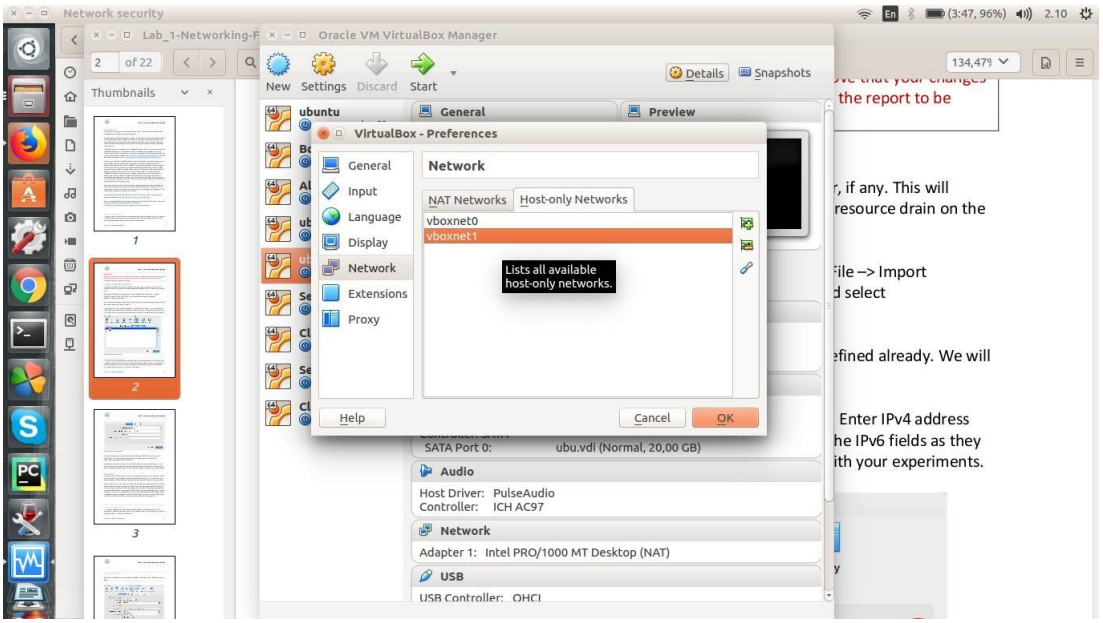
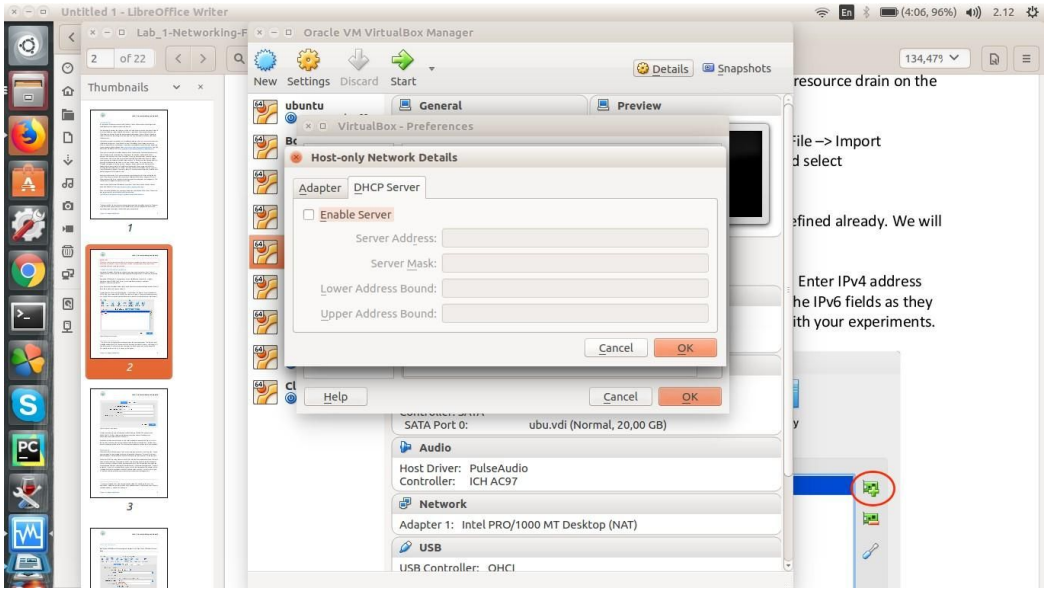
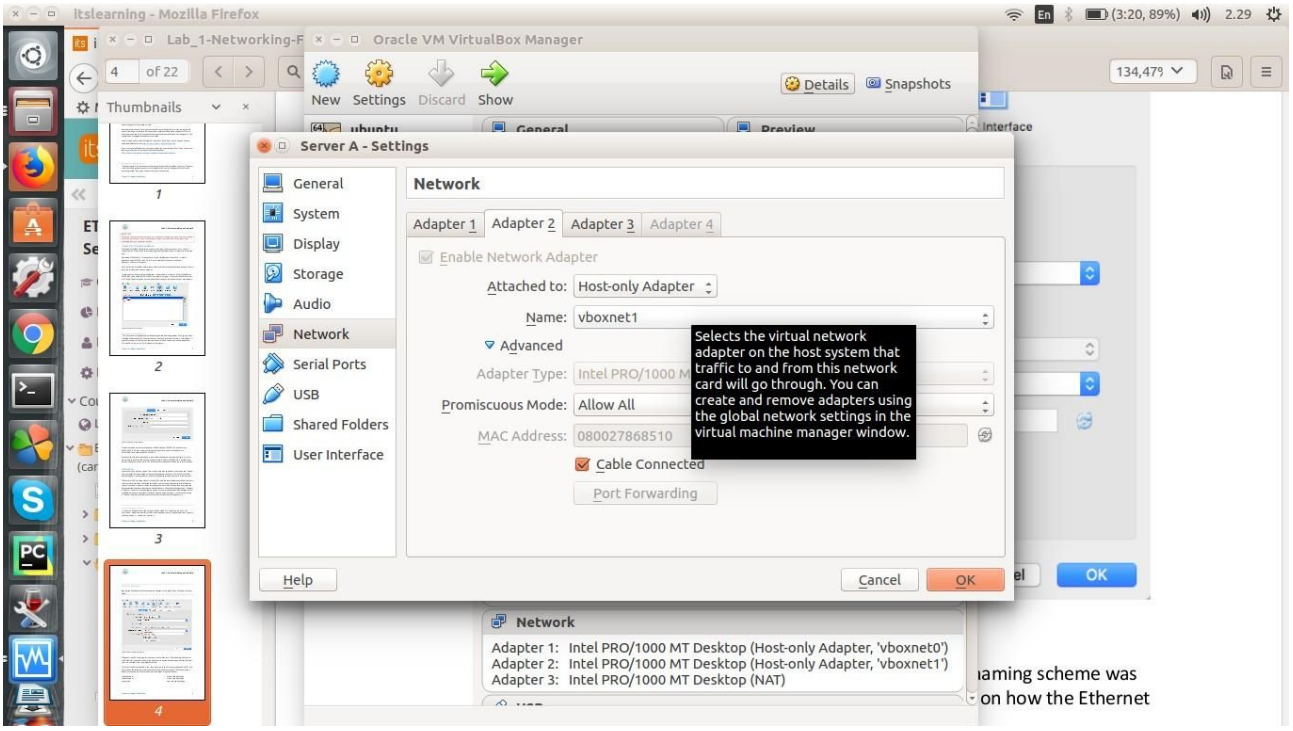
LAB 1.1
(security)
Saddam Hossen
9112301917

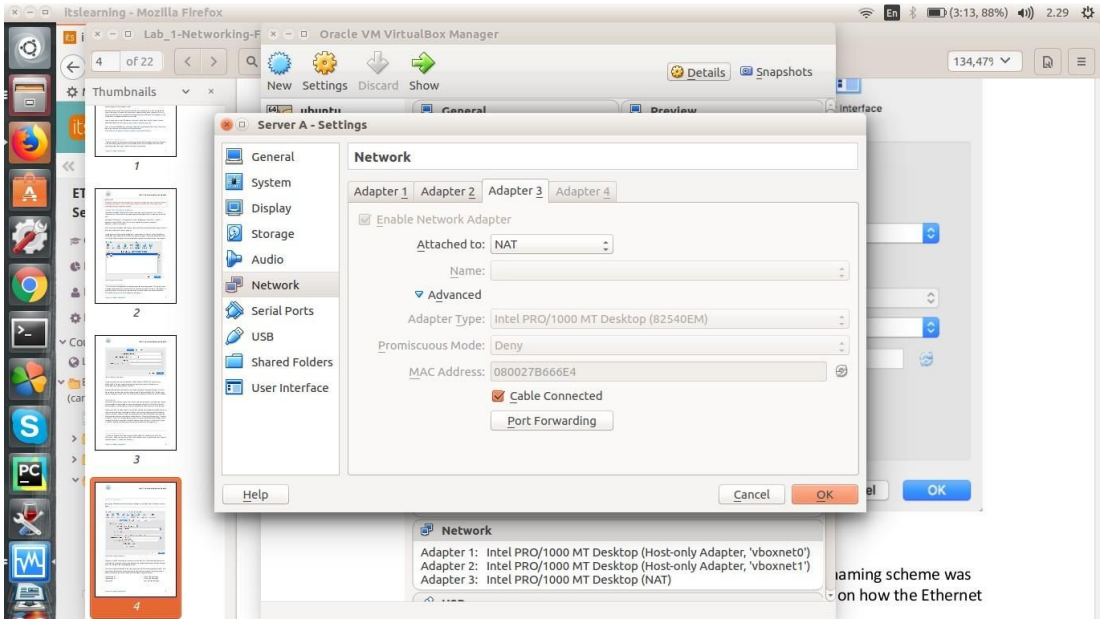
Task 1: MAC addresses:

I have created 2 Host only adapter and one NAT adapter.









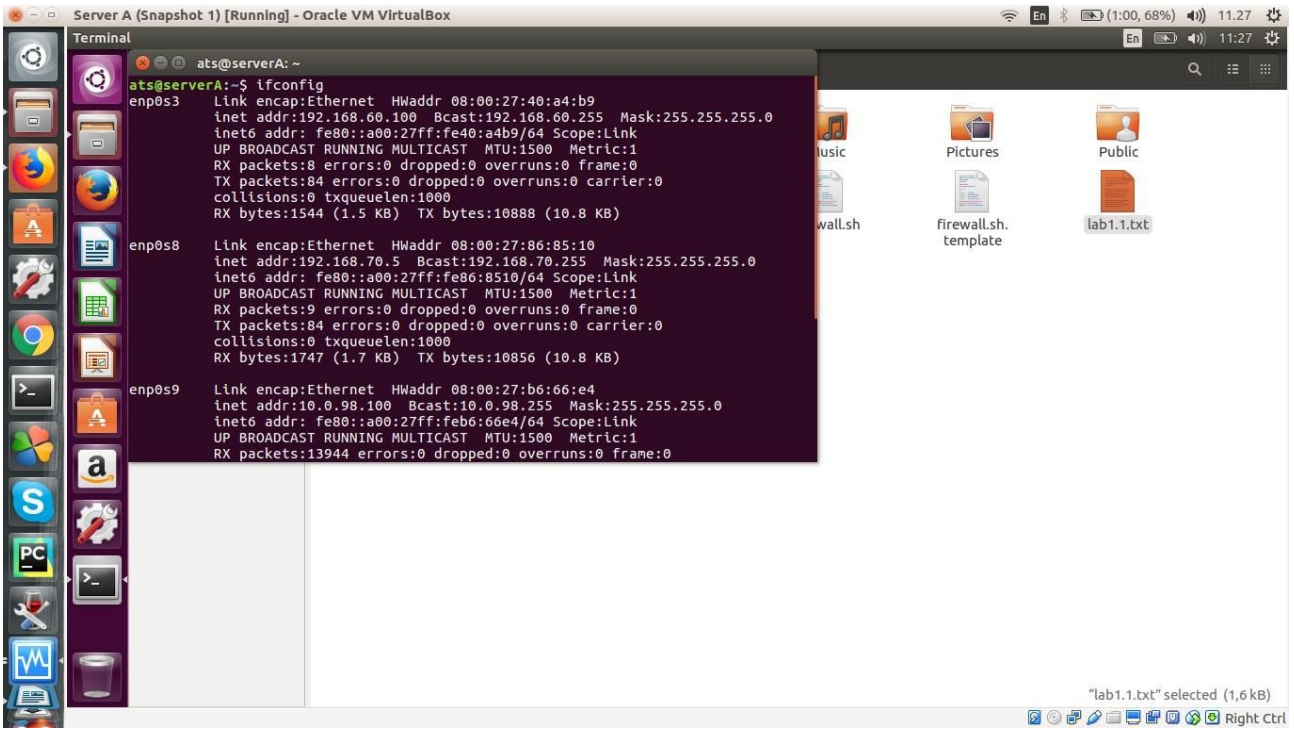
Interface:----------MAC Addresses

vboxnet0 ----------08002740A4B9
vboxnet1----------080027868510
NAT----------080027B666E4

Task 2: Network interfaces

iface ip mac

enp0s3----------192.168.60.100---------08002740A4B9---Host Only Adapter
enp0s8----------192.168.70.5-----------080027868510---Host Only Adapter
enp0s9----------10.0.98.100-------------080027B666E4-- NAT Adapter



Task 3: IP addresses, netmasks and subnet

NAT interface auto
enp0s9
iface enp0s9 inet static address
10.0.98.100
netmask 255.255.255.0

Network address: 10.0.98.0

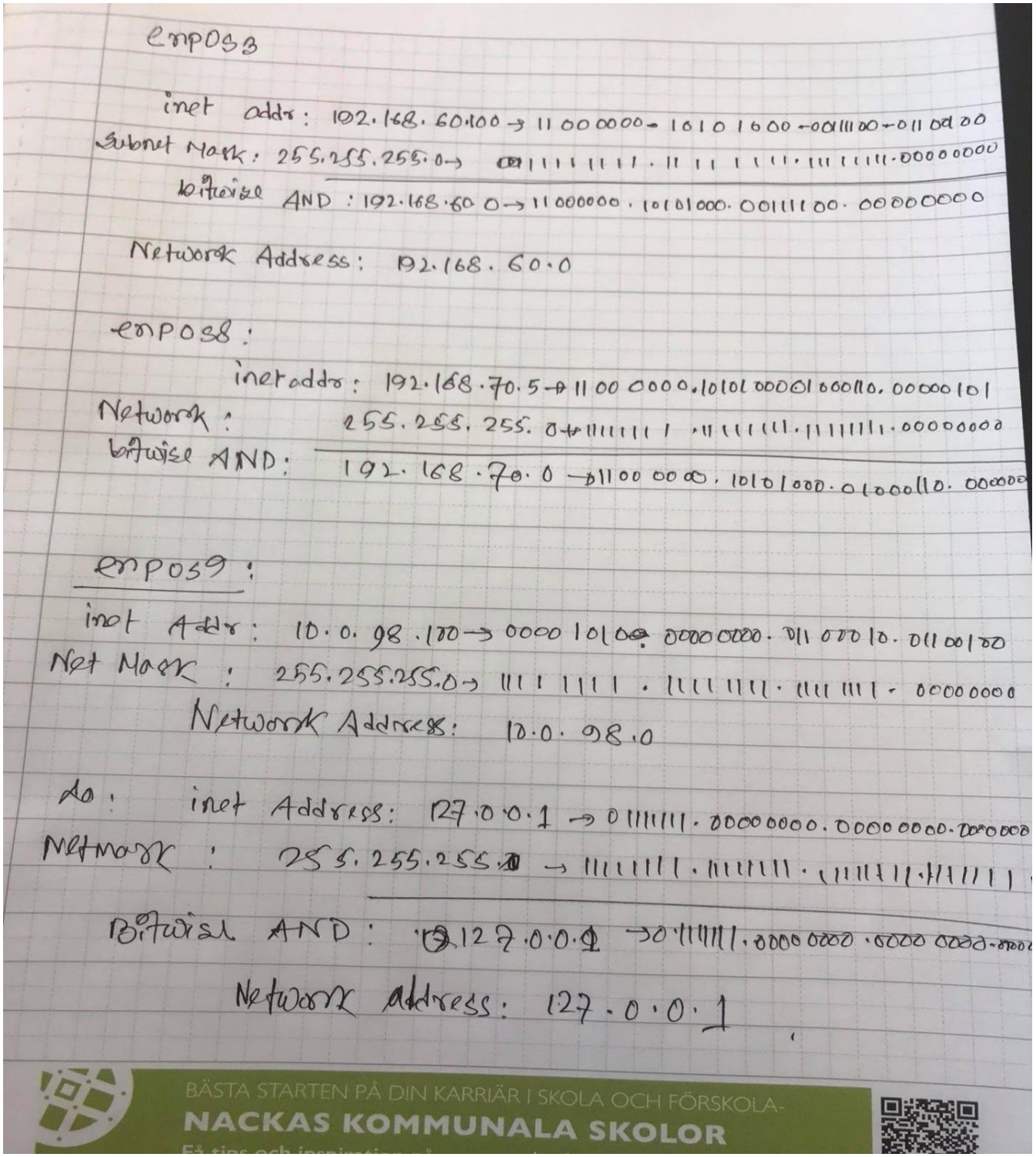
dns-nameservers 10.0.98.3
gateway 10.0.98.2

Host-only interface (for internal use) auto enp0s3
iface enp0s3 inet static address
192.168.60.100
netmask 255.255.255.0

Network address: 10.0.60.0

Host-only interface (for exernal use) auto enp0s8
iface enp0s8 inet static address
192.168.70.5
netmask 255.255.255.0

Network address: 10.0.70.0



Task 4: Host-only interfaces

iface: ip: mask::

enp0s3---------192.168.60.100 255.255.255.0
enp0s8---------192.168.70.5 255.255.255.0
enp0s9---------10.0.98.100 255.0.0.0

Kernel IP routing table

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
0.0.0.0	10.0.98.2	0.0.0.0	UG	0	0	0	enp0s9
10.0.98.0	0.0.0.0	255.255.255.0	U	0	0	0	enp0s9
169.254.0.0	0.0.0.0	255.255.0.0	U	1000	0	0	enp0s3
192.168.60.0	0.0.0.0	255.255.255.0	U	0	0	0	enp0s3
192.168.70.0	0.0.0.0	255.255.255.0	U	0	0	0	enp0s8

ats@serverA:~$ ip -4 route
default via 10.0.98.2 dev enp0s9 onlink
10.0.98.0/24 dev enp0s9 proto kernel scope link src 10.0.98.100
169.254.0.0/16 dev enp0s3 scope link metric 1000
192.168.60.0/24 dev enp0s3 proto kernel scope link src 192.168.60.100
192.168.70.0/24 dev enp0s8 proto kernel scope link src 192.168.70.5

Host-only interface	----------	----IPv4 Address	----------Subnet Mask
vboxnet0		192.168.60.1	255.255.255.0
vboxnet1		192.168.70.1	255.255.255.0
vboxnet2		192.168.80.1	255.255.255.0

By the command ipconfig/all in the host OS, I can get interface list from host OS. The available host-only interfaces are vboxnet0, vboxnet1 and vboxnet2

Through enp0s9 I can reach the defaut gateway because enp0s9 is the default gateway interface.

