Lab 1.1: Linux Networking and Firewalls

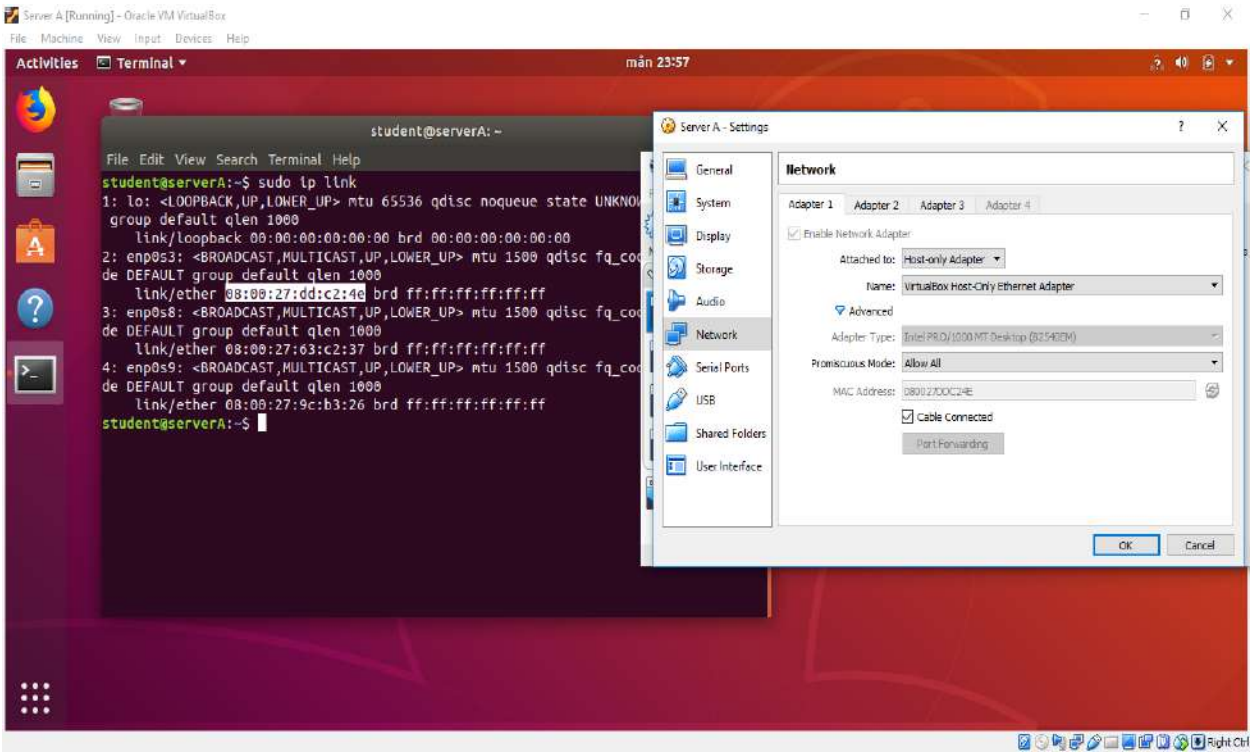
Course: Network Security, ET2540

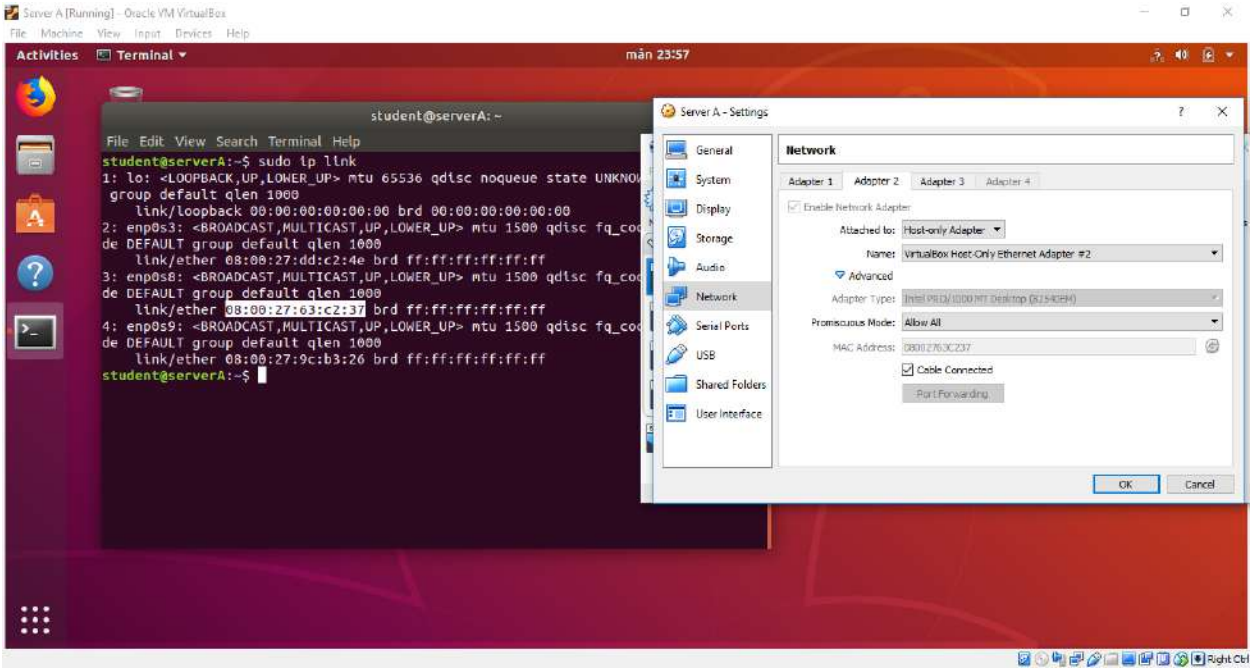
Name: Md Rabiul Ahamed Bin Hanif

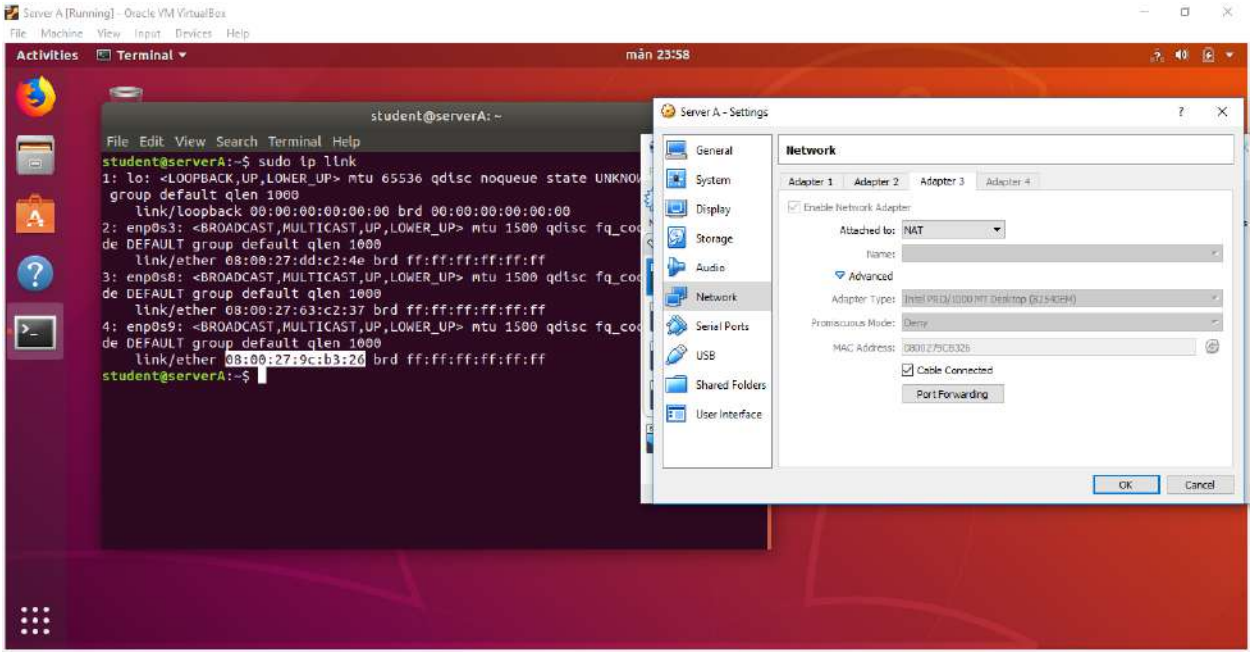
Personal Number: [redacted]

Task 1: MAC Address

Interface	MAC Address
Enp0s3	080027DDC24E
Enp0s8	08002763C237
Enp0s9	0800279CB326




Server A [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Terminal
mån 23:57
student@serverA: ~
File Edit View Search Terminal Help
student@serverA:~$ sudo ip link
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOW
group default qlen 1000
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_cod
de DEFAULT group default qlen 1000
link/ether 08:00:27:dd:c2:4e brd ff:ff:ff:ff:ff:ff
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_cod
de DEFAULT group default qlen 1000
link/ether 08:00:27:63:c2:37 brd ff:ff:ff:ff:ff:ff
4: enp0s9: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_cod
de DEFAULT group default qlen 1000
link/ether 08:00:27:9c:b3:26 brd ff:ff:ff:ff:ff:ff
student@serverA:~$
Server A - Settings
General
System
Display
Storage
Audio
Network
Serial Ports
USB
Shared Folders
User Interface
Network
Adapter 1
Adapter 2
Adapter 3
Adapter 4
Enable Network Adapter
Attached to: Host-only Adapter
Name: VirtualBox Host-Only Ethernet Adapter #2
Advanced
Adapter Type:
Promiscuous Mode: Allow All
MAC Address:
Cable Connected
Port Forwarding
OK
Cancel
Right Ctrl


Server A [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Terminal
mån 23:58
student@serverA: ~
File Edit View Search Terminal Help
student@serverA:~$ sudo ip link
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOW
group default qlen 1000
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_cod
de DEFAULT group default qlen 1000
link/ether 08:00:27:dd:c2:4e brd ff:ff:ff:ff:ff:ff
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_cod
de DEFAULT group default qlen 1000
link/ether 08:00:27:63:c2:37 brd ff:ff:ff:ff:ff:ff
4: enp0s9: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_cod
de DEFAULT group default qlen 1000
link/ether 08:00:27:9c:b3:26 brd ff:ff:ff:ff:ff:ff
student@serverA:~$
Server A - Settings
General
System
Display
Storage
Audio
Network
Serial Ports
USB
Shared Folders
User Interface
Network
Adapter 1
Adapter 2
Adapter 3
Adapter 4
Enable Network Adapter
Attached to: NAT
Name:
Advanced
Adapter Type:
Promiscuous Mode: Deny
MAC Address:
Cable Connected
Port Forwarding
OK
Cancel

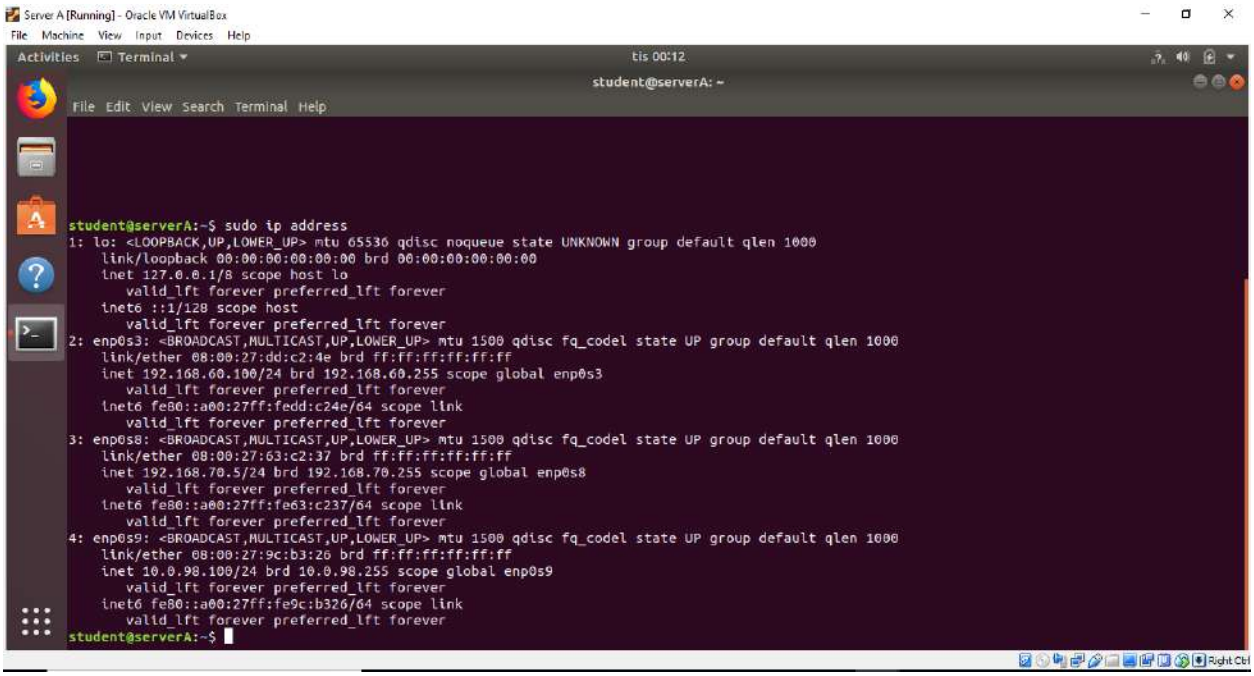
Task 2: Network Interfaces

Now in guest command window run this command.

sudo ip address

I can find the Interface, IPv4 address , MAC Address and adapter also.

