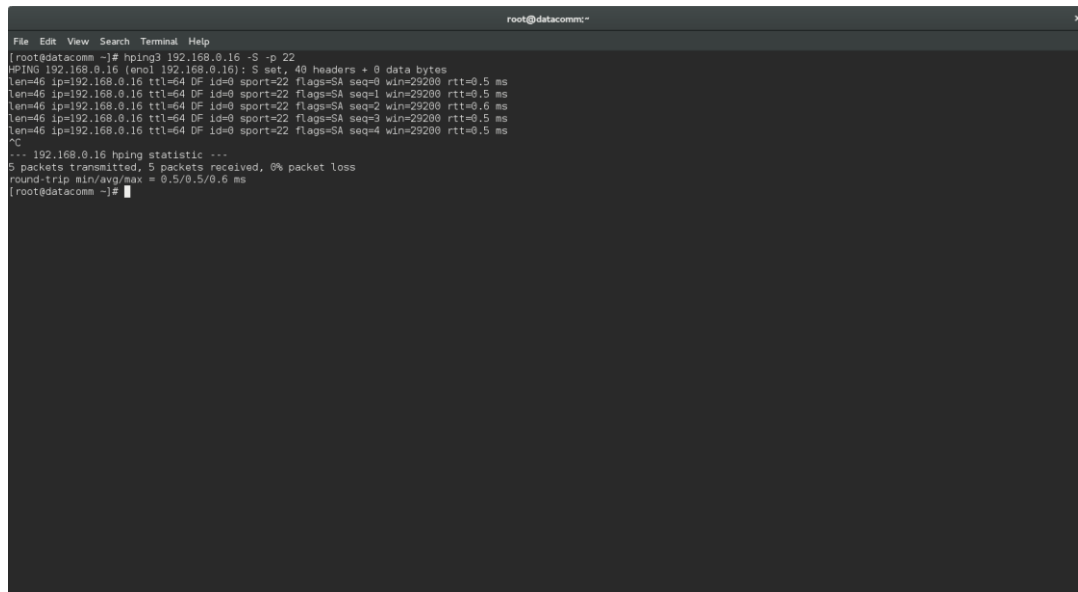
Chain other_traffic (12 references)
pkts bytes target prot opt in out source destination
41 20896 ACCEPT all -- any any anywhere anywhere

Chain ssh_traffic (4 references)
pkts bytes target prot opt in out source destination
257 34854 ACCEPT all -- any any anywhere anywhere

[root@datacomm Assignment 1]# hping3 192.168.0.15 -S -p 22
HPING 192.168.0.15 (en0 192.168.0.15): S set, 40 headers + 0 data bytes
len=46 ip=192.168.0.15 ttl=64 DF id=0 sport=22 flags=SA seq=0 win=29208 rtt=0.5 ms
len=46 ip=192.168.0.15 ttl=64 DF id=0 sport=22 flags=SA seq=1 win=29208 rtt=0.4 ms
len=46 ip=192.168.0.15 ttl=64 DF id=0 sport=22 flags=SA seq=2 win=29208 rtt=0.4 ms
len=46 ip=192.168.0.15 ttl=64 DF id=0 sport=22 flags=SA seq=3 win=29208 rtt=0.5 ms
len=46 ip=192.168.0.15 ttl=64 DF id=0 sport=22 flags=SA seq=4 win=29208 rtt=0.6 ms
^C
--- 192.168.0.15 hping statistic ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.4/0.5/0.6 ms
[root@datacomm Assignment 1]#

```

Figure 9 Use hping3 to test the SSH port (FW)

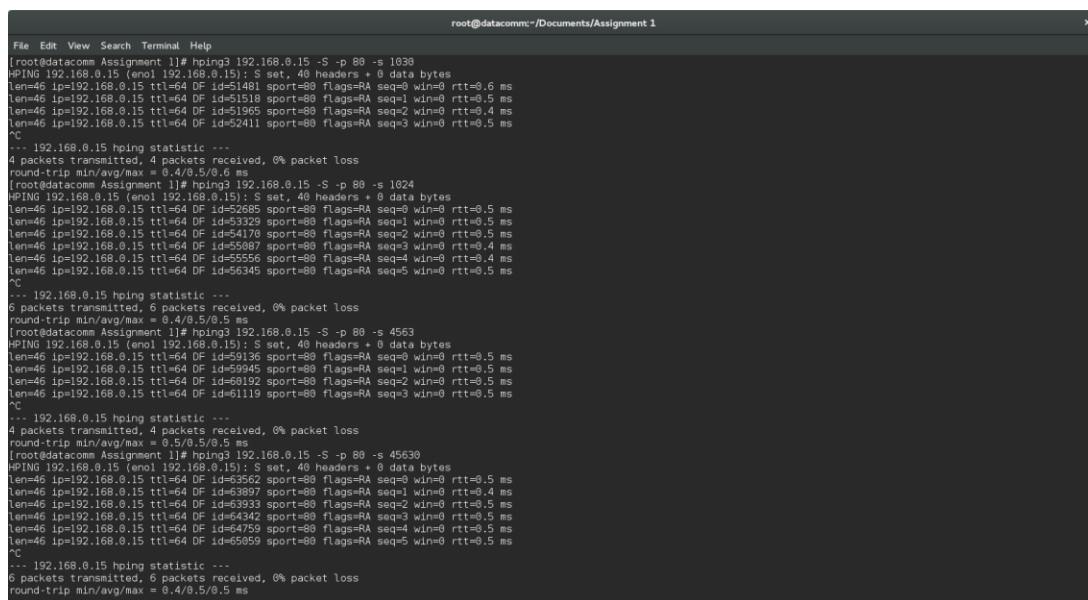


