

Testing:

The testing during the implementation of the script was not documented. After completion it was tested using hping3 as well as some other tools.

TEST LIST

Test #	Test Description / Tool Used	Excepted Result	Pass / Fail	Figure
1	Verify that port 22(ssh) and 80(www) are listening / nmap	Ports should be open	Pass	Fig 1
2	Verify that ssh works / ssh command	Connection should be established	Pass	Fig 2
3	Test for Inbound ssh packets / hping3	Firewall should allow it	Pass	Fig 3
4	Test for Outbound ssh packets / hping3	Firewall should allow it	Pass	Fig 4
5	Test for Inbound http packets with source port > 1024 / hping3	Firewall should allow it	Pass	Fig 5
6	Test for Inbound http packets with source port < 1024 / hping3	Firewall should drop it	Pass	Fig 6
7	Test for Outbound http packets / hping3	Firewall should allow it	Pass	Fig 7
8	Test for Inbound packets to reserved port 0 / hping3	Firewall should drop it	Pass	Fig 8
9	Test for Outbound packets to reserved port 0 / hping3	Firewall should drop it	Pass	Fig 9
10	Test for Inbound SYN packets / hping3	Firewall should drop it	Pass	Fig 10
11	Test for Inbound/Outbound DNS / web browsing	It should resolve address	Pass	Fig 11
12	Check for Inbound/Outbound DNS / dhclient	It should lease an ip address	Pass	Fig 12
13	Check for Inbound ICMPs / hping3	Firewall should drop them	Pass	Fig 13
14	Check for Inbound http / web browsing	Page should load	Pass	Fig 14
15	Check for Accounting of all chains / verbose mode	It should show all the traffic for the period the test	Pass	Fig 15