Task 5: Routing tables in the host OS

By using netstat -4

–rn route -n

ip -4 route

on host os I got this…

```
saddam@saddam-bth:~$ ip -4 route
default via 192.168.0.1 dev wlp2s0  proto static  metric 600
169.254.0.0/16 dev wlp2s0  scope link  metric 1000
192.168.0.0/24 dev wlp2s0  proto kernel  scope link  src 192.168.0.7  metric 600
192.168.56.0/24 dev vboxnet0  proto kernel  scope link  src 192.168.56.1
192.168.57.0/24 dev vboxnet1  proto kernel  scope link  src 192.168.57.1
192.168.58.0/24 dev vboxnet2  proto kernel  scope link  src 192.168.58.1
192.168.122.0/24 dev virbr0  proto kernel  scope link  src 192.168.122.1 linkdown

saddam@saddam-bth:~$
```

Default gateway to connect the internet is wlp2s0

(wifi). For interface wlp2s0 I can reach by the

default gateway 192.168.0.1

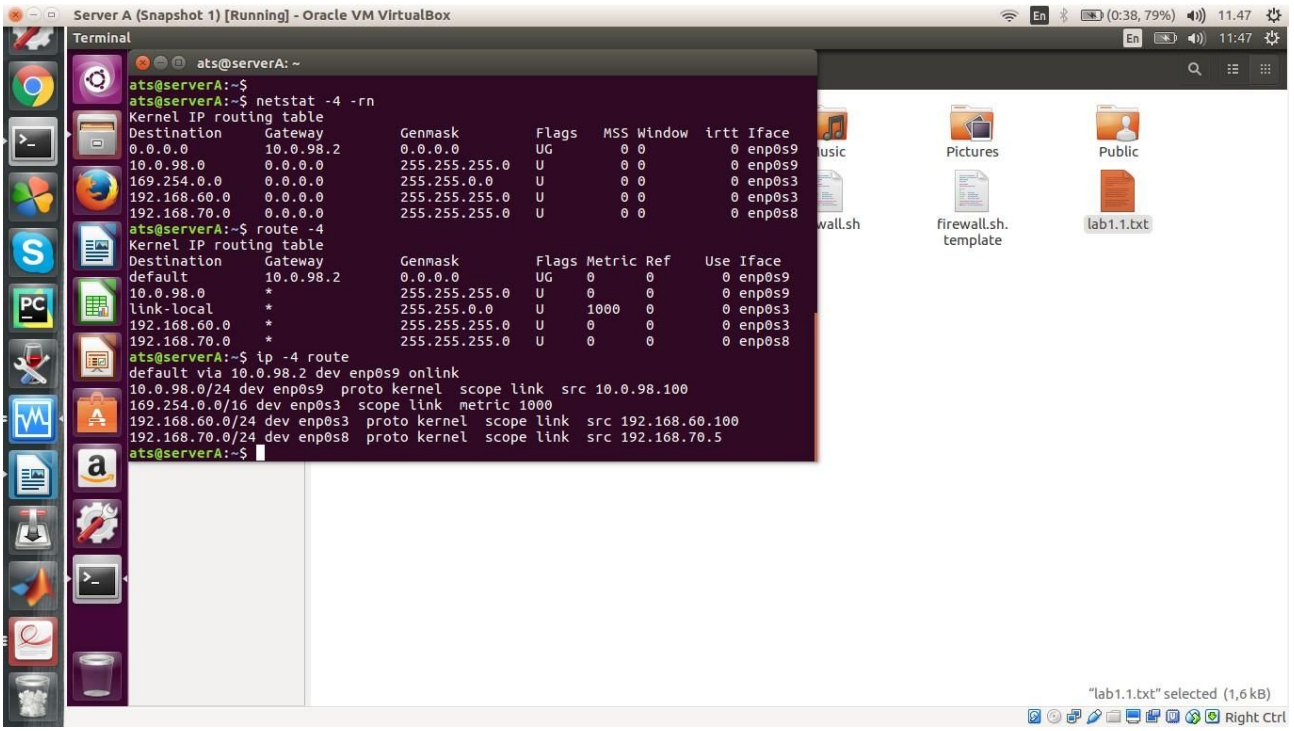
Task 6: Routing tables in the guest OS

By using netstat -4

–rn route -n

ip -4 route

on guest os I got this



I have reached the default gateway 10.0.98.2 by interface enp0s9.

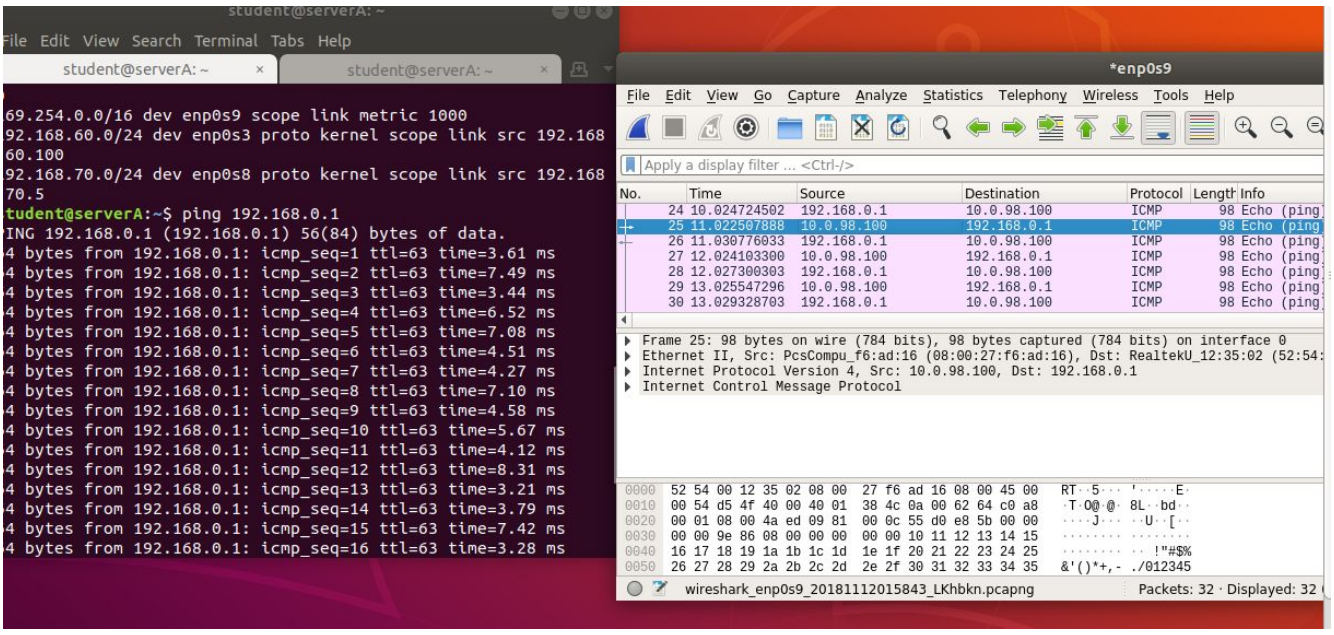
enp0s9 is NAT interface.

Task 7: Ping the host-based host-onlyinterface

Ping accordingly and got below icmp request and reply both Host and Guest OS.

At guest OS, ping the IP address 192.168.60.1 which is corresponding of the host only interface in the host OS. Then I have stopped the ping and taken Wireshark screenshot. From the screenshot .I can observe that the ICMP traffic of the Wireshark are identical.

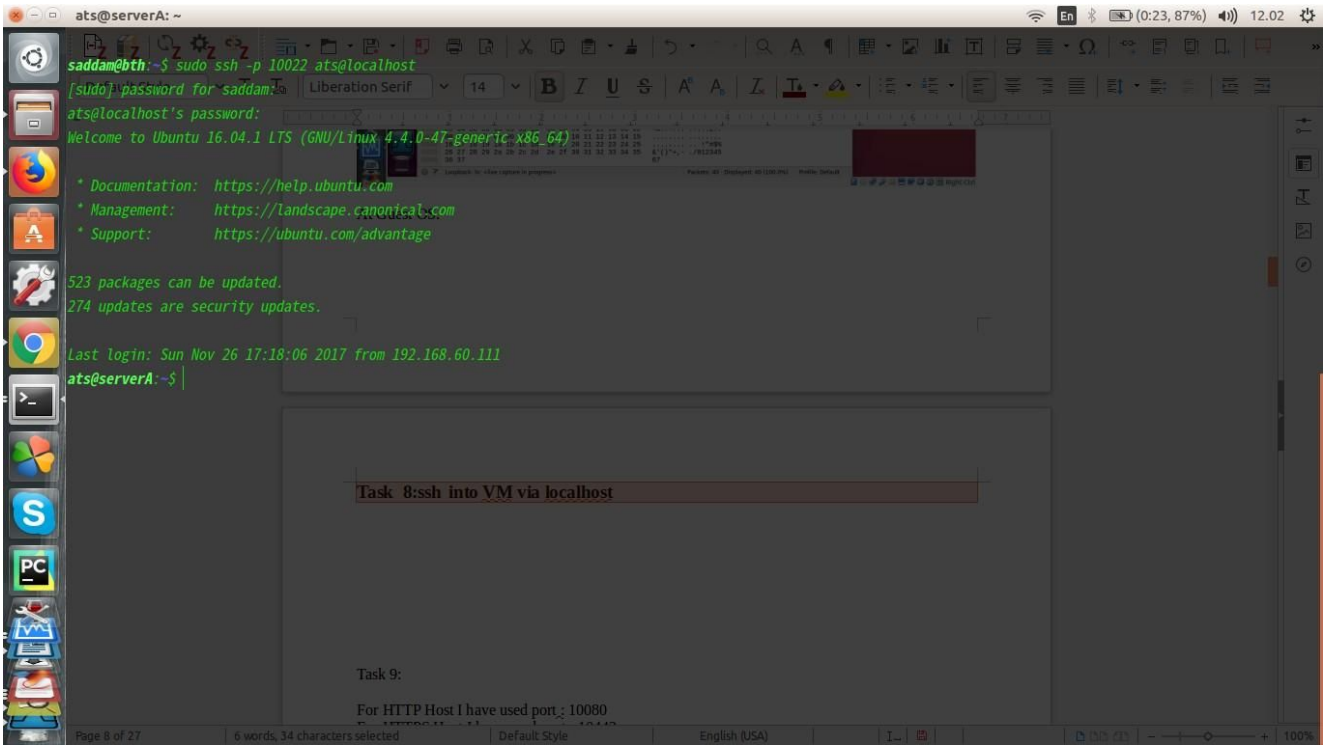
At Host OS



Task 8: ssh into VM via localhost

I have opened a remote shell to Server A and I can run any console commands in it log into serverA from host OS.

sudo ssh -p 10022 ats@localhost

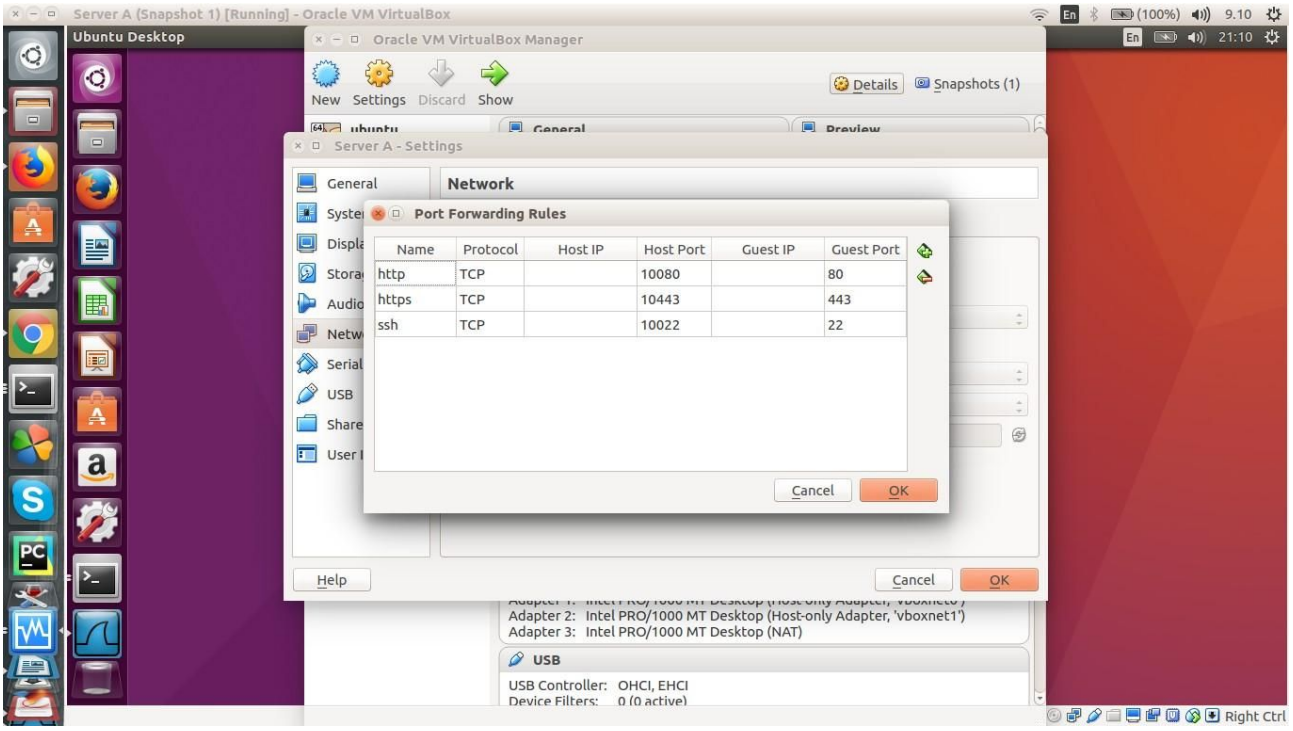


Task 9:

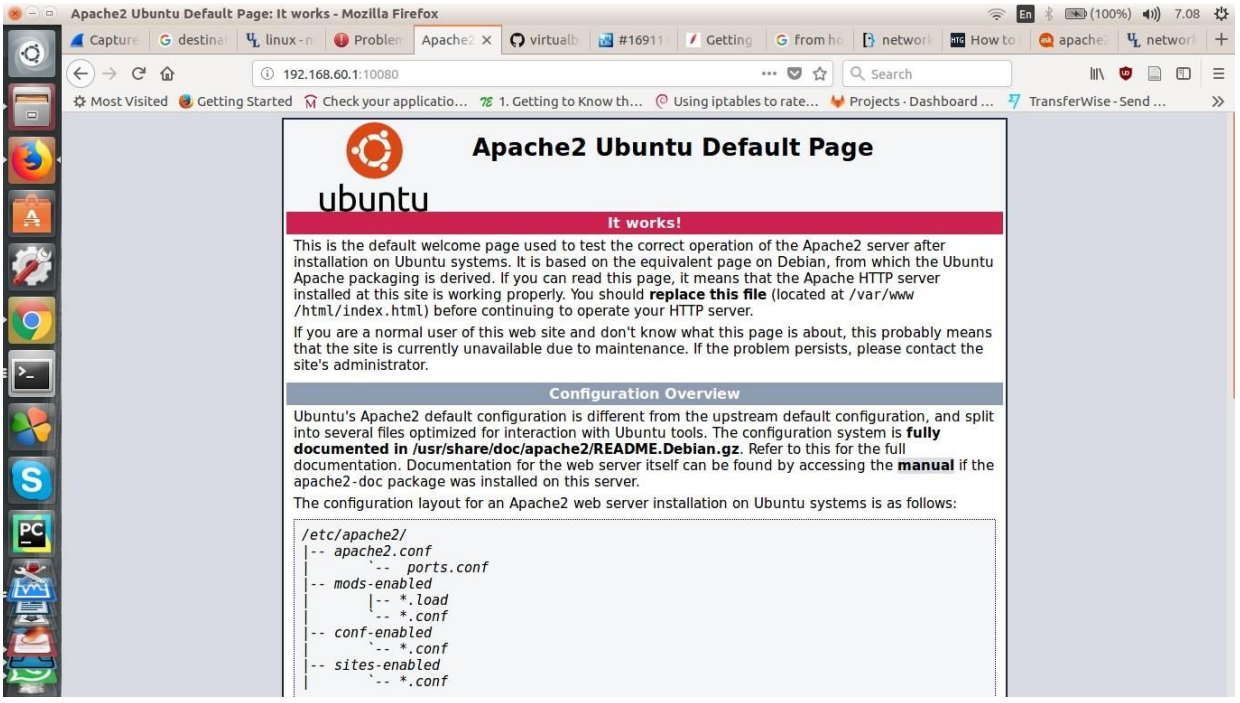
For HTTP Host I have used port :
10080 For HTTPS Host I have used
port : 10443