```
File Edit View Search Terminal Help
[root@datacomm ~]# hping3 192.168.0.16 -S -p 22
hPING 192.168.0.16 (enol 192.168.0.16): S set, 40 headers + 0 data bytes
len=46 ip=192.168.0.16 ttl=64 DF id=0 sport=22 flags=SA seq=0 win=29200 rtt=0.5 ms
len=46 ip=192.168.0.16 ttl=64 DF id=0 sport=22 flags=SA seq=1 win=29200 rtt=0.5 ms
len=46 ip=192.168.0.16 ttl=64 DF id=0 sport=22 flags=SA seq=2 win=29200 rtt=0.6 ms
len=46 ip=192.168.0.16 ttl=64 DF id=0 sport=22 flags=SA seq=3 win=29200 rtt=0.5 ms
len=46 ip=192.168.0.16 ttl=64 DF id=0 sport=22 flags=SA seq=4 win=29200 rtt=0.5 ms
^C
--- 192.168.0.16 hping statistic ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.5/0.5/0.6 ms
[root@datacomm ~]#
```

Figure 10 Use hping3 to test the SSH port (T)

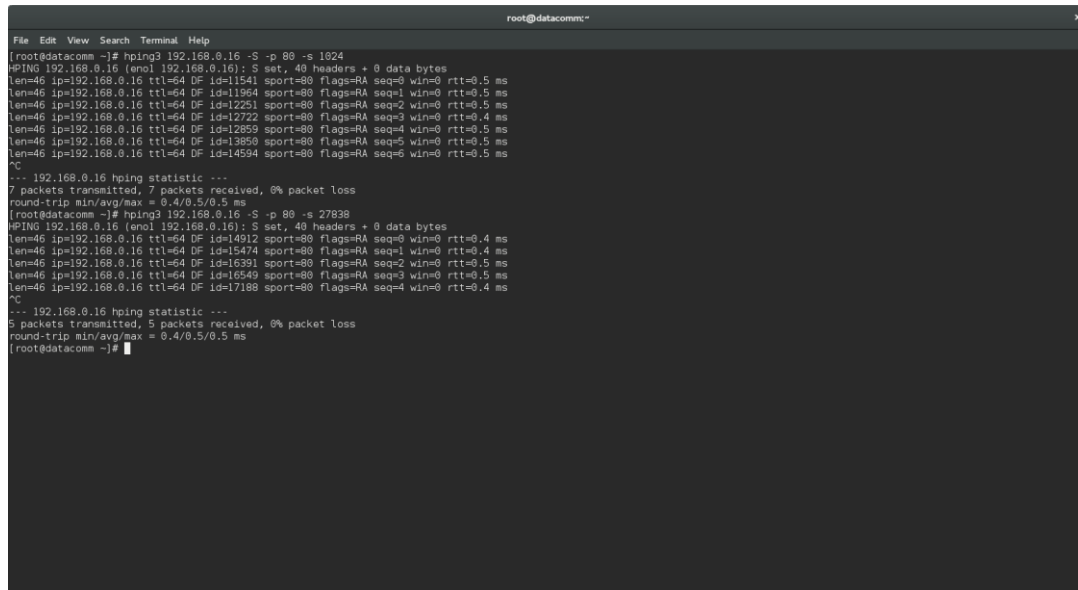
5. HTTP port test

For the HTTP port test first we are going to test the connectivity of http from ports above 1024, since we allow those ports, they work as they show a 0% packet loss.



```
File Edit View Search Terminal Help
[root@datacomm Assignment 1]# hping3 192.168.0.15 -S -p 80 -s 1030
hPING 192.168.0.15 (enol 192.168.0.15): S set, 40 headers + 0 data bytes
len=46 ip=192.168.0.15 ttl=64 DF id=51481 sport=80 flags=RA seq=0 win=0 rtt=0.6 ms
len=46 ip=192.168.0.15 ttl=64 DF id=51518 sport=80 flags=RA seq=1 win=0 rtt=0.5 ms
len=46 ip=192.168.0.15 ttl=64 DF id=51985 sport=80 flags=RA seq=2 win=0 rtt=0.4 ms
len=46 ip=192.168.0.15 ttl=64 DF id=52411 sport=80 flags=RA seq=3 win=0 rtt=0.5 ms
^C
--- 192.168.0.15 hping statistic ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 0.4/0.5/0.6 ms
[root@datacomm Assignment 1]# hping3 192.168.0.15 -S -p 80 -s 1024
hPING 192.168.0.15 (enol 192.168.0.15): S set, 40 headers + 0 data bytes
len=46 ip=192.168.0.15 ttl=64 DF id=52685 sport=80 flags=RA seq=0 win=0 rtt=0.5 ms
len=46 ip=192.168.0.15 ttl=64 DF id=53329 sport=80 flags=RA seq=1 win=0 rtt=0.5 ms
len=46 ip=192.168.0.15 ttl=64 DF id=54176 sport=80 flags=RA seq=2 win=0 rtt=0.5 ms
len=46 ip=192.168.0.15 ttl=64 DF id=55087 sport=80 flags=RA seq=3 win=0 rtt=0.4 ms
len=46 ip=192.168.0.15 ttl=64 DF id=55556 sport=80 flags=RA seq=4 win=0 rtt=0.4 ms
len=46 ip=192.168.0.15 ttl=64 DF id=56345 sport=80 flags=RA seq=5 win=0 rtt=0.5 ms
^C
--- 192.168.0.15 hping statistic ---
6 packets transmitted, 6 packets received, 0% packet loss
round-trip min/avg/max = 0.4/0.5/0.5 ms
[root@datacomm Assignment 1]# hping3 192.168.0.15 -S -p 80 -s 4563
hPING 192.168.0.15 (enol 192.168.0.15): S set, 40 headers + 0 data bytes
len=46 ip=192.168.0.15 ttl=64 DF id=59136 sport=80 flags=RA seq=0 win=0 rtt=0.5 ms
len=46 ip=192.168.0.15 ttl=64 DF id=59945 sport=80 flags=RA seq=1 win=0 rtt=0.5 ms
len=46 ip=192.168.0.15 ttl=64 DF id=60192 sport=80 flags=RA seq=2 win=0 rtt=0.5 ms
len=46 ip=192.168.0.15 ttl=64 DF id=61119 sport=80 flags=RA seq=3 win=0 rtt=0.5 ms
^C
--- 192.168.0.15 hping statistic ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 0.5/0.5/0.5 ms
[root@datacomm Assignment 1]# hping3 192.168.0.15 -S -p 80 -s 45630
hPING 192.168.0.15 (enol 192.168.0.15): S set, 40 headers + 0 data bytes
len=46 ip=192.168.0.15 ttl=64 DF id=63562 sport=80 flags=RA seq=0 win=0 rtt=0.5 ms
len=46 ip=192.168.0.15 ttl=64 DF id=63897 sport=80 flags=RA seq=1 win=0 rtt=0.4 ms
len=46 ip=192.168.0.15 ttl=64 DF id=63933 sport=80 flags=RA seq=2 win=0 rtt=0.5 ms
len=46 ip=192.168.0.15 ttl=64 DF id=64342 sport=80 flags=RA seq=3 win=0 rtt=0.5 ms
len=46 ip=192.168.0.15 ttl=64 DF id=64759 sport=80 flags=RA seq=4 win=0 rtt=0.5 ms
len=46 ip=192.168.0.15 ttl=64 DF id=65059 sport=80 flags=RA seq=5 win=0 rtt=0.5 ms
^C
--- 192.168.0.15 hping statistic ---
6 packets transmitted, 6 packets received, 0% packet loss
round-trip min/avg/max = 0.4/0.5/0.5 ms
```

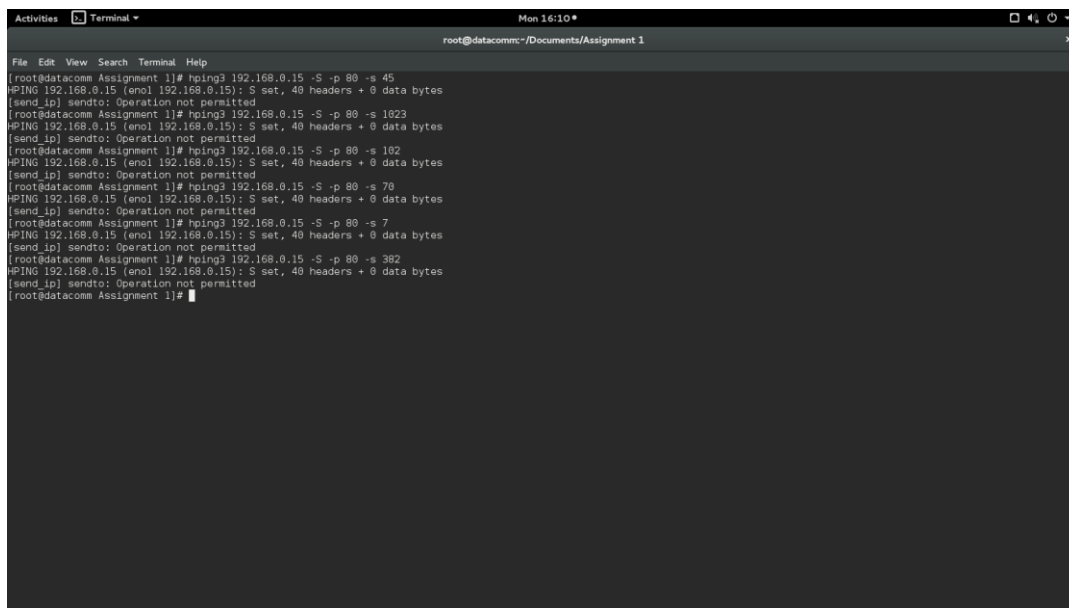
Figure 11 Use hping3 to test HTTP port from a port above 1024 (FW)