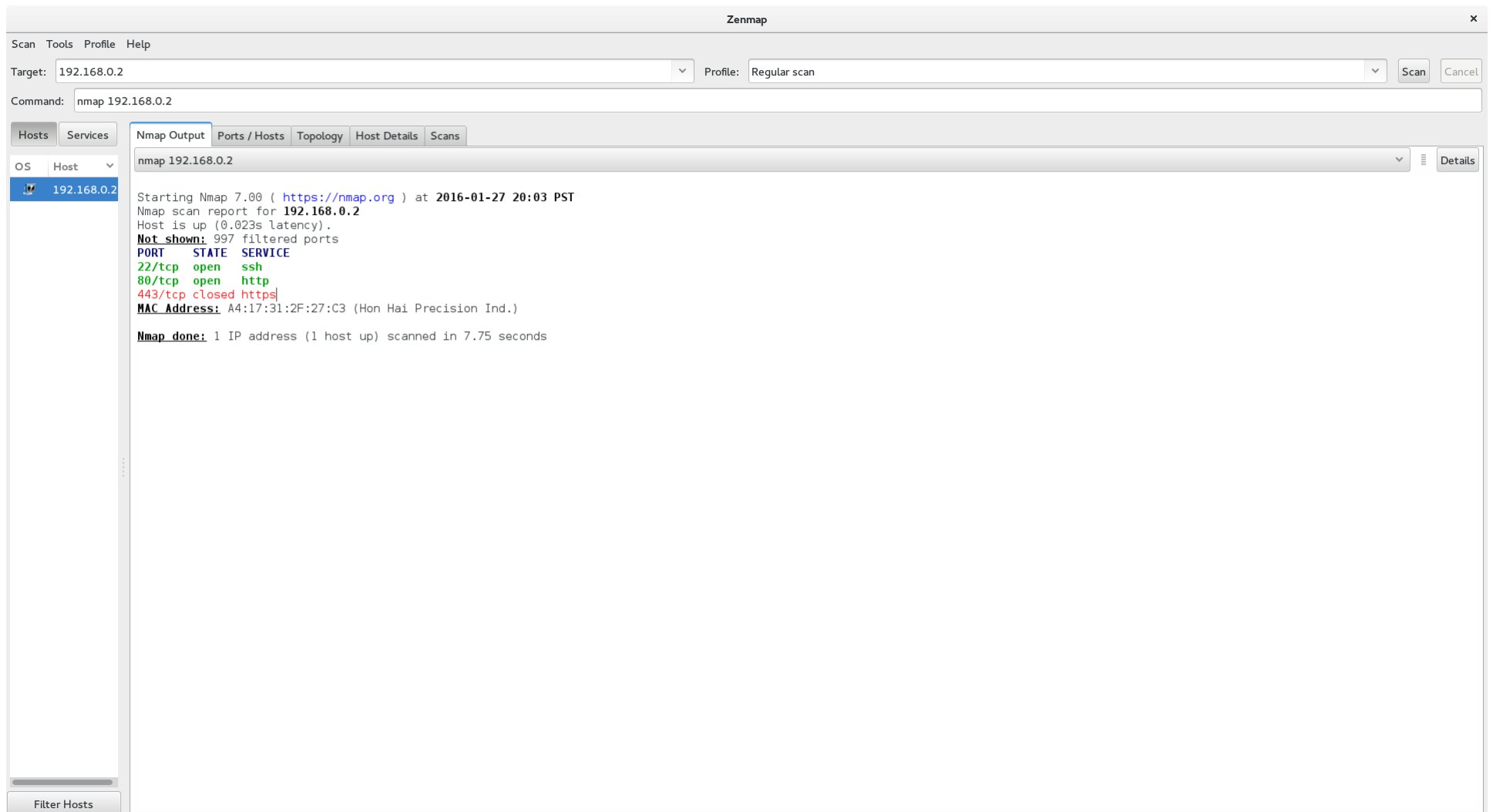
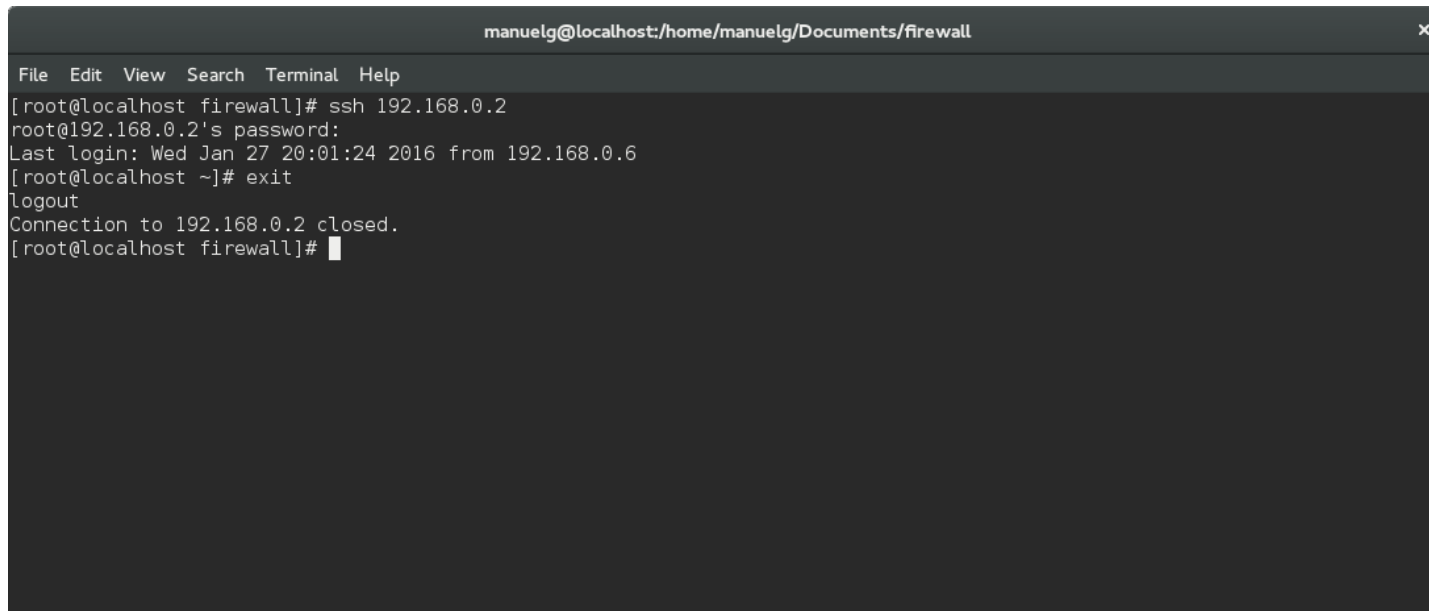
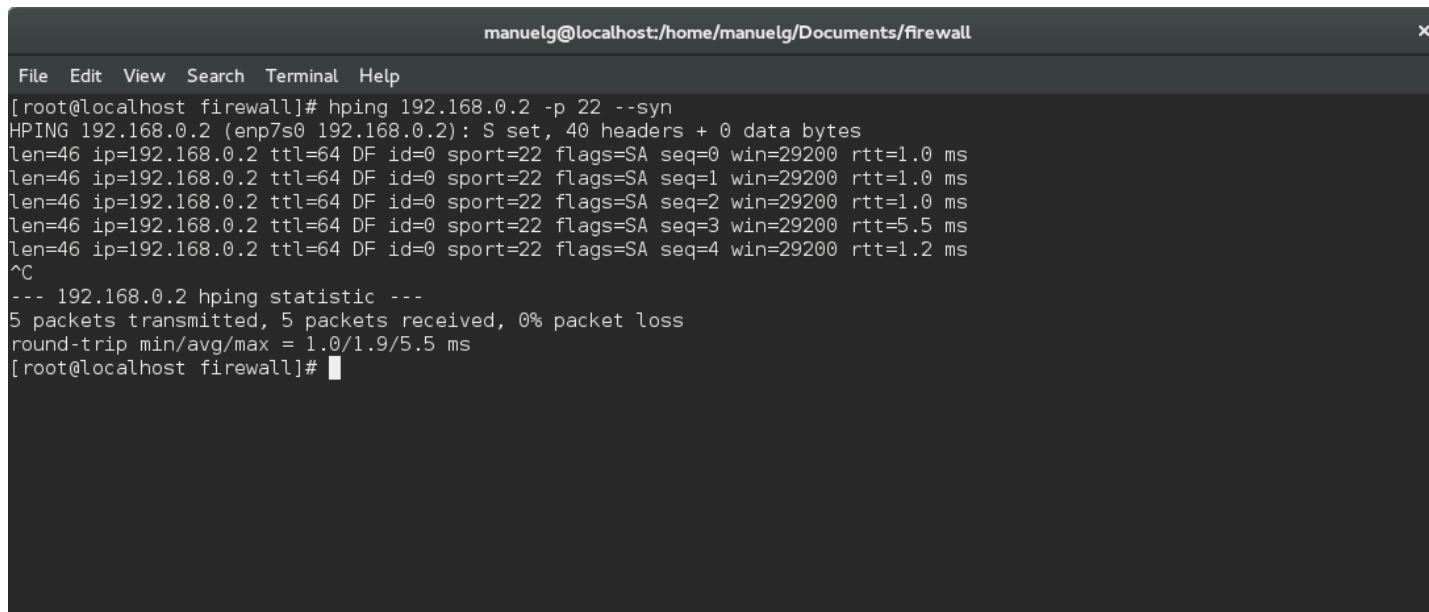


Figure 1



```
manuelg@localhost:/home/manuelg/Documents/firewall
File Edit View Search Terminal Help
[root@localhost firewall]# ssh 192.168.0.2
root@192.168.0.2's password:
Last login: Wed Jan 27 20:01:24 2016 from 192.168.0.6
[root@localhost ~]# exit
logout
Connection to 192.168.0.2 closed.
[root@localhost firewall]#
```

