Mario Enriquez
COMP 8006

A00909441
February 04, 2016

Assignment 02 Report

Design

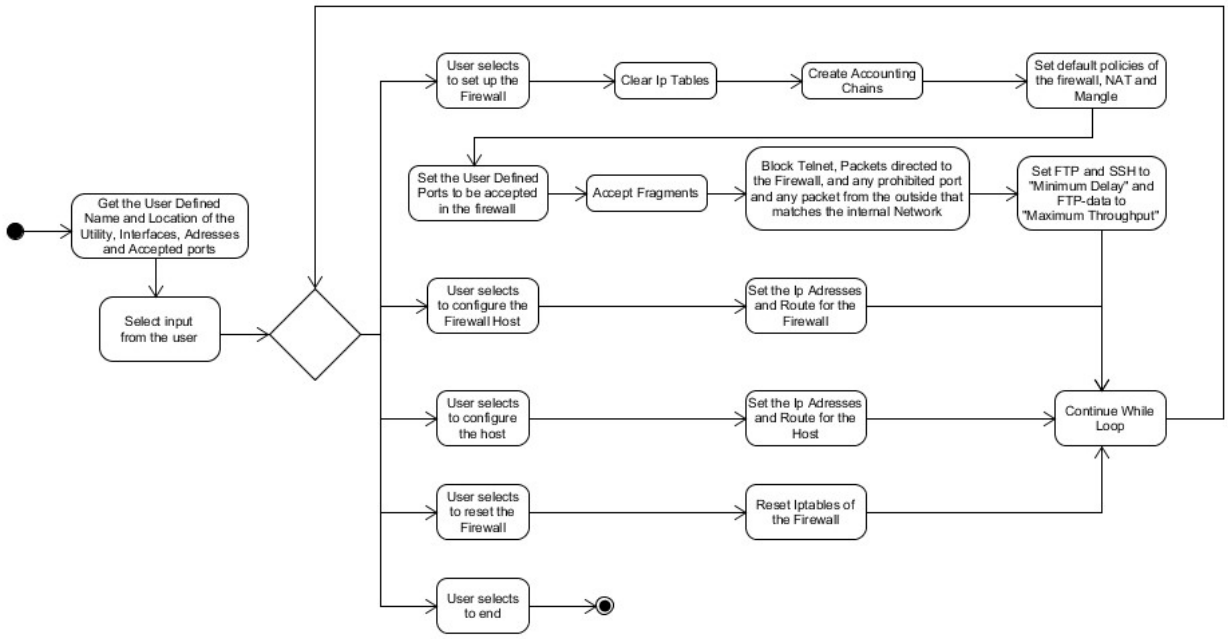


Figure 1 Design work of the shell script

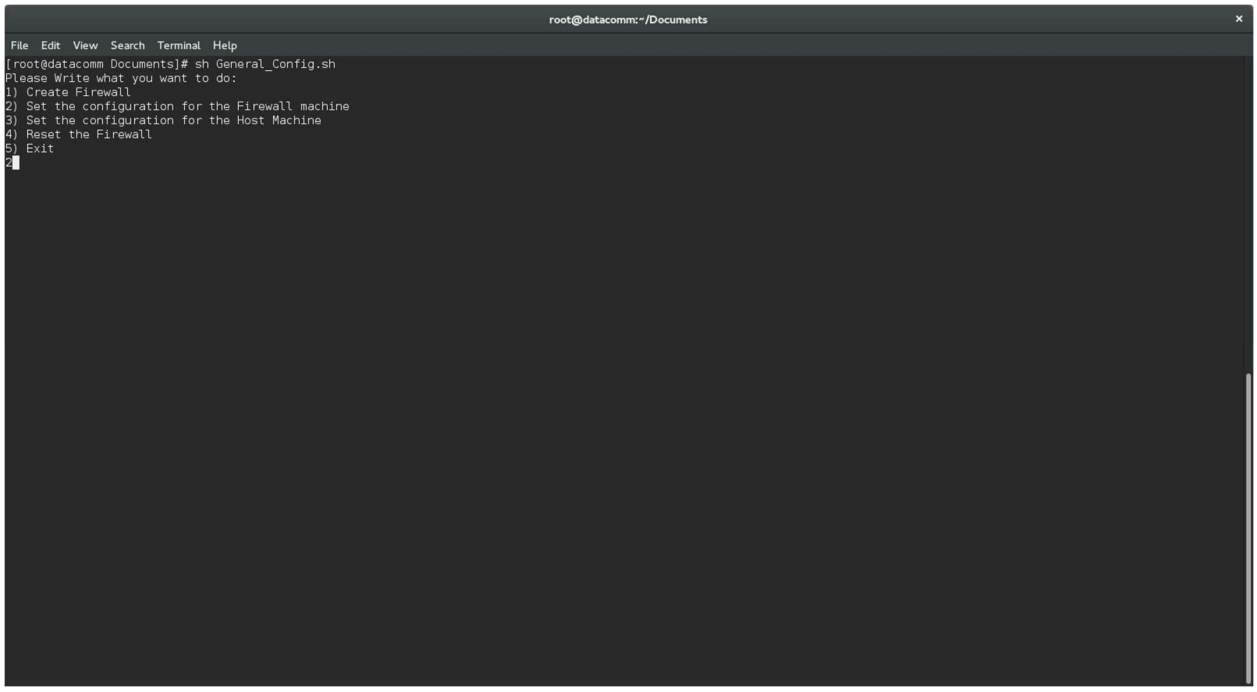
Instructions

How to set the firewall and the host:

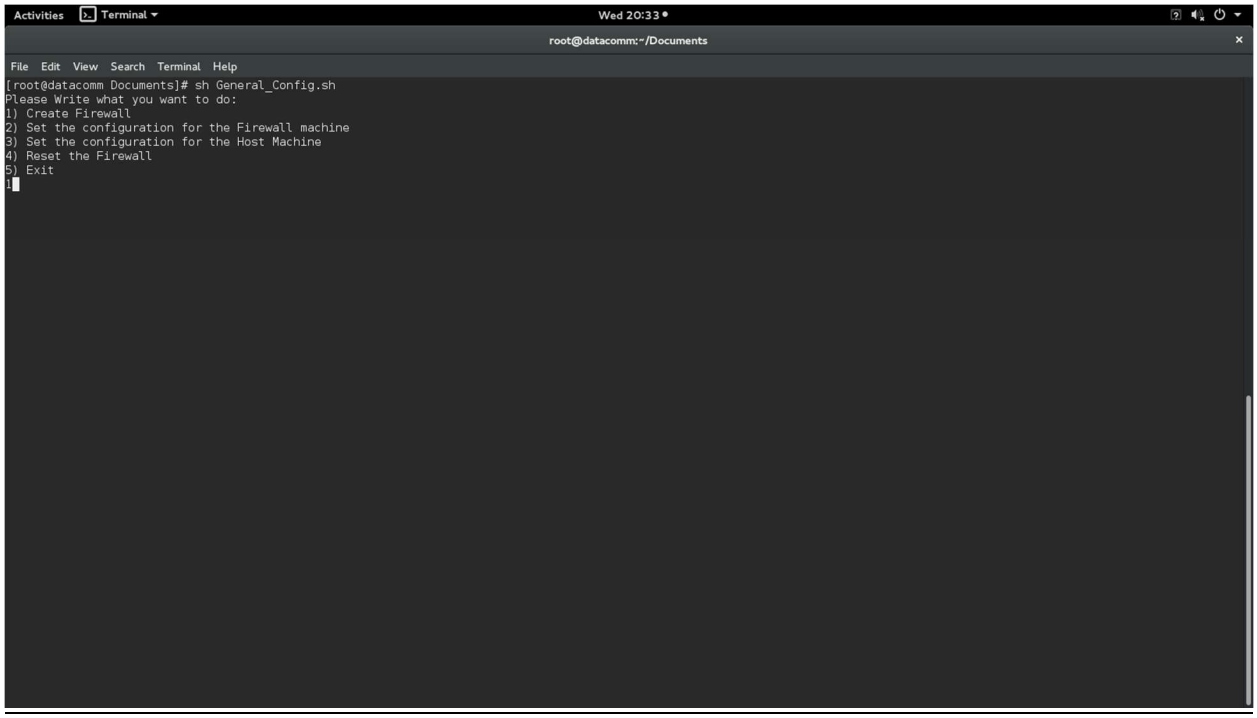
1. Connect the Machine designated as a Firewall with the Machine designated as a Host with an Cross-Cut cable
2. Localize the folder which contains the script General_Config.sh
3. Make the necessary adjustments to the user configuration part of the script and make sure both the firewall and the host have the same configuration parameters
4. Execute General_Config.sh in both Machines