```
root@datacomm:~# hping3 192.168.0.16 -S -p 88 -s 1924
HPING 192.168.0.16 (enol 192.168.0.16): S set, 40 headers + 0 data bytes
len=46 ip=192.168.0.16 ttl=64 DF id=11541 sport=88 flags=RA seq=0 win=0 rtt=0.5 ms
len=46 ip=192.168.0.16 ttl=64 DF id=11964 sport=88 flags=RA seq=1 win=0 rtt=0.5 ms
len=46 ip=192.168.0.16 ttl=64 DF id=12251 sport=88 flags=RA seq=2 win=0 rtt=0.5 ms
len=46 ip=192.168.0.16 ttl=64 DF id=12722 sport=88 flags=RA seq=3 win=0 rtt=0.4 ms
len=46 ip=192.168.0.16 ttl=64 DF id=12859 sport=88 flags=RA seq=4 win=0 rtt=0.5 ms
len=46 ip=192.168.0.16 ttl=64 DF id=13850 sport=88 flags=RA seq=5 win=0 rtt=0.5 ms
len=46 ip=192.168.0.16 ttl=64 DF id=14594 sport=88 flags=RA seq=6 win=0 rtt=0.5 ms
^C
-- 192.168.0.16 hping statistic --
7 packets transmitted, 7 packets received, 0% packet loss
round-trip min/avg/max = 0.4/0.5/0.5 ms
root@datacomm:~# hping3 192.168.0.16 -S -p 88 -s 27899
HPING 192.168.0.16 (enol 192.168.0.16): S set, 40 headers + 0 data bytes
len=46 ip=192.168.0.16 ttl=64 DF id=14912 sport=88 flags=RA seq=0 win=0 rtt=0.4 ms
len=46 ip=192.168.0.16 ttl=64 DF id=15474 sport=88 flags=RA seq=1 win=0 rtt=0.4 ms
len=46 ip=192.168.0.16 ttl=64 DF id=16391 sport=88 flags=RA seq=2 win=0 rtt=0.5 ms
len=46 ip=192.168.0.16 ttl=64 DF id=16549 sport=88 flags=RA seq=3 win=0 rtt=0.5 ms
len=46 ip=192.168.0.16 ttl=64 DF id=17188 sport=88 flags=RA seq=4 win=0 rtt=0.4 ms
^C
-- 192.168.0.16 hping statistic --
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.4/0.5/0.5 ms
root@datacomm:~#
```

Figure 12 Use hping3 to test HTTP port from a port above 1024 (T)

For the second test, we are going to test the connectivity of http from ports below 1024, since we blocked those ports, they don't work. And either we get a 100% loss since those ports are blocked or we don't have permission to do the operation.