Interface	IPv4 Address	MAC Address	Adapter
Enp0s3	192.168.60.100	080027DDC24E	Host Only
Enp0s8	192.168.70.5	08002763C237	Host Only
Enp0s9	10.0.98.100	0800279CB326	NAT



Task 3: IP addresses, netmasks and subnet

(IPv4 address) AND (Netmasks)= Subnet

Interface	IPv4 address	MAC Address	Subnet
enp0s3	192.168.60.1	080027C56E84	192.168.60
enp0s8	192.168.70.1	08002797F5E0	192.168.70
enp0s9	10.0.98.100	0800272841E0	10.0.98.0

For enp0s3:

IP Address (Decimal)	192	168	60	1
IP Address (Binary)	11000000	10101000	00111100	00000001
Netmasks (B)	11111111	11111111	11111111	00000000
AND operation				
Subnet (B)	11000000	10101000	00111100	00000000
Subnet (D)	192	168	60	0

For enp0s8:

IP Address (Decimal)	192	168	70	1
IP Address (Binary)	11000000	10101000	01010000	00000001
Netmasks (B)	11111111	11111111	11111111	00000000
AND operation				
Subnet (B)	11000000	10101000	01010000	00000000
Subnet (D)	192	168	70	0

For enp0s9:

IP Address (Decimal)	10	0	98	100
IP Address (Binary)	00001010	00000000	01100010	01100100
Netmasks (B)	11111111	11111111	11111111	00000000
AND operation				
Subnet (B)	00001010	00000000	01100010	01100100
Subnet (D)	10	0	98	0

Task 4: Host-only interfaces

In host OS command window I run this command

ipconfig/all

I found the host interface list from the host OS.

Host-Only interface	IPv4 Address On Host	Subnet Mask	Host Only Interface in the Guest	IP address on the Guest
Ethernet adapter VirtualBox Host-Only Network	**192.168.60.1**	**255.255.255.0**	**enp0s3**	**192.168.60.100**
Ethernet adapter VirtualBox Host-Only Network #2	**192.168.70.1**	**255.255.255.0**	**enp0s8**	**192.168.70.5**

The host only interface is Ethernet adapter Virtual Box-Host-Only Network (192.168.60.1) which is connected to enp0s3 (192.168.60.100) of Gust OS & Ethernet adapter Virtual Box Host-Only network #2 (192.168.70.1) which connected to enp0s8 (192.168.70.5) of guest OS.

```
Ethernet adapter VirtualBox Host-Only Network:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : VirtualBox Host-Only Ethernet Adapter
   Physical Address. . . . . . . . . : 0A-00-27-00-00-11
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::5002:c40e:7229:8faa%17(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.60.1(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :
   DHCPv6 IAID . . . . . . . . . . . : 84541479
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-23-92-69-F6-74-86-7A-59-E9-77
   DNS Servers . . . . . . . . . . . : fec0:0:0:ffff::1%1
                                       fec0:0:0:ffff::2%1
                                       fec0:0:0:ffff::3%1
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