Figure 2



```
manuelg@localhost:/home/manuelg/Documents/firewall
File Edit View Search Terminal Help
[root@localhost firewall]# hping 192.168.0.2 -p 22 --syn
HPING 192.168.0.2 (enp7s0 192.168.0.2): S set, 40 headers + 0 data bytes
len=46 ip=192.168.0.2 ttl=64 DF id=0 sport=22 flags=SA seq=0 win=29200 rtt=1.0 ms
len=46 ip=192.168.0.2 ttl=64 DF id=0 sport=22 flags=SA seq=1 win=29200 rtt=1.0 ms
len=46 ip=192.168.0.2 ttl=64 DF id=0 sport=22 flags=SA seq=2 win=29200 rtt=1.0 ms
len=46 ip=192.168.0.2 ttl=64 DF id=0 sport=22 flags=SA seq=3 win=29200 rtt=5.5 ms
len=46 ip=192.168.0.2 ttl=64 DF id=0 sport=22 flags=SA seq=4 win=29200 rtt=1.2 ms
^C
--- 192.168.0.2 hping statistic ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 1.0/1.9/5.5 ms
[root@localhost firewall]#
```

Figure 3

```
manuelg@localhost:/home/manuelg/Documents/firewall
File Edit View Search Terminal Help
[root@localhost firewall]# hping 192.168.0.2 -s 22 -p 22 --syn
HPING 192.168.0.2 (enp7s0 192.168.0.2): S set, 40 headers + 0 data bytes
len=46 ip=192.168.0.2 ttl=64 DF id=0 sport=22 flags=SA seq=0 win=29200 rtt=1.1 ms
len=46 ip=192.168.0.2 ttl=64 DF id=0 sport=22 flags=SA seq=1 win=29200 rtt=1.3 ms
len=46 ip=192.168.0.2 ttl=64 DF id=0 sport=22 flags=SA seq=2 win=29200 rtt=1.2 ms
len=46 ip=192.168.0.2 ttl=64 DF id=0 sport=22 flags=SA seq=3 win=29200 rtt=1.2 ms
len=46 ip=192.168.0.2 ttl=64 DF id=0 sport=22 flags=SA seq=4 win=29200 rtt=1.1 ms
^C
--- 192.168.0.2 hping statistic ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 1.1/1.2/1.3 ms
[root@localhost firewall]#
```

Figure 4

```
manuelg@localhost:/home/manuelg/Documents/firewall
File Edit View Search Terminal Help
[root@localhost firewall]# hping 192.168.0.2 -s 1025 -p 80 --syn
HPING 192.168.0.2 (enp7s0 192.168.0.2): S set, 40 headers + 0 data bytes
len=46 ip=192.168.0.2 ttl=64 DF id=0 sport=80 flags=SA seq=0 win=29200 rtt=1.0 ms
len=46 ip=192.168.0.2 ttl=64 DF id=0 sport=80 flags=SA seq=1 win=29200 rtt=1.2 ms
len=46 ip=192.168.0.2 ttl=64 DF id=0 sport=80 flags=SA seq=2 win=29200 rtt=1.2 ms
len=46 ip=192.168.0.2 ttl=64 DF id=0 sport=80 flags=SA seq=3 win=29200 rtt=1.1 ms
len=46 ip=192.168.0.2 ttl=64 DF id=0 sport=80 flags=SA seq=4 win=29200 rtt=1.1 ms
^C
--- 192.168.0.2 hping statistic ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 1.0/1.1/1.2 ms
[root@localhost firewall]#
```

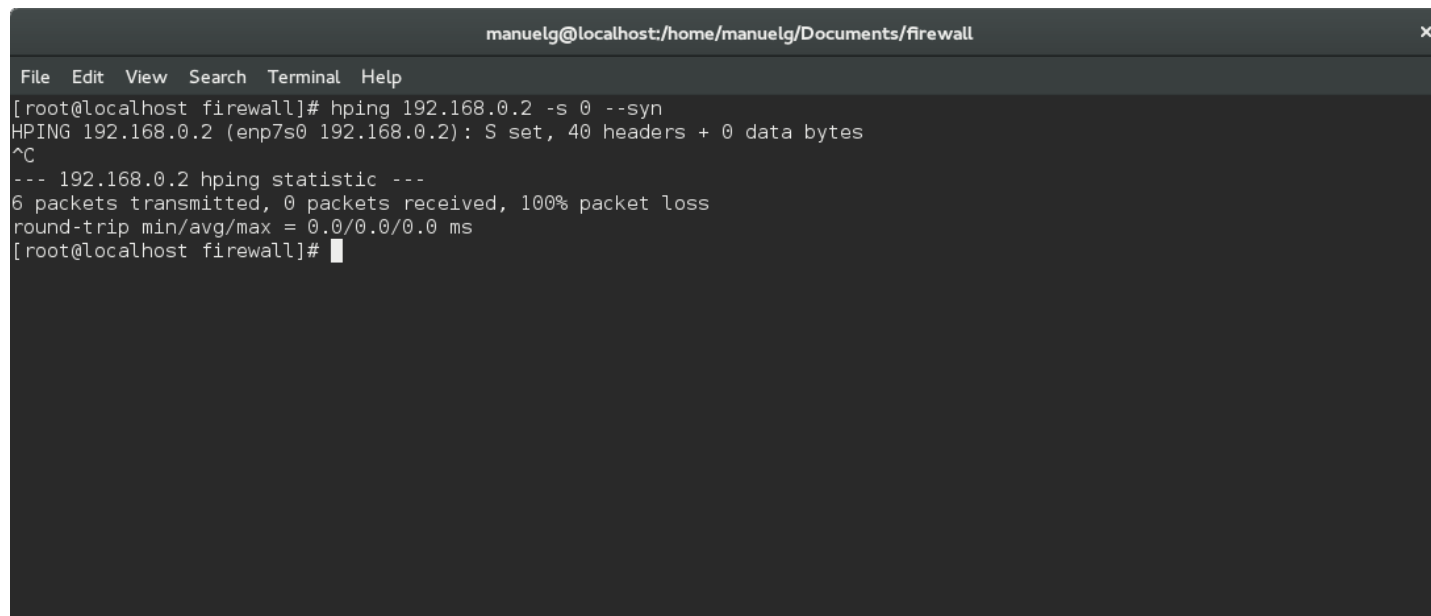
Figure 5

```
manuelg@localhost:/home/manuelg/Documents/firewall
File Edit View Search Terminal Help
[root@localhost firewall]# hping 192.168.0.2 -s 120 -p 80 --syn
HPING 192.168.0.2 (enp7s0 192.168.0.2): S set, 40 headers + 0 data bytes
^C
--- 192.168.0.2 hping statistic ---
7 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
[root@localhost firewall]#
```

