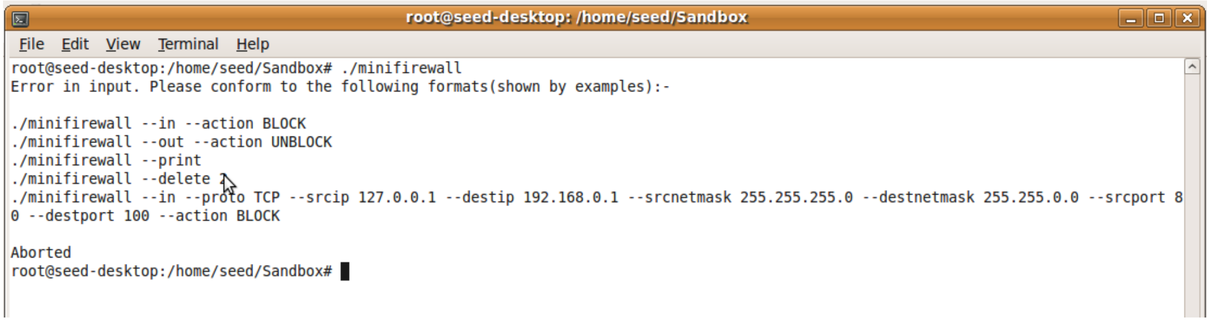
A0106504U:CS5231:Assignment 3

Task 1:

1. Successfully send parameters into kernel space

There are 2 proc entries created by the custom developed netfilter module. First is named netfilter and the other is netfilterhelper(which is used as a helper file to support operations in netfilter. The utility called minifirewall is used to configure firewall rules for the user. The following image shows the usage of minifirewall utility.

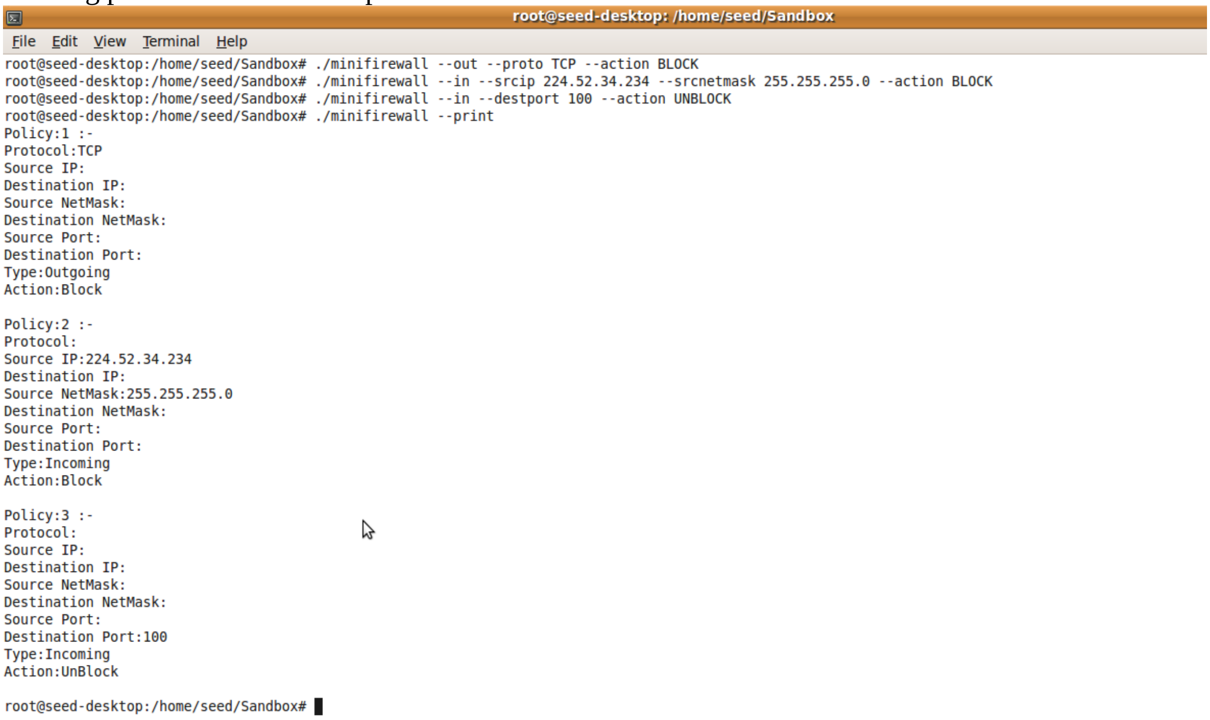
Screenshot showing general usage of minifirewall utility:



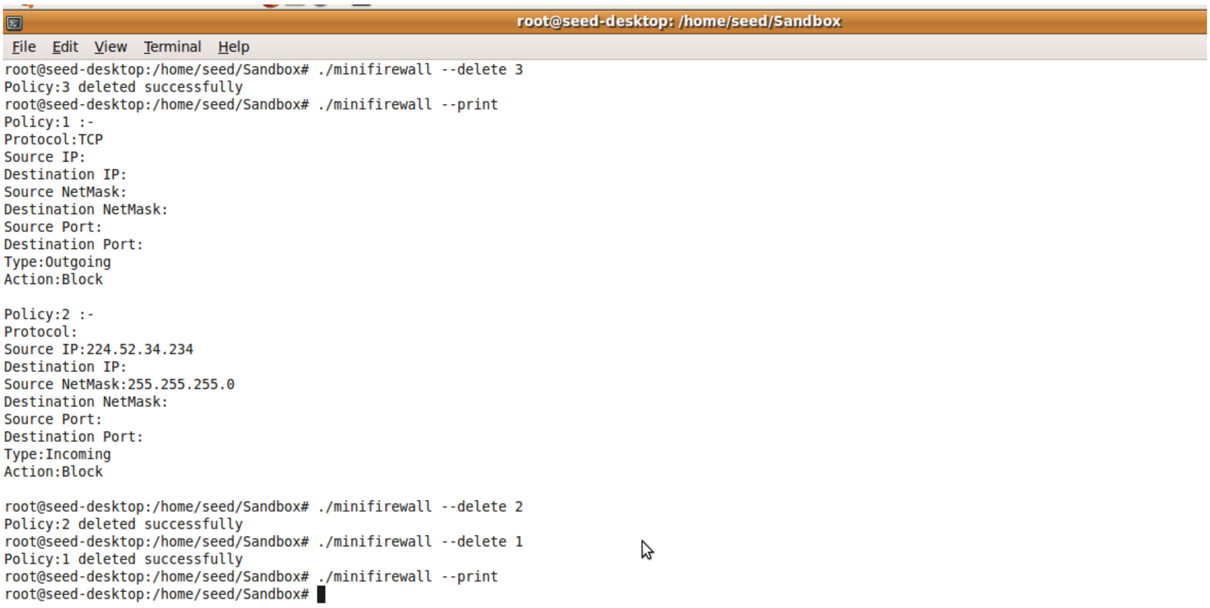
```
root@seed-desktop:/home/seed/Sandbox# ./minifirewall
Error in input. Please conform to the following formats(shown by examples):-

./minifirewall --in --action BLOCK
./minifirewall --out --action UNBLOCK
./minifirewall --print
./minifirewall --delete 2
./minifirewall --in --proto TCP --srcip 127.0.0.1 --destip 192.168.0.1 --srcnetmask 255.255.255.0 --destnetmask 255.255.0.0 --srcport 8
0 --destport 100 --action BLOCK

Aborted
root@seed-desktop:/home/seed/Sandbox# 
```

The screenshots below prove that the parameters were passed from user space to kernel space correctly, as it is able to write to and read from proc files via the utility options.