```
root@datacomm:~/Documents/Assignment 1# hping3 192.168.0.15 -S -p 80 -s 45
HPING 192.168.0.15 (enol 192.168.0.15): S set, 40 headers + 0 data bytes
[send_ip] sendto: Operation not permitted
root@datacomm:~/Documents/Assignment 1# hping3 192.168.0.15 -S -p 80 -s 1023
HPING 192.168.0.15 (enol 192.168.0.15): S set, 40 headers + 0 data bytes
[send_ip] sendto: Operation not permitted
root@datacomm:~/Documents/Assignment 1# hping3 192.168.0.15 -S -p 80 -s 102
HPING 192.168.0.15 (enol 192.168.0.15): S set, 40 headers + 0 data bytes
[send_ip] sendto: Operation not permitted
root@datacomm:~/Documents/Assignment 1# hping3 192.168.0.15 -S -p 80 -s 70
HPING 192.168.0.15 (enol 192.168.0.15): S set, 40 headers + 0 data bytes
[send_ip] sendto: Operation not permitted
root@datacomm:~/Documents/Assignment 1# hping3 192.168.0.15 -S -p 80 -s 7
HPING 192.168.0.15 (enol 192.168.0.15): S set, 40 headers + 0 data bytes
[send_ip] sendto: Operation not permitted
root@datacomm:~/Documents/Assignment 1#
```

Figure 13 Use hping3 to test HTTP port from a port below 1024 (FW)

```
root@datacomm~  
File Edit View Search Terminal Help  
[root@datacomm ~]# hping3 192.168.0.16 -S -p 80 -s 102  
HPING 192.168.0.16 (enl 192.168.0.16): S set, 40 headers + 0 data bytes  
^C  
--- 192.168.0.16 hping statistic ---  
6 packets transmitted, 0 packets received, 100% packet loss  
round-trip min/avg/max = 0.0/0.0/0.0 ms  
[root@datacomm ~]# hping3 192.168.0.16 -S -p 80 -s 1000  
HPING 192.168.0.16 (enl 192.168.0.16): S set, 40 headers + 0 data bytes  
^C  
--- 192.168.0.16 hping statistic ---  
9 packets transmitted, 0 packets received, 100% packet loss  
round-trip min/avg/max = 0.0/0.0/0.0 ms  
[root@datacomm ~]# hping3 192.168.0.16 -S -p 80 -s 80  
HPING 192.168.0.16 (enl 192.168.0.16): S set, 40 headers + 0 data bytes  
^C  
--- 192.168.0.16 hping statistic ---  
4 packets transmitted, 0 packets received, 100% packet loss  
round-trip min/avg/max = 0.0/0.0/0.0 ms  
[root@datacomm ~]# hping3 192.168.0.16 -S -p 80 -s 457  
HPING 192.168.0.16 (enl 192.168.0.16): S set, 40 headers + 0 data bytes  
^C  
--- 192.168.0.16 hping statistic ---  
37 packets transmitted, 0 packets received, 100% packet loss  
round-trip min/avg/max = 0.0/0.0/0.0 ms  
[root@datacomm ~]# hping3 192.168.0.16 -S -p 80 -s 369  
HPING 192.168.0.16 (enl 192.168.0.16): S set, 40 headers + 0 data bytes  
^C  
--- 192.168.0.16 hping statistic ---  
18 packets transmitted, 0 packets received, 100% packet loss  
round-trip min/avg/max = 0.0/0.0/0.0 ms  
[root@datacomm ~]#
```

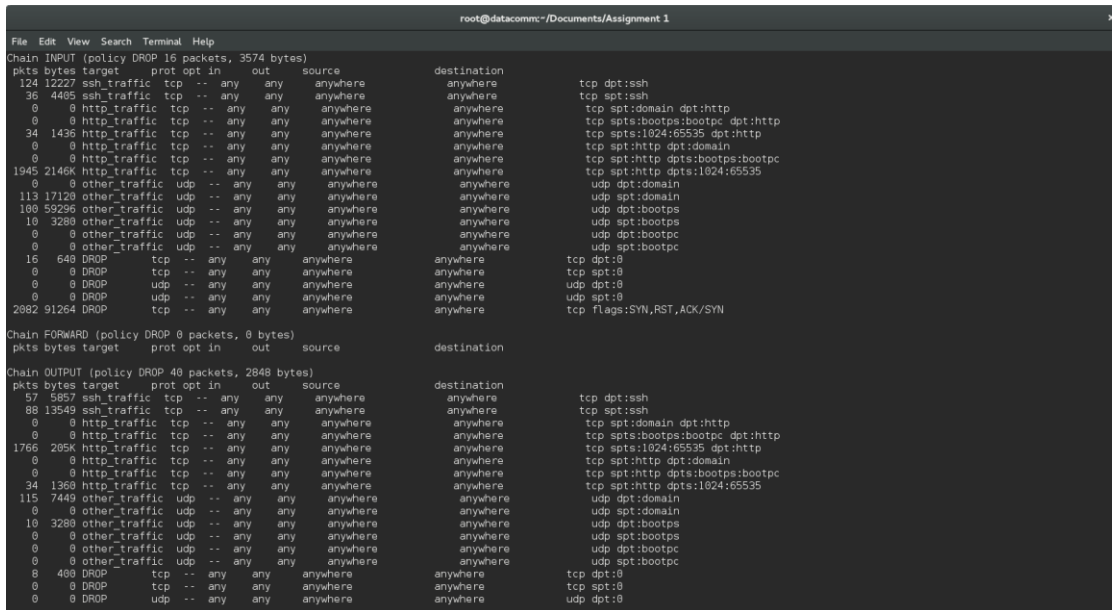
Figure 14 Figure 13 Use hping3 to test HTTP port from a port below 1024 (T)

Lastly we are going to test going to a website, in this case cnn.com since it uses the http protocol, and it works fine.

The screenshot shows a dual-pane view. On the left, a Firefox browser window displays the CNN homepage with a headline about Hillary Clinton's lead over Bernie Sanders. On the right, a terminal window shows the output of a network analysis tool, likely Wireshark, displaying a list of network packets. The packets are categorized by protocol (TCP, UDP, ICMP) and show details like source/destination ports and flags. The terminal output includes a summary of the traffic chains, such as 'Chain http_traffic (12 references)' and 'Chain other_traffic (12 references)'. The terminal prompt at the bottom indicates the user is at the root@datacomm machine.

Figure 15 Website visit

When we check the accounting chains, we can see all the transmissions to HTTP ports, every HTTP successful traffic is added to the http traffic account chain. In addition we can see that we are blocking any SYN related message that is not authorized.

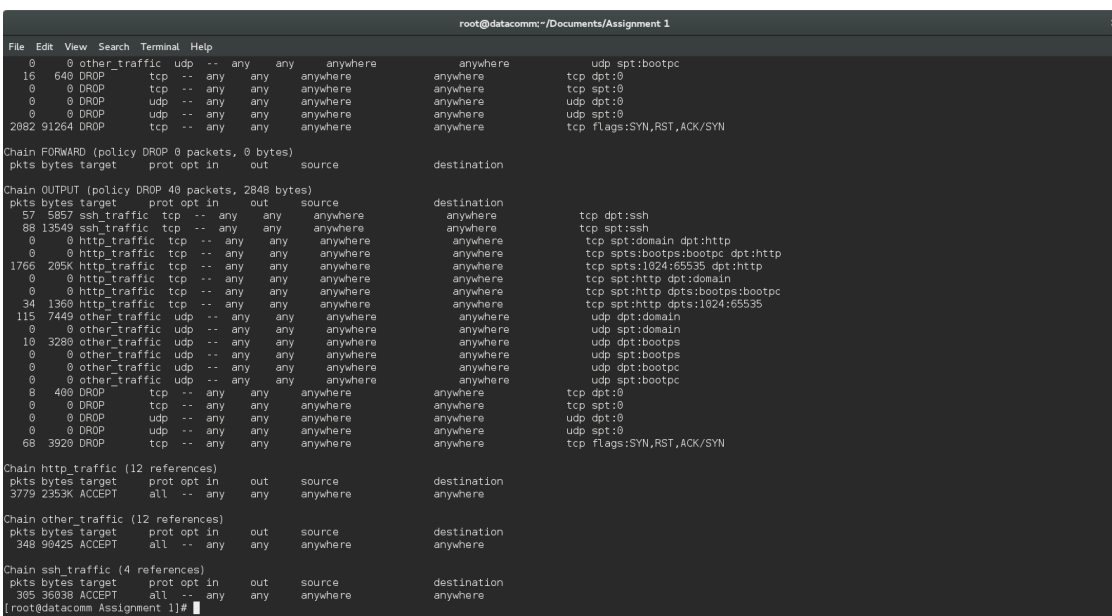