Figure 6

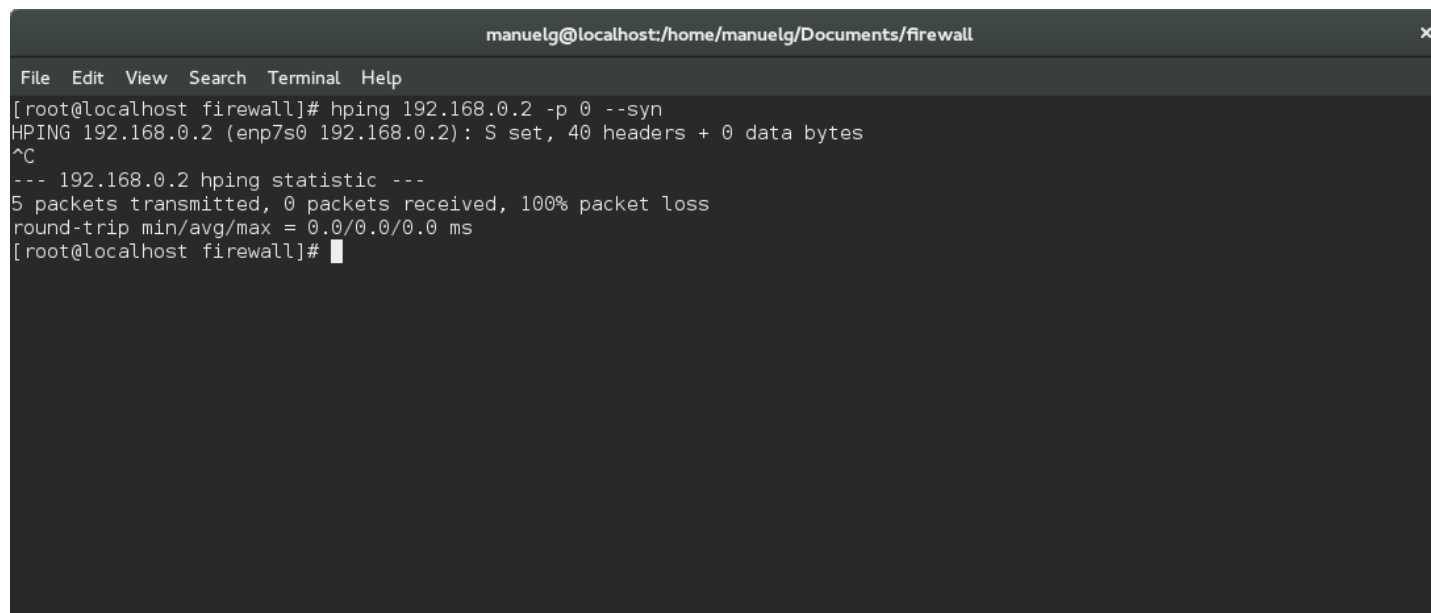
```
manuelg@localhost:/home/manuelg/Documents/firewall
File Edit View Search Terminal Help
[root@localhost firewall]# hping 192.168.0.2 -s 80 -p 22 --syn
HPING 192.168.0.2 (enp7s0 192.168.0.2): S set, 40 headers + 0 data bytes
len=46 ip=192.168.0.2 ttl=64 DF id=0 sport=22 flags=SA seq=0 win=29200 rtt=1.1 ms
len=46 ip=192.168.0.2 ttl=64 DF id=0 sport=22 flags=SA seq=1 win=29200 rtt=1.2 ms
len=46 ip=192.168.0.2 ttl=64 DF id=0 sport=22 flags=SA seq=2 win=29200 rtt=1.2 ms
len=46 ip=192.168.0.2 ttl=64 DF id=0 sport=22 flags=SA seq=3 win=29200 rtt=1.5 ms
len=46 ip=192.168.0.2 ttl=64 DF id=0 sport=22 flags=SA seq=4 win=29200 rtt=1.1 ms
^C
--- 192.168.0.2 hping statistic ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 1.1/1.2/1.5 ms
[root@localhost firewall]#
```