```
Ethernet adapter VirtualBox Host-Only Network #2:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : VirtualBox Host-Only Ethernet Adapter #2
   Physical Address. . . . . . . . . : 0A-00-27-00-00-2B
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::b9b6:6262:5d93:a485%43(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.70.1(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :
   DHCPv6 IAID . . . . . . . . . . . : 722075687
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-23-92-69-F6-74-86-7A-59-E9-77
   DNS Servers . . . . . . . . . . . : fec0:0:0:ffff::1%1
                                       fec0:0:0:ffff::2%1
                                       fec0:0:0:ffff::3%1
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

```
Ethernet adapter VirtualBox Host-Only Network #3:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : VirtualBox Host-Only Ethernet Adapter #3
   Physical Address. . . . . . . . . : 0A-00-27-00-00-2F
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::c50:e4e:60b5:3ccb%47(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.80.1(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :
   DHCPv6 IAID . . . . . . . . . . . : 789184551
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-23-92-69-F6-74-86-7A-59-E9-77
   DNS Servers . . . . . . . . . . . : fec0:0:0:ffff::1%1
                                       fec0:0:0:ffff::2%1
                                       fec0:0:0:ffff::3%1
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

Task 5: Routing tables in the host OS

I have run the command route -4 PRINT

By the interface 10.59.0.64 and I can reach the gateway 10.59.0.64 for the host OS.

Command Prompt

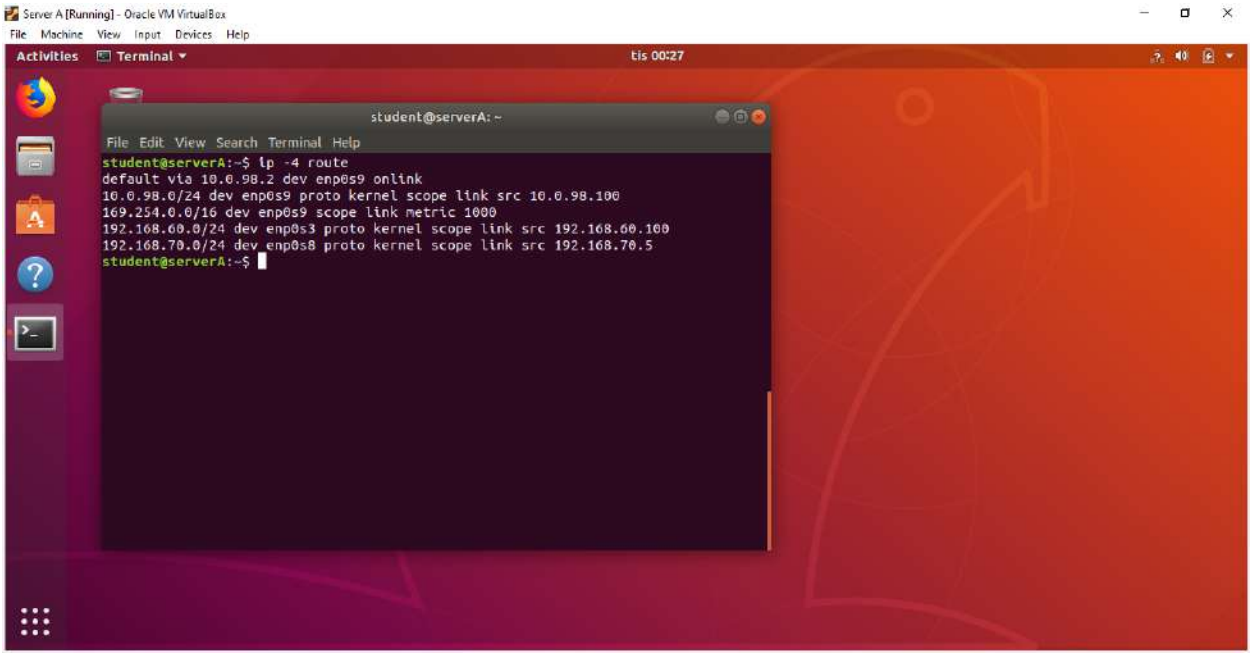
```
C:\Users\purno>route -4 PRINT
===========================================================================
Interface List
  6...74 86 7a 59 e9 77 ......Realtek PCIe FE Family Controller
 17...0a 00 27 00 00 11 ......VirtualBox Host-Only Ethernet Adapter
 43...0a 00 27 00 00 2b ......VirtualBox Host-Only Ethernet Adapter #2
 47...0a 00 27 00 00 2f ......VirtualBox Host-Only Ethernet Adapter #3
  9...16 5a 04 ac ad a2 ......Microsoft Wi-Fi Direct Virtual Adapter
  7...64 5a 04 ac ad a2 ......Dell Wireless 1705 802.11b|g|n (2.4GHZ)
 14...64 5a 04 ac ad a3 ......Bluetooth Device (Personal Area Network)
  1...........................Software Loopback Interface 1
 15...00 00 00 00 00 00 00 e0 Microsoft Teredo Tunneling Adapter
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0       10.59.0.1       10.59.0.64     55
       10.59.0.0    255.255.255.0         On-link        10.59.0.64    311
      10.59.0.64  255.255.255.255         On-link        10.59.0.64    311
     10.59.0.255  255.255.255.255         On-link        10.59.0.64    311
       127.0.0.0        255.0.0.0         On-link         127.0.0.1    331
       127.0.0.1  255.255.255.255         On-link         127.0.0.1    331
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    331
    192.168.60.0    255.255.255.0         On-link      192.168.60.1    281
    192.168.60.1  255.255.255.255         On-link      192.168.60.1    281
  192.168.60.255  255.255.255.255         On-link      192.168.60.1    281