For HTTP Guest I have used port :
80 For HTTP Guest I have used port
: 443

Here host port number 10080 for HTTP and 10443 for HTTPS

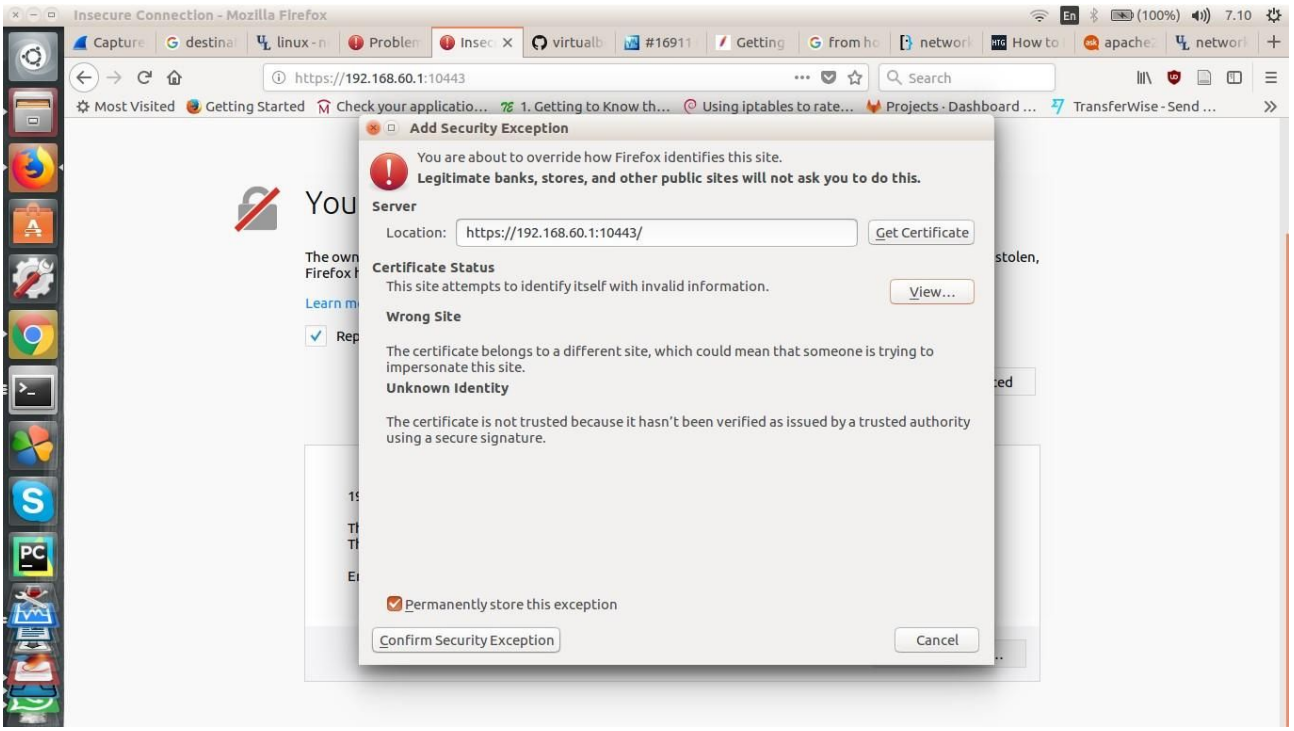

Server A (Snapshot 1) [Running] - Oracle VM VirtualBox
Ubuntu Desktop
Oracle VM VirtualBox Manager
New
Settings
Discard
Show
Details
Snapshots (1)
Server A - Settings
General
Network
Port Forwarding Rules
Name
Protocol
Host IP
Host Port
Guest IP
Guest Port
http
TCP
10080
80
https
TCP
10443
443
ssh
TCP
10022
22
Cancel
OK
Help
Adapter 2: Intel PRO/1000 MT Desktop (Host-only Adapter, 'vboxnet1')
Adapter 3: Intel PRO/1000 MT Desktop (NAT)
USB
USB Controller: OHCI, EHCI
Right Ctrl

x

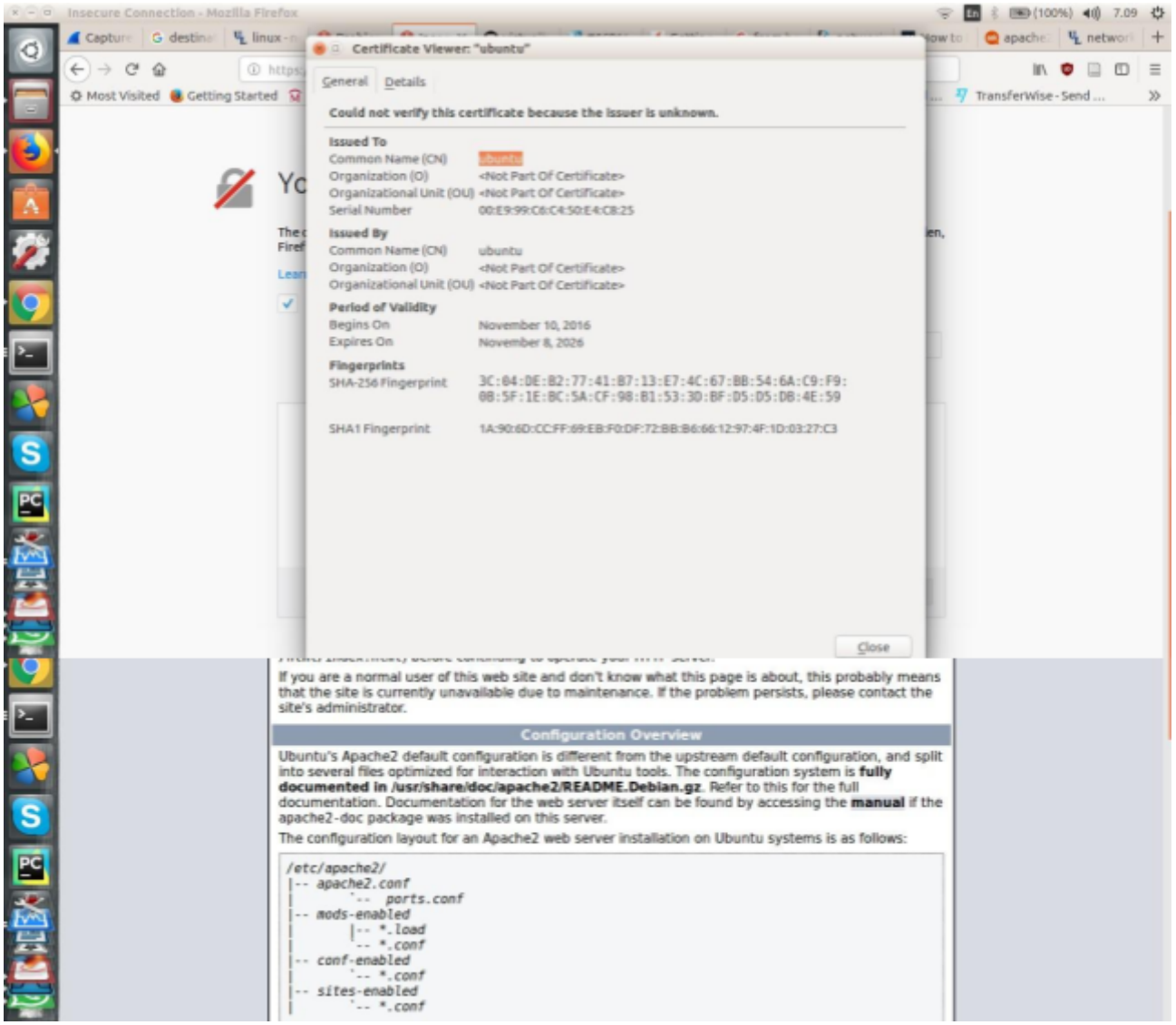

Apache2 Ubuntu Default Page: It works - Mozilla Firefox
192.168.60.1:10080
Apache2 Ubuntu Default Page
ubuntu
It works!
This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should replace this file (located at /var/www/html/index.html) before continuing to operate your HTTP server.
If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.
Configuration Overview
Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is fully documented in /usr/share/doc/apache2/README.Debian.gz. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the manual if the apache2-doc package was installed on this server.
The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:
/etc/apache2/
|-- apache2.conf
| `-- ports.conf
|-- mods-enabled
| |-- *.load
| `-- *.conf
|-- conf-enabled
| `-- *.conf
|-- sites-enabled
| `-- *.conf

For Host

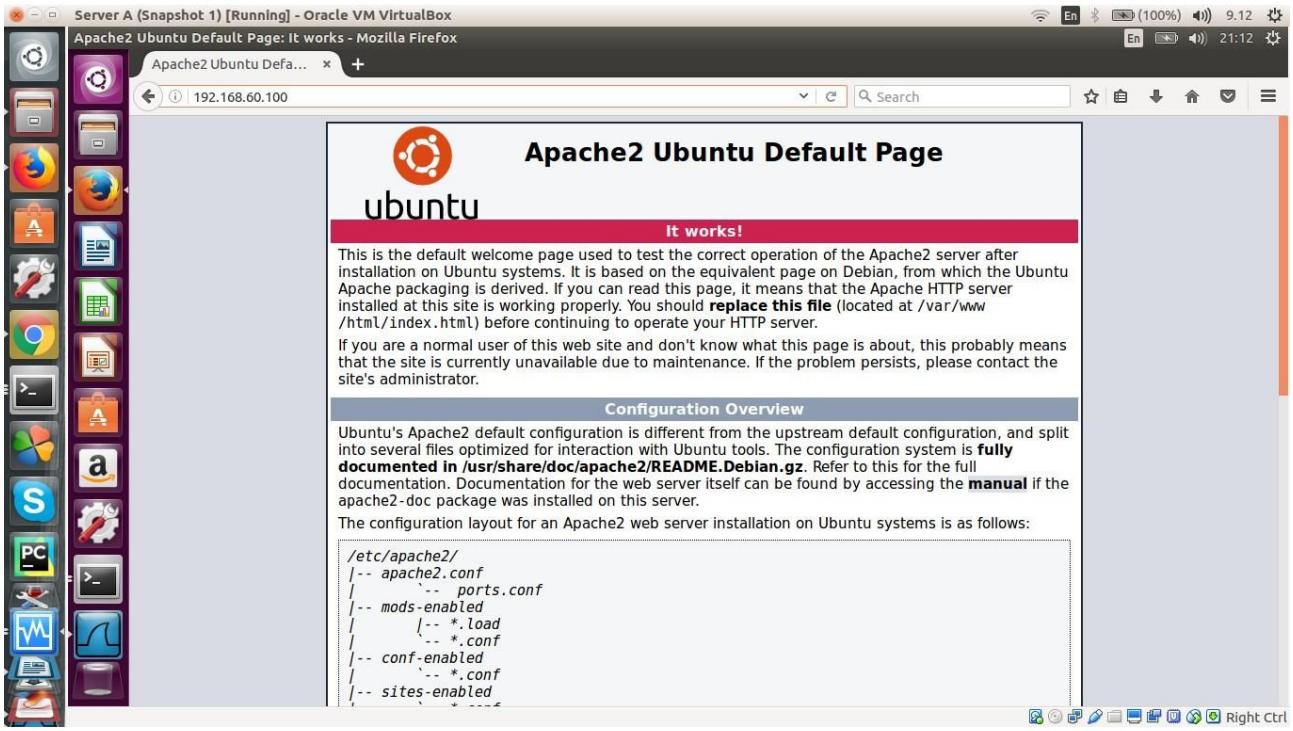
Host HTTPS



HOST HTTPS



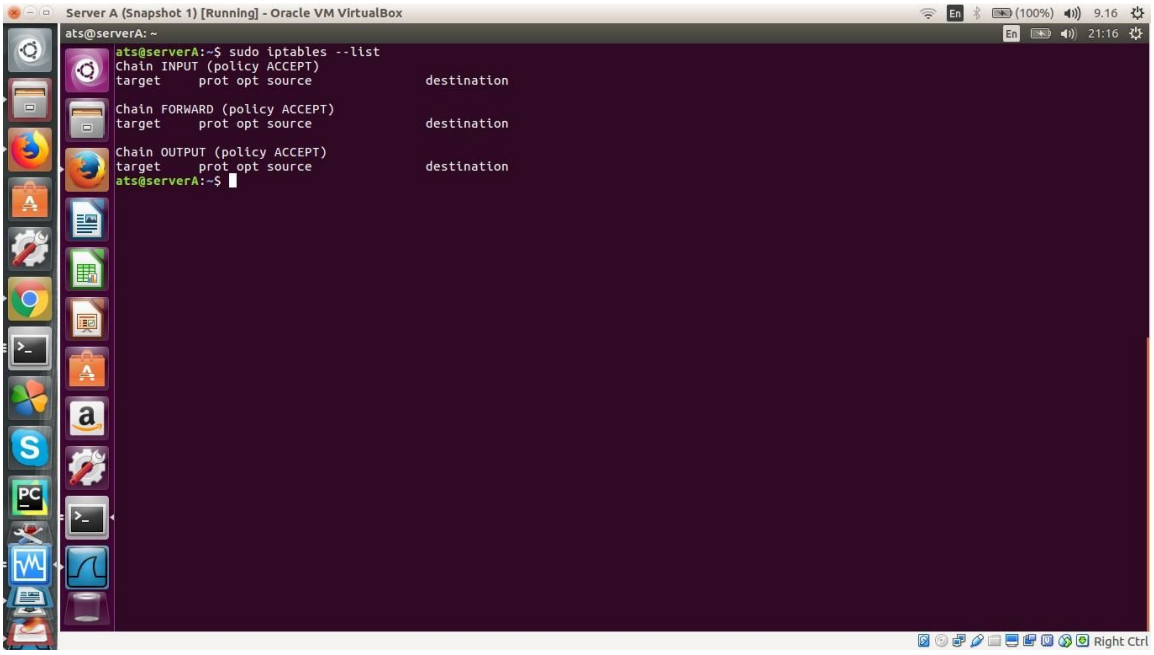
Host: Https



Guest Apache2 server.

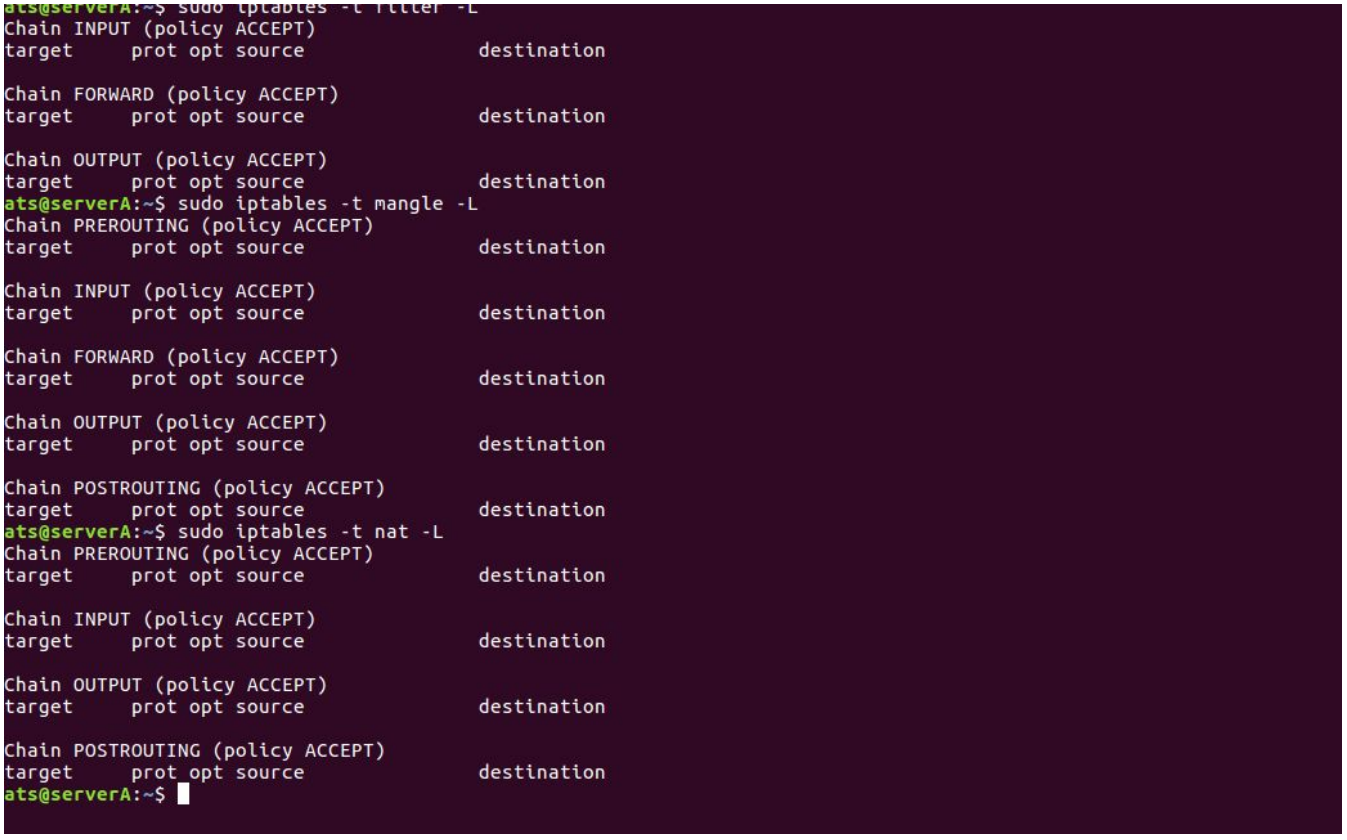
Task 10:

After giving *sudo iptables --list* command I got the below list and it showing all chain(INPUT,OUTPUT,FORWARD) will accept all data. There is no Drop or return filter used. This is the default policy.