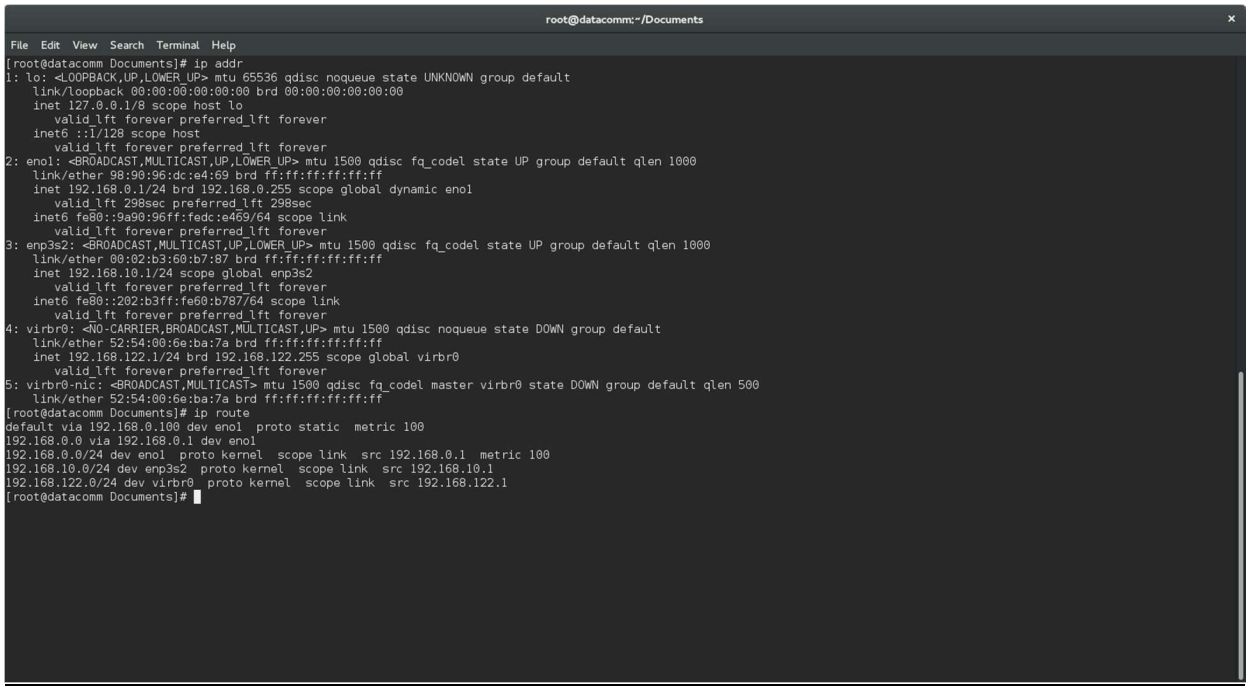
Firewall

5. Select Option 2 which sets the basic configuration for the network



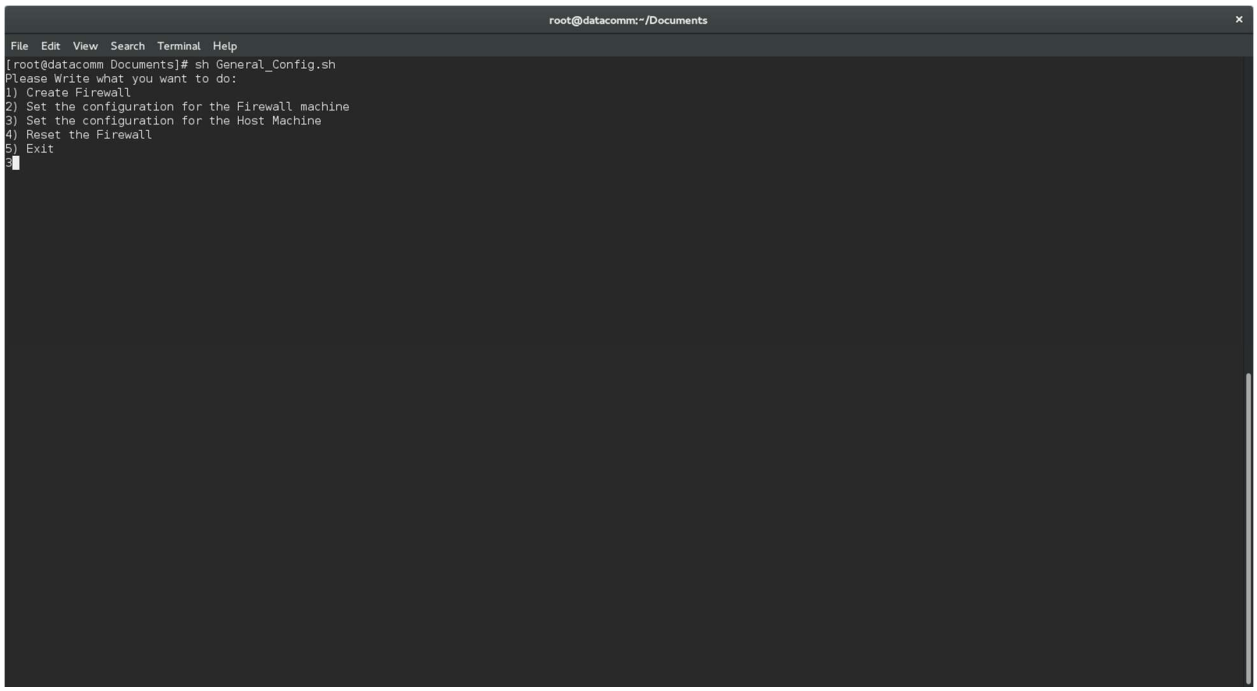
6. Select Option 1 which sets the rules of the Firewall