```
root@datacomm:~/Documents/Assignment 1
File Edit View Search Terminal Help
Chain INPUT (policy DROP 16 packets, 3574 bytes)
pkts bytes target prot opt in out source destination
124 12227 ssh_traffic tcp -- any any anywhere anywhere tcp dpt:ssh
96 4485 ssh_traffic tcp -- any any anywhere anywhere tcp spt:ssh
0 0 http_traffic tcp -- any any anywhere anywhere tcp spt:domain dpt:http
0 0 http_traffic tcp -- any any anywhere anywhere tcp spts:bootps:bootpc dpt:http
34 1436 http_traffic tcp -- any any anywhere anywhere tcp spts:1024:65535 dpt:http
0 0 http_traffic tcp -- any any anywhere anywhere tcp spt:http dpt:domain
0 0 http_traffic tcp -- any any anywhere anywhere tcp spt:http dpts:bootps:bootpc
1945 2146K http_traffic tcp -- any any anywhere anywhere tcp spt:http dpts:1024:65535
0 0 other_traffic udp -- any any anywhere anywhere udp dpt:domain
113 17120 other_traffic udp -- any any anywhere anywhere udp spt:domain
108 59295 other_traffic udp -- any any anywhere anywhere udp dpt:bootps
10 3280 other_traffic udp -- any any anywhere anywhere udp spt:bootps
0 0 other_traffic udp -- any any anywhere anywhere udp dpt:bootpc
0 0 other_traffic udp -- any any anywhere anywhere udp spt:bootpc
16 640 DROP tcp -- any any anywhere anywhere tcp dpt:0
0 0 DROP tcp -- any any anywhere anywhere tcp spt:0
0 0 DROP udp -- any any anywhere anywhere udp dpt:0
0 0 DROP udp -- any any anywhere anywhere udp spt:0
2082 91264 DROP tcp -- any any anywhere anywhere tcp flags:SYN,RST,ACK:SYN

Chain FORWARD (policy DROP 0 packets, 0 bytes)
pkts bytes target prot opt in out source destination

Chain OUTPUT (policy DROP 40 packets, 2848 bytes)
pkts bytes target prot opt in out source destination
57 5857 ssh_traffic tcp -- any any anywhere anywhere tcp dpt:ssh
88 13549 ssh_traffic tcp -- any any anywhere anywhere tcp spt:ssh
0 0 http_traffic tcp -- any any anywhere anywhere tcp spt:domain dpt:http
0 0 http_traffic tcp -- any any anywhere anywhere tcp spts:bootps:bootpc dpt:http
1766 205K http_traffic tcp -- any any anywhere anywhere tcp spts:1024:65535 dpt:http
0 0 http_traffic tcp -- any any anywhere anywhere tcp spt:http dpt:domain
34 1360 http_traffic tcp -- any any anywhere anywhere tcp spt:http dpts:bootps:bootpc
115 7449 other_traffic udp -- any any anywhere anywhere udp dpt:domain
0 0 other_traffic udp -- any any anywhere anywhere udp spt:domain
10 3280 other_traffic udp -- any any anywhere anywhere udp dpt:bootps
0 0 other_traffic udp -- any any anywhere anywhere udp spt:bootps
0 0 other_traffic udp -- any any anywhere anywhere udp dpt:bootpc
0 0 other_traffic udp -- any any anywhere anywhere udp spt:bootpc
8 480 DROP tcp -- any any anywhere anywhere tcp dpt:0
0 0 DROP tcp -- any any anywhere anywhere tcp spt:0
0 0 DROP udp -- any any anywhere anywhere udp dpt:0
0 0 DROP udp -- any any anywhere anywhere udp spt:0
2082 91264 DROP tcp -- any any anywhere anywhere tcp flags:SYN,RST,ACK:SYN
```

Figure 16 Chain after visiting a website part 1 (FW)



```
root@datacomm:~/Documents/Assignment 1
File Edit View Search Terminal Help
0 0 other_traffic udp -- any any anywhere anywhere udp spt:bootpc
16 640 DROP tcp -- any any anywhere anywhere tcp dpt:0
0 0 DROP tcp -- any any anywhere anywhere tcp spt:0
0 0 DROP udp -- any any anywhere anywhere udp dpt:0
0 0 DROP udp -- any any anywhere anywhere udp spt:0
2082 91264 DROP tcp -- any any anywhere anywhere tcp flags:SYN,RST,ACK:SYN

Chain FORWARD (policy DROP 0 packets, 0 bytes)
pkts bytes target prot opt in out source destination