I have run the following commands for filter, mangle, and nat rules:

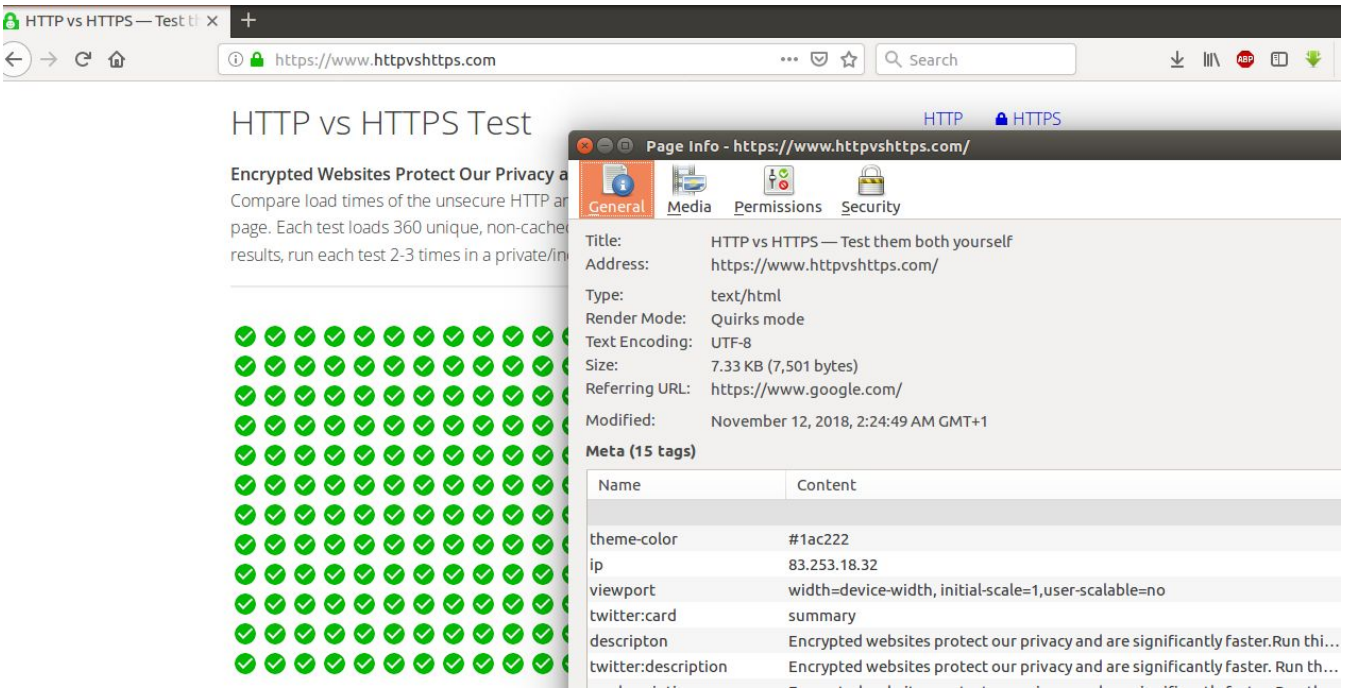
sudo iptables –t filter -L
sudo iptables –t mangle -L
sudo iptables –t nat -L



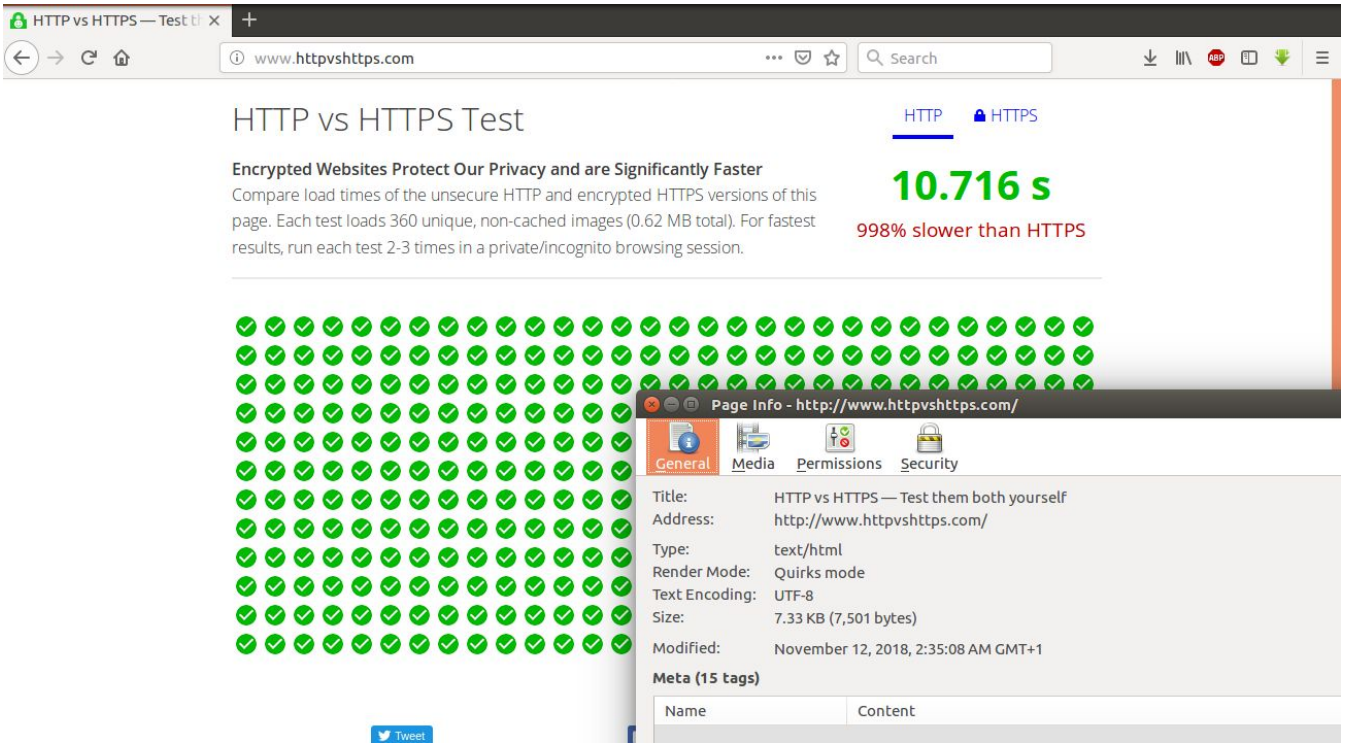
Task 11:Block HTTP-browsing in the guest OS

To verify http and htttps connection to the host and guest os I have used http://www.httpvshttps.com/ url as per instruction.

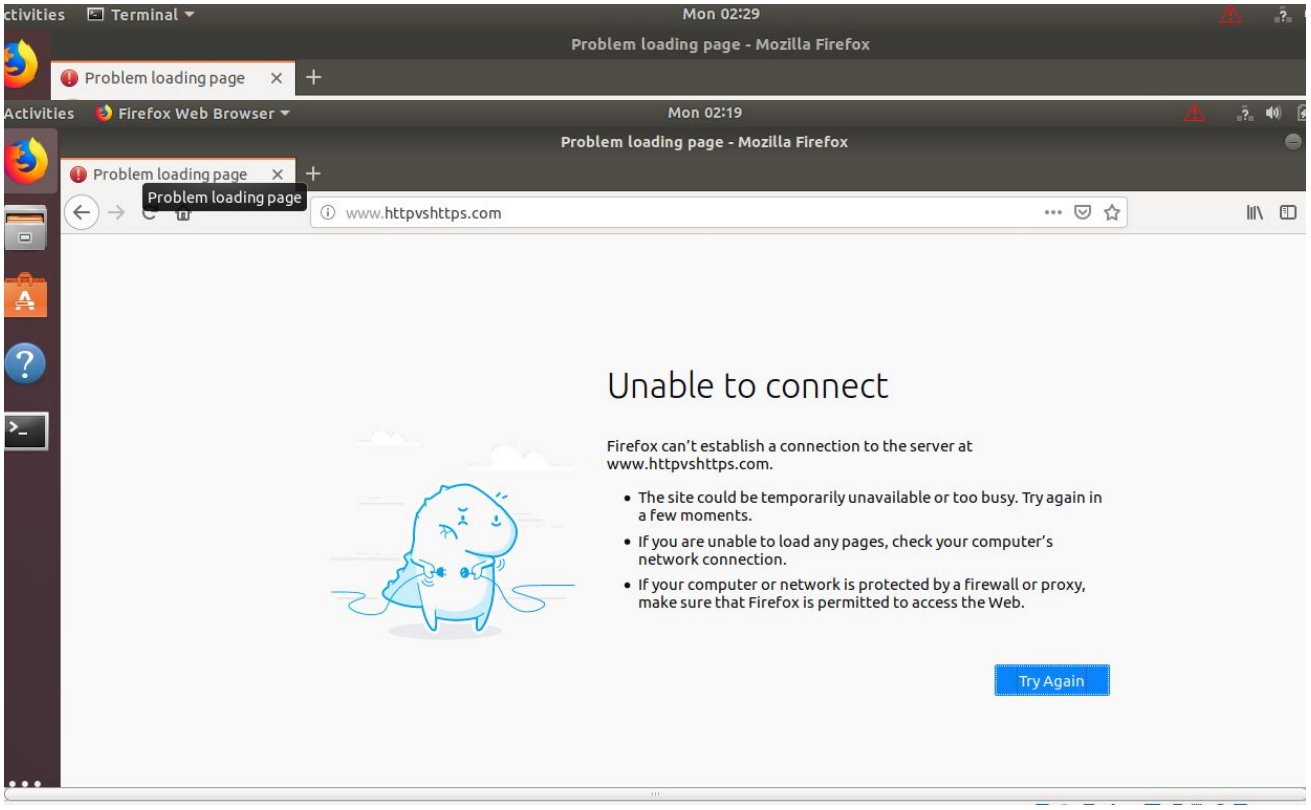
For Host : HTTPS



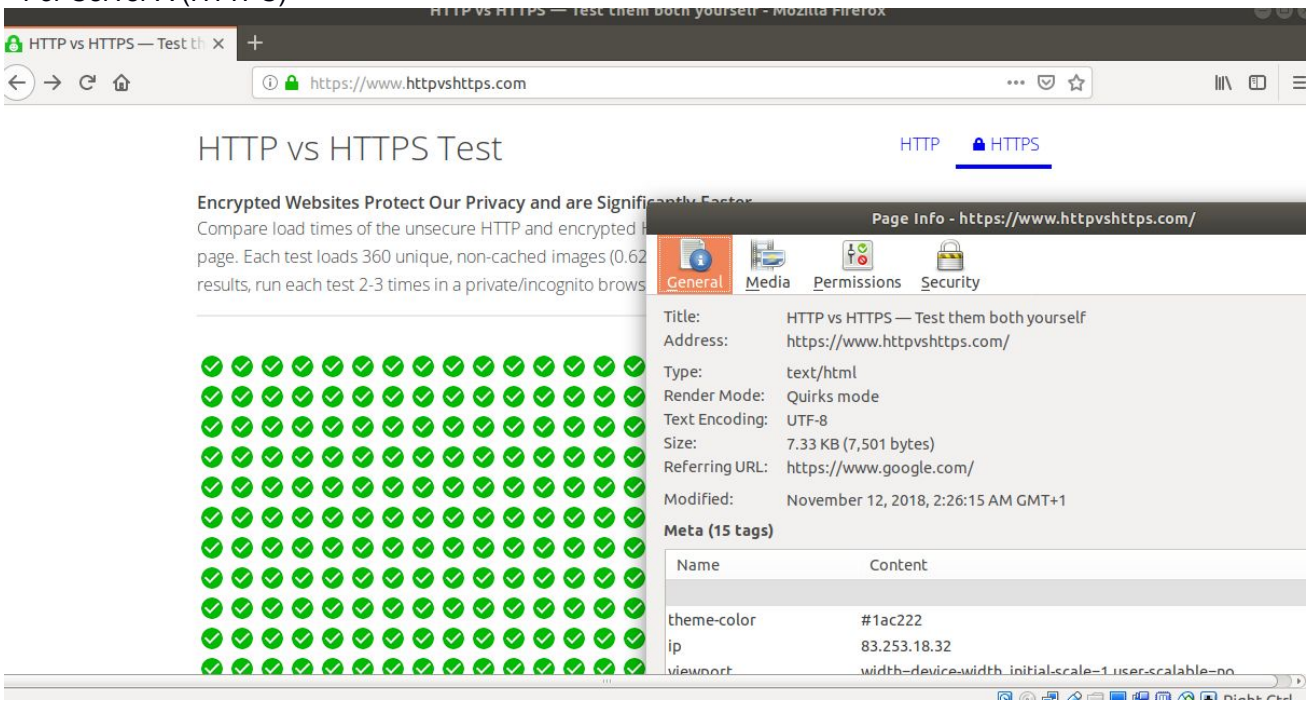
For Host OS : HTTP



For Server A (HTTP)



For Server A (HTTPS)

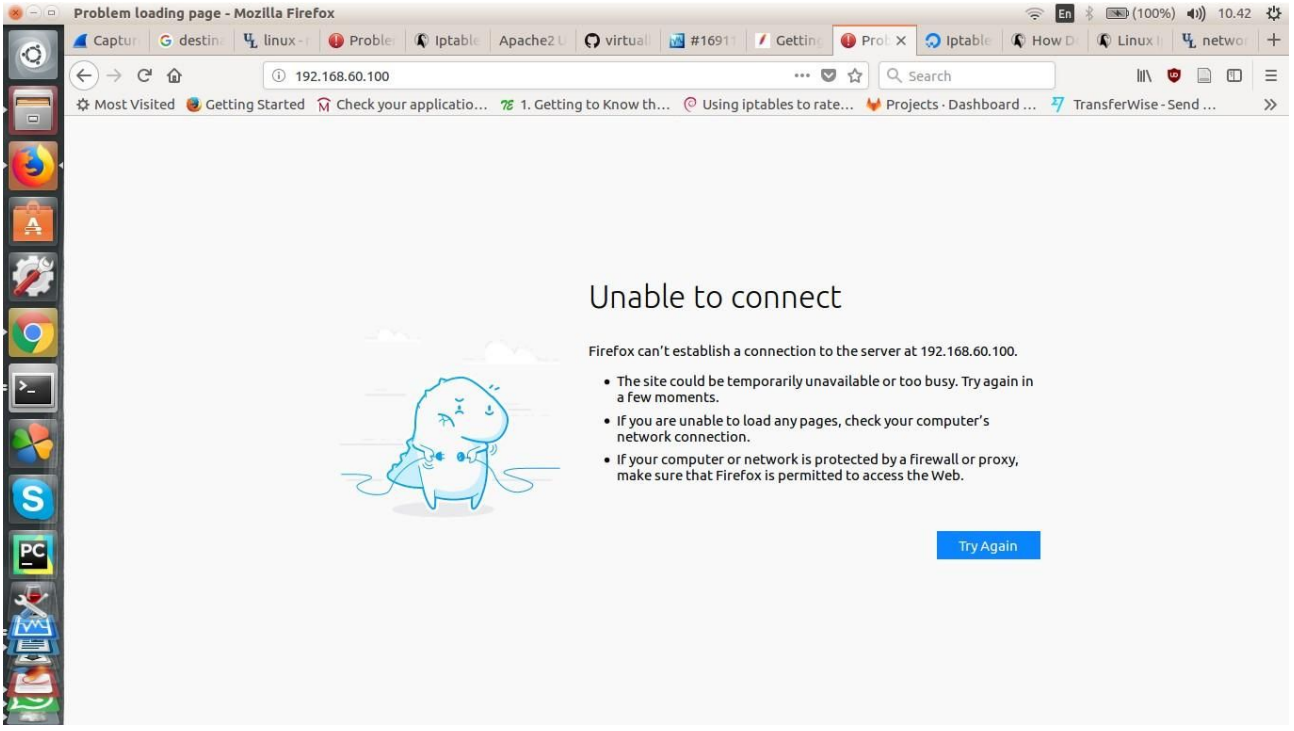


After blocking for verification purpose I tried to visit that previous website http://www.httpvshttps.com website and its confirmed that it has blocked.