    192.168.70.0    255.255.255.0         On-link      192.168.70.1    330
    192.168.70.1  255.255.255.255         On-link      192.168.70.1    330
  192.168.70.255  255.255.255.255         On-link      192.168.70.1    330
    192.168.80.0    255.255.255.0         On-link      192.168.80.1    330
    192.168.80.1  255.255.255.255         On-link      192.168.80.1    330
  192.168.80.255  255.255.255.255         On-link      192.168.80.1    330
       224.0.0.0        240.0.0.0         On-link         127.0.0.1    331
       224.0.0.0        240.0.0.0         On-link      192.168.60.1    281
       224.0.0.0        240.0.0.0         On-link        10.59.0.64    311
       224.0.0.0        240.0.0.0         On-link      192.168.70.1    330
       224.0.0.0        240.0.0.0         On-link      192.168.80.1    330
  255.255.255.255  255.255.255.255         On-link         127.0.0.1    331
  255.255.255.255  255.255.255.255         On-link      192.168.60.1    281
  255.255.255.255  255.255.255.255         On-link        10.59.0.64    311
  255.255.255.255  255.255.255.255         On-link      192.168.70.1    330
  255.255.255.255  255.255.255.255         On-link      192.168.80.1    330
```

Task 6: Routing tables in the guest OS

I run in the guest OS this command

ip -4 route

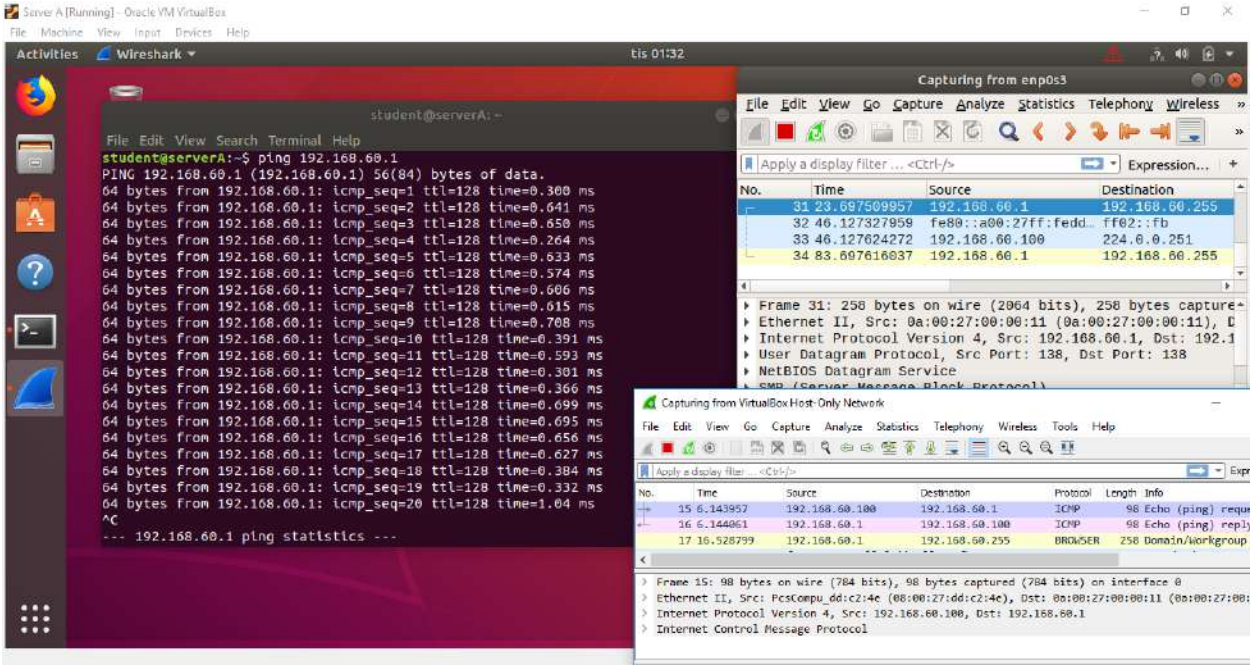
By the NAT interface enp0s9 I can found default gateway 10.0.98.2.

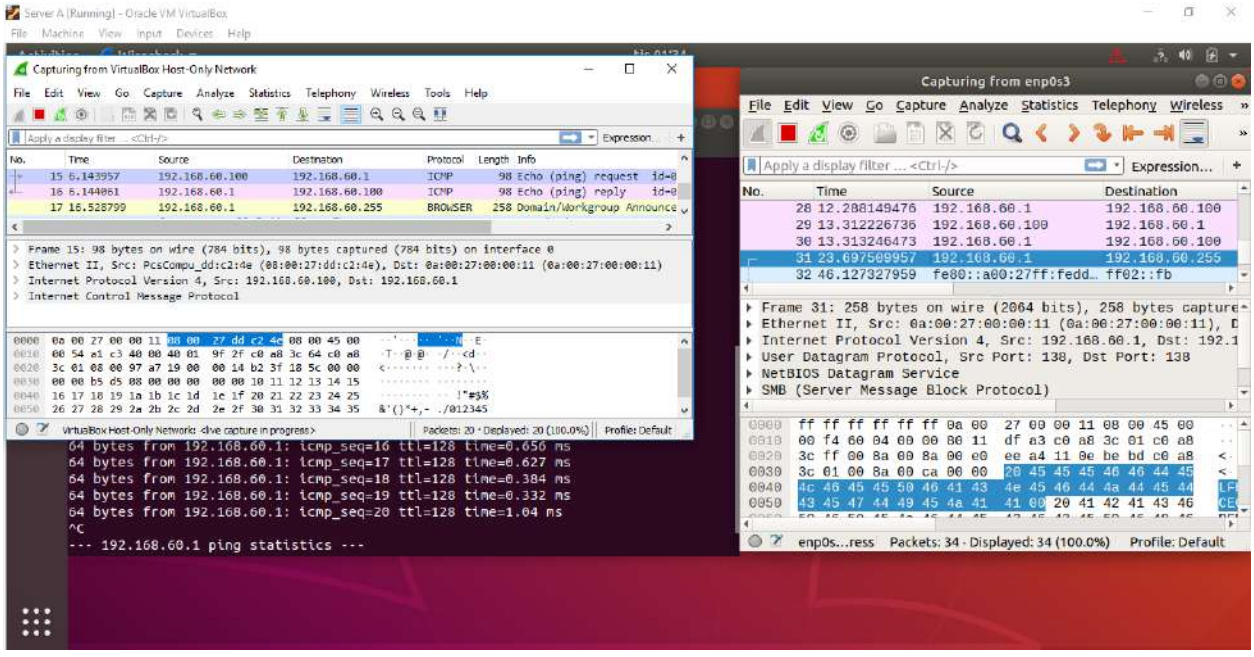


Task 7: Ping the host-based host-only interface

In this task at first turn off the firewall system of the Host OS after that I run the command