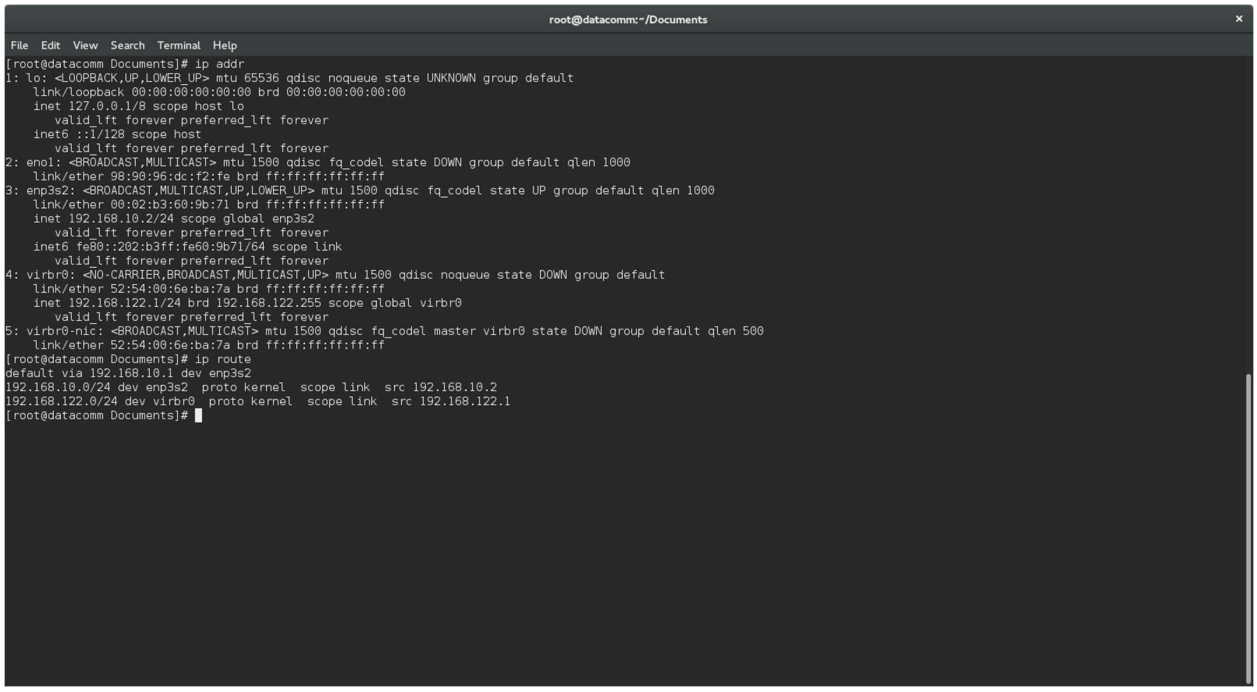




Host

5. Select Option 3 which sets the basic configuration for the network





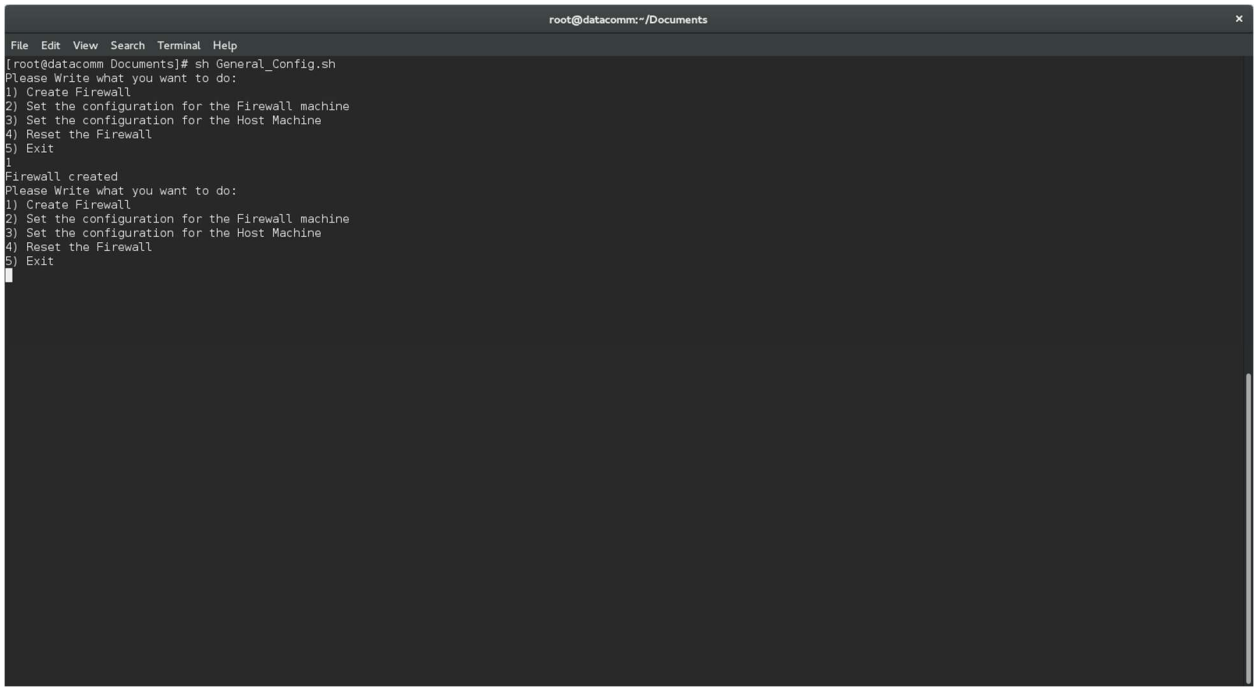
NOTE: if there is any problems, try to redo step 5 in both machines