Task 12:

For Blocking apache server I have used below iptable rule.

sudo iptables -A INPUT -p tcp --dport http -i enp0s9 -j REJECT



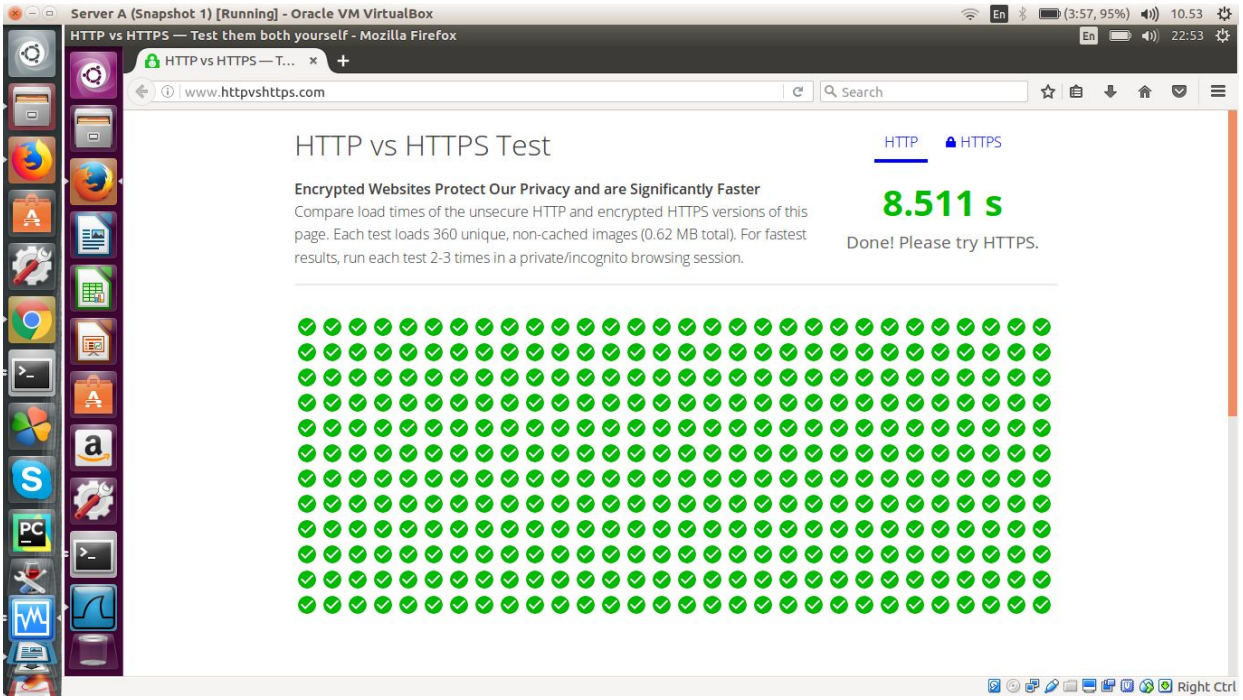
Task 13: Unblock HTTP-browsing in the guest OS

I have blocked the http at task 11 .
Now for unblocking that I have used below command:

sudo iptables -D INPUT -p tcp --dport 80 -m conntrack --ctstate NEW,ESTABLISHED
-j DROP

sudo iptables -D INPUT -p tcp --sport 80 -m conntrack --ctstate ESTABLISHED -j DROP

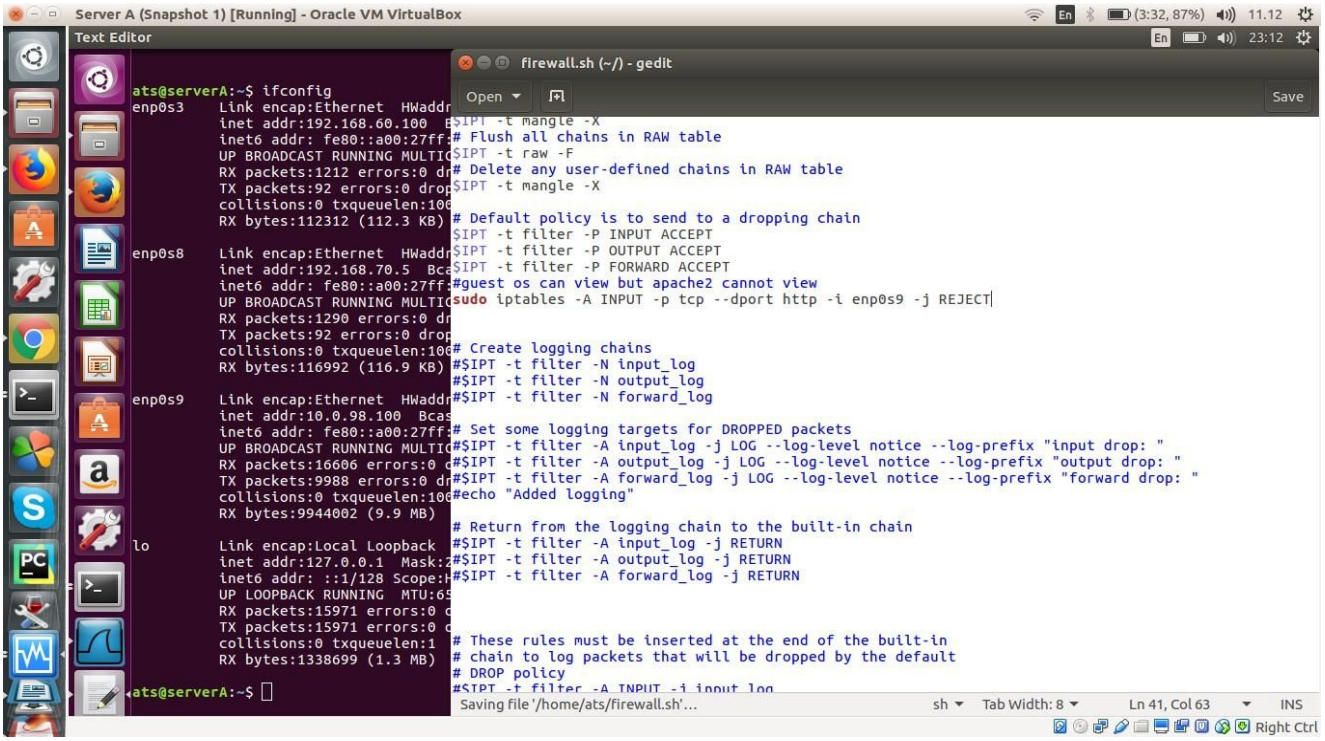
All http request starts accepting.



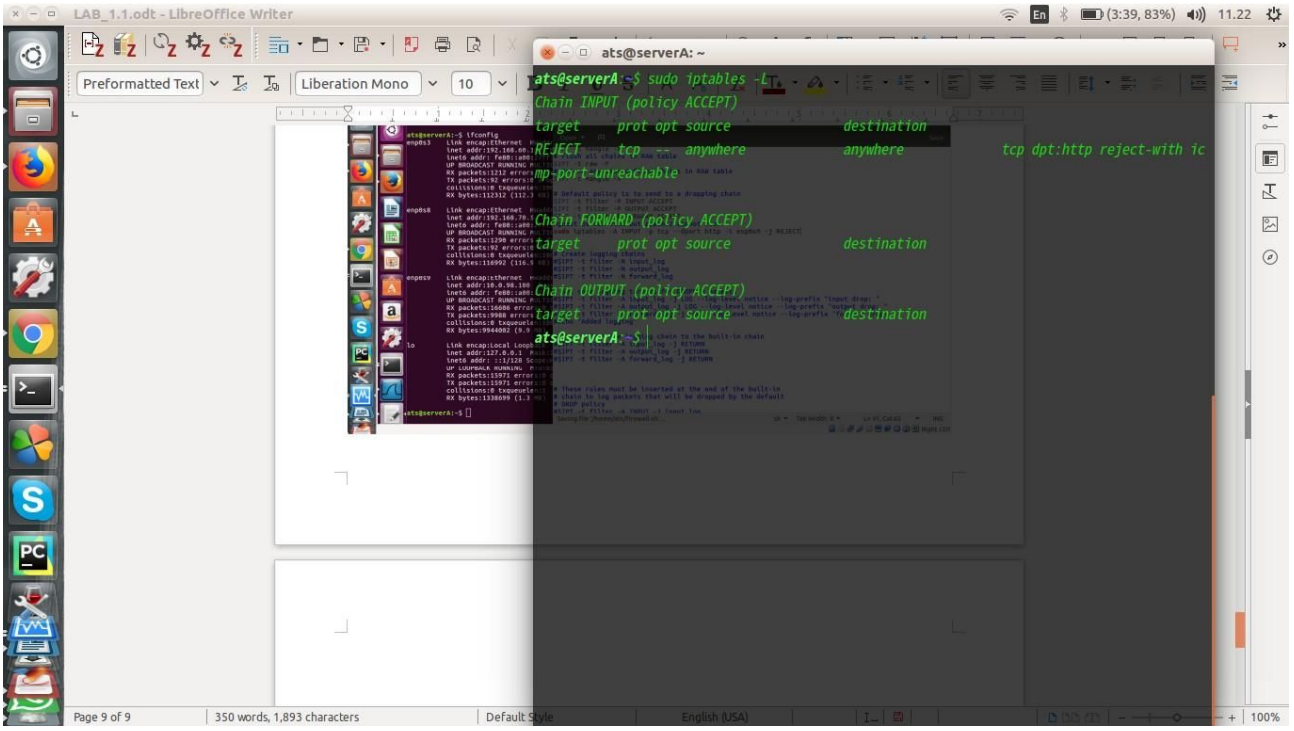
Task 14: Use firewall.sh to configure the firewall:

For the task guest OS can view HTTP and HTTPS pages, but apache2 server is blocked from serving HTTP content I have added the below command to firewall.sh file.

Sudo iptables -A INPUT -p tcp —dport http -i enp0s9 -j REJECT



I have changed the rule and after giving iptable -L command found below:



Now I comment out that command and make the firewall initial state.

Task 15: Change default firewall policy to DROP

I have removed the rules from Task 14 as per instruction and executed the script.
Then I have modified the firewall.sh script by the following commands to make default firewall policy to DROP:
$IPT -t filter -P INPUT DROP
$IPT -t filter -P OUTPUT DROP
$IPT -t filter -P FORWARD DROP
And I add it to the firewall.sh file.

Now Server A dropping all packet and stop all connection to the outside world.

Don't even get ping from the loopback/localhost.

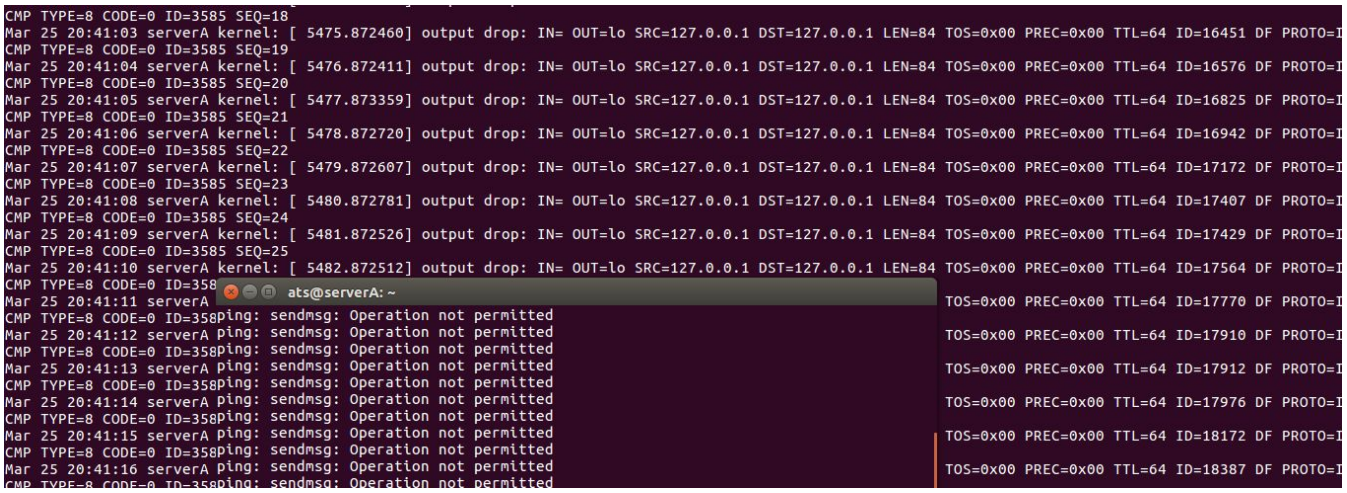
```
ats@serverA:~$ sudo iptables -L
Chain INPUT (policy DROP)
target     prot opt source               destination

Chain FORWARD (policy DROP)
target     prot opt source               destination

Chain OUTPUT (policy DROP)
target     prot opt source               destination
REJECT     tcp  --  anywhere             anywhere             tcp dpt:http reject-with icmp-port-unreachable
ats@serverA:~$
```

Task 16: Logging DROPPED packets

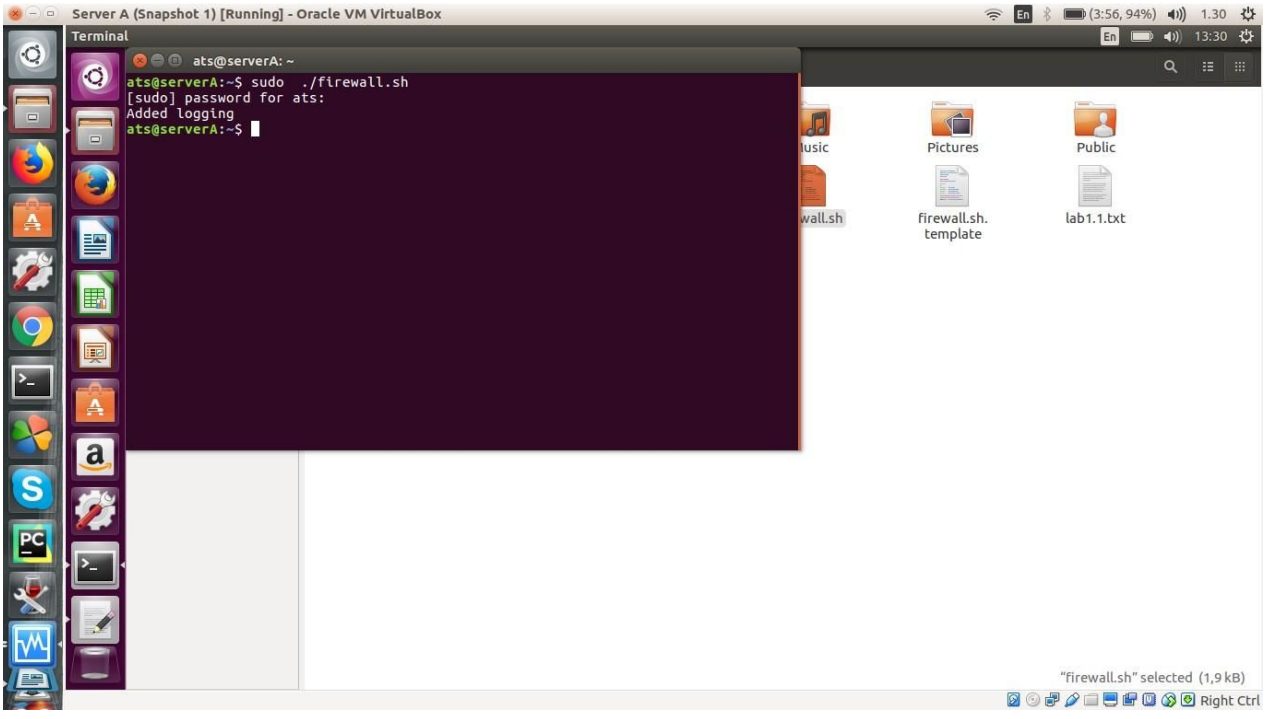
I have modified the firewall script as per instruction and executed it
Then in the terminal window, I have run the following command:

sudo tail -f /var/log/kern.log

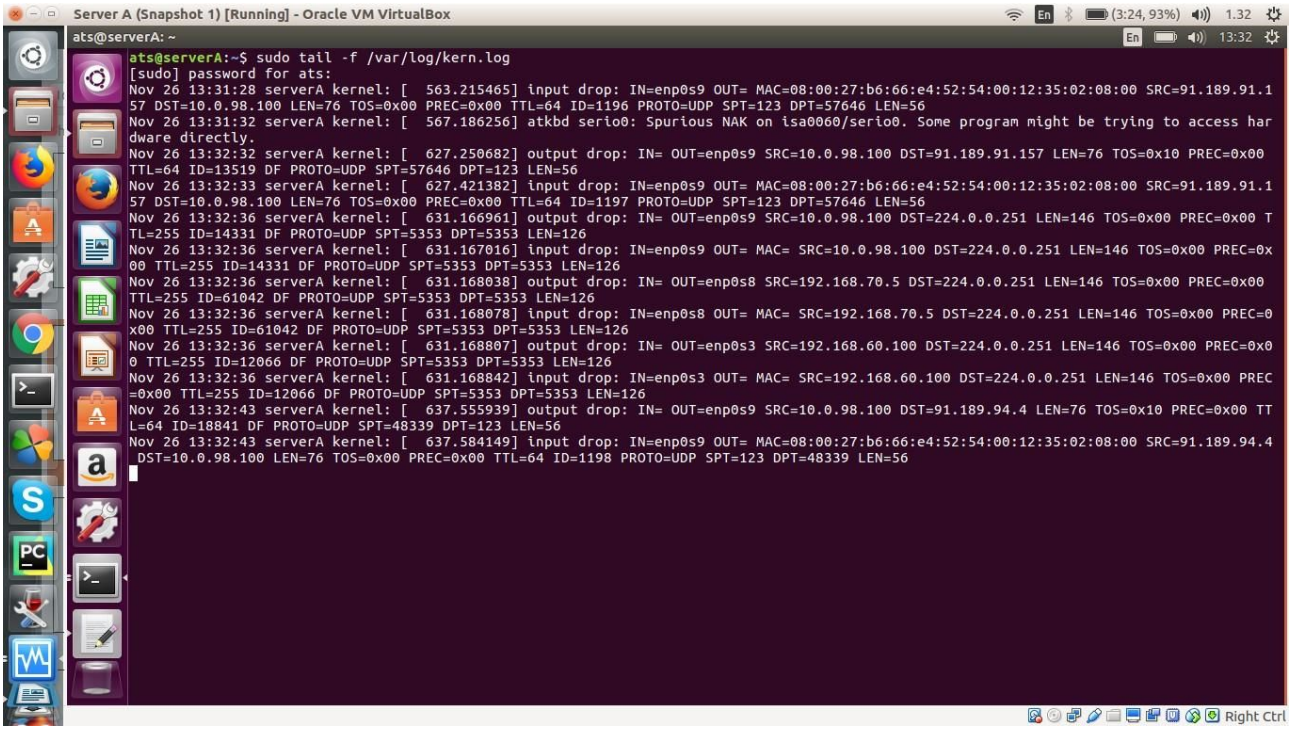
Now I am able to see live logs from the Linux kernel. I have started pinging the loopback interface in another terminal window and I can see all outputs are dropped .