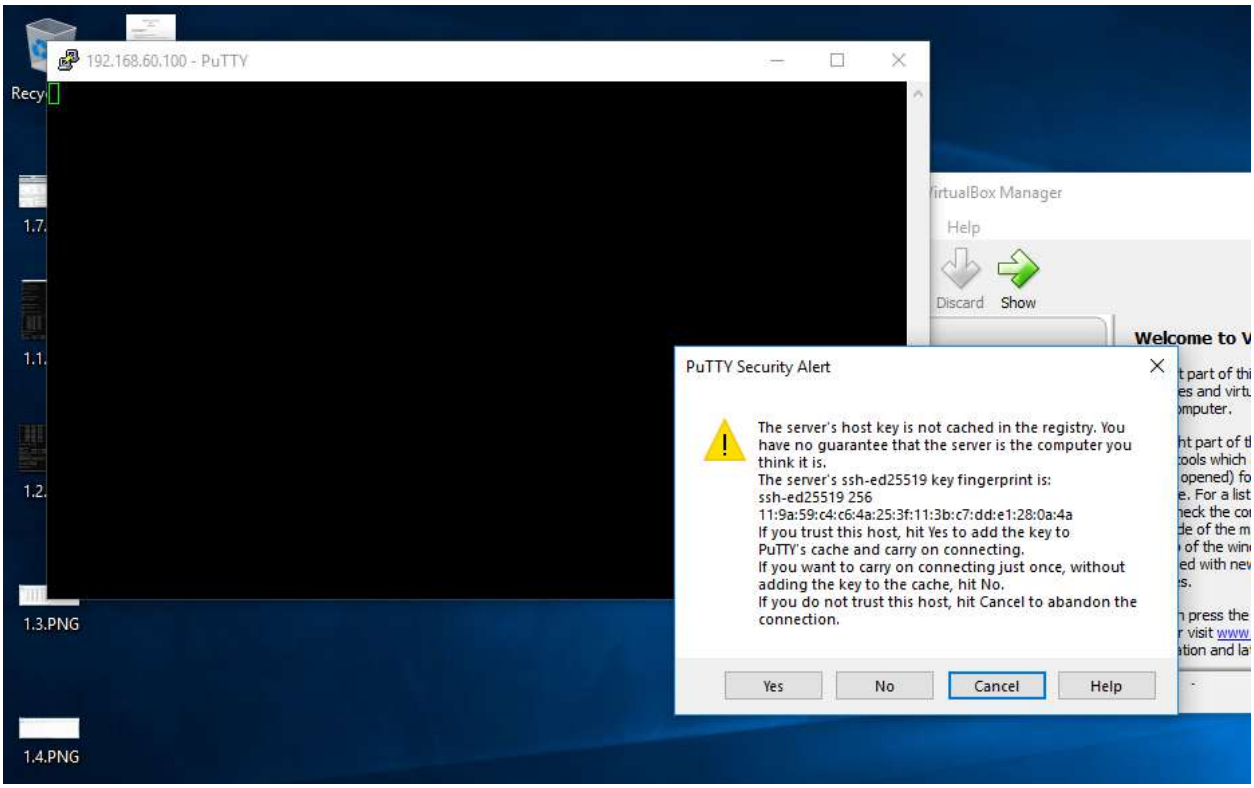
ping 192.168.60.1 in guest OS beside that I opened both wireshark check the both ping signal no loss.

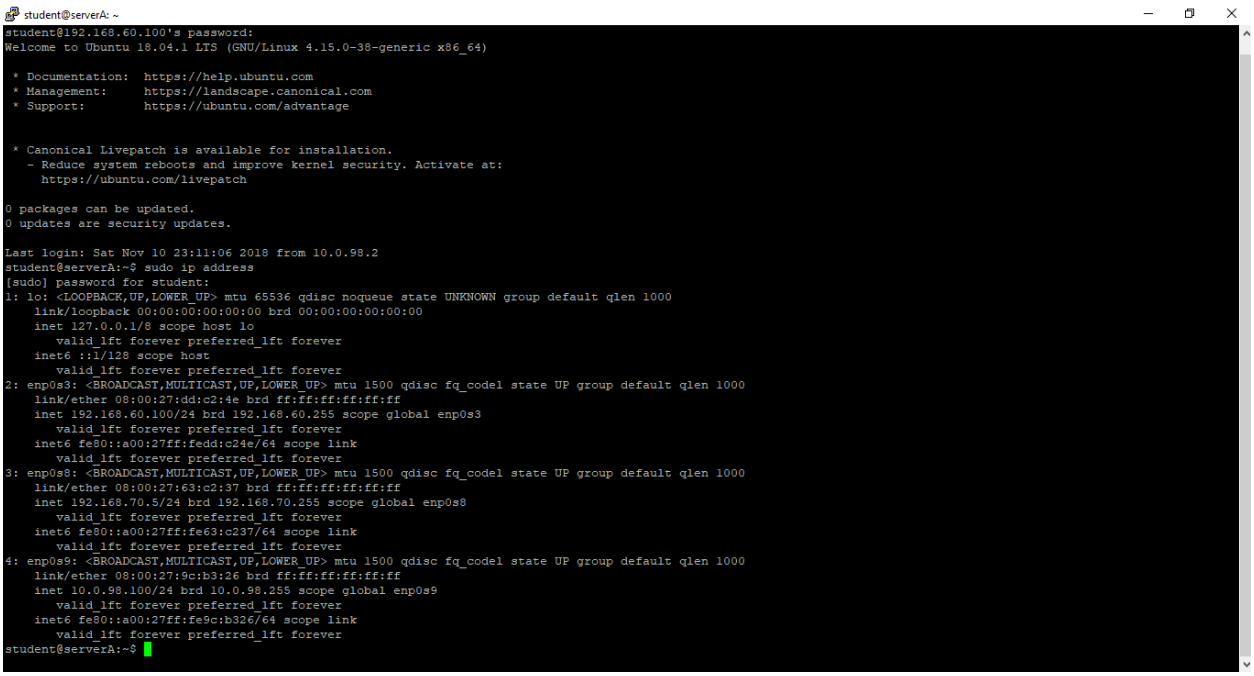




Task 8: SSH into VM via localhost

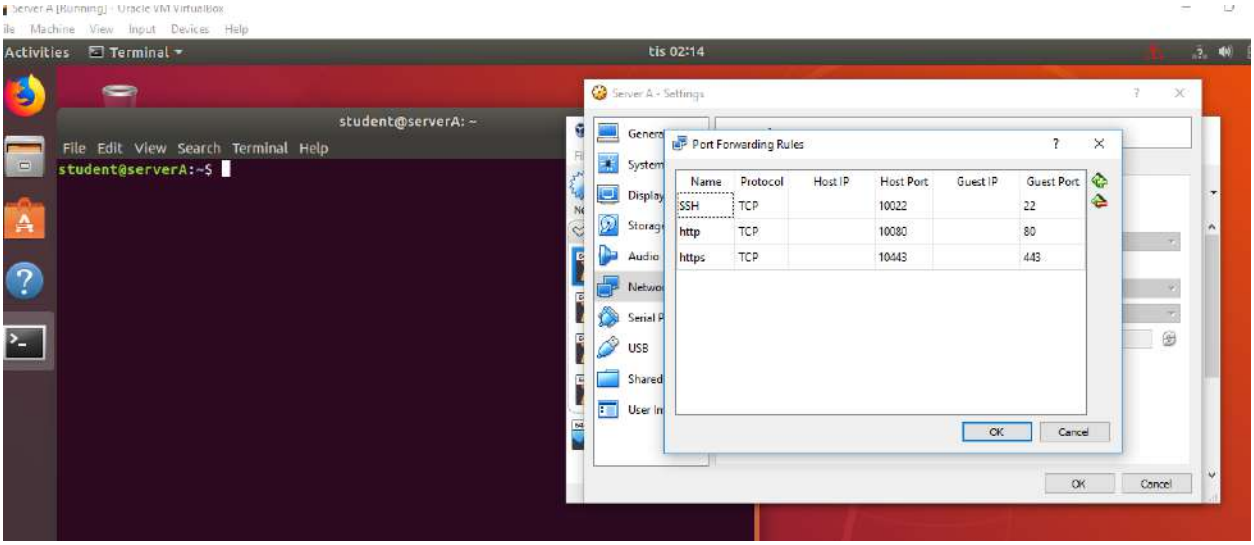
I have opened remote shell server use putty software and it successfully worked.



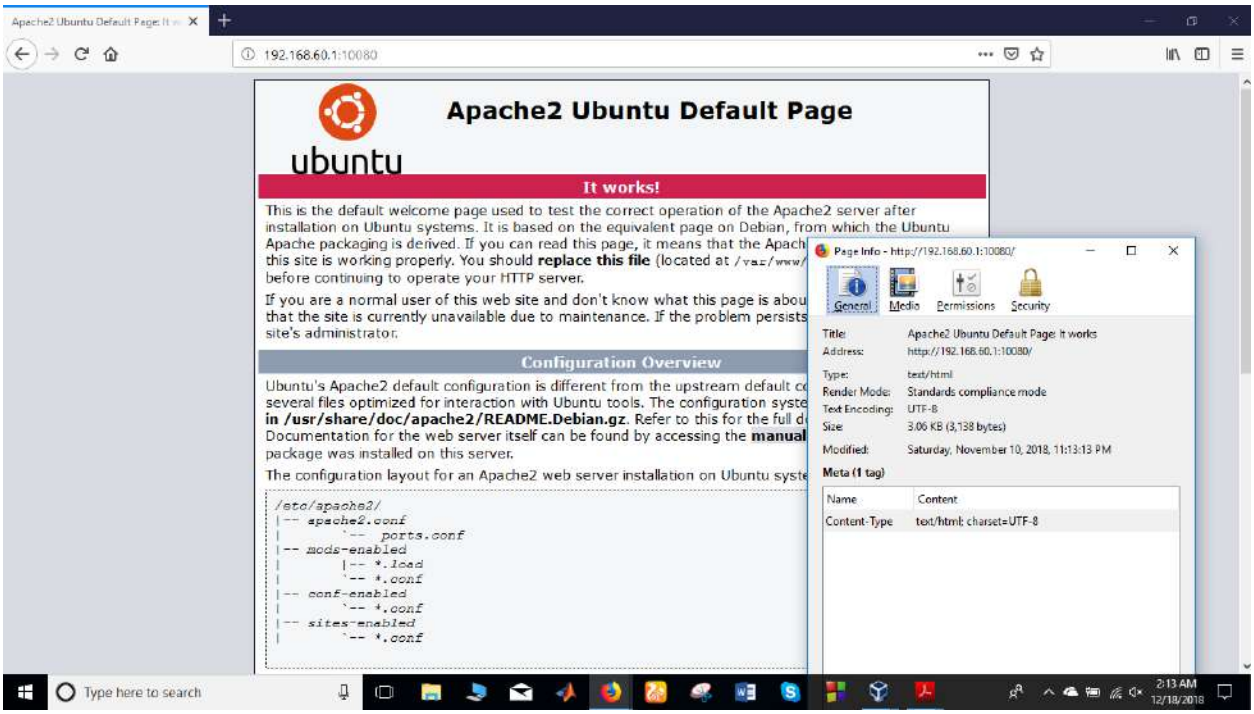


Task 9: Add forwarding rules for HTTP and HTTPS in VirtualBox

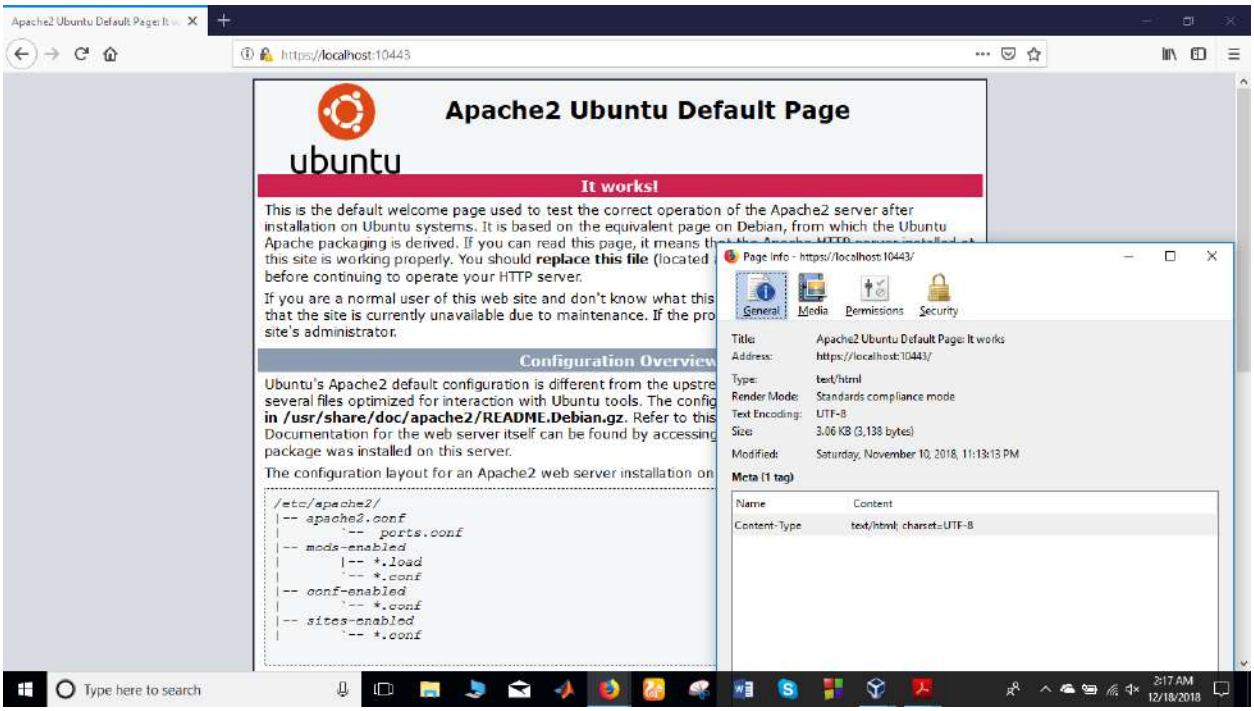
I have used host port number 10080 for HTTP and 10443 for HTTPS.



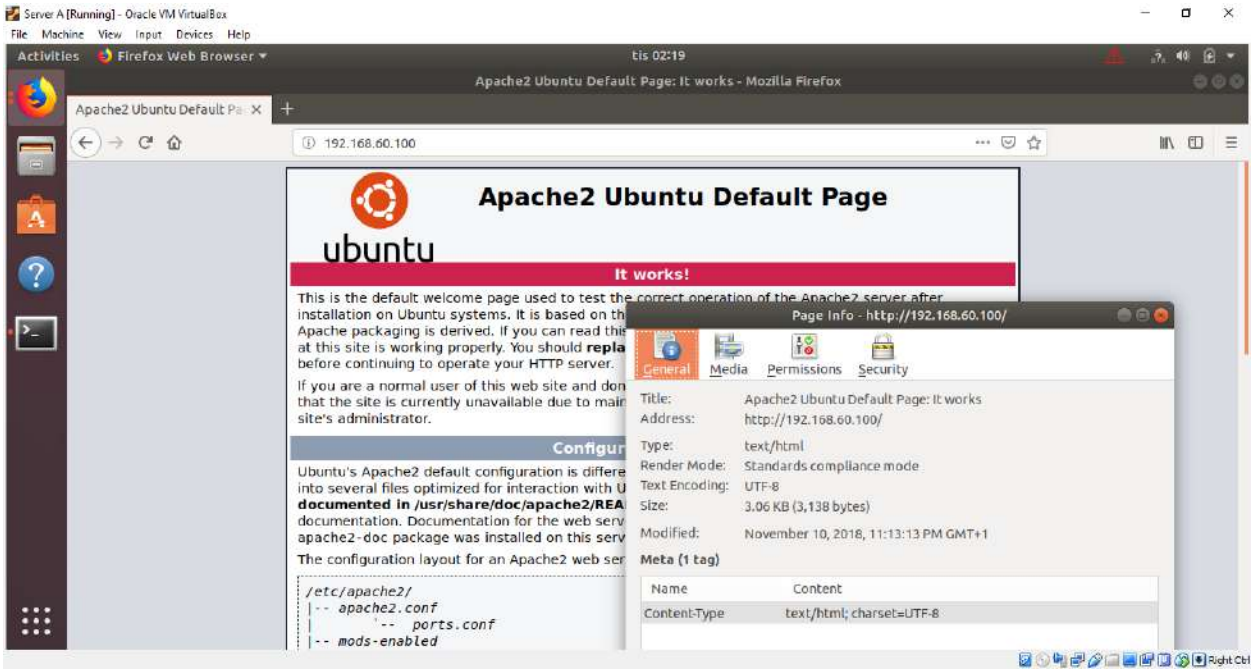
Apache2 server in the host over HTTP



Apache2 server in the host over HTTPS

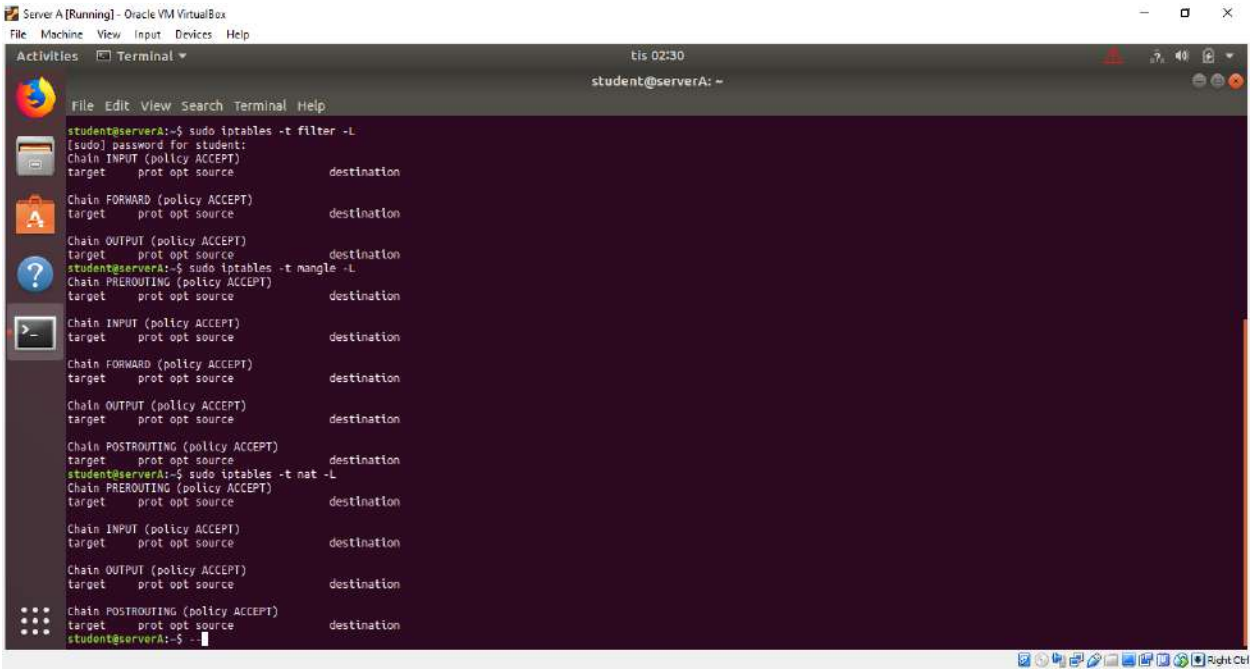


Apache2 server in the guest over HTTP



Task 10: Default firewall policy and rules

I have run the following commands
sudo iptables –t filter -L
sudo iptables –t mangle -L
sudo iptables –t nat -L
For INPUT, OUTPUT and FORWARD chains, they allow all data, do not drop any data.



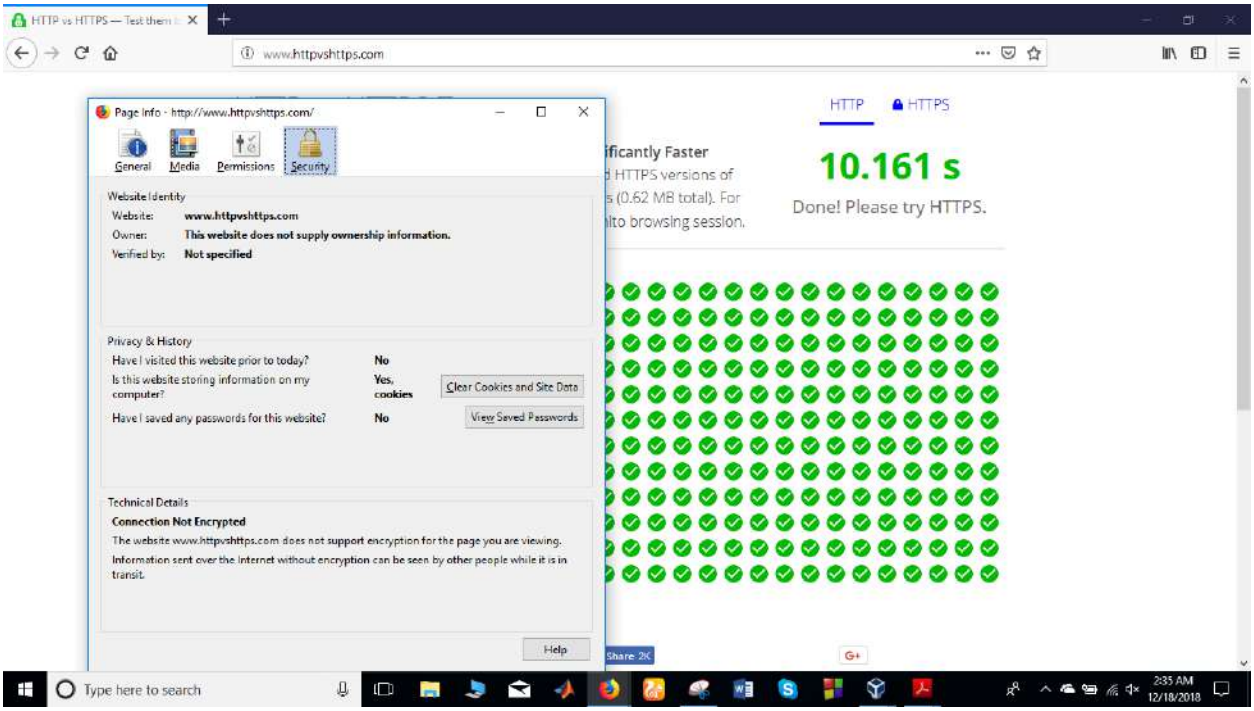
Task 11: Block HTTP-browsing in the guest OS

I haverun this iptables rules

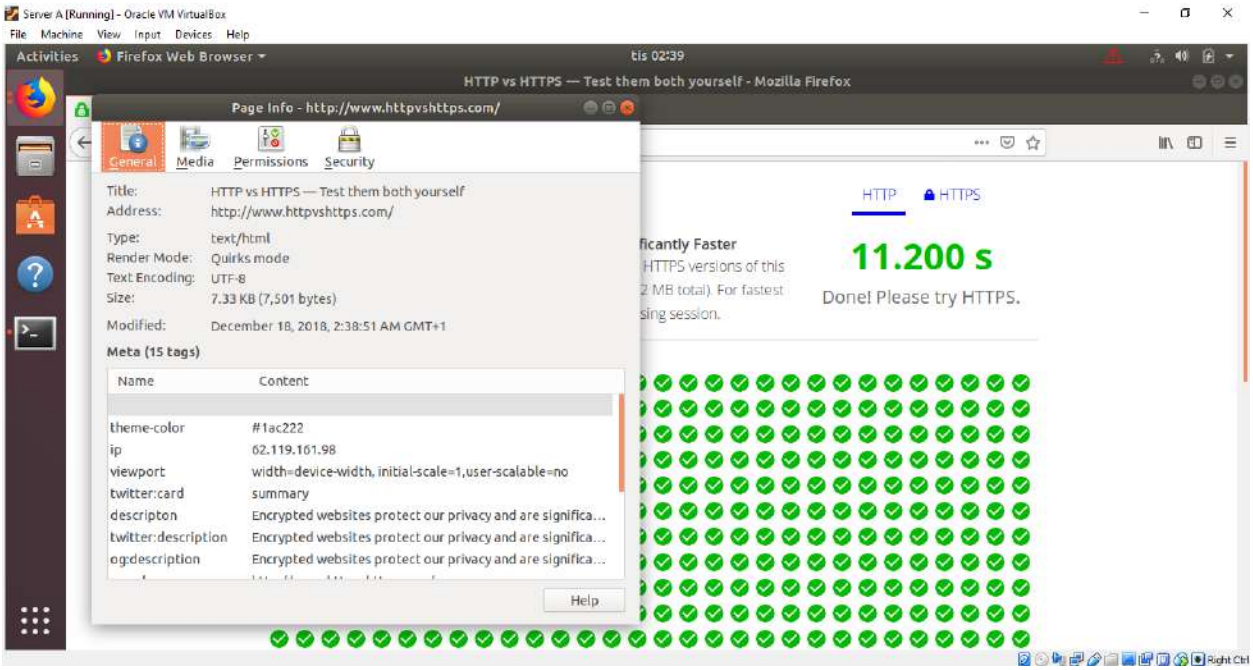
sudo iptables -A OUTPUT -p tcp --dport 80 -j REJECT

this rules block the user in the guest OS for HTTP .

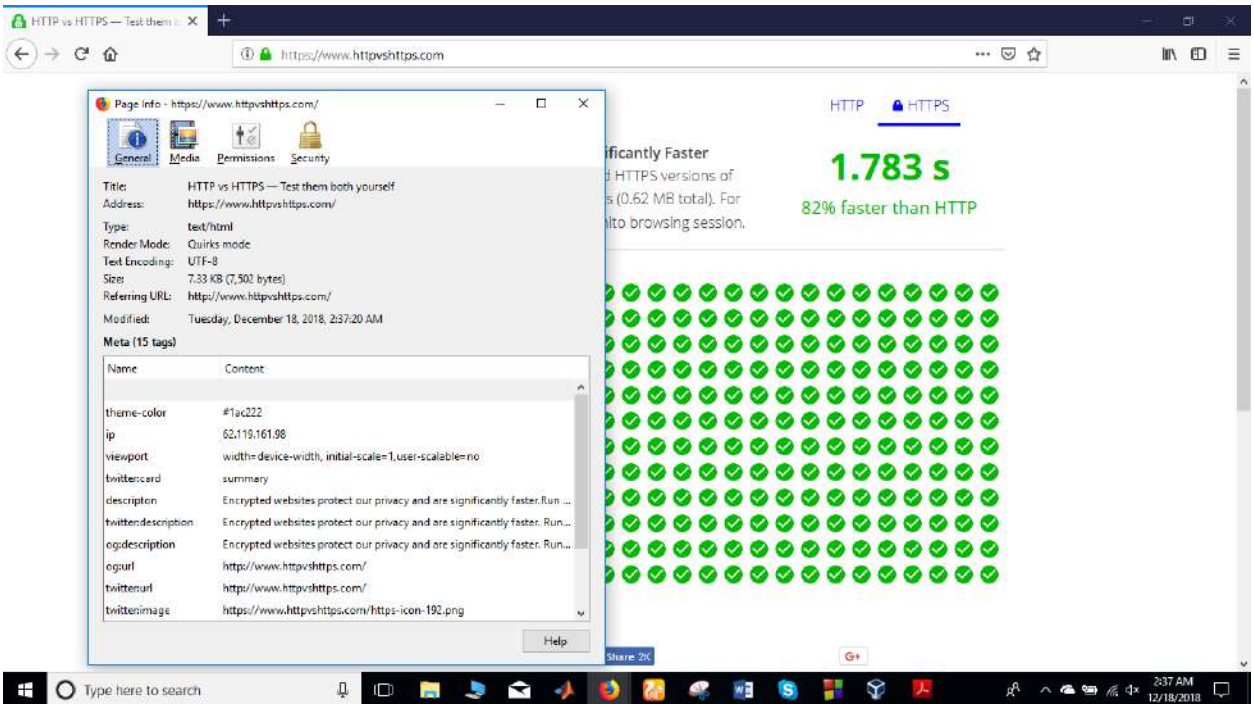
Web page over HTTP on Host



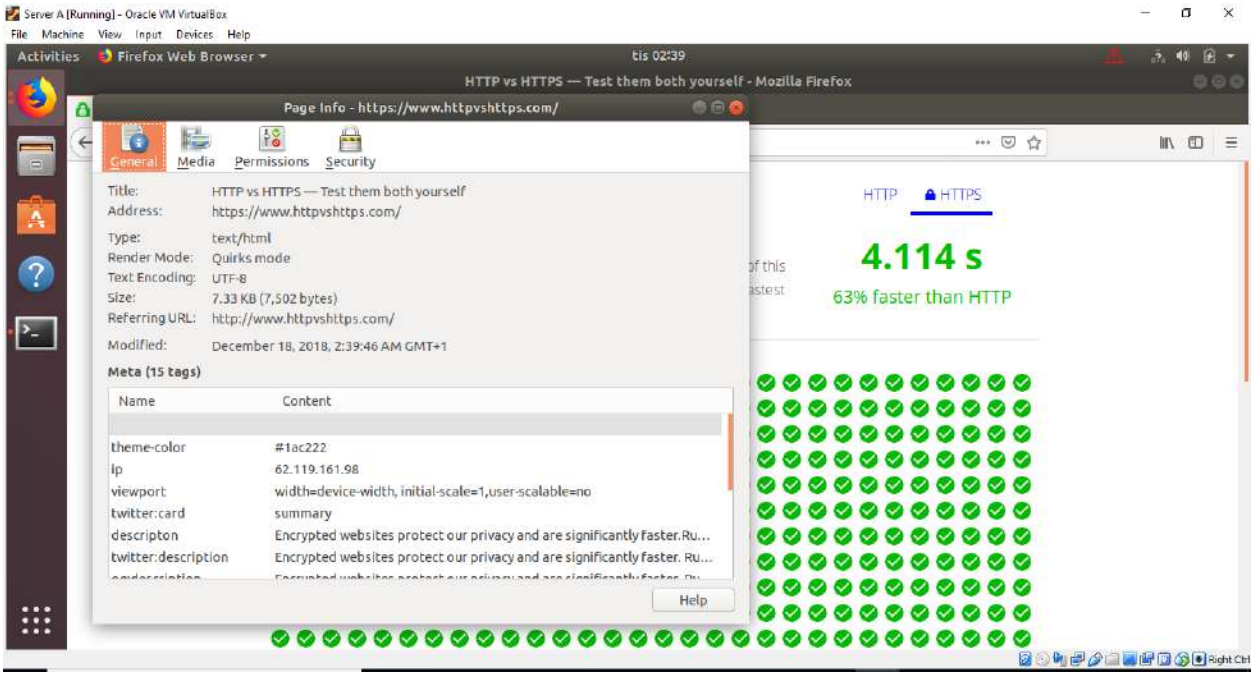
Web page over HTTP on Guest



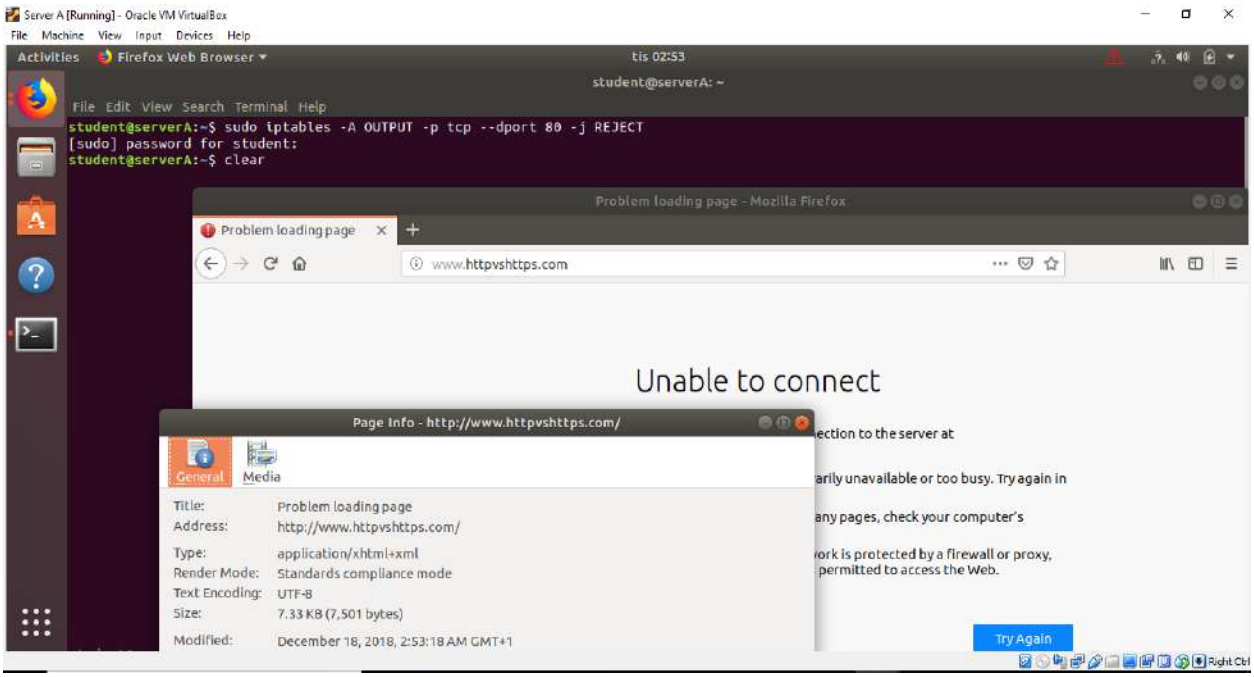
Web page over HTTPS on Host



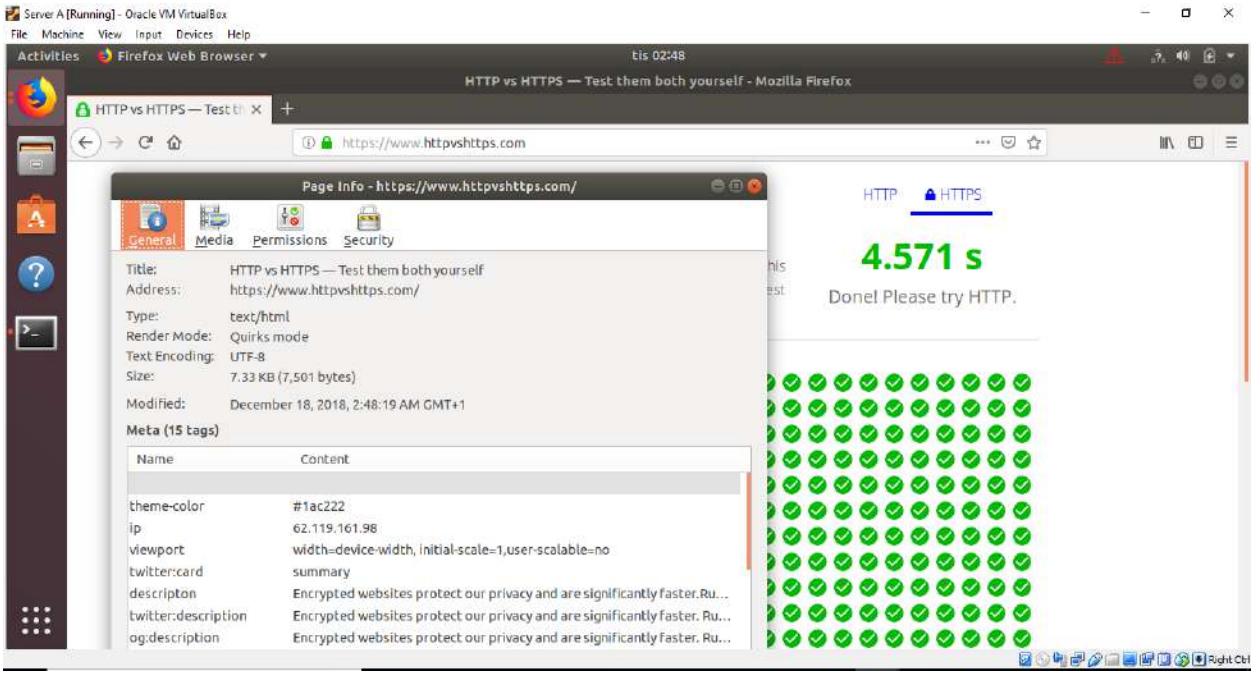
Web page over HTTPS on Guest