Sending parameters to kernel space via minifirewall:



```
root@seed-desktop:/home/seed/Sandbox# ./minifirewall --out --proto TCP --action BLOCK
root@seed-desktop:/home/seed/Sandbox# ./minifirewall --in --srcip 224.52.34.234 --srcnetmask 255.255.255.0 --action BLOCK
root@seed-desktop:/home/seed/Sandbox# ./minifirewall --in --destport 100 --action UNBLOCK
root@seed-desktop:/home/seed/Sandbox# ./minifirewall --print
Policy:1 :-
Protocol:TCP
Source IP:
Destination IP:
Source NetMask:
Destination NetMask:
Source Port:
Destination Port:
Type:Outgoing
Action:Block

Policy:2 :-
Protocol:
Source IP:224.52.34.234
Destination IP:
Source NetMask:255.255.255.0
Destination NetMask:
Source Port:
Destination Port:
Type:Incoming
Action:Block

Policy:3 :-
Protocol:
Source IP:
Destination IP:
Source NetMask:
Destination NetMask:
Source Port:
Destination Port:100
Type:Incoming
Action:UnBlock

root@seed-desktop:/home/seed/Sandbox# 
```


root@seed-desktop: /home/seed/Sandbox
File Edit View Terminal Help

```
root@seed-desktop:/home/seed/Sandbox# ./minifirewall --delete 3
Policy:3 deleted successfully
root@seed-desktop:/home/seed/Sandbox# ./minifirewall --print
Policy:1 :-
Protocol:TCP
Source IP:
Destination IP:
Source NetMask:
Destination NetMask:
Source Port:
Destination Port:
Type:Outgoing
Action:Block

Policy:2 :-
Protocol:
Source IP:224.52.34.234
Destination IP:
Source NetMask:255.255.255.0
Destination NetMask:
Source Port:
Destination Port:
Type:Incoming
Action:Block

root@seed-desktop:/home/seed/Sandbox# ./minifirewall --delete 2
Policy:2 deleted successfully
root@seed-desktop:/home/seed/Sandbox# ./minifirewall --delete 1
Policy:1 deleted successfully
root@seed-desktop:/home/seed/Sandbox# ./minifirewall --print
root@seed-desktop:/home/seed/Sandbox# 
```

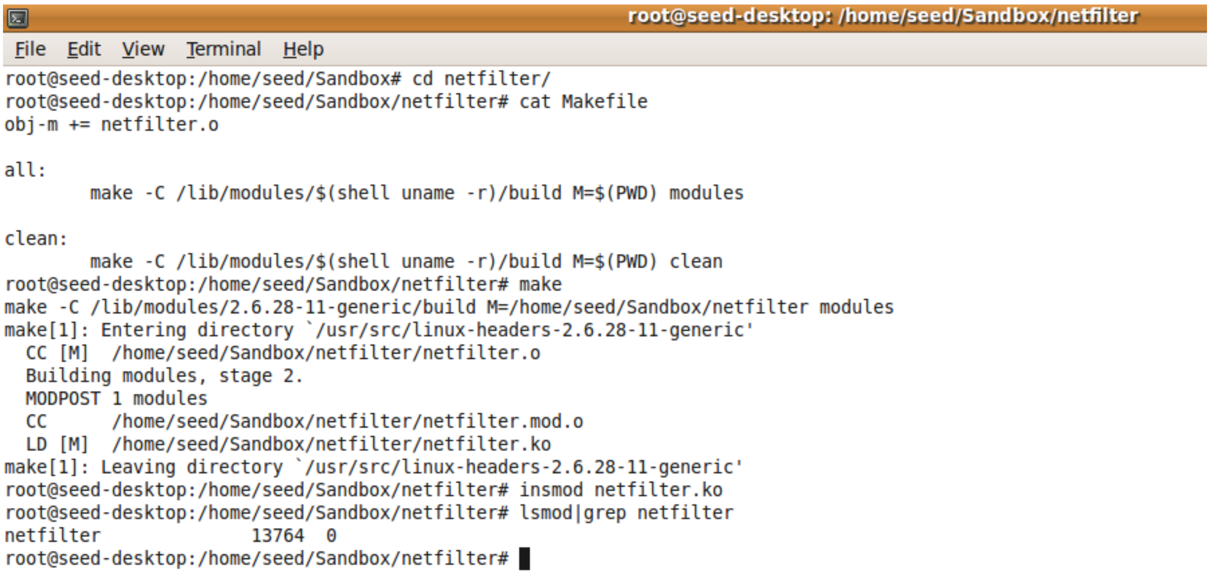
2. Successfully parse parameters in either kernel or user space

As shown by the screenshots (from (1)), the parameters were parsed successfully.

Task 2:

1. Successfully insert your module into linux kernel without causing kernel crash or panic

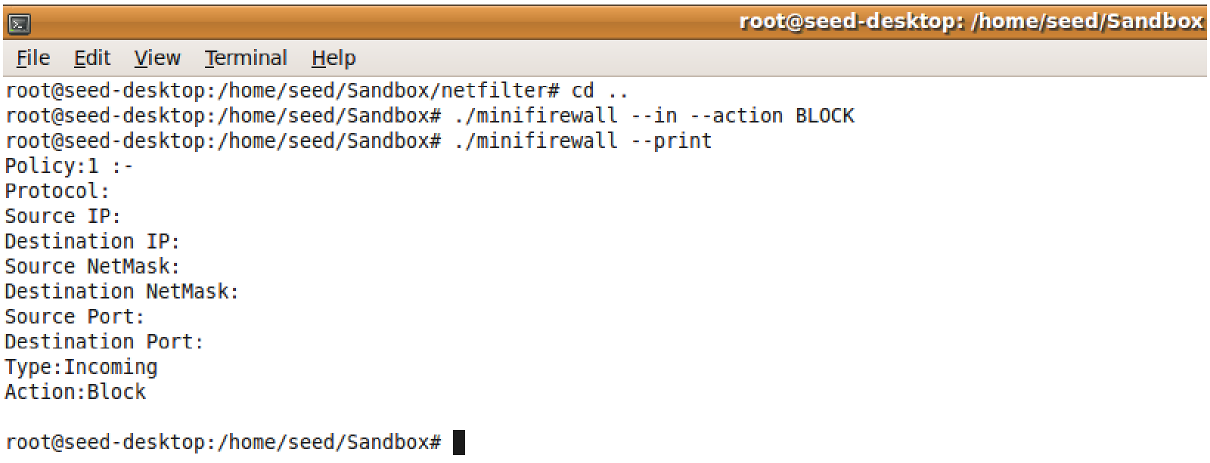
Screenshot:


root@seed-desktop: /home/seed/Sandbox/netfilter
File Edit View Terminal Help

```
root@seed-desktop:/home/seed/Sandbox# cd netfilter/
root@seed-desktop:/home/seed/Sandbox/netfilter# cat Makefile
obj-m += netfilter.o

all:
        make -C /lib/modules/$(shell uname -r)/build M=$(PWD) modules

clean:
        make -C /lib/modules/$(shell uname -r)/build M=$(PWD) clean
root@seed-desktop:/home/seed/Sandbox/netfilter# make
make -C /lib/modules/2.6.28-11-generic/build M=/home/seed/Sandbox/netfilter modules
make[1]: Entering directory `/usr/src/linux-headers-2.6.28-11-generic'
  CC [M]  /home/seed/Sandbox/netfilter/netfilter.o
  Building modules, stage 2.
  MODPOST 1 modules
  CC      /home/seed/Sandbox/netfilter/netfilter.mod.o
  LD [M]  /home/seed/Sandbox/netfilter/netfilter.ko
make[1]: Leaving directory `/usr/src/linux-headers-2.6.28-11-generic'
root@seed-desktop:/home/seed/Sandbox/netfilter# insmod netfilter.ko
root@seed-desktop:/home/seed/Sandbox/netfilter# lsmod|grep netfilter
netfilter              13764  0
root@seed-desktop:/home/seed/Sandbox/netfilter# 
```

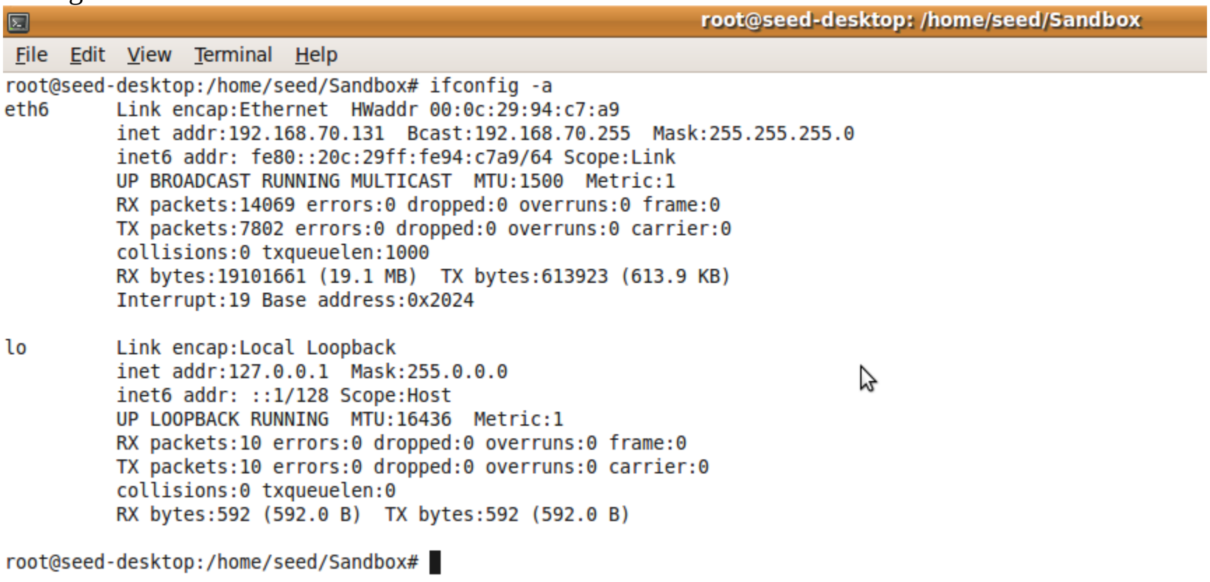
2. Successfully achieve all the functionality of packet filtering in examples

    a. Block all incoming traffic


root@seed-desktop: /home/seed/Sandbox
File Edit View Terminal Help

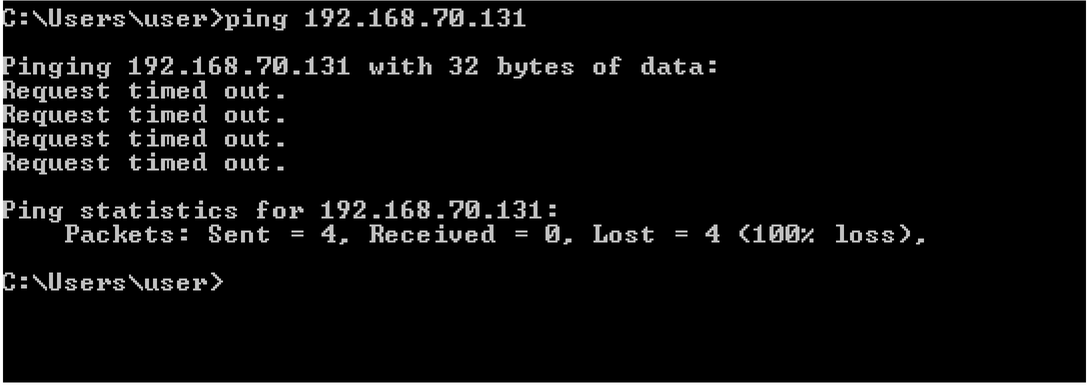
```
root@seed-desktop:/home/seed/Sandbox/netfilter# cd ..
root@seed-desktop:/home/seed/Sandbox# ./minifirewall --in --action BLOCK
root@seed-desktop:/home/seed/Sandbox# ./minifirewall --print
Policy:1 :-
Protocol:
Source IP:
Destination IP:
Source NetMask:
Destination NetMask:
Source Port:
Destination Port:
Type:Incoming
Action:Block

root@seed-desktop:/home/seed/Sandbox#
```