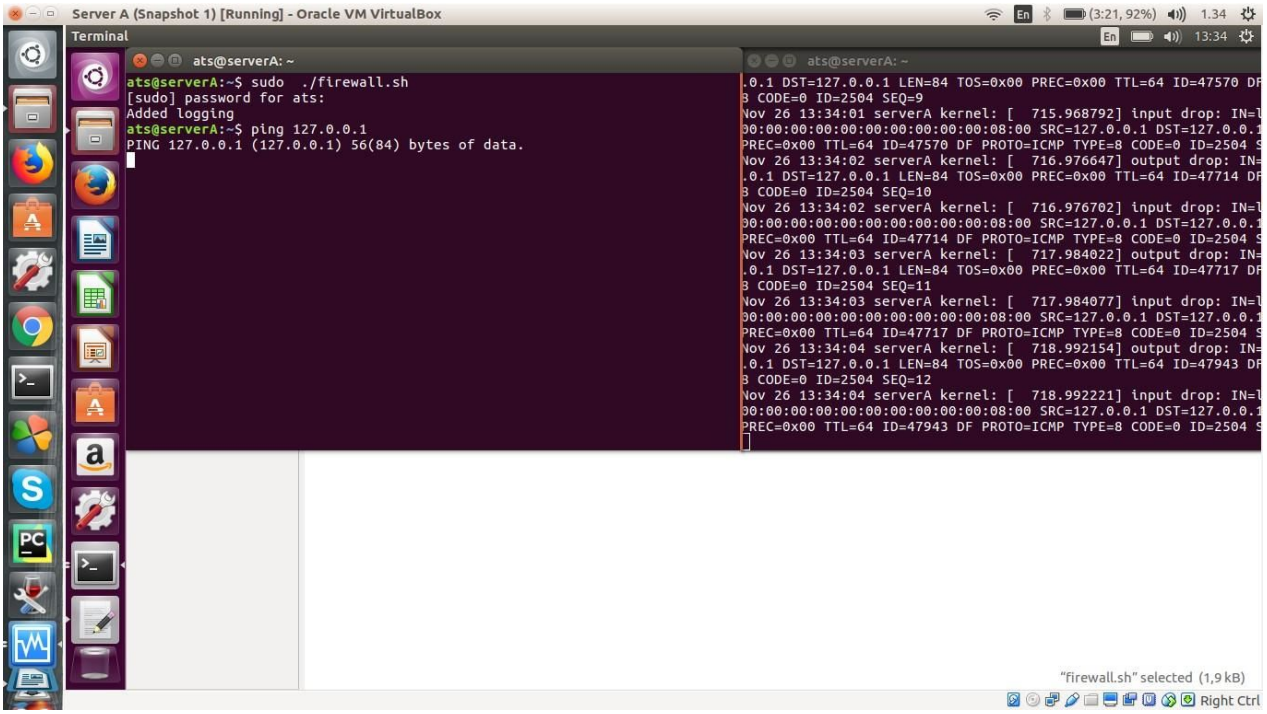
Added logging:



After Blocking I have seen that all inputs are dropped.



Try to ping loopback but it also dropping that.



Task 17: Enable traffic from loopback interface

For enabling traffic from loopback I have applied below rules:

Sudo iptables -A INPUT -i lo -j ACCEPT

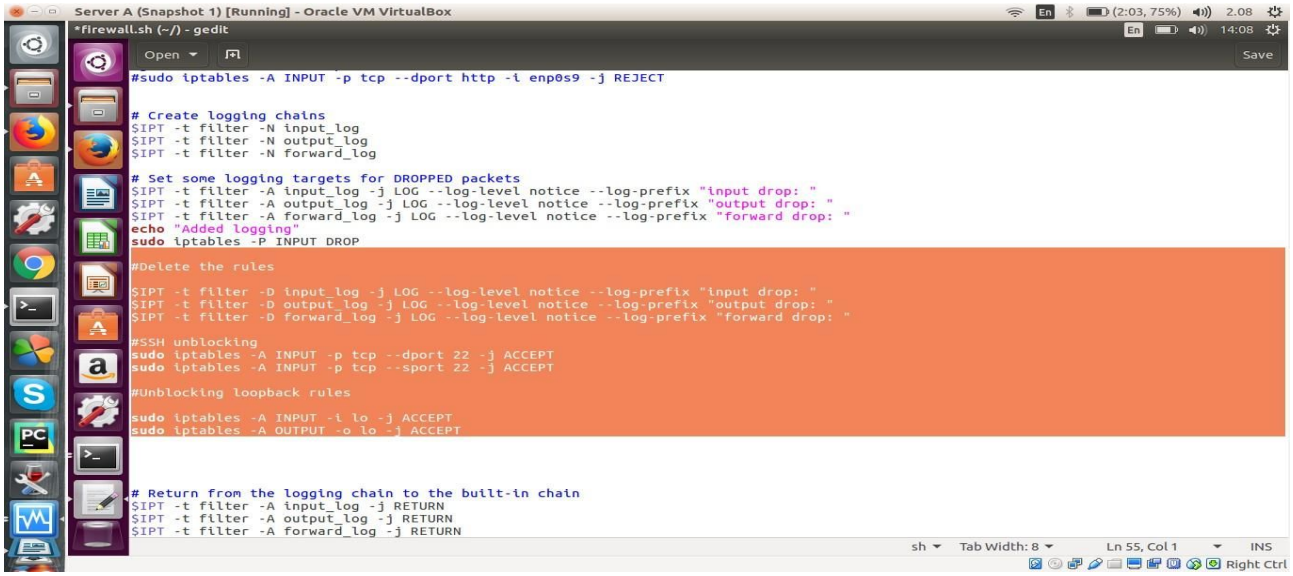
Sudo iptables -A OUTPUT -o lo -j ACCEPT

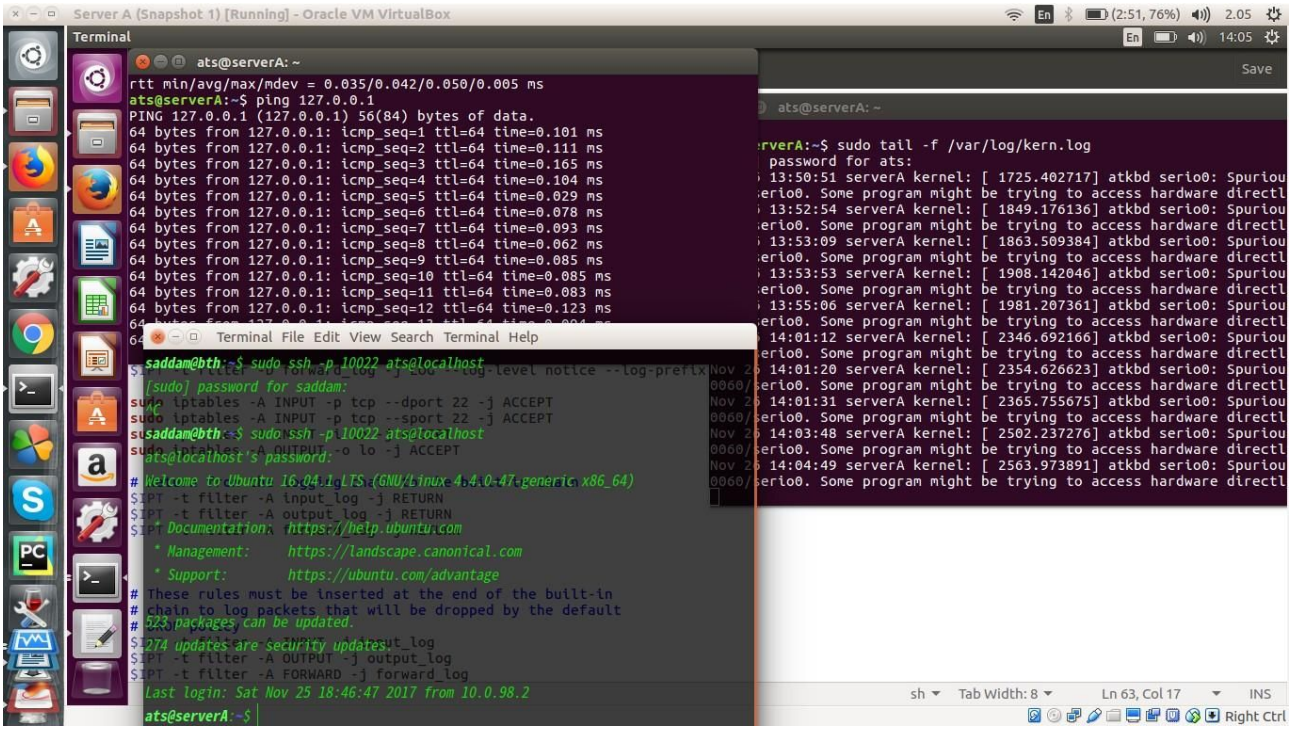
Fro enabling SSH I have applied below rules:

sudo iptables -A INPUT -p tcp --dport 22 -j ACCEPT sudo iptables -A OUTPUT -p tcp --sport 22 -j ACCEPT

Now I am getting ping to the loopback and ssh from my host.

```
ats@serverA:~$ ssh localhost
ats@localhost's password:
Welcome to Ubuntu 16.04.1 LTS (GNU/Linux 4.4.0-104-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

416 packages can be updated.
136 updates are security updates.

Last login: Mon Nov 27 18:44:25 2017 from 10.0.98.2
ats@serverA:~$ logout
Connection to localhost closed.
ats@serverA:~$
```

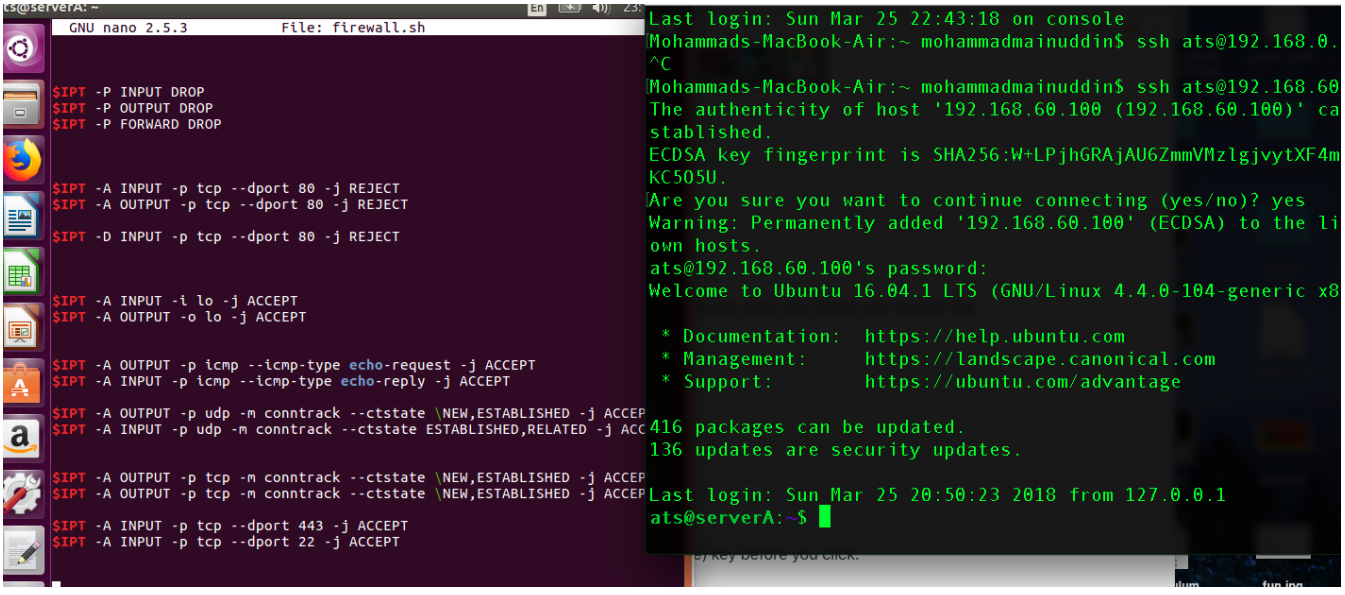




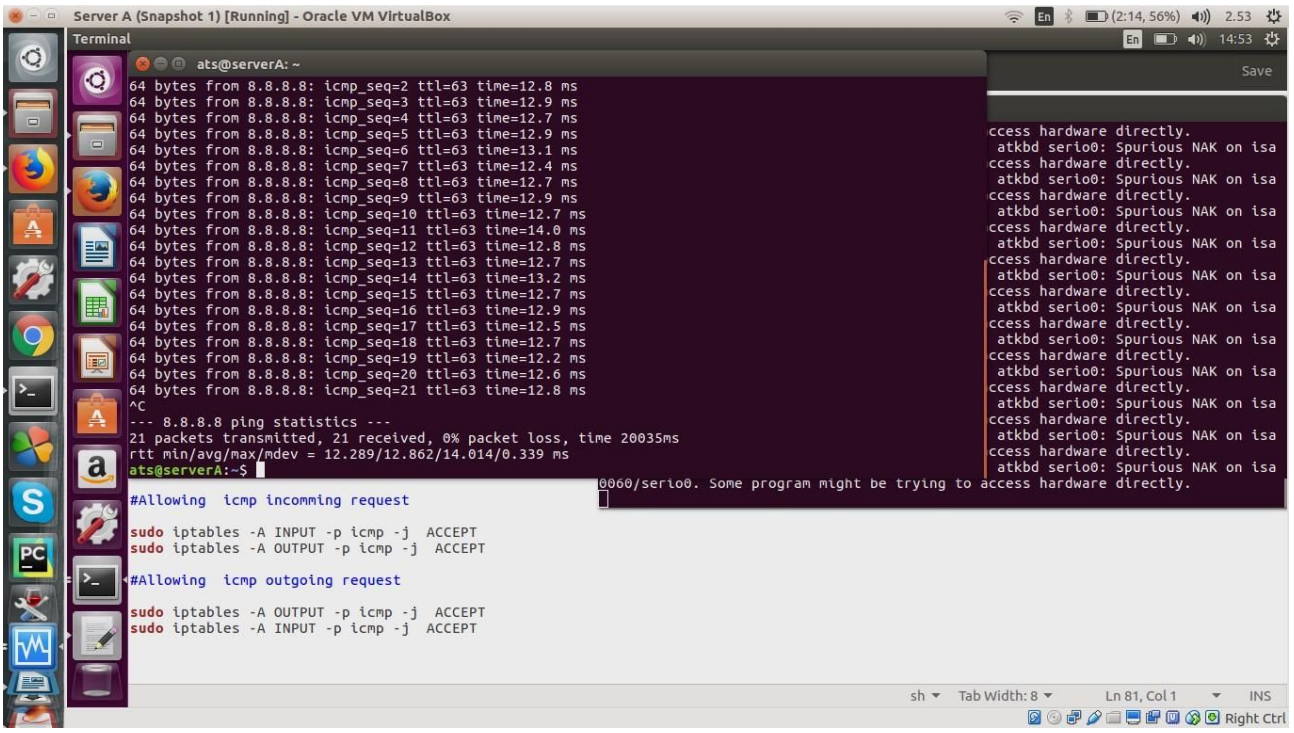
Task 18: Allow Server A to ping the other interfaces:

For allowing icmp to the outside world I have set below rules:

$IPT -A OUTPUT -p icmp --icmp-type echo-request -j ACCEPT
$IPT -A INPUT -p icmp --icmp-type echo-reply -j ACCEPT



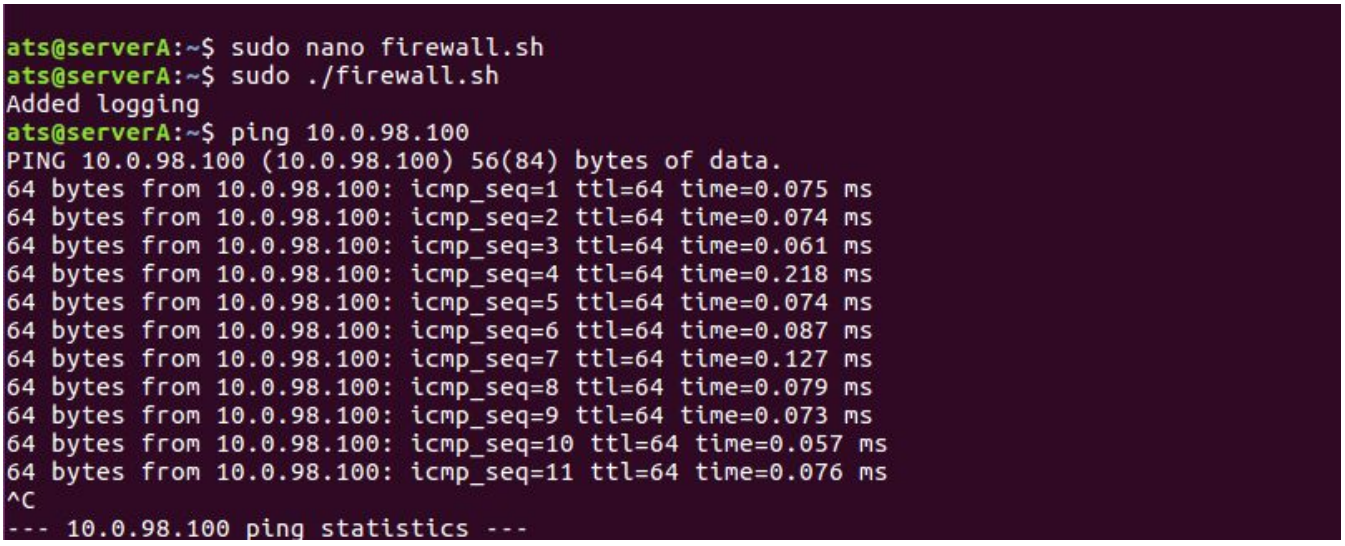
I can ping google dns server 8.8.8.8 from my server A.

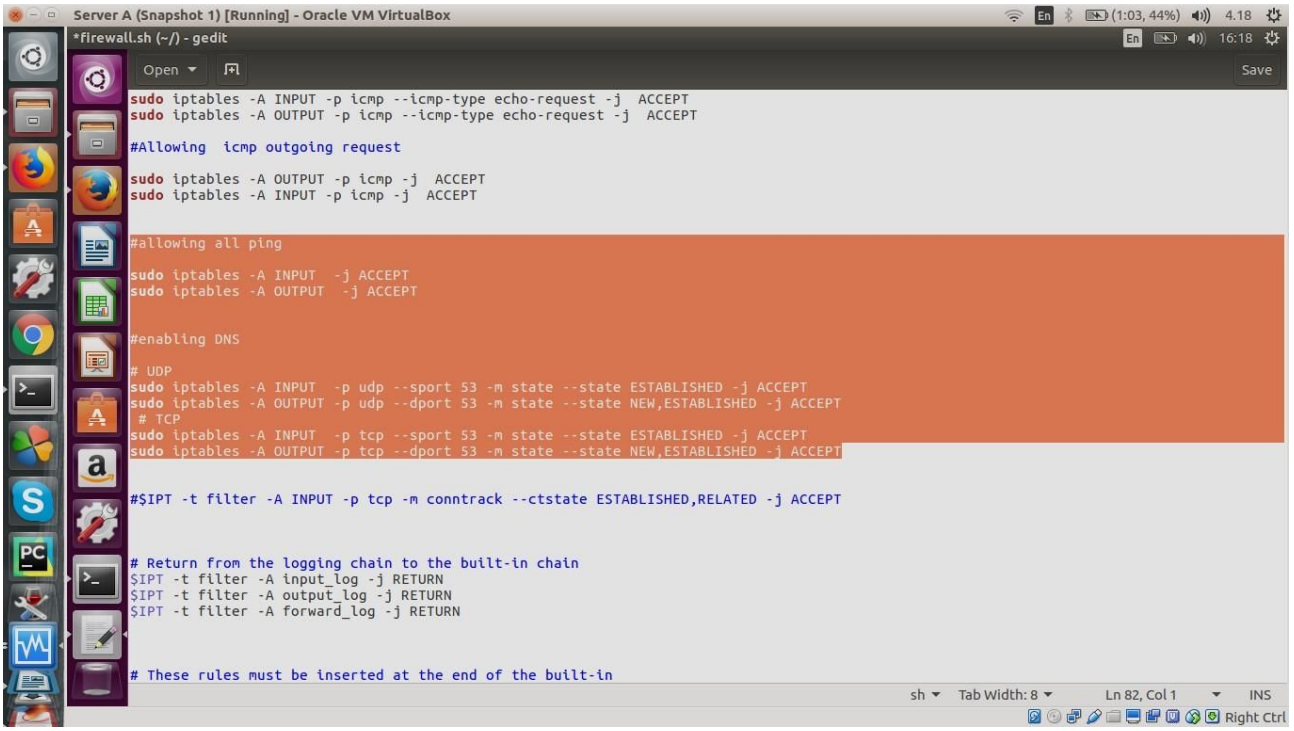


Task 19: Allow Server A to ping all hosts

For allowing all ping and DNS server I have used below rules:

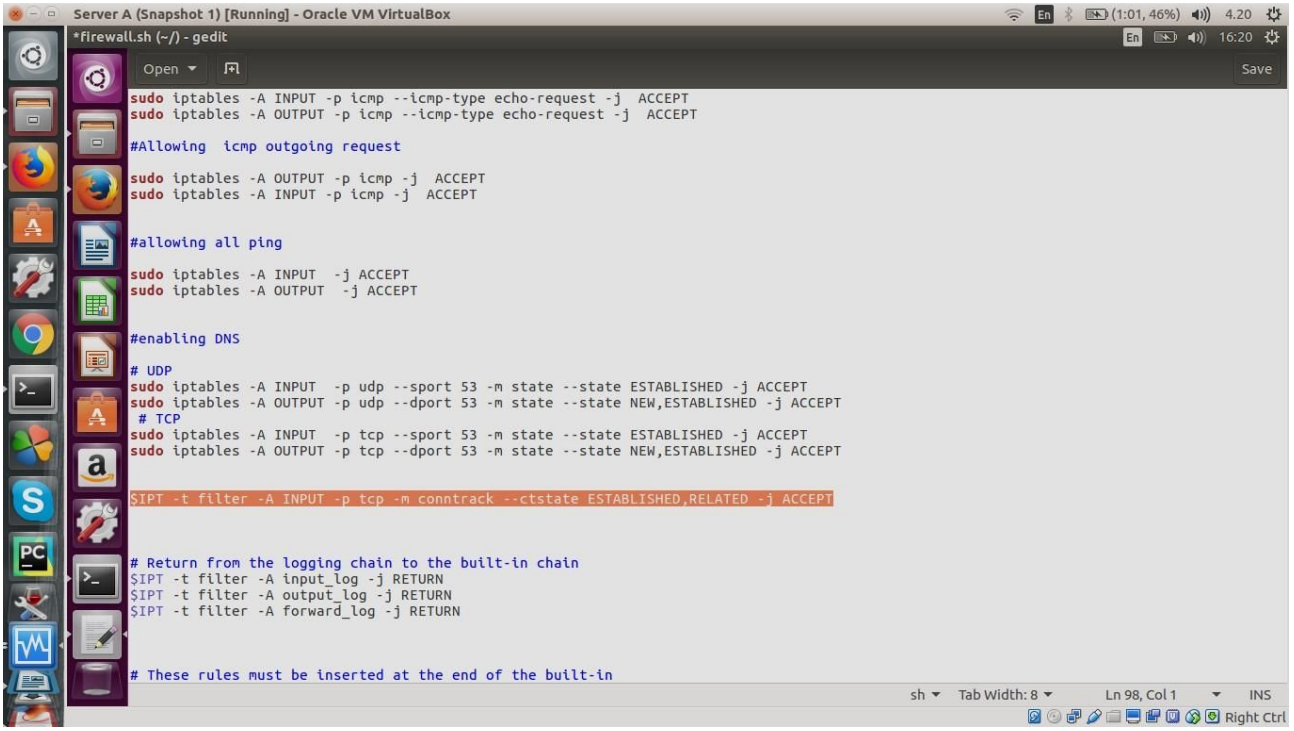
I have modified the firewall script by following rules to allow server A to ping all hosts:
$IPT -A OUTPUT -j ACCEPT
$IPT -A INPUT -j ACCEPT
$IPT -A OUTPUT -p udp -m udp --dport 53 -j ACCEPT
$IPT -A INPUT -p udp -m udp --sport 53 -j ACCEPT
$IPT -A OUTPUT -p icmp --icmp-type echo-reply -j ACCEPT
$IPT -A INPUT -p icmp --icmp-type echo-request -j ACCEPT





Task 20:

Sudo iptables -t filter -A INPUT -p tcp -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT



Now outside connection has established and I can browse www.facebook.com from server A

Task 21:

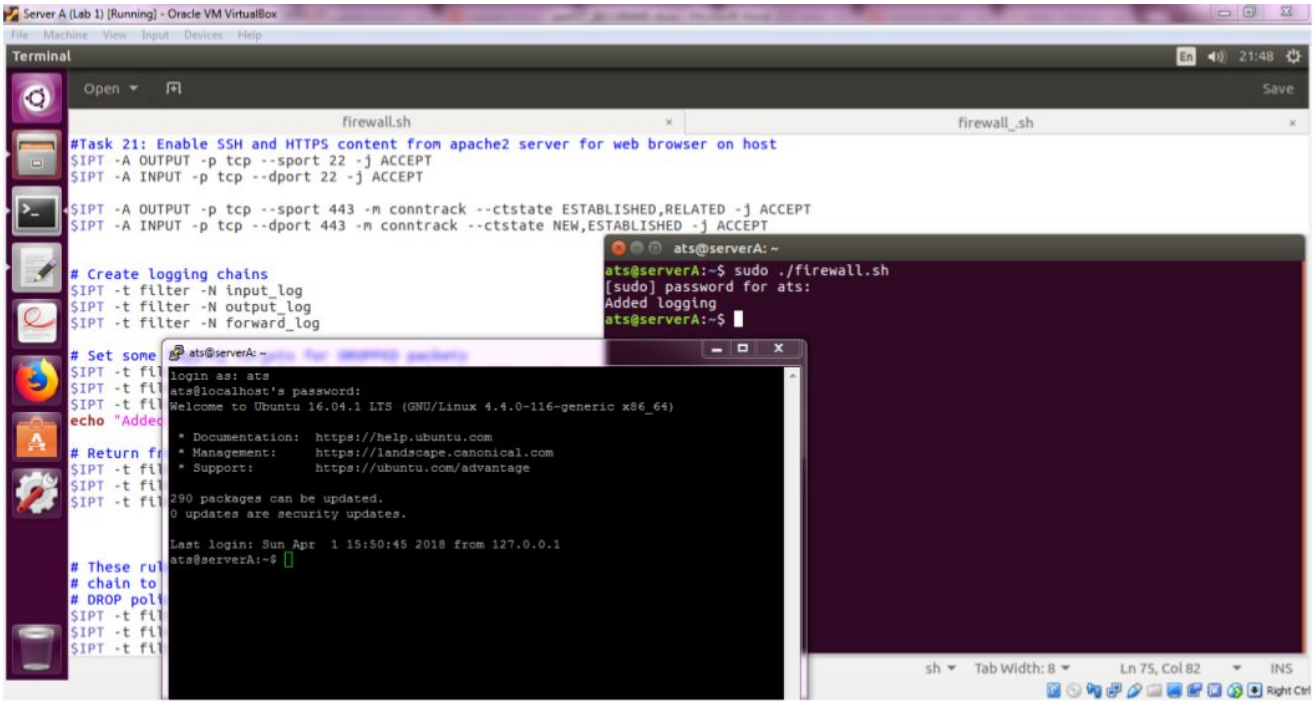
To add the following rules to the firewall.sh script and executing it and thus enable TCP connections to be established to any destination, so we can able to browse websites with the Firefox browser from Server A.

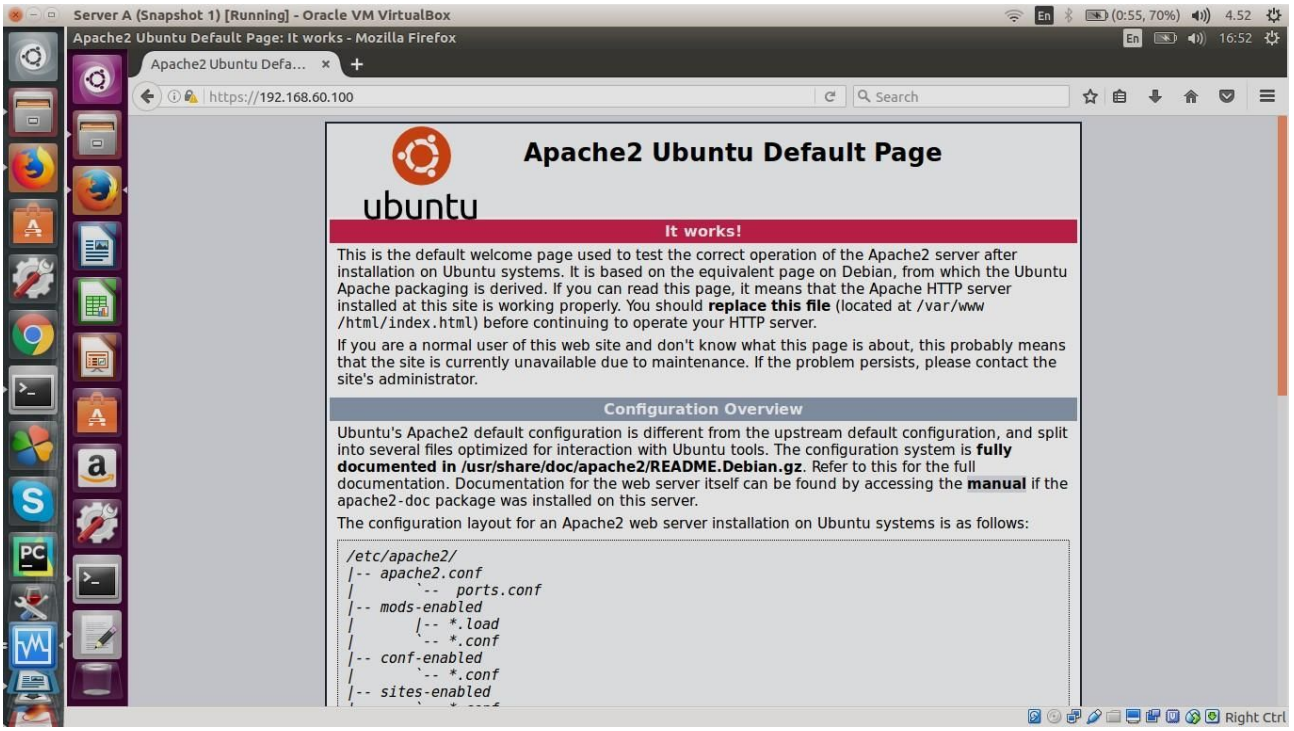
$IPT -A OUTPUT -p tcp --sport 22 -j ACCEPT
$IPT -A INPUT -p tcp --dport 22 -j ACCEPT

Sudo iptables –A OUTPUT –p tcp –m conntrack --ctstate NEW,ESTABLISHED –j ACCEPT

“sudo iptables –A INPUT –p tcp –m conntrack --ctstate ESTABLISHED,RELATED –j ACCEPT

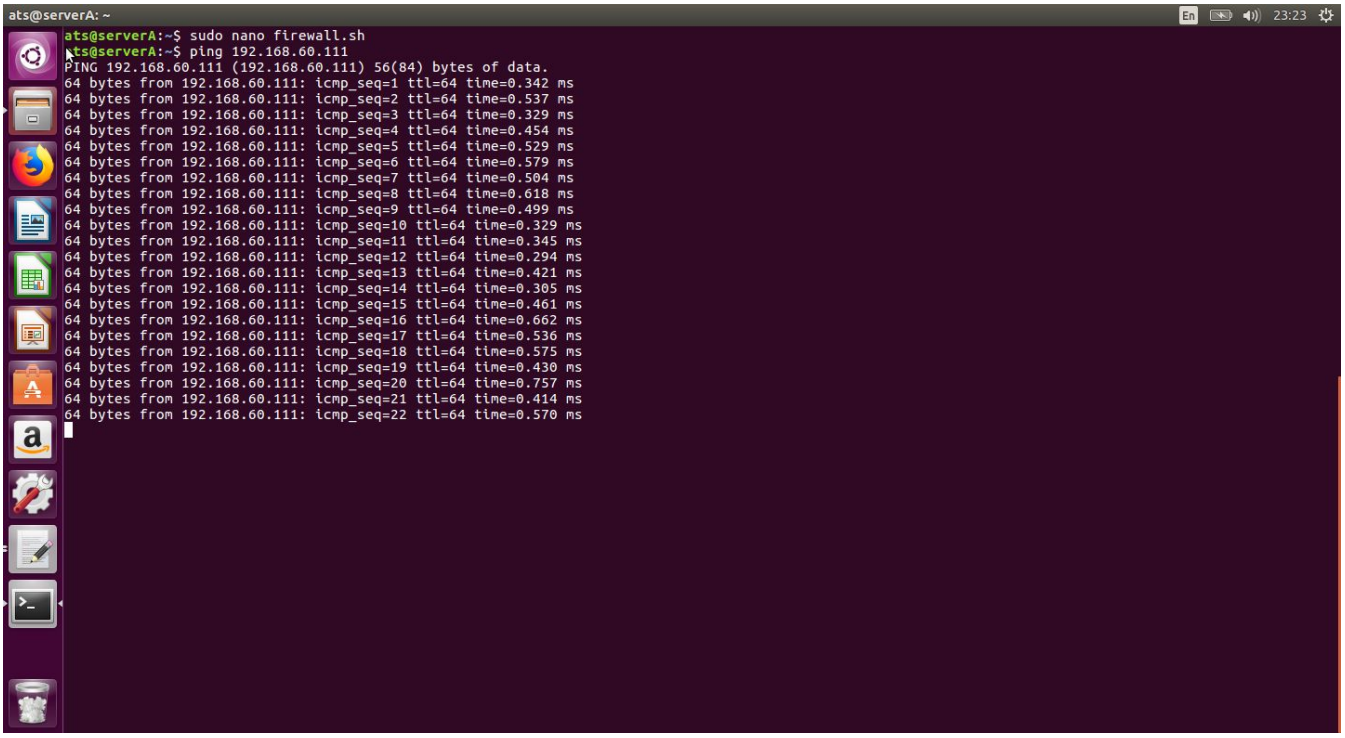
I can browse https apache2 server.