After running the command block the HTTP



But still can browse HTTPS

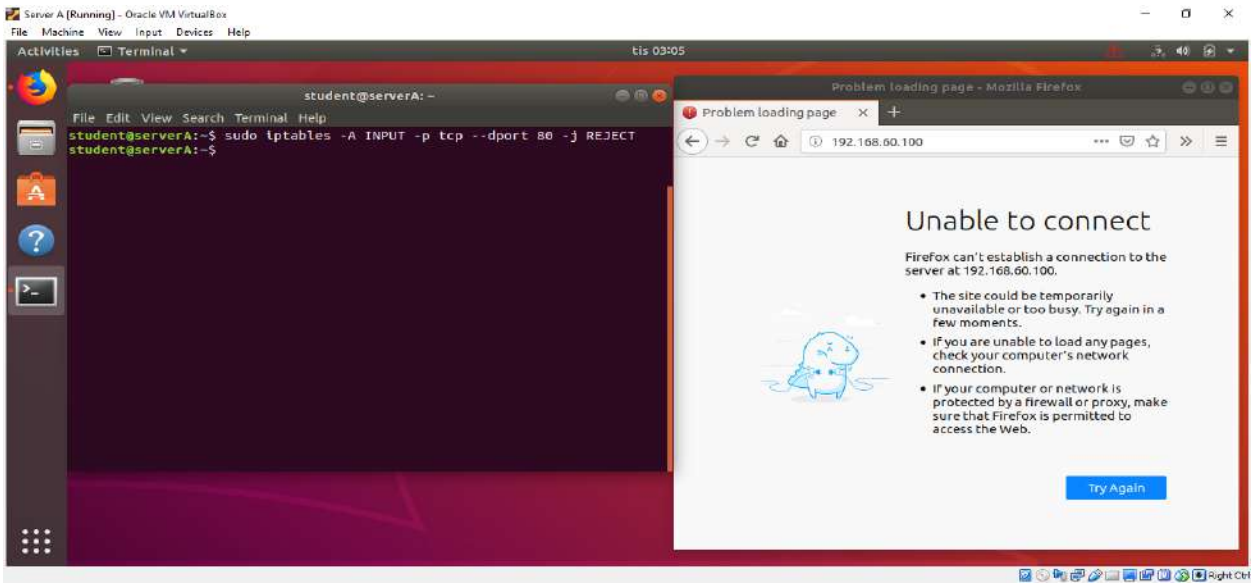


Task 12: Block Apache web server from serving content over HTTP

In guest command window

sudo iptables -A INPUT -p tcp --dport 80 -j REJECT

After run upper command host cannot view HTTP content from the apache2 server in the guest OS.

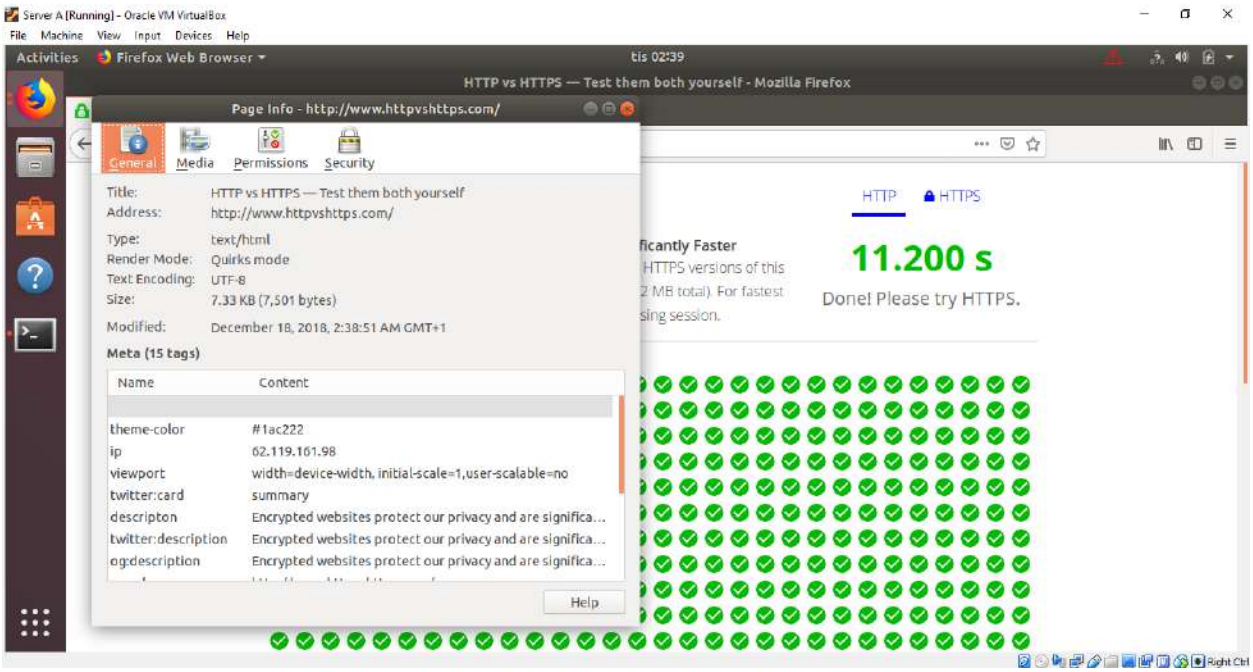


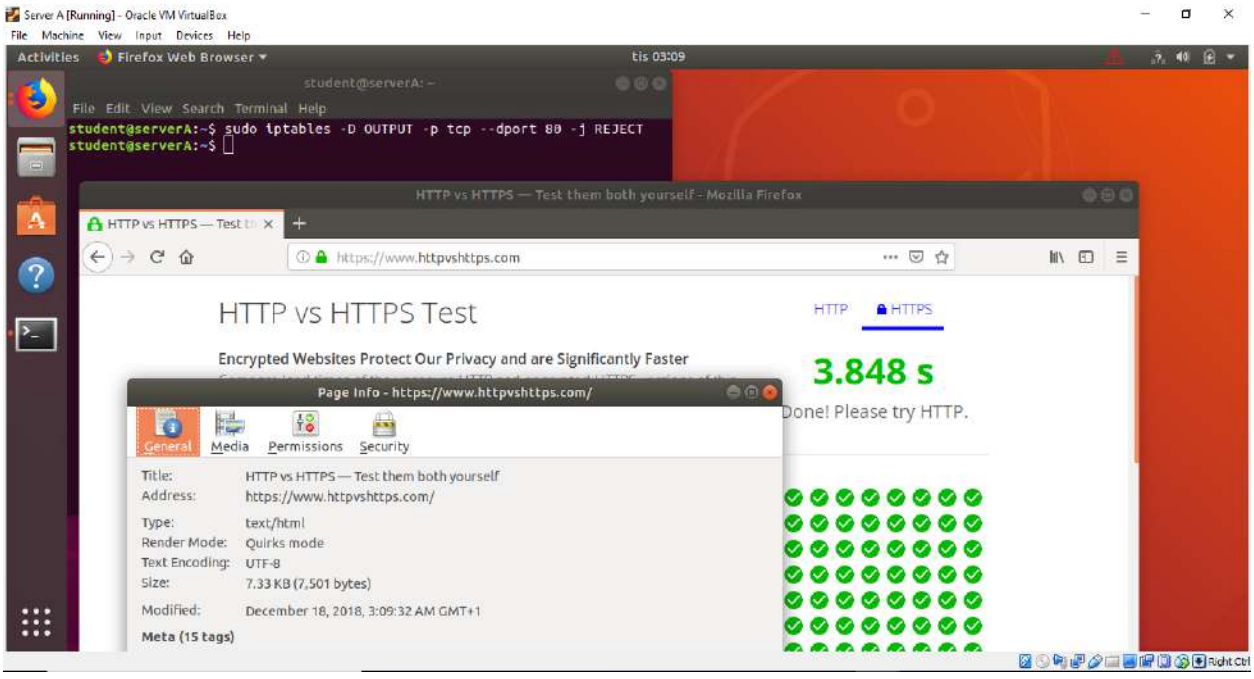
Task 13: Unblock HTTP-browsing in the guest OS

In guest command window run I have run this rule

sudo iptables -D OUTPUT -p tcp --dport 80 -j REJECT

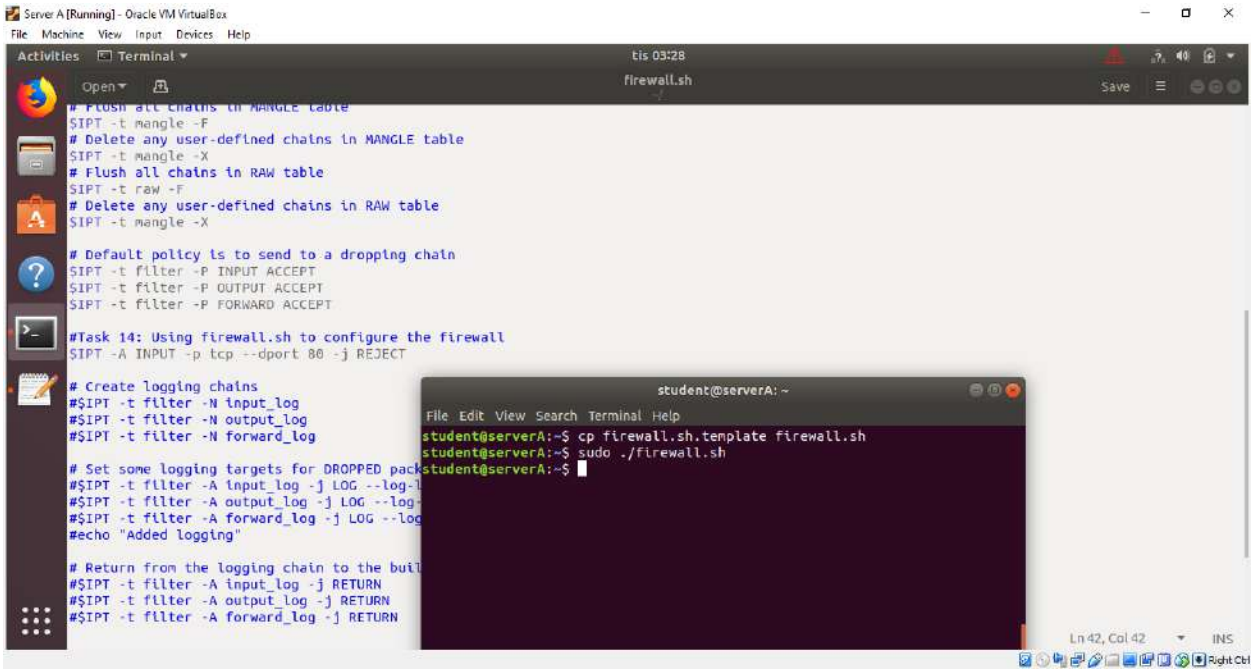
After that I can browse both HTTP and HTTPS, so this rule is effective.

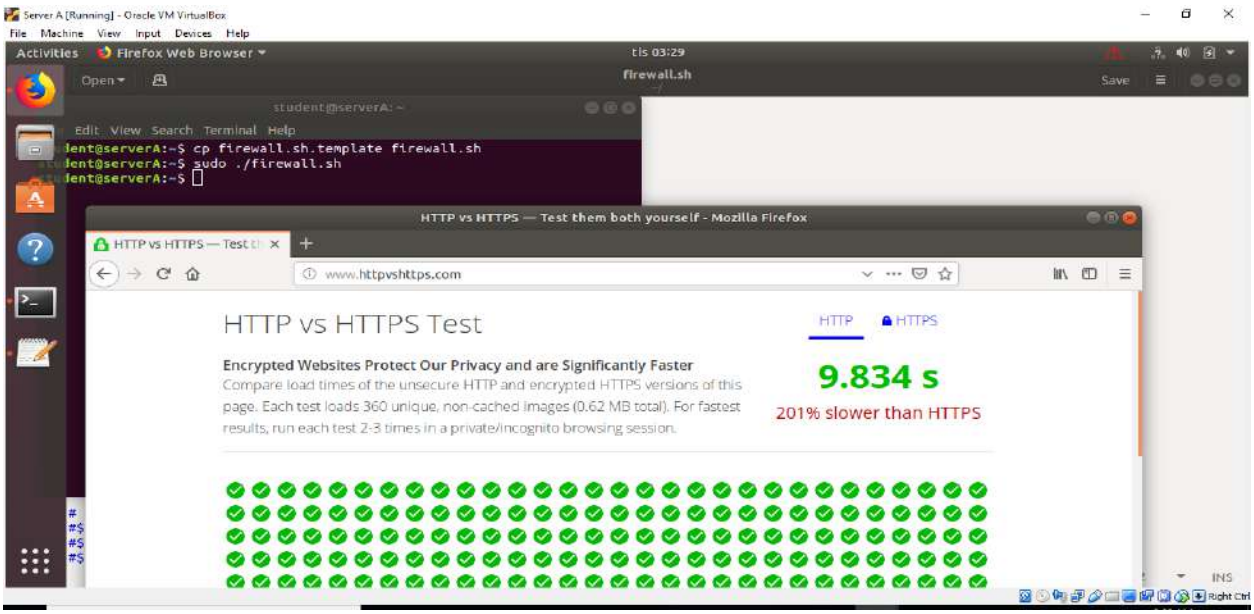


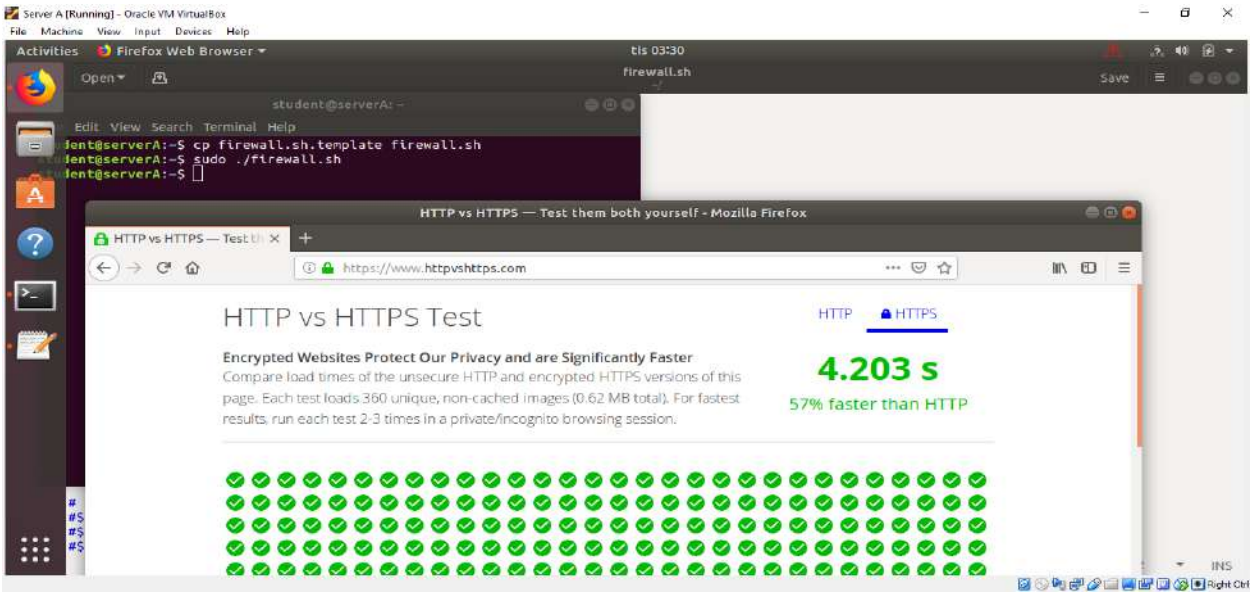


Task 14: Use firewall.sh to configure the firewall

I have modified the firewall.sh script as Task 13
$IPT -A INPUT -p tcp --dport 80 -j REJECT
And executed the script by entering in guest command window
sudo ./firewall.sh
So, the guest OS can view HTTP and HTTPS pages, but apache2 server is blocked from serving HTTP content.







Task 15: Change default firewall policy to DROP

I have removed the rules from Task 14.

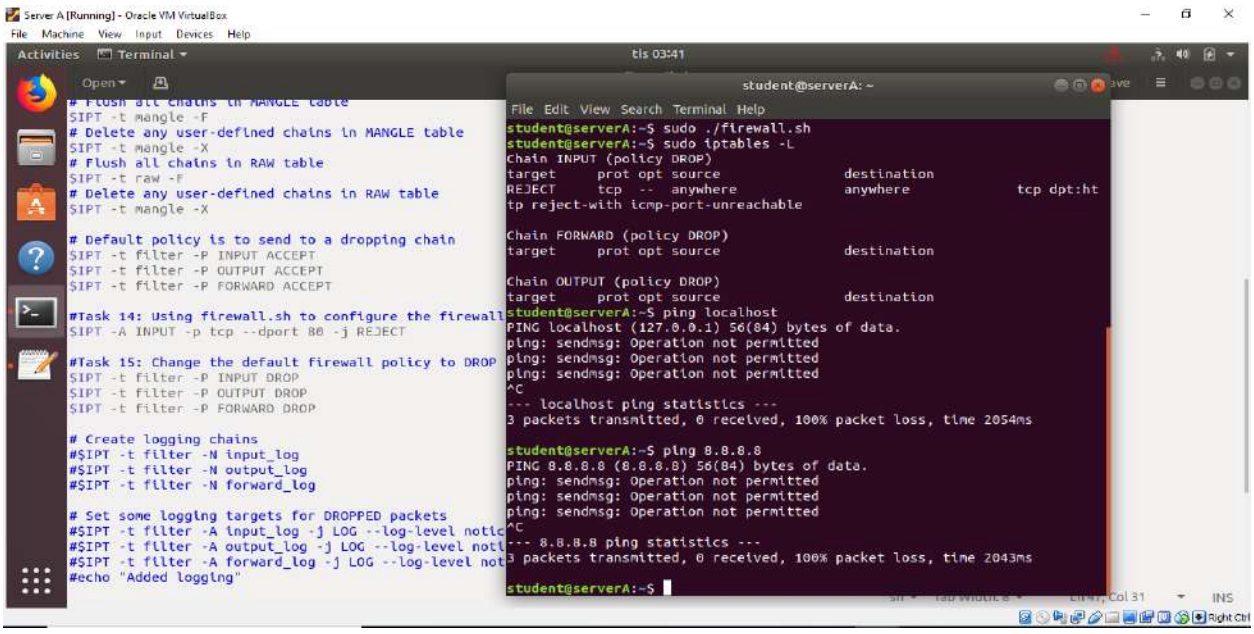
Modify the script

$IPT -t filter -P INPUT DROP

$IPT -t filter -P OUTPUT DROP

$IPT -t filter -P FORWARD DROP

After executed the rule server A cannot ping to the localhost.



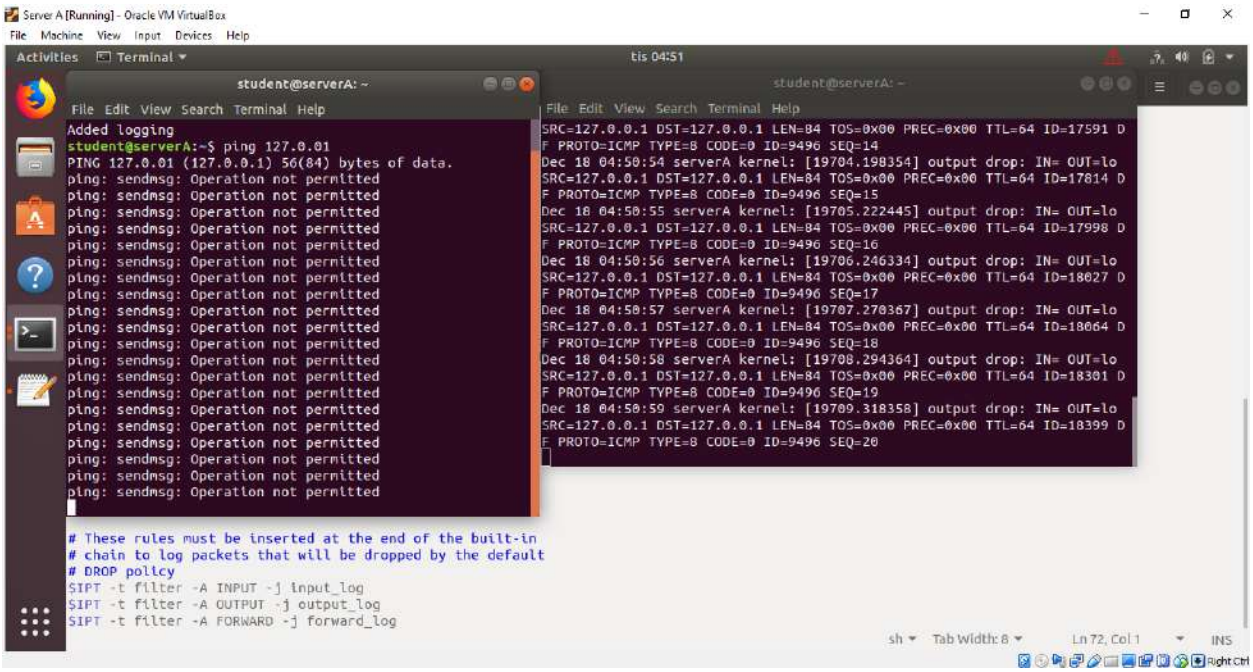
Task 16: Logging DROPPED packets

Modify my firewall script error

Run the terminal window this code

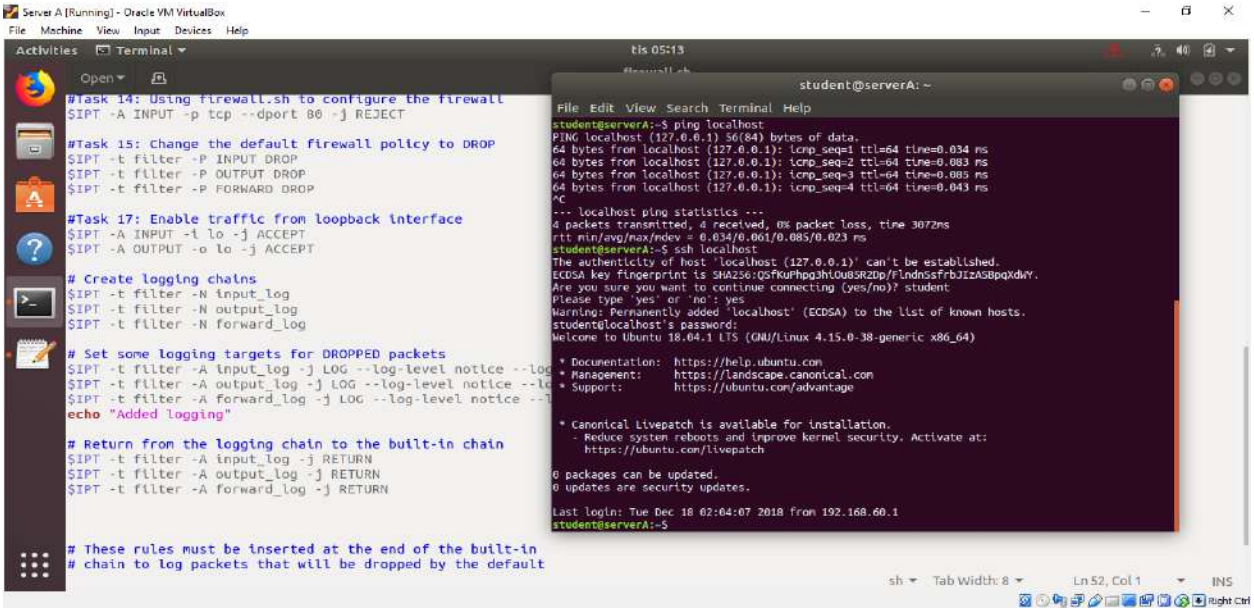