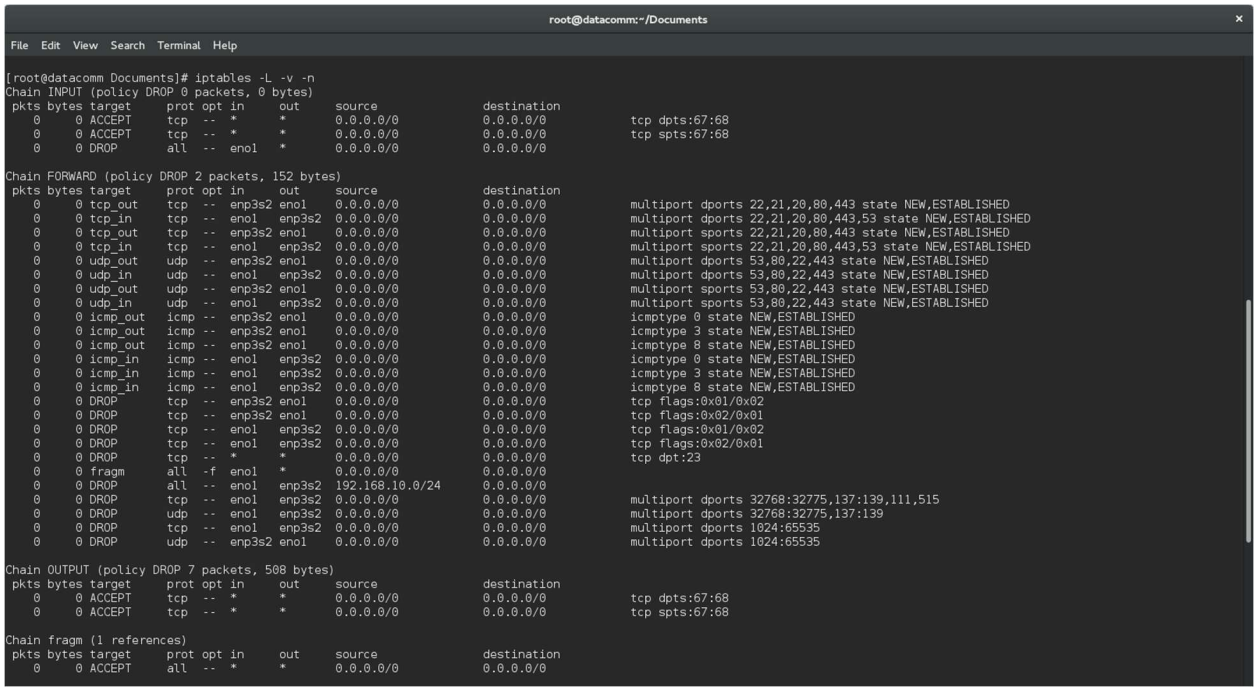
Tests

Test Number	Description	Tool Used	Machine Used	Expected Result	Actual Result
1	Set The firewall	Shell script, iptables	Firewall Machine	Firewall created and iptables shown	Success, Firewall is working with the iptables
2	Review the NAT table	iptables	Firewall Machine	Masquerade and DNAT Pre-routing shown	Success, and we can see both ready
3	Check if we have communication from the host to the exterior	Ping, ip route and ip address if fails	Host Machine	Response to ping 8.8.8.8 and a host in the outer network	Success, we can see that there is response
4	Ping allowed TCP ports	Hping3	Host Machine	Response to the host	Success, we can see replies
5	Ping ICMP ports	Hping3	Host Machine	Response to the host	Success, we can see replies
6	Ping UDP ports	Hping3	Host Machine	Response to the Host	Failure, we can see that they are only accepted one way during

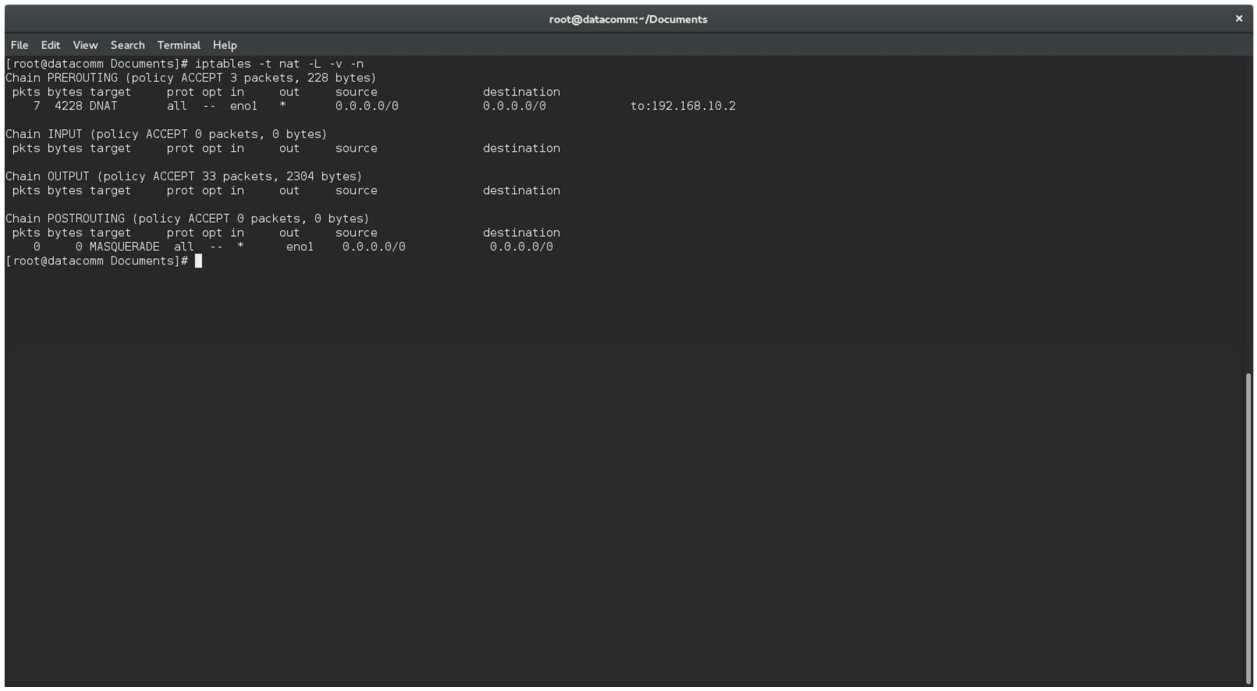
					the IP forwarding
7	Test invalid ports	Hping3	External Machine	Rejection of the ports	Success, Drop rate is 100%
8	Checking if UDP ports are open in destination	Nmap	External Machine	Nmap results	Semi-Success, we can see that the port is filtered but not enough information