Figure 7



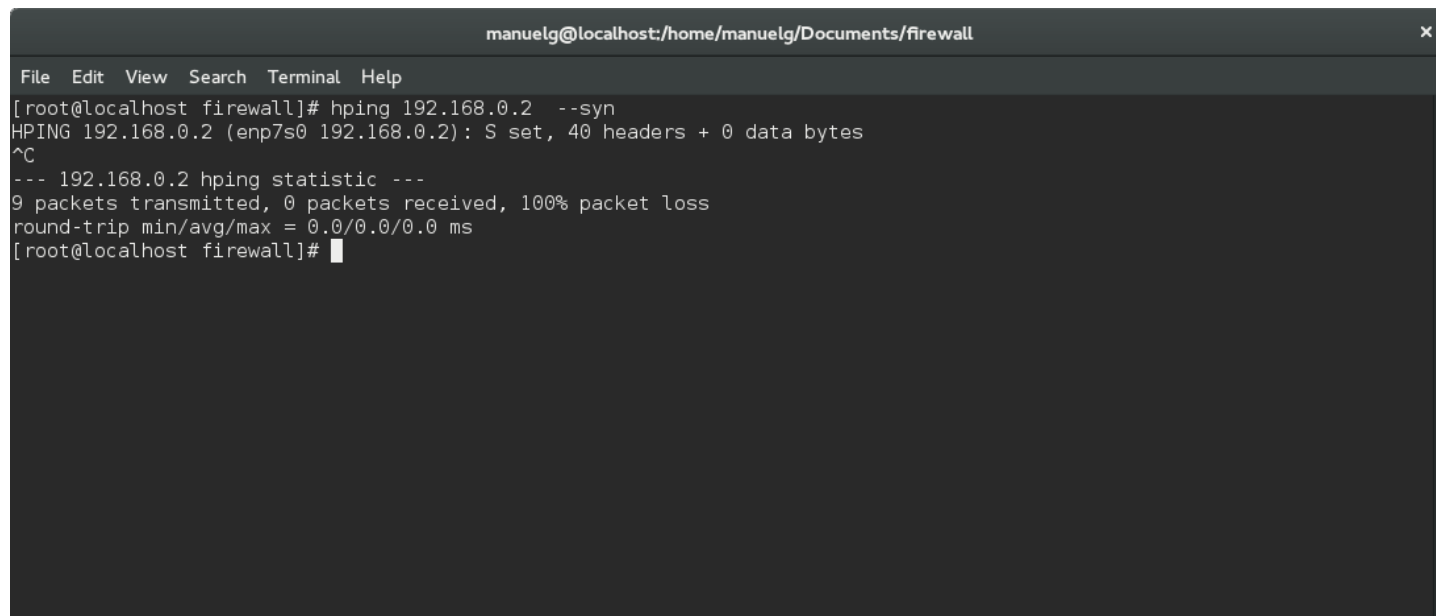
```
manuelg@localhost:/home/manuelg/Documents/firewall
File Edit View Search Terminal Help
[root@localhost firewall]# hping 192.168.0.2 -s 0 --syn
HPING 192.168.0.2 (enp7s0 192.168.0.2): S set, 40 headers + 0 data bytes
^C
--- 192.168.0.2 hping statistic ---
6 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
[root@localhost firewall]#
```

Figure 8



```
manuelg@localhost:/home/manuelg/Documents/firewall
File Edit View Search Terminal Help
[root@localhost firewall]# hping 192.168.0.2 -p 0 --syn
HPING 192.168.0.2 (enp7s0 192.168.0.2): S set, 40 headers + 0 data bytes
^C
--- 192.168.0.2 hping statistic ---
5 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
[root@localhost firewall]#
```

Figure 9



A terminal window titled "manuelg@localhost:/home/manuelg/Documents/firewall" with a close button in the top right corner. The window contains a menu bar with "File", "Edit", "View", "Search", "Terminal", and "Help". The terminal output shows the execution of the "hping" command to ping 192.168.0.2 with the "--syn" flag. The output indicates that the connection was set successfully. After pressing Ctrl-C, it displays hping statistics: 9 packets transmitted, 0 packets received, 100% packet loss, and a round-trip time of 0.0/0.0/0.0 ms.

```
manuelg@localhost:/home/manuelg/Documents/firewall
File Edit View Search Terminal Help
[root@localhost firewall]# hping 192.168.0.2 --syn
HPING 192.168.0.2 (enp7s0 192.168.0.2): S set, 40 headers + 0 data bytes
^C
--- 192.168.0.2 hping statistic ---
9 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
[root@localhost firewall]#
```