Chain OUTPUT (policy DROP 40 packets, 2848 bytes)
pkts bytes target prot opt in out source destination
57 5857 ssh_traffic tcp -- any any anywhere anywhere tcp dpt:ssh
88 13549 ssh_traffic tcp -- any any anywhere anywhere tcp spt:ssh
0 0 http_traffic tcp -- any any anywhere anywhere tcp spt:domain dpt:http
0 0 http_traffic tcp -- any any anywhere anywhere tcp spts:bootps:bootpc dpt:http
1766 205K http_traffic tcp -- any any anywhere anywhere tcp spts:1024:65535 dpt:http
0 0 http_traffic tcp -- any any anywhere anywhere tcp spt:http dpt:domain
34 1360 http_traffic tcp -- any any anywhere anywhere tcp spt:http dpts:bootps:bootpc
115 7449 other_traffic udp -- any any anywhere anywhere udp dpt:domain
0 0 other_traffic udp -- any any anywhere anywhere udp spt:domain
10 3280 other_traffic udp -- any any anywhere anywhere udp dpt:bootps
0 0 other_traffic udp -- any any anywhere anywhere udp spt:bootps
0 0 other_traffic udp -- any any anywhere anywhere udp dpt:bootpc
0 0 other_traffic udp -- any any anywhere anywhere udp spt:bootpc
8 480 DROP tcp -- any any anywhere anywhere tcp dpt:0
0 0 DROP tcp -- any any anywhere anywhere tcp spt:0
0 0 DROP udp -- any any anywhere anywhere udp dpt:0
0 0 DROP udp -- any any anywhere anywhere udp spt:0
68 3920 DROP tcp -- any any anywhere anywhere tcp flags:SYN,RST,ACK:SYN

Chain http_traffic (12 references)
pkts bytes target prot opt in out source destination
3779 2353K ACCEPT all -- any any anywhere anywhere

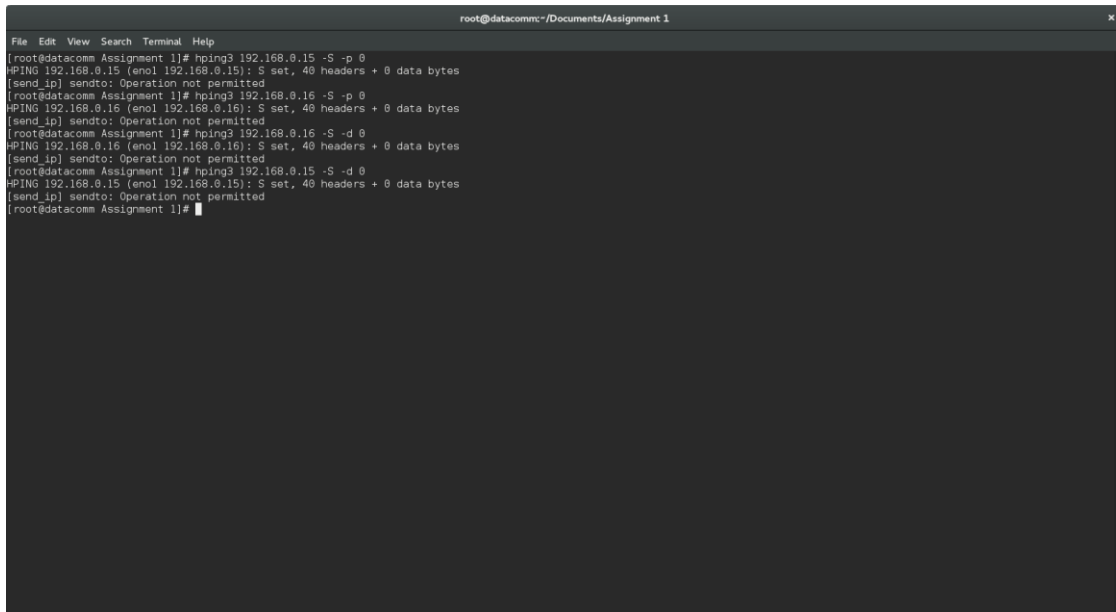
Chain other_traffic (12 references)
pkts bytes target prot opt in out source destination
348 98425 ACCEPT all -- any any anywhere anywhere

Chain ssh_traffic (4 references)
pkts bytes target prot opt in out source destination
305 36838 ACCEPT all -- any any anywhere anywhere
[root@datacomm Assignment 1]#
```

Figure 17 Chain after visiting a website part 2 (FW)

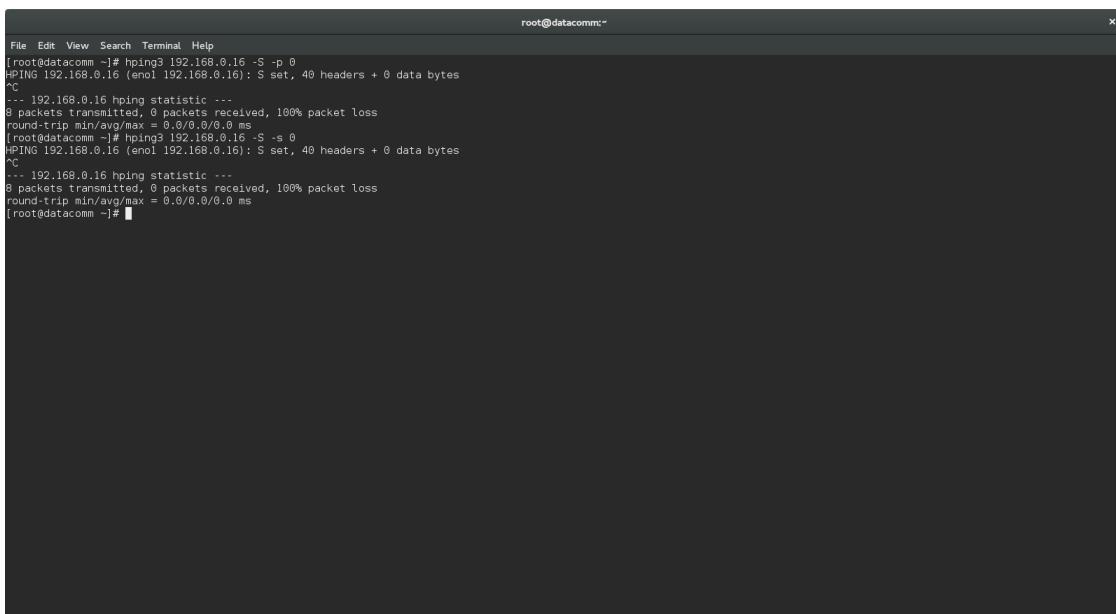
6. Port 0 test

For the port 0 test we use hping3 to try reaching the port. It doesn't work as the results show that either we don't have permission to do it or there was a 100% packet loss.