Test 1




root@datacomm:~/Documents
File Edit View Search Terminal Help
[root@datacomm Documents]# iptables -L -v -n
Chain INPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target   prot opt in   out   source   destination
    0   0 ACCEPT   tcp -- *   *   0.0.0.0/0   0.0.0.0/0   tcp dpts:67:68
    0   0 ACCEPT   tcp -- *   *   0.0.0.0/0   0.0.0.0/0   tcp spts:67:68
    0   0 DROP   all -- eno1   *   0.0.0.0/0   0.0.0.0/0
Chain FORWARD (policy DROP 2 packets, 152 bytes)
 pkts bytes target   prot opt in   out   source   destination
    0   0 tcp_out   tcp -- enp3s2 eno1   0.0.0.0/0   0.0.0.0/0   multiport dports 22,21,20,80,443 state NEW,ESTABLISHED
    0   0 tcp_in   tcp -- eno1   enp3s2 0.0.0.0/0   0.0.0.0/0   multiport dports 22,21,20,80,443,53 state NEW,ESTABLISHED
    0   0 tcp_out   tcp -- enp3s2 eno1   0.0.0.0/0   0.0.0.0/0   multiport sports 22,21,20,80,443 state NEW,ESTABLISHED
    0   0 tcp_in   tcp -- eno1   enp3s2 0.0.0.0/0   0.0.0.0/0   multiport sports 22,21,20,80,443,53 state NEW,ESTABLISHED
    0   0 udp_out   udp -- enp3s2 eno1   0.0.0.0/0   0.0.0.0/0   multiport dports 53,80,22,443 state NEW,ESTABLISHED
    0   0 udp_in   udp -- eno1   enp3s2 0.0.0.0/0   0.0.0.0/0   multiport dports 53,80,22,443 state NEW,ESTABLISHED
    0   0 udp_out   udp -- enp3s2 eno1   0.0.0.0/0   0.0.0.0/0   multiport sports 53,80,22,443 state NEW,ESTABLISHED
    0   0 udp_in   udp -- eno1   enp3s2 0.0.0.0/0   0.0.0.0/0   multiport sports 53,80,22,443 state NEW,ESTABLISHED
    0   0 icmp_out   icmp -- enp3s2 eno1   0.0.0.0/0   0.0.0.0/0   icmptype 0 state NEW,ESTABLISHED
    0   0 icmp_out   icmp -- enp3s2 eno1   0.0.0.0/0   0.0.0.0/0   icmptype 3 state NEW,ESTABLISHED
    0   0 icmp_out   icmp -- enp3s2 eno1   0.0.0.0/0   0.0.0.0/0   icmptype 8 state NEW,ESTABLISHED
    0   0 icmp_in   icmp -- eno1   enp3s2 0.0.0.0/0   0.0.0.0/0   icmptype 0 state NEW,ESTABLISHED
    0   0 icmp_in   icmp -- eno1   enp3s2 0.0.0.0/0   0.0.0.0/0   icmptype 3 state NEW,ESTABLISHED
    0   0 icmp_in   icmp -- eno1   enp3s2 0.0.0.0/0   0.0.0.0/0   icmptype 8 state NEW,ESTABLISHED
    0   0 DROP   tcp -- enp3s2 eno1   0.0.0.0/0   0.0.0.0/0   tcp flags:0x01/0x02
    0   0 DROP   tcp -- enp3s2 eno1   0.0.0.0/0   0.0.0.0/0   tcp flags:0x02/0x01
    0   0 DROP   tcp -- eno1   enp3s2 0.0.0.0/0   0.0.0.0/0   tcp flags:0x01/0x02
    0   0 DROP   tcp -- eno1   enp3s2 0.0.0.0/0   0.0.0.0/0   tcp flags:0x02/0x01
    0   0 DROP   tcp -- *   *   0.0.0.0/0   0.0.0.0/0   tcp dpt:23
    0   0 fragm   all -f eno1   *   0.0.0.0/0   0.0.0.0/0
    0   0 DROP   all -- eno1   enp3s2 192.168.10.0/24   0.0.0.0/0
    0   0 DROP   tcp -- eno1   enp3s2 0.0.0.0/0   0.0.0.0/0   multiport dports 32768:32775,137:139,111,515
    0   0 DROP   udp -- eno1   enp3s2 0.0.0.0/0   0.0.0.0/0   multiport dports 32768:32775,137:139
    0   0 DROP   tcp -- eno1   enp3s2 0.0.0.0/0   0.0.0.0/0   multiport dports 1024:65535
    0   0 DROP   udp -- enp3s2 eno1   0.0.0.0/0   0.0.0.0/0   multiport dports 1024:65535
Chain OUTPUT (policy DROP 7 packets, 508 bytes)
 pkts bytes target   prot opt in   out   source   destination
    0   0 ACCEPT   tcp -- *   *   0.0.0.0/0   0.0.0.0/0   tcp dpts:67:68
    0   0 ACCEPT   tcp -- *   *   0.0.0.0/0   0.0.0.0/0   tcp spts:67:68
Chain fragm (1 references)
 pkts bytes target   prot opt in   out   source   destination
    0   0 ACCEPT   all -- *   *   0.0.0.0/0   0.0.0.0/0

Test 2


root@datacomm:~/Documents
File Edit View Search Terminal Help
[root@datacomm Documents]# iptables -t nat -L -v -n
Chain PREROUTING (policy ACCEPT 3 packets, 228 bytes)
 pkts bytes target   prot opt in   out   source   destination
    7 4228 DNAT   all -- eno1   *   0.0.0.0/0   0.0.0.0/0   to:192.168.10.2
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target   prot opt in   out   source   destination
Chain OUTPUT (policy ACCEPT 33 packets, 2304 bytes)
 pkts bytes target   prot opt in   out   source   destination
Chain POSTROUTING (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target   prot opt in   out   source   destination
    0   0 MASQUERADE all -- *   eno1   0.0.0.0/0   0.0.0.0/0
[root@datacomm Documents]#

Test 3

```
[root@datacomm Documents]# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=54 time=7.36 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=54 time=6.17 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=54 time=5.94 ms
^C
--- 8.8.8.8 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 5.942/6.492/7.363/0.626 ms
```

```
[root@datacomm Documents]# ping 192.168.0.11
PING 192.168.0.11 (192.168.0.11) 56(84) bytes of data.
64 bytes from 192.168.0.11: icmp_seq=1 ttl=63 time=1.12 ms
64 bytes from 192.168.0.11: icmp_seq=2 ttl=63 time=0.746 ms
64 bytes from 192.168.0.11: icmp_seq=3 ttl=63 time=0.733 ms
^C
--- 192.168.0.11 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2001ms
rtt min/avg/max/mdev = 0.733/0.867/1.122/0.180 ms
```