Task 22:

I can ping from Client A to Server A.

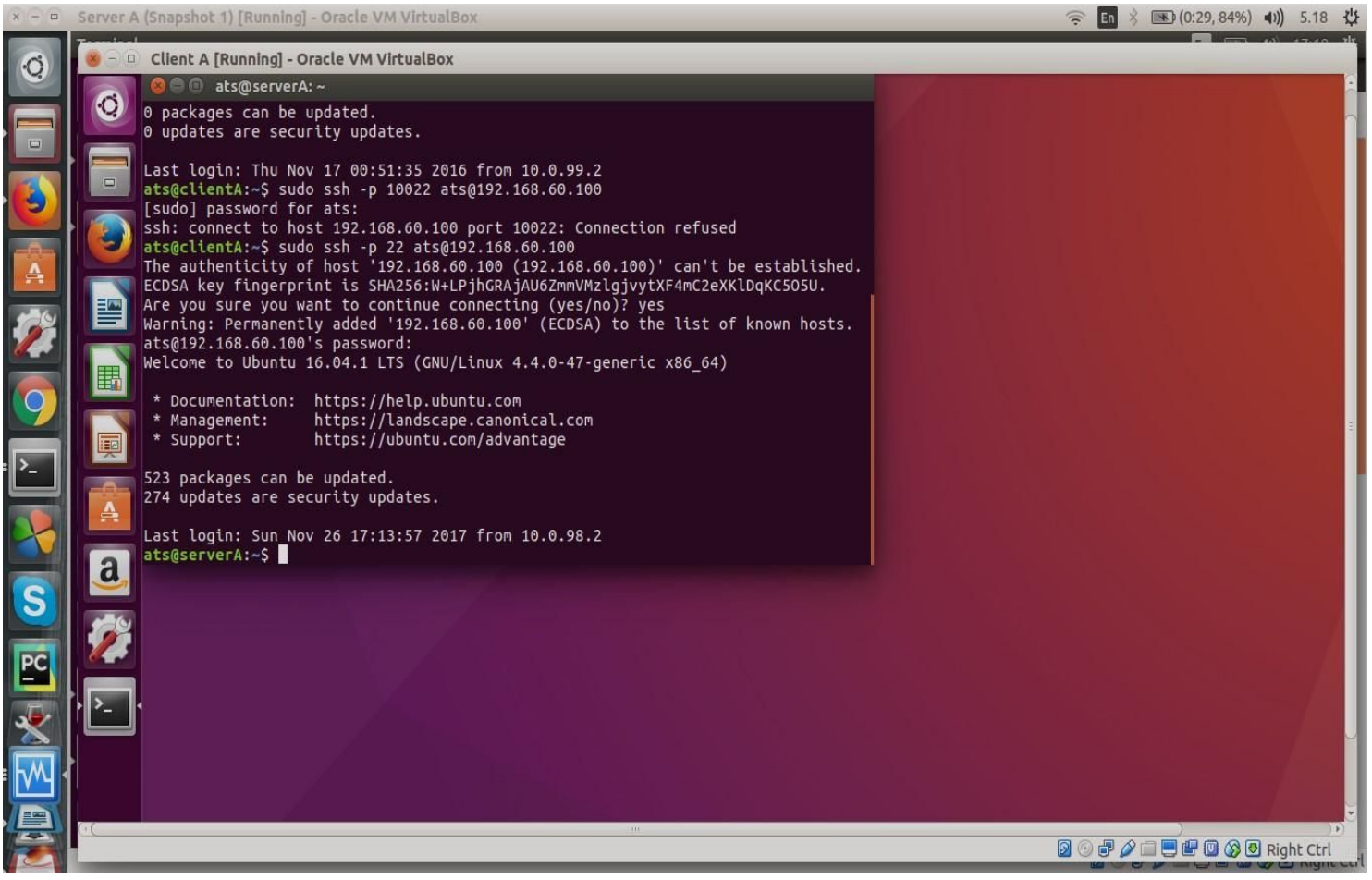


Task 23:

To fix the firewall rules such that we can SSH from Client A to Server A. Add the following rules to the firewall.

sudo iptables -I INPUT -s 192.168.60.111 -p tcp -m tcp --dport 22 -j ACCEPT

```
ats@serverA: ~
ats@clientA:~$ sudo ssh ats@192.168.60.100
[sudo] password for ats:
ats@192.168.60.100's password:
Welcome to Ubuntu 16.04.1 LTS (GNU/Linux 4.4.0-104-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

416 packages can be updated.
136 updates are security updates.

Last login: Sun Mar 25 23:12:31 2018 from 192.168.60.1
ats@serverA:~$
```



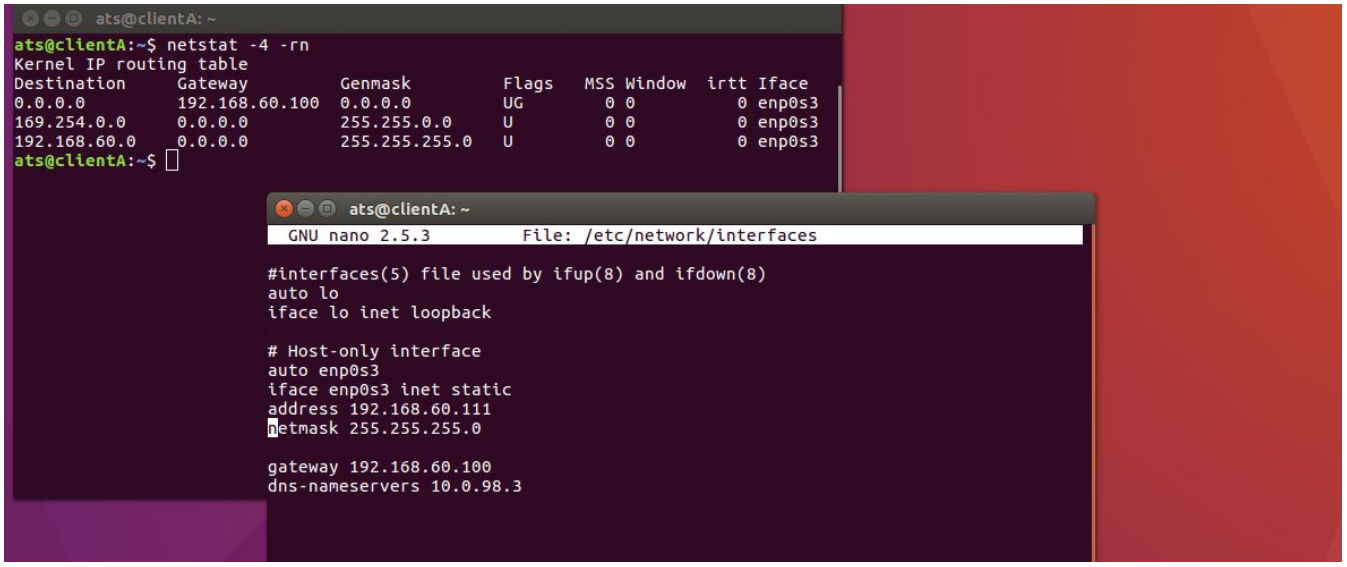
For ssh I used below command.

Sudo ssh -p 22 ats@192.168.60.100

Task 24:

Forwarded the traffic to Server A by following command.

Gateway 192.168.60.100
dns-nameservers 10.0.98.3



Task 25:

Follow these command :

sudo sysctl –w net.ipv4.ip_forward=1
sudo syscltl -p

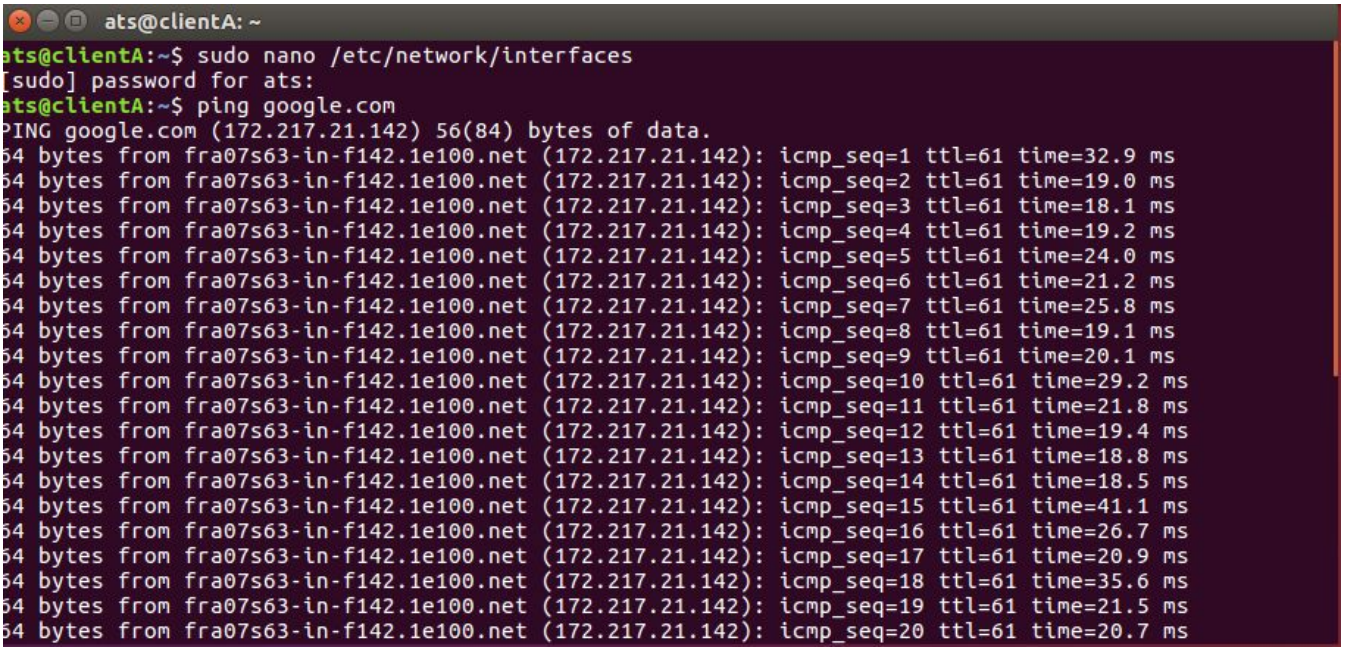
Task 26 & 27:

Using Server A as a router to forward traffic from outside to Client A I have used below command--------

sudo iptables –t filter -A FORWARD -i $HIF –j ACCEPT

sudo iptables –t filter -A FORWARD -i $NIF –m conntrack –ctstate ESTABLISHED,RELATED -j ACCEPT

sudo iptables –t nat –A POSTROUTING -j SNAT -o $NIF --to $NIP



I am getting ping and Client A is connected to the world.

```
#!/bin/sh

IPT=/sbin/iptables

# NAT interface
NIF=enp0s9
# NAT IP address
NIP='10.0.98.100'
# Host-only interface
HIF=enp0s3
# Host-only IP addres
HIP='192.168.60.100'
# DNS nameserver
NS='10.0.98.3'
## Reset the firewall to an empty, but friendly state
# Flush all chains in FILTER table
$IPT -t filter -F
# Delete any user-defined chains in FILTER table
$IPT -t filter -X
# Flush all chains in NAT table
$IPT -t nat -F
# Delete any user-defined chains in NAT table$IPT -t nat -X
# Flush all chains in MANGLE table
$IPT -t mangle -F
# Delete any user-defined chains in MANGLE table
$IPT -t mangle -X
# Flush all chains in RAW table
$IPT -t raw -F
# Delete any user-defined chains in RAW table
$IPT -t mangle -X
# Default policy is to send to a dropping chain
$IPT -t filter -P INPUT ACCEPT
$IPT -t filter -P OUTPUT ACCEPT
$IPT -t filter -P FORWARD ACCEPT
#Task 14: Guest OS can view HTTP and HTTPS pages, but apache2 server is blocked from serving HTTP
content.
$IPT -A INPUT -p tcp --dport 80 -j REJECT
#Task 15: Change default firewall policy to DROP
$IPT -t filter -P INPUT DROP
$IPT -t filter -P OUTPUT DROP
$IPT -t filter -P FORWARD DROP
#Task 17: Enable traffic from loopback interface
$IPT -A INPUT -i lo -j ACCEPT$IPT -A OUTPUT -o lo -j ACCEPT
#Task 18: Allow Server A to ping the other interfaces
$IPT -A OUTPUT -p icmp --icmp-type echo-request -j ACCEPT
$IPT -A INPUT -p icmp --icmp-type echo-reply -j ACCEPT
#Task 19: Allow Server A to ping all hosts
$IPT -A OUTPUT -j ACCEPT
$IPT -A INPUT -j ACCEPT
$IPT -A OUTPUT -p udp -m udp --dport 53 -j ACCEPT
$IPT -A INPUT -p udp -m udp --sport 53 -j ACCEPT
$IPT -A OUTPUT -p icmp --icmp-type echo-reply -j ACCEPT
$IPT -A INPUT -p icmp --icmp-type echo-request -j ACCEPT
#Task 20: Enable stateful firewall
$IPT -t filter -A INPUT -p tcp -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT
#Task 21: Enable SSH and HTTPS content from apache2 server for web browser on host
$IPT -A OUTPUT -p tcp --sport 22 -j ACCEPT
$IPT -A INPUT -p tcp --dport 22 -j ACCEPT
$IPT -A OUTPUT -p tcp --sport 443 -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT
$IPT -A INPUT -p tcp --dport 443 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT#Task 23: SSH from
Client A to Server A
$IPT -A INPUT -p tcp -s 192.168.60.111 --dport 22 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT
```

```
#Task 26: Change iptables to forward packets
$IPT -t filter -A FORWARD -i $HIF -j ACCEPT
$IPT -t filter -A FORWARD -i $NIF -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT
#Task 27: Enable SNAT on Server A
$IPT -t nat -A POSTROUTING -j SNAT -o $NIF --to $NIP
# Create logging chains
$IPT -t filter -N input_log
$IPT -t filter -N output_log
$IPT -t filter -N forward_log
# Set some logging targets for DROPPED packets
$IPT -t filter -A input_log -j LOG --log-level notice --log-prefix "input drop: "
$IPT -t filter -A output_log -j LOG --log-level notice --log-prefix "output drop: "
$IPT -t filter -A forward_log -j LOG --log-level notice --log-prefix "forward drop: "
echo "Added logging"
# Return from the logging chain to the built-in chain
$IPT -t filter -A input_log -j RETURN
$IPT -t filter -A output_log -j RETURN$IPT -t filter -A forward_log -j RETURN
# These rules must be inserted at the end of the built-in
# chain to log packets that will be dropped by the default
# DROP policy
$IPT -t filter -A INPUT -j input_log
$IPT -t filter -A OUTPUT -j output_log
$IPT -t filter -A FORWARD -j forward_log
```

Thanks
Saddam Hossen