Figure 10

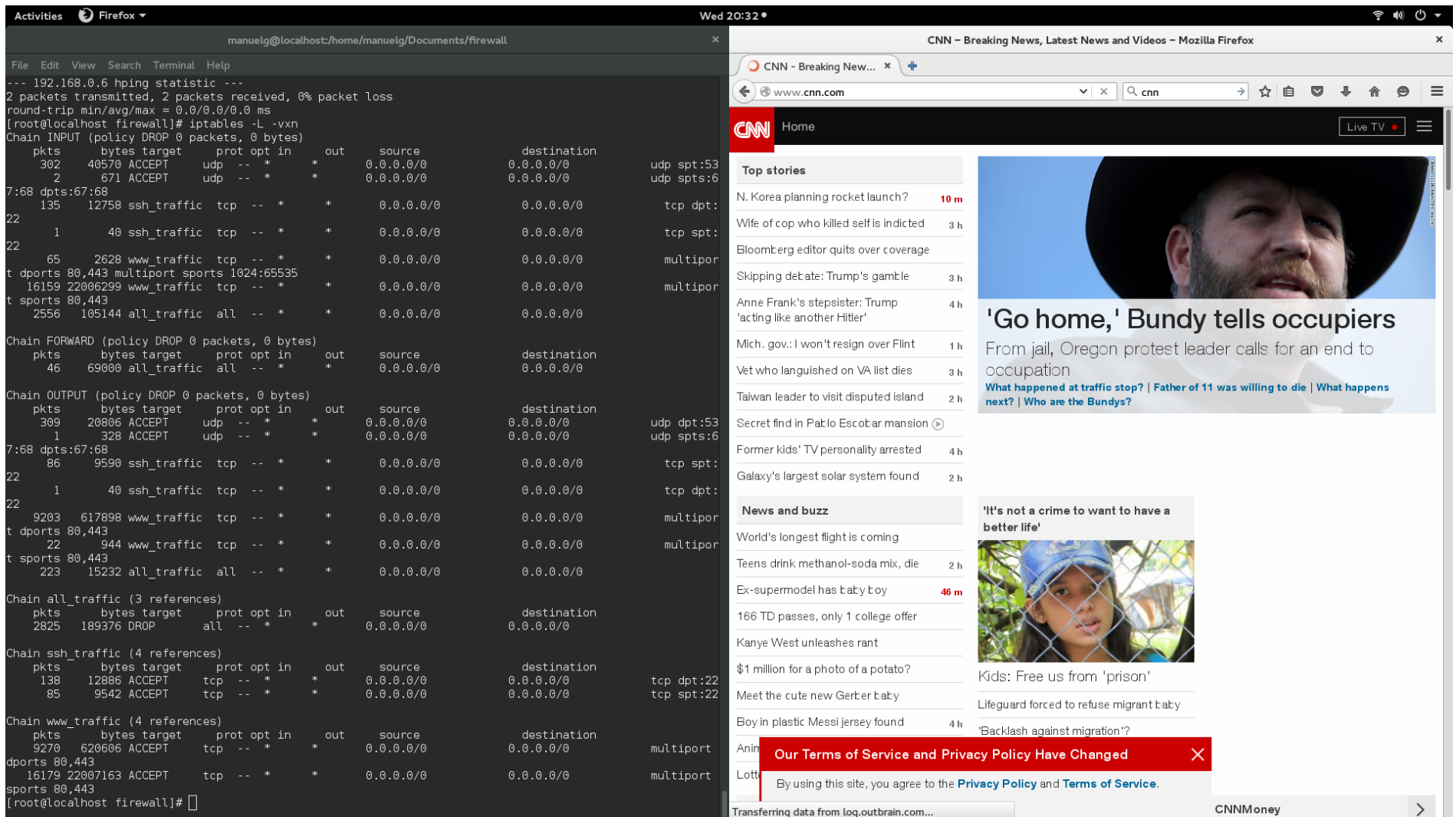


Figure 11

Activities

Terminal

Wed 20:39

manuelg@localhost:/home/manuelg/Documents/firewall

manuelg@localhost:/home/manuelg/Documents/firewall

File Edit View Search Terminal Help

TX packets 0 bytes 0 (0.0 B)

TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

wlp2s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500

inet6 fe80::a617:31ff:fe2f:27c3 prefixlen 64 scopeid 0x20<link>

ether a4:17:31:2f:27:c3 txqueuelen 1000 (Ethernet)

RX packets 136955 bytes 182509135 (174.0 MiB)

RX errors 0 dropped 0 overruns 0 frame 0

TX packets 75212 bytes 7354850 (7.0 MiB)

TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

[root@localhost firewall]# dhclient

[root@localhost firewall]# ifconfig

enp3s0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500

ether 90:b1:1c:7c:15:b6 txqueuelen 1000 (Ethernet)

RX packets 0 bytes 0 (0.0 B)

RX errors 0 dropped 0 overruns 0 frame 0

TX packets 0 bytes 0 (0.0 B)

TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536

inet 127.0.0.1 netmask 255.0.0.0

inet6 ::1 prefixlen 128 scopeid 0x10<host>

loop txqueuelen 0 (Local Loopback)

RX packets 6 bytes 480 (480.0 B)

RX errors 0 dropped 0 overruns 0 frame 0

TX packets 6 bytes 480 (480.0 B)

TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

virbr0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500

inet 192.168.122.1 netmask 255.255.255.0 broadcast 192.168.122.255

ether 52:54:00:da:09:16 txqueuelen 0 (Ethernet)

RX packets 0 bytes 0 (0.0 B)

RX errors 0 dropped 0 overruns 0 frame 0

TX packets 0 bytes 0 (0.0 B)

TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

virbr0-nic: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500

ether 52:54:00:da:09:16 txqueuelen 500 (Ethernet)

RX packets 0 bytes 0 (0.0 B)

RX errors 0 dropped 0 overruns 0 frame 0

TX packets 0 bytes 0 (0.0 B)

TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

wlp2s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500

inet 192.168.0.2 netmask 255.255.255.0 broadcast 192.168.0.255

inet6 fe80::a617:31ff:fe2f:27c3 prefixlen 64 scopeid 0x20<link>

ether a4:17:31:2f:27:c3 txqueuelen 1000 (Ethernet)

RX packets 137108 bytes 182533704 (174.0 MiB)

RX errors 0 dropped 0 overruns 0 frame 0

TX packets 75297 bytes 7363972 (7.0 MiB)

TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

[root@localhost firewall]#

File Edit View Search Terminal Help

[root@localhost firewall]# iptables -L -vxn

Chain INPUT (policy DROP 0 packets, 0 bytes)

pkts	bytes	target	prot	opt	in	out	source	destination	
799	111897	ACCEPT	udp	--	*	*	0.0.0.0/0	0.0.0.0/0	udp spt:53
5	1655	ACCEPT	udp	--	*	*	0.0.0.0/0	0.0.0.0/0	udp spts:6
7:68	dpts:67:68								
135	12758	ssh_traffic	tcp	--	*	*	0.0.0.0/0	0.0.0.0/0	tcp dpt:
22	1	40 ssh_traffic	tcp	--	*	*	0.0.0.0/0	0.0.0.0/0	tcp spt:
22	65	2628 www_traffic	tcp	--	*	*	0.0.0.0/0	0.0.0.0/0	multiport
t dports	80,443	multiport	sports	1024:65535					
31498	39432235	www_traffic	tcp	--	*	*	0.0.0.0/0	0.0.0.0/0	multiport
t sports	80,443								
2650	107972	all_traffic	all	--	*	*	0.0.0.0/0	0.0.0.0/0	

Chain FORWARD (policy DROP 0 packets, 0 bytes)

pkts	bytes	target	prot	opt	in	out	source	destination	
90	135000	all_traffic	all	--	*	*	0.0.0.0/0	0.0.0.0/0	