Test 4

```
[root@datacomm Documents]# hping3 192.168.0.11 -S -p 80
HPING 192.168.0.11 (enp3s2 192.168.0.11): S set, 40 headers + 0 data bytes
len=46 ip=192.168.0.11 ttl=63 DF id=21649 sport=80 flags=RA seq=0 win=0 rtt=0.9 ms
len=46 ip=192.168.0.11 ttl=63 DF id=21797 sport=80 flags=RA seq=1 win=0 rtt=0.8 ms
len=46 ip=192.168.0.11 ttl=63 DF id=22556 sport=80 flags=RA seq=2 win=0 rtt=0.8 ms
len=46 ip=192.168.0.11 ttl=63 DF id=23465 sport=80 flags=RA seq=3 win=0 rtt=0.9 ms
^C
--- 192.168.0.11 hping statistic ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 0.8/0.8/0.9 ms
[root@datacomm Documents]# hping3 192.168.0.11 -S -p 22
HPING 192.168.0.11 (enp3s2 192.168.0.11): S set, 40 headers + 0 data bytes
len=46 ip=192.168.0.11 ttl=63 DF id=0 sport=22 flags=SA seq=0 win=29200 rtt=0.9 ms
len=46 ip=192.168.0.11 ttl=63 DF id=0 sport=22 flags=SA seq=1 win=29200 rtt=0.9 ms
len=46 ip=192.168.0.11 ttl=63 DF id=0 sport=22 flags=SA seq=2 win=29200 rtt=0.9 ms
len=46 ip=192.168.0.11 ttl=63 DF id=0 sport=22 flags=SA seq=3 win=29200 rtt=0.9 ms
^C
--- 192.168.0.11 hping statistic ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 0.9/0.9/0.9 ms
```

```
Chain FORWARD (policy DROP 1998 packets, 58940 bytes)
 pkts bytes target     prot opt in     out     source               destination
   13   520 tcp_out    tcp  --  enp3s2 eno1    0.0.0.0/0            0.0.0.0/0           multiport dports 22,21,20,80,443 state NEW,ESTABLISHED
    0     0 tcp_in     tcp  --  eno1   enp3s2  0.0.0.0/0            0.0.0.0/0           multiport dports 22,21,20,80,443,53 state NEW,ESTABLISHED
    0     0 tcp_out    tcp  --  enp3s2 eno1    0.0.0.0/0            0.0.0.0/0           multiport sports 22,21,20,80,443 state NEW,ESTABLISHED
    9   376 tcp_in     tcp  --  eno1   enp3s2  0.0.0.0/0            0.0.0.0/0           multiport sports 22,21,20,80,443,53 state NEW,ESTABLISHED
```

Test 5

```
[root@datacomm Documents]# hping3 192.168.0.11 --icmp -V
using enp3s2, addr: 192.168.10.2, MTU: 1500
HPING 192.168.0.11 (enp3s2 192.168.0.11): icmp mode set, 28 headers + 0 data bytes
len=46 ip=192.168.0.11 ttl=63 id=38301 tos=0 iplen=28
icmp_seq=0 rtt=0.8 ms
len=46 ip=192.168.0.11 ttl=63 id=38891 tos=0 iplen=28
icmp_seq=1 rtt=0.7 ms
len=46 ip=192.168.0.11 ttl=63 id=39206 tos=0 iplen=28
icmp_seq=2 rtt=0.8 ms
^C
--- 192.168.0.11 hping statistic ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 0.7/0.8/0.8 ms
```

```
    0     0 icmp_out   icmp --  enp3s2 eno1    0.0.0.0/0           0.0.0.0/0           icmptype 0 state NEW,ESTABLISHED
    0     0 icmp_out   icmp --  enp3s2 eno1    0.0.0.0/0           0.0.0.0/0           icmptype 3 state NEW,ESTABLISHED
   13   700 icmp_out   icmp --  enp3s2 eno1    0.0.0.0/0           0.0.0.0/0           icmptype 8 state NEW,ESTABLISHED
   13   700 icmp_in    icmp --  eno1   enp3s2  0.0.0.0/0           0.0.0.0/0           icmptype 0 state NEW,ESTABLISHED
    0     0 icmp_in    icmp --  eno1   enp3s2  0.0.0.0/0           0.0.0.0/0           icmptype 3 state NEW,ESTABLISHED
    0     0 icmp_in    icmp --  eno1   enp3s2  0.0.0.0/0           0.0.0.0/0           icmptype 8 state NEW,ESTABLISHED
```

Test 6

```
[root@datacomm Documents]# hping3 192.168.0.11 --udp -p 53
HPING 192.168.0.11 (enp3s2 192.168.0.11): udp mode set, 28 headers + 0 data bytes
^C
--- 192.168.0.11 hping statistic ---
2 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
[root@datacomm Documents]# hping3 192.168.0.11 --udp -p 57
HPING 192.168.0.11 (enp3s2 192.168.0.11): udp mode set, 28 headers + 0 data bytes
^C
--- 192.168.0.11 hping statistic ---
2 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
[root@datacomm Documents]# hping3 192.168.0.11 --udp -p 571
HPING 192.168.0.11 (enp3s2 192.168.0.11): udp mode set, 28 headers + 0 data bytes
^C
--- 192.168.0.11 hping statistic ---
2 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
[root@datacomm Documents]# hping3 192.168.0.11 --udp
HPING 192.168.0.11 (enp3s2 192.168.0.11): udp mode set, 28 headers + 0 data bytes
^C
--- 192.168.0.11 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 Documents]#
```

```
 9   252 udp_out    udp  --  enp3s2 eno1    0.0.0.0/0           0.0.0.0/0           multiport dports 53,80,22,443 state NEW,ESTABLISHED
12   542 udp_in     udp  --  eno1   enp3s2  0.0.0.0/0           0.0.0.0/0           multiport dports 53,80,22,443 state NEW,ESTABLISHED
 0     0 udp_out    udp  --  enp3s2 eno1    0.0.0.0/0           0.0.0.0/0           multiport sports 53,80,22,443 state NEW,ESTABLISHED
 0     0 udp_in     udp  --  eno1   enp3s2  0.0.0.0/0           0.0.0.0/0           multiport sports 53,80,22,443 state NEW,ESTABLISHED
```

We can think that the problem may be either an omission in the ip table state like being Related, which I would need to confirm with further tests.