IP of guest Ubuntu VM:


root@seed-desktop: /home/seed/Sandbox
File Edit View Terminal Help

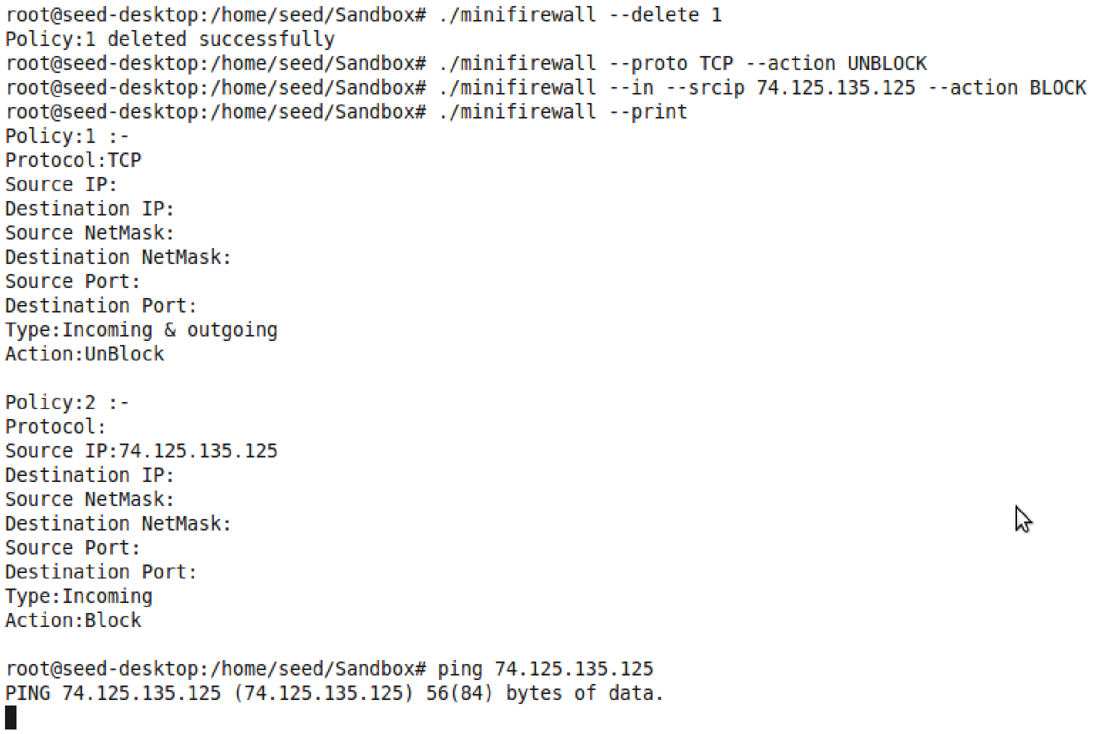
```
root@seed-desktop:/home/seed/Sandbox# ifconfig -a
eth6      Link encap:Ethernet  HWaddr 00:0c:29:94:c7:a9
          inet addr:192.168.70.131  Bcast:192.168.70.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe94:c7a9/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:14069 errors:0 dropped:0 overruns:0 frame:0
          TX packets:7802 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:19101661 (19.1 MB)  TX bytes:613923 (613.9 KB)
          Interrupt:19 Base address:0x2024

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:10 errors:0 dropped:0 overruns:0 frame:0
          TX packets:10 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:592 (592.0 B)  TX bytes:592 (592.0 B)

root@seed-desktop:/home/seed/Sandbox#
```

Ping from host windows:



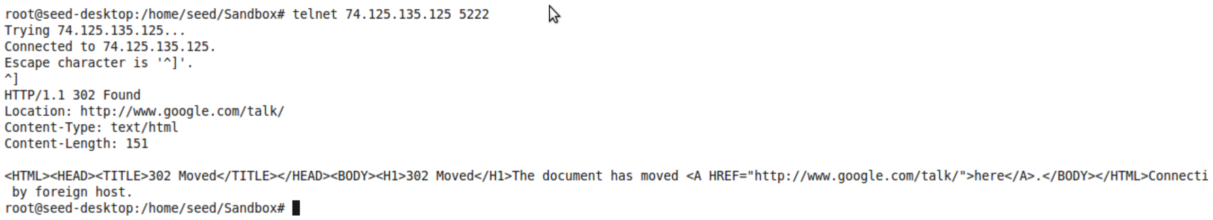
```
C:\Users\user>ping 192.168.70.131

Pinging 192.168.70.131 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.70.131:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\user>
```

b. Delete previous configuration, and add new one to Unblock TCP protocol and block all traffic coming from host IP address



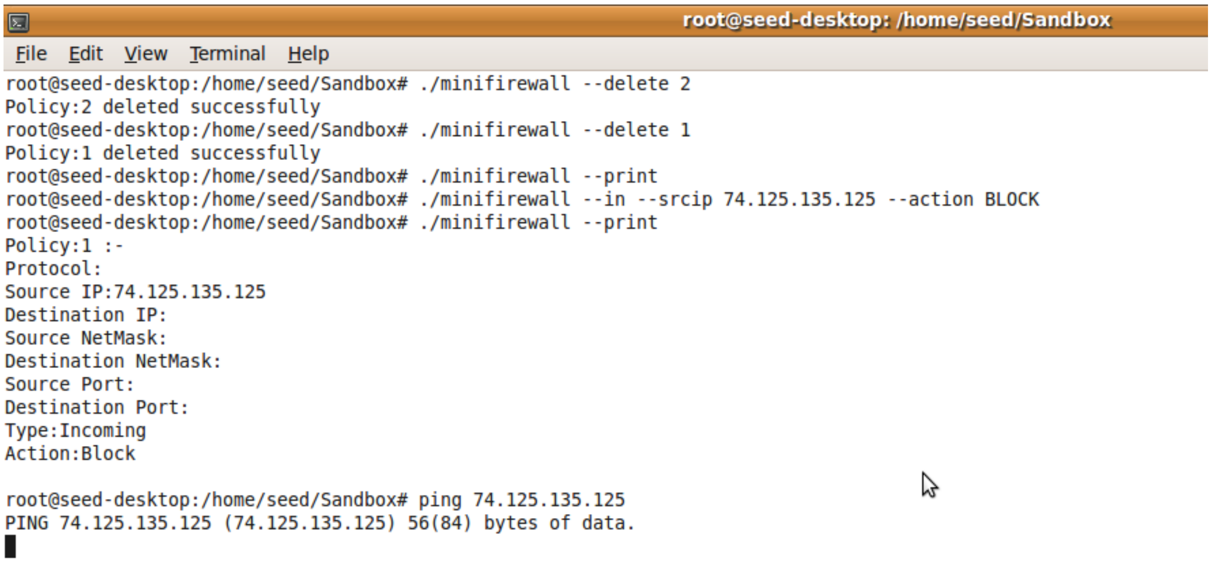
```
root@seed-desktop:/home/seed/Sandbox# ./minifirewall --delete 1
Policy:1 deleted successfully
root@seed-desktop:/home/seed/Sandbox# ./minifirewall --proto TCP --action UNBLOCK
root@seed-desktop:/home/seed/Sandbox# ./minifirewall --in --srcip 74.125.135.125 --action BLOCK
root@seed-desktop:/home/seed/Sandbox# ./minifirewall --print
Policy:1 :-
Protocol:TCP
Source IP:
Destination IP:
Source NetMask:
Destination NetMask:
Source Port:
Destination Port:
Type:Incoming & outgoing
Action:UnBlock

Policy:2 :-
Protocol:
Source IP:74.125.135.125
Destination IP:
Source NetMask:
Destination NetMask:
Source Port:
Destination Port:
Type:Incoming
Action:Block

root@seed-desktop:/home/seed/Sandbox# ping 74.125.135.125
PING 74.125.135.125 (74.125.135.125) 56(84) bytes of data.
```