Chain OUTPUT (policy DROP 0 packets, 0 bytes)

pkts	bytes	target	prot	opt	in	out	source	destination	
808	54447	ACCEPT	udp	--	*	*	0.0.0.0/0	0.0.0.0/0	udp dpt:53
3	984	ACCEPT	udp	--	*	*	0.0.0.0/0	0.0.0.0/0	udp spts:6
7:68	dpts:67:68								
86	9590	ssh_traffic	tcp	--	*	*	0.0.0.0/0	0.0.0.0/0	tcp spt:
22	1	40 ssh_traffic	tcp	--	*	*	0.0.0.0/0	0.0.0.0/0	tcp dpt:
22	20482	1722959 www_traffic	tcp	--	*	*	0.0.0.0/0	0.0.0.0/0	multiport
t dports	80,443								
22	944	www_traffic	tcp	--	*	*	0.0.0.0/0	0.0.0.0/0	multiport
t sports	80,443								
274	19548	all_traffic	all	--	*	*	0.0.0.0/0	0.0.0.0/0	

Chain all_traffic (3 references)

pkts	bytes	target	prot	opt	in	out	source	destination	
3014	262520	DROP	all	--	*	*	0.0.0.0/0	0.0.0.0/0	

Chain ssh_traffic (4 references)

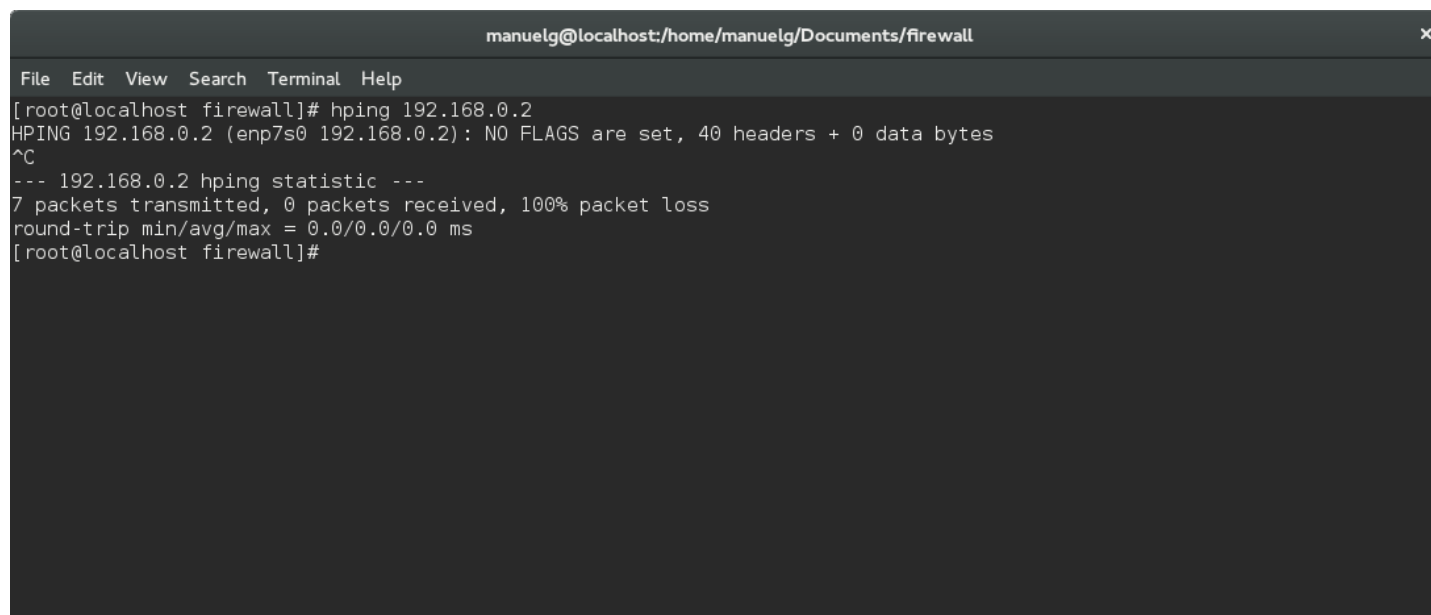
pkts	bytes	target	prot	opt	in	out	source	destination	
138	12886	ACCEPT	tcp	--	*	*	0.0.0.0/0	0.0.0.0/0	tcp dpt:22
85	9542	ACCEPT	tcp	--	*	*	0.0.0.0/0	0.0.0.0/0	tcp spt:22

Chain www_traffic (4 references)

pkts	bytes	target	prot	opt	in	out	source	destination	
20549	1725667	ACCEPT	tcp	--	*	*	0.0.0.0/0	0.0.0.0/0	multiport
dports	80,443								
31518	39433099	ACCEPT	tcp	--	*	*	0.0.0.0/0	0.0.0.0/0	multiport
sports	80,443								

[root@localhost firewall]#

Figure 12

A terminal window titled 'manuelg@localhost:/home/manuelg/Documents/firewall' with a standard menu bar (File, Edit, View, Search, Terminal, Help). The terminal shows the execution of the 'hping' command against IP 192.168.0.2. The output indicates that no flags are set and that 100% of the transmitted packets were lost. The user then presses Ctrl-C to interrupt the process.

```
manuelg@localhost:/home/manuelg/Documents/firewall
File Edit View Search Terminal Help
[root@localhost firewall]# hping 192.168.0.2
HPING 192.168.0.2 (enp7s0 192.168.0.2): NO FLAGS are set, 40 headers + 0 data bytes
^C
--- 192.168.0.2 hping statistic ---
7 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
[root@localhost firewall]#
```