Additionally it could be that Hping3 is ill suited for UDP tests or I committed an error using it as this example shows when I tried to use it between same network machines:

```
[root@datacomm Downloads]# hping3 192.168.0.11 --udp
HPING 192.168.0.11 (eno1 192.168.0.11): udp mode set, 28 headers + 0 data bytes
ICMP Port Unreachable from ip=192.168.0.11 name=UNKNOWN
ICMP Port Unreachable from ip=192.168.0.11 name=UNKNOWN
ICMP Port Unreachable from ip=192.168.0.11 name=UNKNOWN
^C
--- 192.168.0.11 hping statistic ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
[root@datacomm Downloads]# hping3 192.168.0.16 --udp
HPING 192.168.0.16 (eno1 192.168.0.16): udp mode set, 28 headers + 0 data bytes
^C
--- 192.168.0.16 hping statistic ---
3 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
[root@datacomm Downloads]# hping3 192.168.0.10 --udp
HPING 192.168.0.10 (eno1 192.168.0.10): udp mode set, 28 headers + 0 data bytes
ICMP Port Unreachable from ip=192.168.0.10 name=UNKNOWN
ICMP Port Unreachable from ip=192.168.0.10 name=UNKNOWN
ICMP Port Unreachable from ip=192.168.0.10 name=UNKNOWN
^C
--- 192.168.0.10 hping statistic ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
[root@datacomm Downloads]#
```

Test 7

```
[root@datacomm Downloads]# hping3 192.168.0.1 -p 65000 -s 80
HPING 192.168.0.1 (eno1 192.168.0.1): NO FLAGS are set, 40 headers + 0 data bytes
^C
--- 192.168.0.1 hping statistic ---
3 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
[root@datacomm Downloads]# hping3 192.168.0.1 -p 23
HPING 192.168.0.1 (eno1 192.168.0.1): NO FLAGS are set, 40 headers + 0 data bytes
^C
--- 192.168.0.1 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 Downloads]# hping3 192.168.0.1 -p 115
HPING 192.168.0.1 (eno1 192.168.0.1): NO FLAGS are set, 40 headers + 0 data bytes
^C
--- 192.168.0.1 hping statistic ---
3 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
[root@datacomm Downloads]# hping3 192.168.0.1 -p 117
HPING 192.168.0.1 (eno1 192.168.0.1): NO FLAGS are set, 40 headers + 0 data bytes
^C
--- 192.168.0.1 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 Downloads]# hping3 192.168.0.1 -p 117^C
[root@datacomm Downloads]# ping 192.168.0.13
PING 192.168.0.13 (192.168.0.13) 56(84) bytes of data.
^C
--- 192.168.0.13 ping statistics ---
6 packets transmitted, 0 received, 100% packet loss, time 4999ms
```

```
    0     0 DROP       tcp  --  eno1   enp3s2  0.0.0.0/0            0.0.0.0/0           multiport dports 32768:32775,137:139,111,515
   22   716 DROP       udp  --  eno1   enp3s2  0.0.0.0/0            0.0.0.0/0           multiport dports 32768:32775,137:139
    4   160 DROP       tcp  --  eno1   enp3s2  0.0.0.0/0            0.0.0.0/0           multiport dports 1024:65535
    0     0 DROP       udp  --  enp3s2 eno1    0.0.0.0/0            0.0.0.0/0           multiport dports 1024:65535
```

Test 8

```
[root@datacomm Downloads]# nmap -sU -v 192.168.0.1 -p 53

Starting Nmap 7.00 ( https://nmap.org ) at 2016-02-03 20:43 PST
Initiating ARP Ping Scan at 20:43
Scanning 192.168.0.1 [1 port]
Completed ARP Ping Scan at 20:43, 0.01s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 20:43
Completed Parallel DNS resolution of 1 host. at 20:43, 6.50s elapsed
Initiating UDP Scan at 20:43
Scanning 192.168.0.1 [1 port]
Completed UDP Scan at 20:43, 0.21s elapsed (1 total ports)
Nmap scan report for 192.168.0.1
Host is up (0.00034s latency).
PORT   STATE         SERVICE
53/udp open|filtered domain
MAC Address: 98:90:96:DC:E4:69 (Dell)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 6.77 seconds
           Raw packets sent: 3 (108B) | Rcvd: 1 (28B)
[root@datacomm Downloads]#
```

Pseudocode

Get the User defined utility, path, ports, addresses and subnets to implement

While loop until user selects 5

Ask user input
If user selects 1
- Reset Netfilter
- Create Accounting Chains
- Set Default Policies to Drop
- Set The Policies to accept forwarding User input TCP, UDP and ICMP
- Set policies to drop FIN/SYN flags
- Set policies to drop specific ports
- Set policies to accept fragments
- Set policies to check for spoofing addresses
- Drop packets destined for the Firewall host from the outside
- Set Masquerading and Pre-routing
- Set Minimum Delay to FTP and SSH, and Maximum Throughput to FTP

End if
If user selects 2
- Set Firewall Addresses
- Set Firewall Routes
- Set Ethernet link up

```
End if
If user selects 2
        Set Host Addresses
        Set Host Routes
        Set Ethernet link up
End if
If user selects 4
        Reset iptables to accept all
End if
End While loop
```