```
root@datacomm:~/Documents/Assignment 1
File Edit View Search Terminal Help
[root@datacomm Assignment 1]# hping3 192.168.0.15 -S -p 0
HPING 192.168.0.15 (enol 192.168.0.15): S set, 40 headers + 0 data bytes
[send_ip] sendto: Operation not permitted
[root@datacomm Assignment 1]# hping3 192.168.0.16 -S -p 0
HPING 192.168.0.16 (enol 192.168.0.16): S set, 40 headers + 0 data bytes
[send_ip] sendto: Operation not permitted
[root@datacomm Assignment 1]# hping3 192.168.0.16 -S -d 0
HPING 192.168.0.16 (enol 192.168.0.16): S set, 40 headers + 0 data bytes
[send_ip] sendto: Operation not permitted
[root@datacomm Assignment 1]# hping3 192.168.0.15 -S -d 0
HPING 192.168.0.15 (enol 192.168.0.15): S set, 40 headers + 0 data bytes
[send_ip] sendto: Operation not permitted
[root@datacomm Assignment 1]#
```

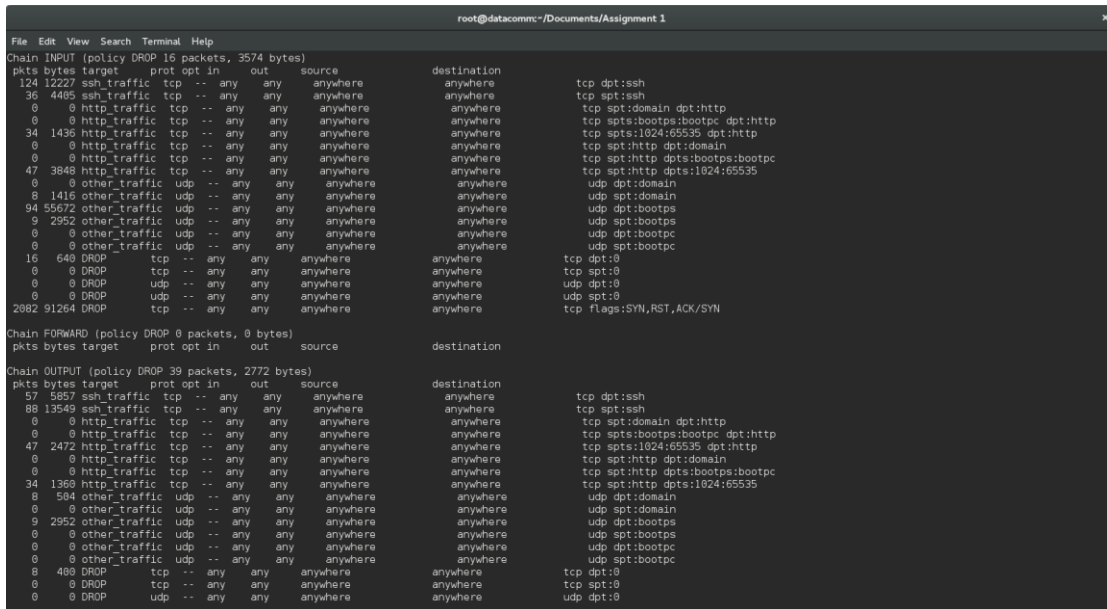
Figure 18 Use hping3 to test the port 0 (FW)