Telnet works:



```
root@seed-desktop:/home/seed/Sandbox# telnet 74.125.135.125 5222
Trying 74.125.135.125...
Connected to 74.125.135.125.
Escape character is '^]'.
^]
HTTP/1.1 302 Found
Location: http://www.google.com/talk/
Content-Type: text/html
Content-Length: 151

<HTML><HEAD><TITLE>302 Moved</TITLE></HEAD><BODY><H1>302 Moved</H1>The document has moved <A HREF="http://www.google.com/talk/">here</A>.</BODY></HTML>Connecti
 by foreign host.
root@seed-desktop:/home/seed/Sandbox# 
```

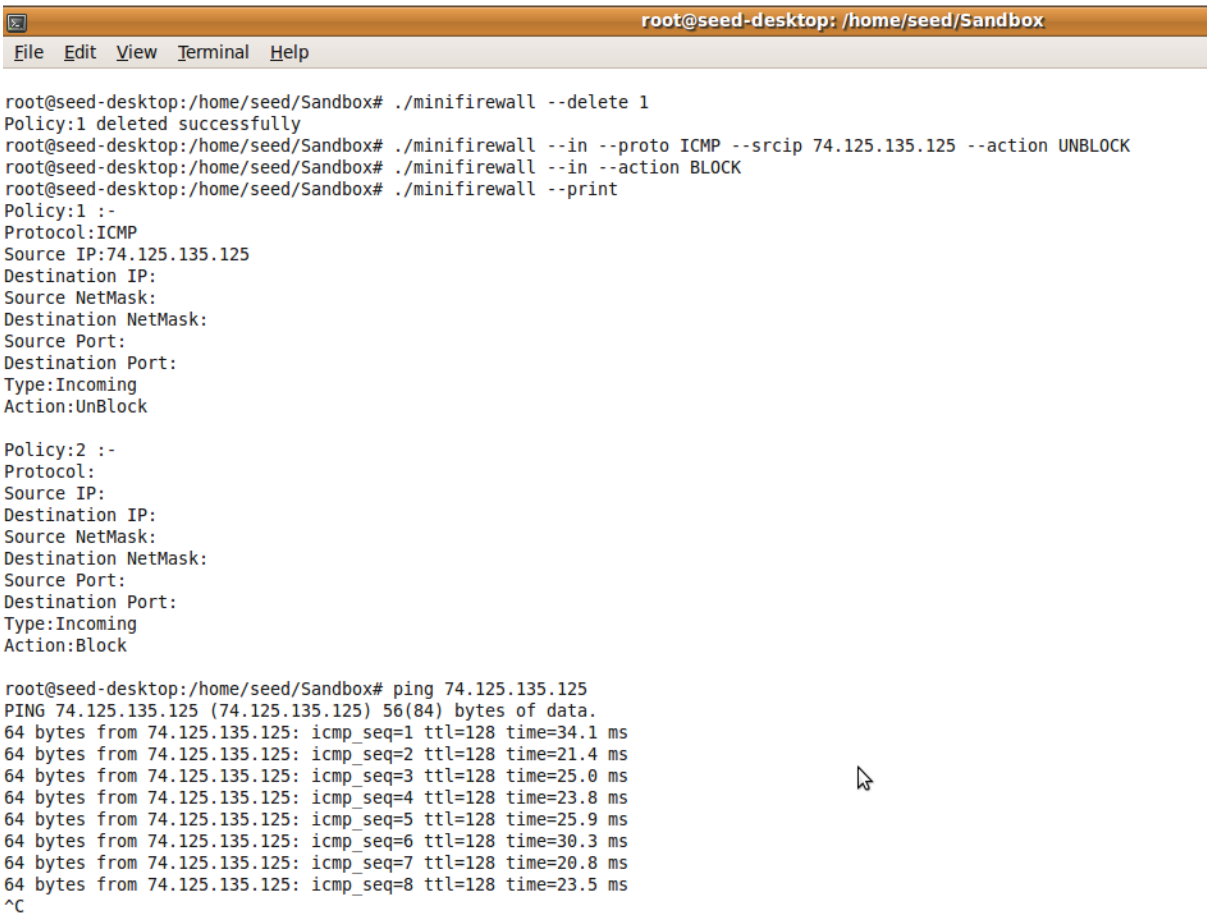
c. Delete previous configuration and add new one to block all traffic coming from Host IP address



root@seed-desktop: /home/seed/Sandbox
File Edit View Terminal Help

```
root@seed-desktop:/home/seed/Sandbox# ./minifirewall --delete 2
Policy:2 deleted successfully
root@seed-desktop:/home/seed/Sandbox# ./minifirewall --delete 1
Policy:1 deleted successfully
root@seed-desktop:/home/seed/Sandbox# ./minifirewall --print
root@seed-desktop:/home/seed/Sandbox# ./minifirewall --in --srcip 74.125.135.125 --action BLOCK
root@seed-desktop:/home/seed/Sandbox# ./minifirewall --print
Policy:1 :-
Protocol:
Source IP:74.125.135.125
Destination IP:
Source NetMask:
Destination NetMask:
Source Port:
Destination Port:
Type:Incoming
Action:Block

root@seed-desktop:/home/seed/Sandbox# ping 74.125.135.125
PING 74.125.135.125 (74.125.135.125) 56(84) bytes of data.
```

d. Delete previous configuration and new one to Unblock ICMP traffic from host IP address and block all other traffic.