Figure 13

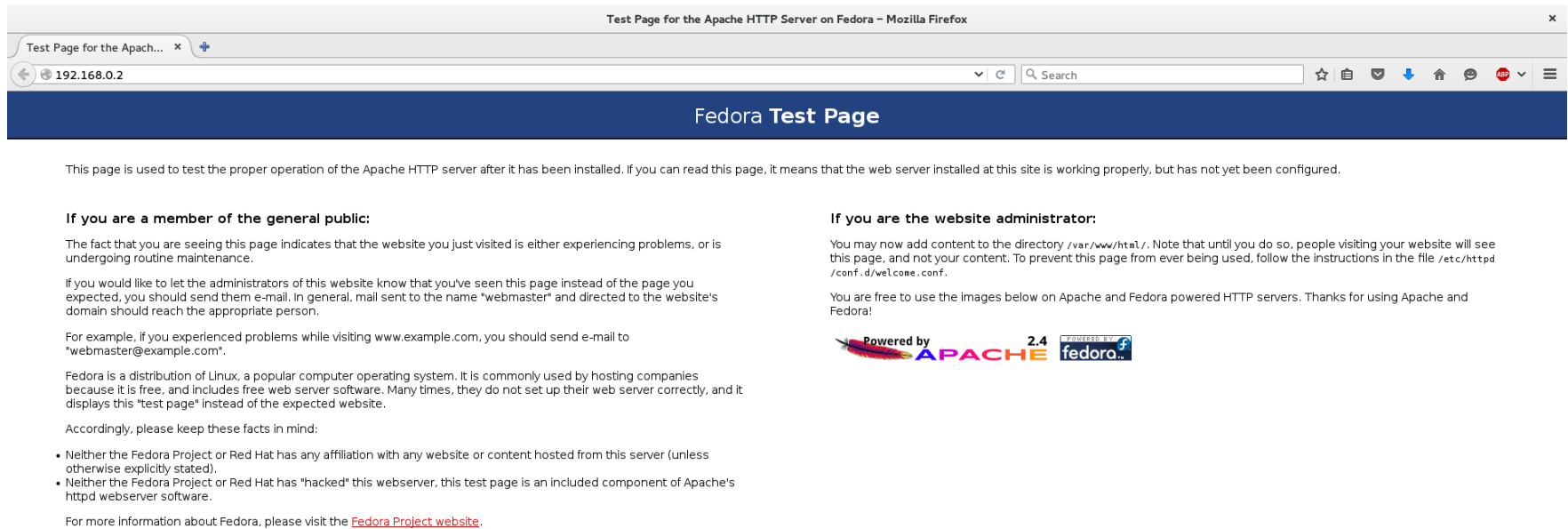


Figure 14

File Edit View Search Terminal Help

[root@localhost firewall]# iptables -L -vxn

Chain INPUT (policy DROP 0 packets, 0 bytes)

pkts	bytes	target	prot	opt	in	out	source	destination	
827	116141	ACCEPT	udp	--	*	*	0.0.0.0/0	0.0.0.0/0	udp spt:53
5	1655	ACCEPT	udp	--	*	*	0.0.0.0/0	0.0.0.0/0	udp spts:67:68 dpts:67:68
135	12758	ssh_traffic	tcp	--	*	*	0.0.0.0/0	0.0.0.0/0	tcp dpt:22
1	40	ssh_traffic	tcp	--	*	*	0.0.0.0/0	0.0.0.0/0	tcp spt:22
65	2628	www_traffic	tcp	--	*	*	0.0.0.0/0	0.0.0.0/0	multiport dports 80,443 multiport sports 1024:65535
32730	41066211	www_traffic	tcp	--	*	*	0.0.0.0/0	0.0.0.0/0	multiport sports 80,443
2752	111112	all_traffic	all	--	*	*	0.0.0.0/0	0.0.0.0/0	

Chain FORWARD (policy DROP 0 packets, 0 bytes)

pkts	bytes	target	prot	opt	in	out	source	destination
90	135000	all_traffic	all	--	*	*	0.0.0.0/0	0.0.0.0/0

Chain OUTPUT (policy DROP 0 packets, 0 bytes)

pkts	bytes	target	prot	opt	in	out	source	destination	
836	56335	ACCEPT	udp	--	*	*	0.0.0.0/0	0.0.0.0/0	udp dpt:53
3	984	ACCEPT	udp	--	*	*	0.0.0.0/0	0.0.0.0/0	udp spts:67:68 dpts:67:68
86	9590	ssh_traffic	tcp	--	*	*	0.0.0.0/0	0.0.0.0/0	tcp spt:22
1	40	ssh_traffic	tcp	--	*	*	0.0.0.0/0	0.0.0.0/0	tcp dpt:22
21438	1777272	www_traffic	tcp	--	*	*	0.0.0.0/0	0.0.0.0/0	multiport dports 80,443
22	944	www_traffic	tcp	--	*	*	0.0.0.0/0	0.0.0.0/0	multiport sports 80,443
329	23296	all_traffic	all	--	*	*	0.0.0.0/0	0.0.0.0/0	

Chain all_traffic (3 references)

pkts	bytes	target	prot	opt	in	out	source	destination
3171	269408	DROP	all	--	*	*	0.0.0.0/0	0.0.0.0/0

Chain ssh_traffic (4 references)

pkts	bytes	target	prot	opt	in	out	source	destination	
138	12886	ACCEPT	tcp	--	*	*	0.0.0.0/0	0.0.0.0/0	tcp dpt:22
85	9542	ACCEPT	tcp	--	*	*	0.0.0.0/0	0.0.0.0/0	tcp spt:22

Chain www_traffic (4 references)

pkts	bytes	target	prot	opt	in	out	source	destination	
21505	1779980	ACCEPT	tcp	--	*	*	0.0.0.0/0	0.0.0.0/0	multiport dports 80,443
32750	41067075	ACCEPT	tcp	--	*	*	0.0.0.0/0	0.0.0.0/0	multiport sports 80,443

[root@localhost firewall]#

Figure 15