```
root@datacomm:~
File Edit View Search Terminal Help
[root@datacomm ~]# hping3 192.168.0.16 -S -p 0
HPING 192.168.0.16 (enol 192.168.0.16): S set, 40 headers + 0 data bytes
^C
--- 192.168.0.16 hping statistic ---
8 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
[root@datacomm ~]# hping3 192.168.0.16 -S -s 0
HPING 192.168.0.16 (enol 192.168.0.16): S set, 40 headers + 0 data bytes
^C
--- 192.168.0.16 hping statistic ---
8 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
[root@datacomm ~]#
```

Figure 19 Use hping3 to test the port 0 (T)

Here we can see the results of the port 0 attempts, and we can notice that the packets were dropped.



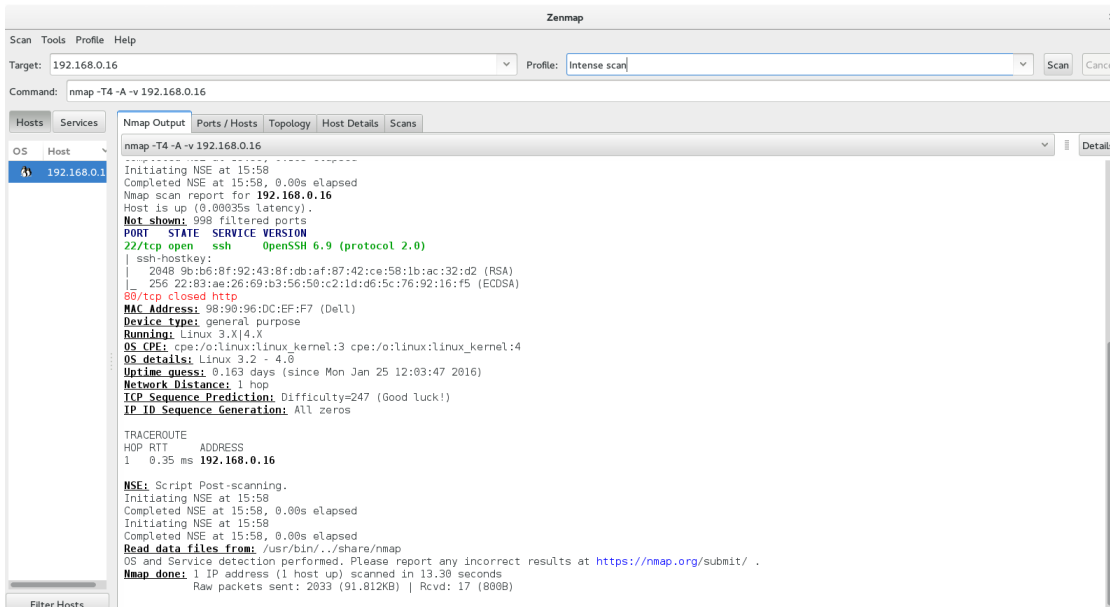
The image shows a Wireshark packet capture window titled "root@datacomm:~/Documents/Assignment 1". It displays three packet lists: Chain INPUT, Chain FORWARD, and Chain OUTPUT. The Chain INPUT list shows various traffic types including ssh, http, and other traffic, with some packets being dropped. The Chain FORWARD list shows similar traffic. The Chain OUTPUT list shows traffic being sent out, including ssh, http, and other traffic. The packet details pane on the right shows the structure of the selected packets, including Ethernet II, Internet Protocol Version 4, and various application-specific protocols like SSH, HTTP, and BOOTPC.

Chain INPUT (policy DROP 16 packets, 3574 bytes)	Chain FORWARD (policy DROP 0 packets, 0 bytes)	Chain OUTPUT (policy DROP 39 packets, 2772 bytes)
pks bytes target prot opt in out source destination	pks bytes target prot opt in out source destination	pks bytes target prot opt in out source destination
124 12227 ssh_traffic tcp -- any any anywhere anywhere tcp dpt:ssh		57 5857 ssh_traffic tcp -- any any anywhere anywhere tcp dpt:ssh
36 4485 ssh_traffic tcp -- any any anywhere anywhere tcp spt:ssh		88 1549 ssh_traffic tcp -- any any anywhere anywhere tcp spt:ssh
0 0 http_traffic tcp -- any any anywhere anywhere tcp spt:domain dpt:http		0 0 http_traffic tcp -- any any anywhere anywhere tcp spt:domain dpt:http
0 0 http_traffic tcp -- any any anywhere anywhere tcp spts:bootps:bootpc dpt:http		0 0 http_traffic tcp -- any any anywhere anywhere tcp spts:bootps:bootpc dpt:http
34 1436 http_traffic tcp -- any any anywhere anywhere tcp spts:1024:65535 dpt:http		47 2472 http_traffic tcp -- any any anywhere anywhere tcp spts:1024:65535 dpt:http
0 0 http_traffic tcp -- any any anywhere anywhere tcp spt:http dpt:domain		0 0 http_traffic tcp -- any any anywhere anywhere tcp spt:http dpt:domain
0 0 http_traffic tcp -- any any anywhere anywhere tcp spt:http dpts:bootps:bootpc		0 0 http_traffic tcp -- any any anywhere anywhere tcp spt:http dpts:bootps:bootpc
47 3848 http_traffic tcp -- any any anywhere anywhere tcp spt:http dpts:1024:65535		34 1360 http_traffic tcp -- any any anywhere anywhere tcp spt:http dpts:1024:65535
0 0 other_traffic udp -- any any anywhere anywhere udp dpt:domain		0 584 other_traffic udp -- any any anywhere anywhere udp dpt:domain
8 1416 other_traffic udp -- any any anywhere anywhere udp spt:domain		0 0 other_traffic udp -- any any anywhere anywhere udp spt:domain
94 55672 other_traffic udp -- any any anywhere anywhere udp dpt:bootps		0 2952 other_traffic udp -- any any anywhere anywhere udp dpt:bootps
9 2952 other_traffic udp -- any any anywhere anywhere udp spt:bootps		0 0 other_traffic udp -- any any anywhere anywhere udp spt:bootps
0 0 other_traffic udp -- any any anywhere anywhere udp dpt:bootpc		0 0 other_traffic udp -- any any anywhere anywhere udp dpt:bootpc
0 0 other_traffic udp -- any any anywhere anywhere udp spt:bootpc		0 0 other_traffic udp -- any any anywhere anywhere udp spt:bootpc
16 640 DROP tcp -- any any anywhere anywhere tcp dpt:0		0 480 DROP tcp -- any any anywhere anywhere tcp dpt:0
0 0 DROP tcp -- any any anywhere anywhere tcp spt:0		0 0 DROP tcp -- any any anywhere anywhere tcp spt:0
0 0 DROP udp -- any any anywhere anywhere udp dpt:0		0 0 DROP udp -- any any anywhere anywhere udp dpt:0
0 0 DROP udp -- any any anywhere anywhere udp spt:0		0 0 DROP udp -- any any anywhere anywhere udp spt:0
2982 91264 DROP tcp -- any any anywhere anywhere tcp flags:SYN,RST,ACK,SYN		

Figure 20 Results after port 0 test

7. Nmap

Additionally to these tests, we can use Nmap to see which ports are open. We can see that Nmap is detecting both port 80 and 22, but in this case port 80 is shown closed as I wasn't running a web server but otherwise is detected.



The image shows the Nmap application interface. The target is 192.168.0.16, and the profile is Intense scan. The command is nmap -T4 -A -v 192.168.0.16. The Nmap Output pane shows the results of the scan, including the host's IP address, OS, and open ports. The output indicates that port 22 is open (SSH) and port 80 is closed (HTTP). The scan was completed at 15:58, and the host is up with a latency of 0.00035s.

Hosts	Services	Nmap Output	Ports / Hosts	Topology	Host Details	Scans
192.168.0.16		<p>Initiating NSE at 15:58 Completed NSE at 15:58, 0.00s elapsed Nmap scan report for 192.168.0.16 Host is up (0.00035s latency). Not shown: 998 filtered ports PORT STATE SERVICE VERSION 22/tcp open ssh OpenSSH 6.9 (protocol 2.0) 80/tcp closed http MAC Address: 98:90:96:DC:EF:F7 (Dell) Device type: general purpose Running: Linux 3.X(4.X) OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4 OS details: Linux 3.2 - 4.0 Uptime guess: 0.163 days (since Mon Jan 25 12:03:47 2016) Network Distance: 1 hop TCP Sequence Prediction: Difficulty=247 (Good luck!) IP ID Sequence Generation: All zeros</p> <p>TRACEROUTE Hop RTT ADDRESS 1 0.35 ms 192.168.0.16</p> <p>NSE: Script Post-scanning. Initiating NSE at 15:58 Completed NSE at 15:58, 0.00s elapsed Initiating NSE at 15:58 Completed NSE at 15:58, 0.00s elapsed Read data files from: /usr/bin/./share/nmap OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/. Nmap done: 1 IP address (1 host up) scanned in 13.30 seconds Raw packets sent: 2033 (91.812KB) Rcvd: 17 (800B)</p>				

Figure 21 Nmap results (T)