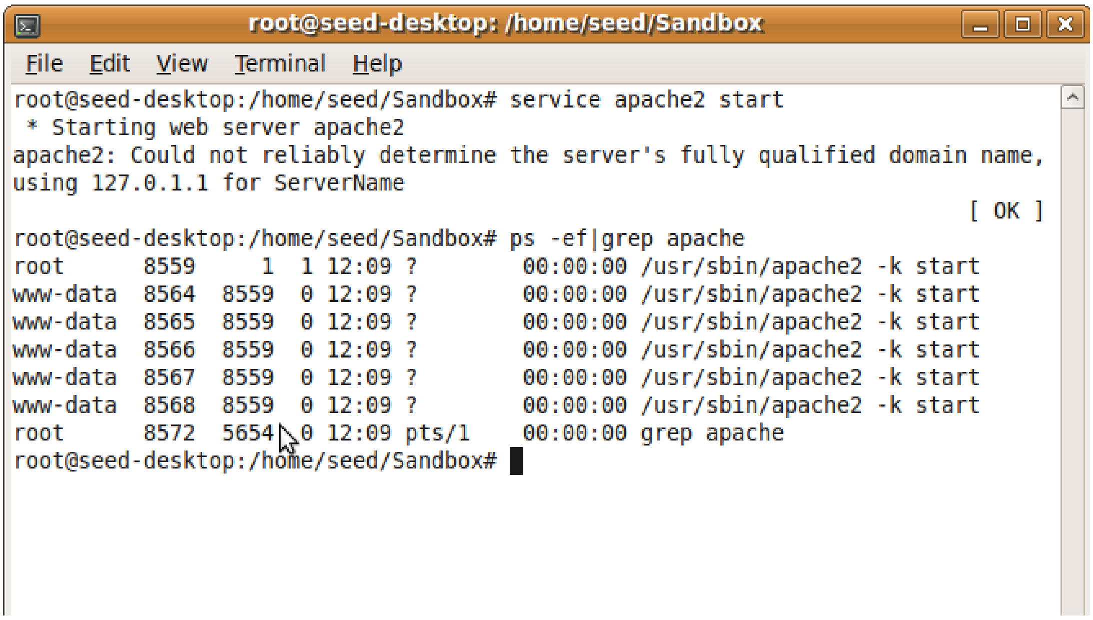

root@seed-desktop: /home/seed/Sandbox
File Edit View Terminal Help

```
root@seed-desktop:/home/seed/Sandbox# ./minifirewall --delete 1
Policy:1 deleted successfully
root@seed-desktop:/home/seed/Sandbox# ./minifirewall --in --proto ICMP --srcip 74.125.135.125 --action UNBLOCK
root@seed-desktop:/home/seed/Sandbox# ./minifirewall --in --action BLOCK
root@seed-desktop:/home/seed/Sandbox# ./minifirewall --print
Policy:1 :-
Protocol:ICMP
Source IP:74.125.135.125
Destination IP:
Source NetMask:
Destination NetMask:
Source Port:
Destination Port:
Type:Incoming
Action:UnBlock

Policy:2 :-
Protocol:
Source IP:
Destination IP:
Source NetMask:
Destination NetMask:
Source Port:
Destination Port:
Type:Incoming
Action:Block

root@seed-desktop:/home/seed/Sandbox# ping 74.125.135.125
PING 74.125.135.125 (74.125.135.125) 56(84) bytes of data.
64 bytes from 74.125.135.125: icmp_seq=1 ttl=128 time=34.1 ms
64 bytes from 74.125.135.125: icmp_seq=2 ttl=128 time=21.4 ms
64 bytes from 74.125.135.125: icmp_seq=3 ttl=128 time=25.0 ms
64 bytes from 74.125.135.125: icmp_seq=4 ttl=128 time=23.8 ms
64 bytes from 74.125.135.125: icmp_seq=5 ttl=128 time=25.9 ms
64 bytes from 74.125.135.125: icmp_seq=6 ttl=128 time=30.3 ms
64 bytes from 74.125.135.125: icmp_seq=7 ttl=128 time=20.8 ms
64 bytes from 74.125.135.125: icmp_seq=8 ttl=128 time=23.5 ms
^C
```

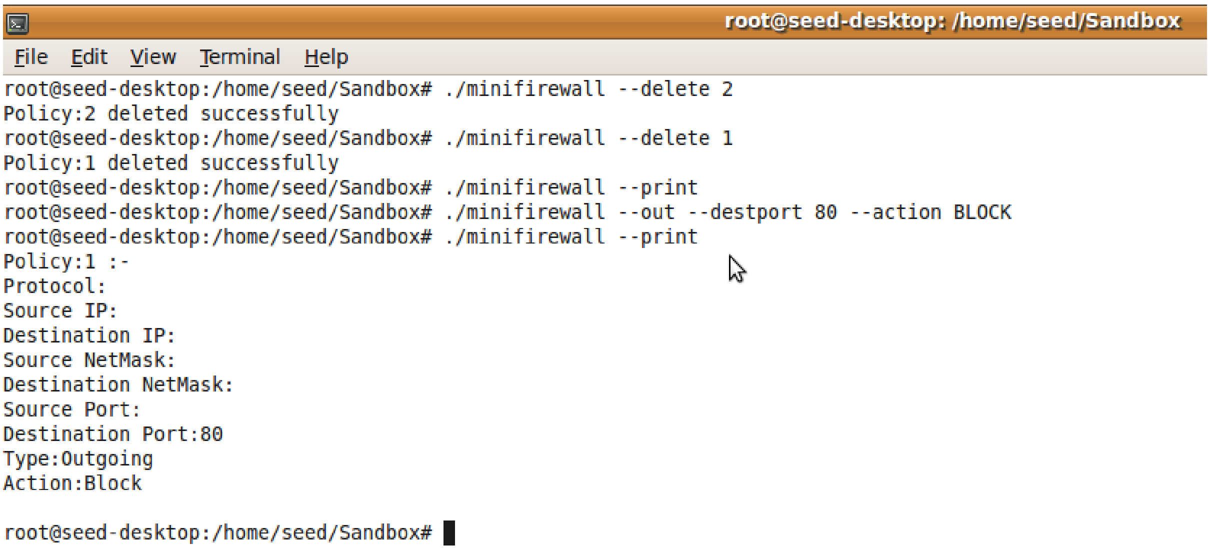
e. Delete previous configuration and add new one to block destination port number 80 in Guest Ubuntu VM

Port 80 is for HTTP server. To properly test the firewall configuration, the apache HTTP server will be utilized.

The apache server is started:


root@seed-desktop: /home/seed/Sandbox
File Edit View Terminal Help

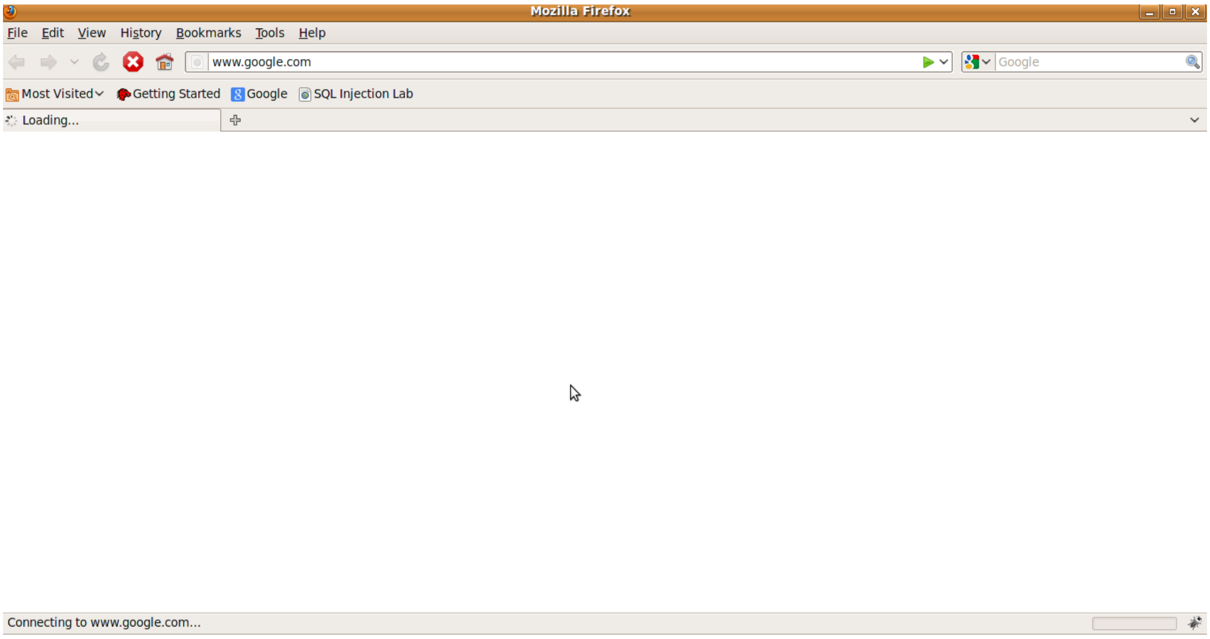
```
root@seed-desktop:/home/seed/Sandbox# service apache2 start
 * Starting web server apache2
apache2: Could not reliably determine the server's fully qualified domain name,
using 127.0.1.1 for ServerName
                                                                         [ OK ]
root@seed-desktop:/home/seed/Sandbox# ps -ef|grep apache
root      8559     1  1 12:09 ?        00:00:00 /usr/sbin/apache2 -k start
www-data  8564  8559  0 12:09 ?        00:00:00 /usr/sbin/apache2 -k start
www-data  8565  8559  0 12:09 ?        00:00:00 /usr/sbin/apache2 -k start
www-data  8566  8559  0 12:09 ?        00:00:00 /usr/sbin/apache2 -k start
www-data  8567  8559  0 12:09 ?        00:00:00 /usr/sbin/apache2 -k start
www-data  8568  8559  0 12:09 ?        00:00:00 /usr/sbin/apache2 -k start
root      8572  5654  0 12:09 pts/1    00:00:00 grep apache
root@seed-desktop:/home/seed/Sandbox# 
```



root@seed-desktop: /home/seed/Sandbox
File Edit View Terminal Help

```
root@seed-desktop:/home/seed/Sandbox# ./minifirewall --delete 2
Policy:2 deleted successfully
root@seed-desktop:/home/seed/Sandbox# ./minifirewall --delete 1
Policy:1 deleted successfully
root@seed-desktop:/home/seed/Sandbox# ./minifirewall --print
root@seed-desktop:/home/seed/Sandbox# ./minifirewall --out --destport 80 --action BLOCK
root@seed-desktop:/home/seed/Sandbox# ./minifirewall --print
Policy:1 :-
Protocol:
Source IP:
Destination IP:
Source NetMask:
Destination NetMask:
Source Port:
Destination Port:80
Type:Outgoing
Action:Block

root@seed-desktop:/home/seed/Sandbox# 
```

Result: When accessing a webpage, the request is discarded and the site does not open(example shown below via google.com)



Connecting to www.google.com...

Task 3:

1. Give a concise explanation of the modifications you made in the kernel module to ensure that only the user you specify and the "minifirewall" binary located in /usr/local/sbin can modify the kernel module (i.e. able to modify the firewall rules)

As of kernel version 2.6.20, task_struct cannot be used directly to retrieve the user id. The procedure to retrieve user id requires the use of function current_uid() present in <linux/cred.h>. The check for uid is done at the “write” functions of netfilter module by the code below:

if(current_uid()==0||current_uid()==1000)

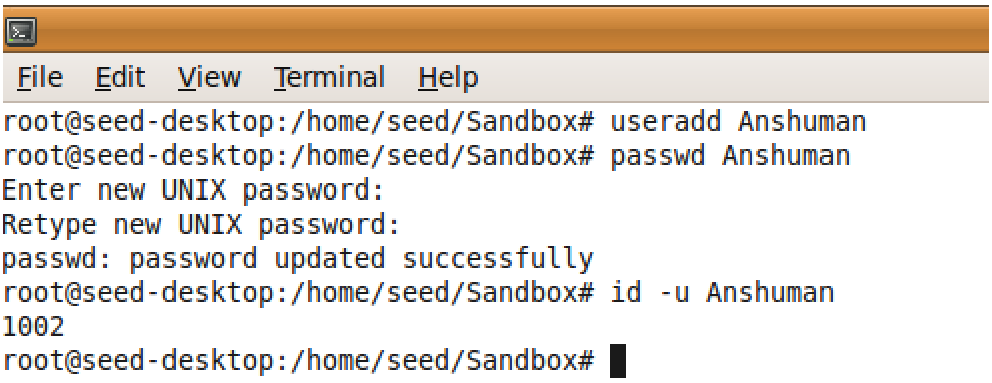
This allows only users of id:0(root) and 1000 to write to the proc files used by the module. For the non-root users to make changes to the proc files used, the permission for the proc files should be changed. This is done by the following:

proc_entry = create_proc_entry("netfilter",0646,NULL);
proc_entry_helper = create_proc_entry("netfilterhelper",0646,NULL);

0646 allows the root and other users to read from and write into the proc file.

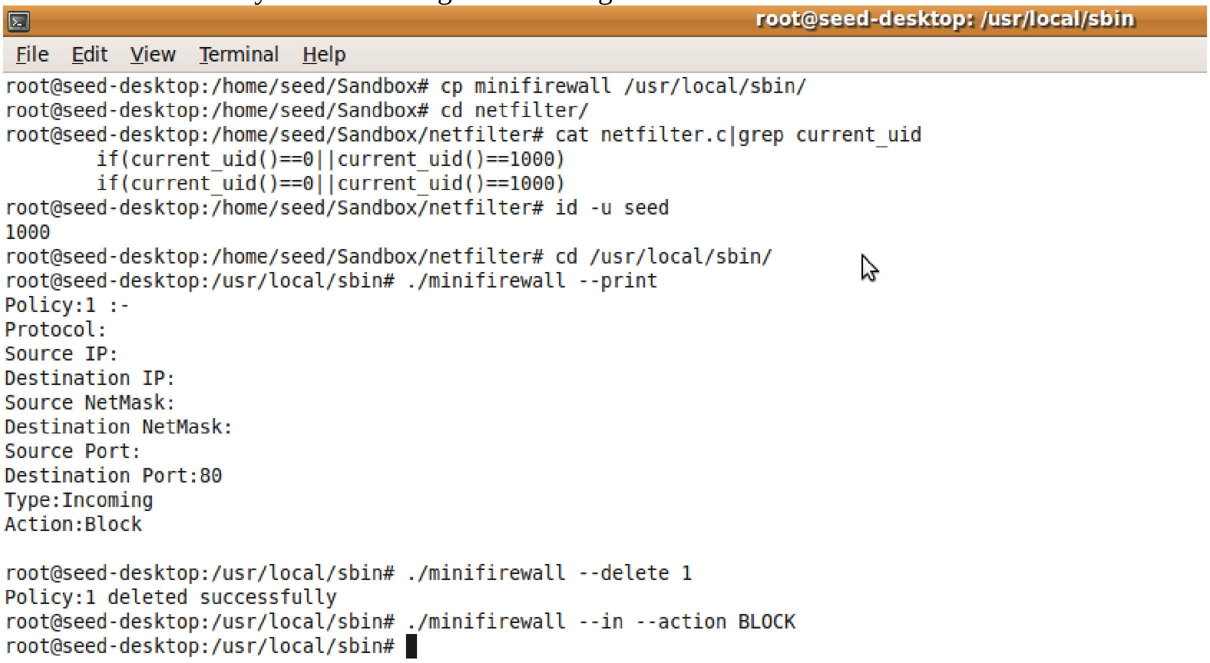
2. Using description or screenshot, give a demonstration that any other user cannot modify the firewall rules

Adding a new user named “Anshuman” to the system:



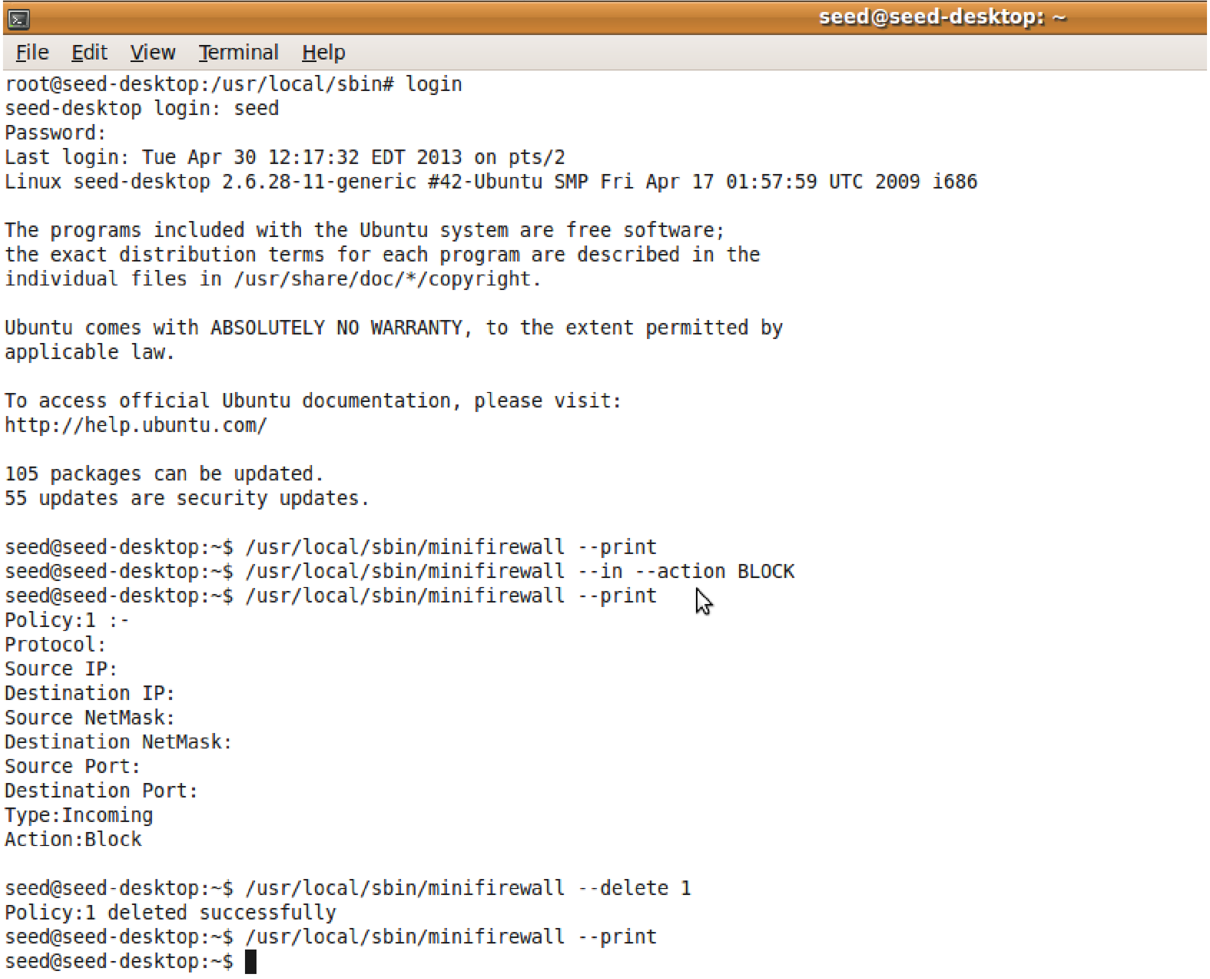
```
root@seed-desktop:/home/seed/Sandbox# useradd Anshuman
root@seed-desktop:/home/seed/Sandbox# passwd Anshuman
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
root@seed-desktop:/home/seed/Sandbox# id -u Anshuman
1002
root@seed-desktop:/home/seed/Sandbox# 
```

The screenshot below shows that the utility was transferred to /usr/local/sbin. It then shows the changes that were made to the module code in netfilter.c to allow the user:seed with id:1000 to use the minifirewall utility and be able to write to the necessary /proc files. As shown by the steps at the end, the user:seed is successfully able to write to and read from proc files, thus accessing the minifirewall utility to make configuration changes.



```
root@seed-desktop:/home/seed/Sandbox# cp minifirewall /usr/local/sbin/
root@seed-desktop:/home/seed/Sandbox# cd netfilter/
root@seed-desktop:/home/seed/Sandbox/netfilter# cat netfilter.c|grep current_uid
        if(current_uid()==0||current_uid()==1000)
        if(current_uid()==0||current_uid()==1000)
root@seed-desktop:/home/seed/Sandbox/netfilter# id -u seed
1000
root@seed-desktop:/home/seed/Sandbox/netfilter# cd /usr/local/sbin/
root@seed-desktop:/usr/local/sbin# ./minifirewall --print
Policy:1 :-
Protocol:
Source IP:
Destination IP:
Source NetMask:
Destination NetMask:
Source Port:
Destination Port:80
Type:Incoming
Action:Block

root@seed-desktop:/usr/local/sbin# ./minifirewall --delete 1
Policy:1 deleted successfully
root@seed-desktop:/usr/local/sbin# ./minifirewall --in --action BLOCK
root@seed-desktop:/usr/local/sbin# 
```

Screenshot showing that any other user different from “root” and “seed” were not able to make configuration changes via minifirewall utility:



```
root@seed-desktop:/usr/local/sbin# login
seed-desktop login: seed
Password:
Last login: Tue Apr 30 12:17:32 EDT 2013 on pts/2
Linux seed-desktop 2.6.28-11-generic #42-Ubuntu SMP Fri Apr 17 01:57:59 UTC 2009 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/

105 packages can be updated.
55 updates are security updates.

seed@seed-desktop:~$ /usr/local/sbin/minifirewall --print
seed@seed-desktop:~$ /usr/local/sbin/minifirewall --in --action BLOCK
seed@seed-desktop:~$ /usr/local/sbin/minifirewall --print
Policy:1 :-
Protocol:
Source IP:
Destination IP:
Source NetMask:
Destination NetMask:
Source Port:
Destination Port:
Type:Incoming
Action:Block

seed@seed-desktop:~$ /usr/local/sbin/minifirewall --delete 1
Policy:1 deleted successfully
seed@seed-desktop:~$ /usr/local/sbin/minifirewall --print
seed@seed-desktop:~$ 
```