sudo tail -f /var/log/kern.log

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



Task 17: Enable traffic from loopback interface

Modified my firewall script as per instruction and executed it. commands
$IPT -A INPUT -i lo -j ACCEPT
$IPT -A OUTPUT -o lo -j ACCEPT
Then I can able lookback localhost and ssh localhost.



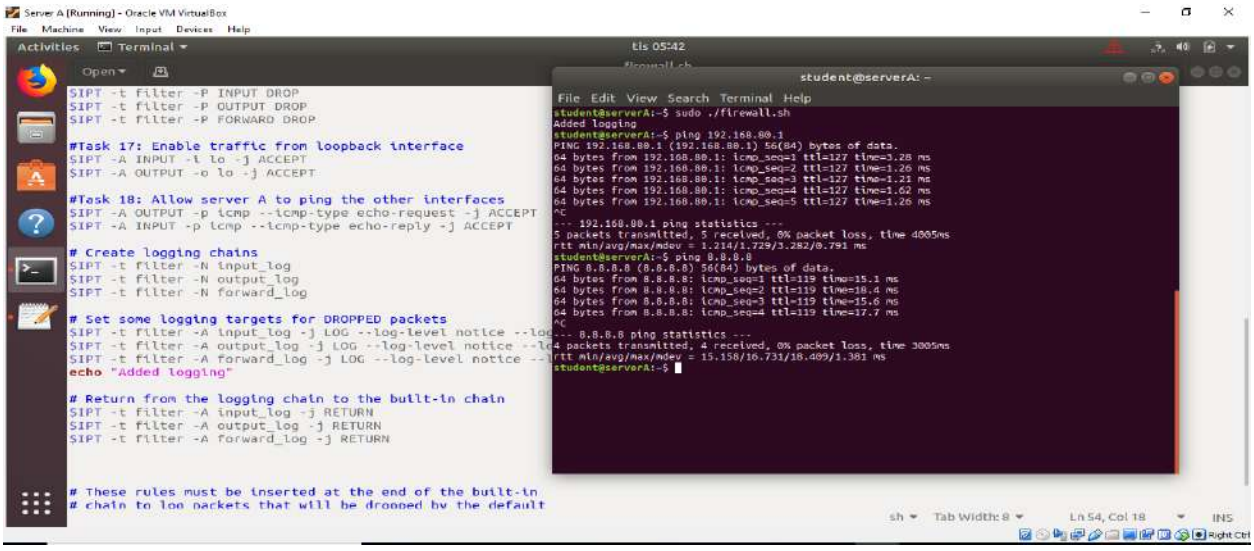
Task 18: Allow Server A to ping the other interfaces

Modified my firewall script as per instruction and executed it. Commands-

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

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

I can manage ping from server A to the outside world.



Task 19: Allow Server A to ping all hosts

Modified my firewall script as per instruction and executed it. Commands

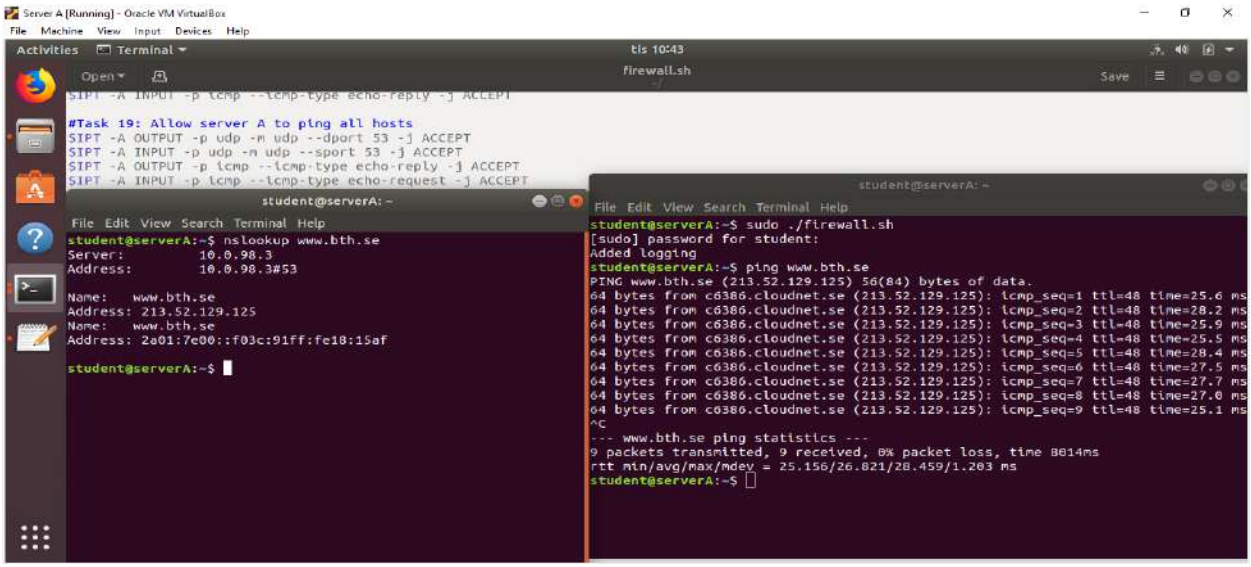
$IPT -A OUTPUT -p udp -m udp --dport 53 -j ACCEPT

$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

Now server A can ping all host

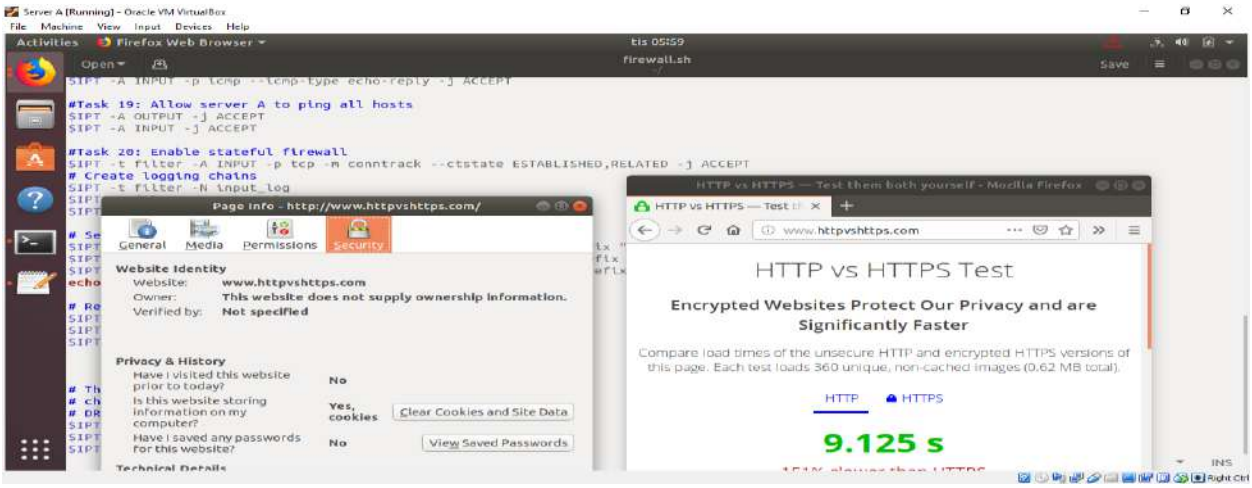


Task 20: Enable stateful firewall

Modified my firewall script as per instruction and executed it. By commands-

$IPT -t filter -A INPUT -p tcp -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT

After that manage to browse both http and https.



Task 21: Enable SSH and HTTPS content from apache2 server for web browser on host

Modified my firewall script as per instruction and executed it. Commands-

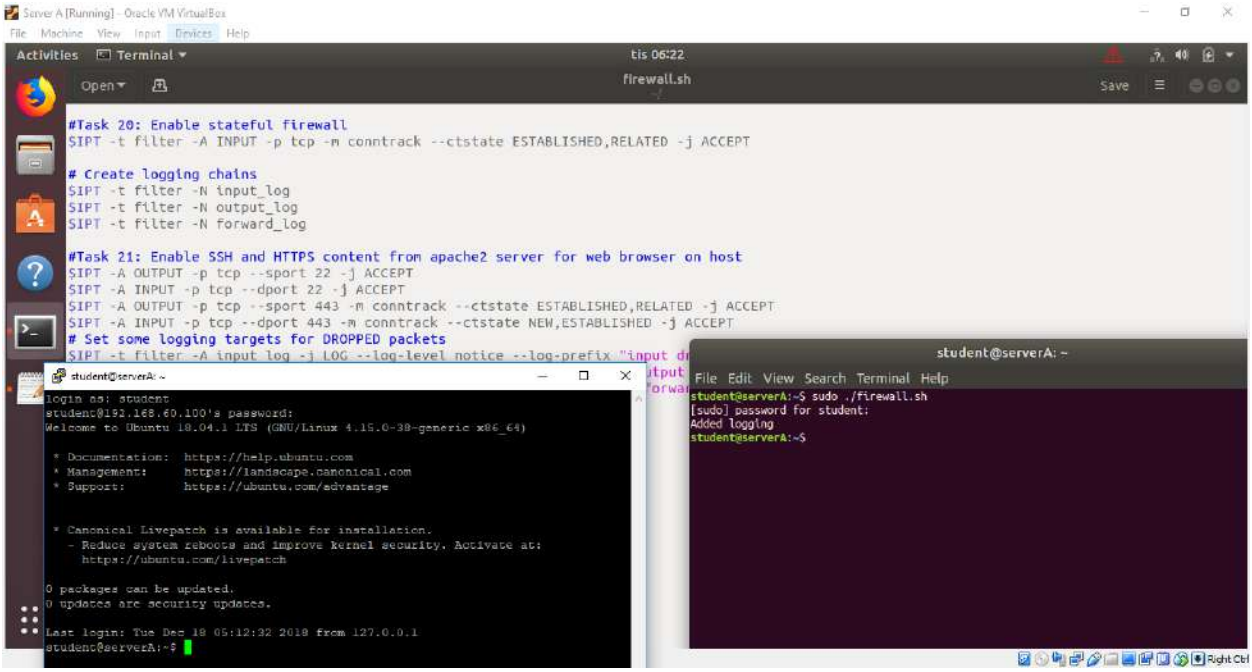
$IPT -A OUTPUT -p tcp --sport 22 -j ACCEPT

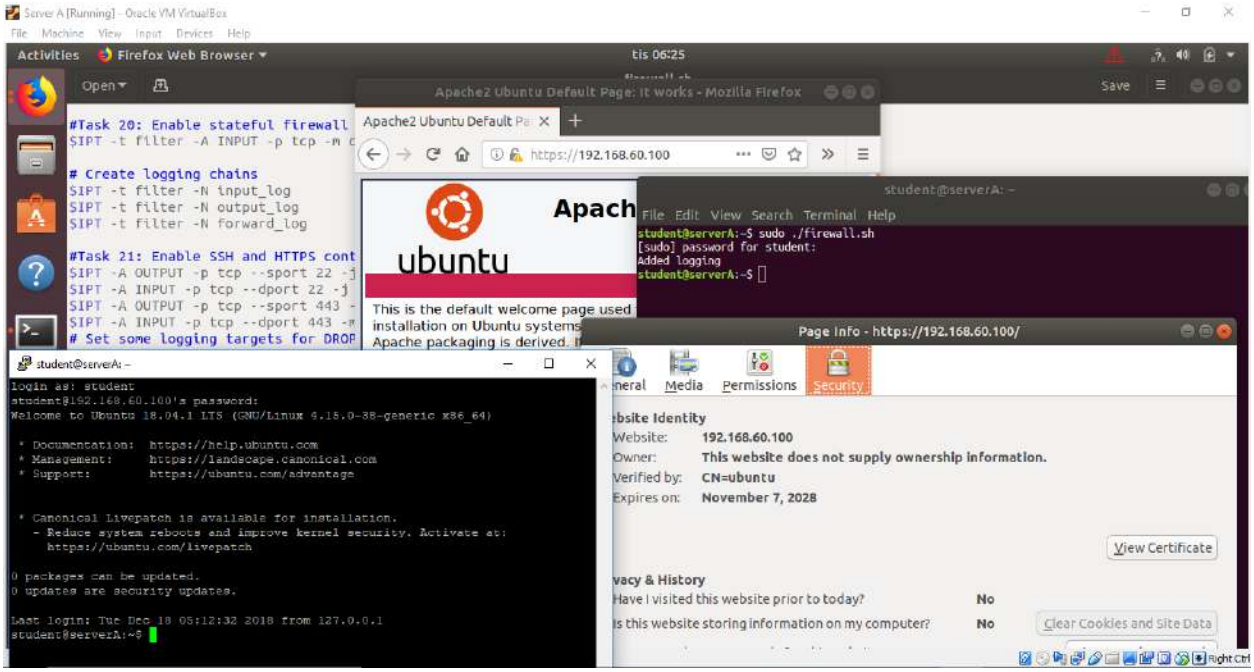
$IPT -A INPUT -p tcp --dport 22 -j ACCEPT

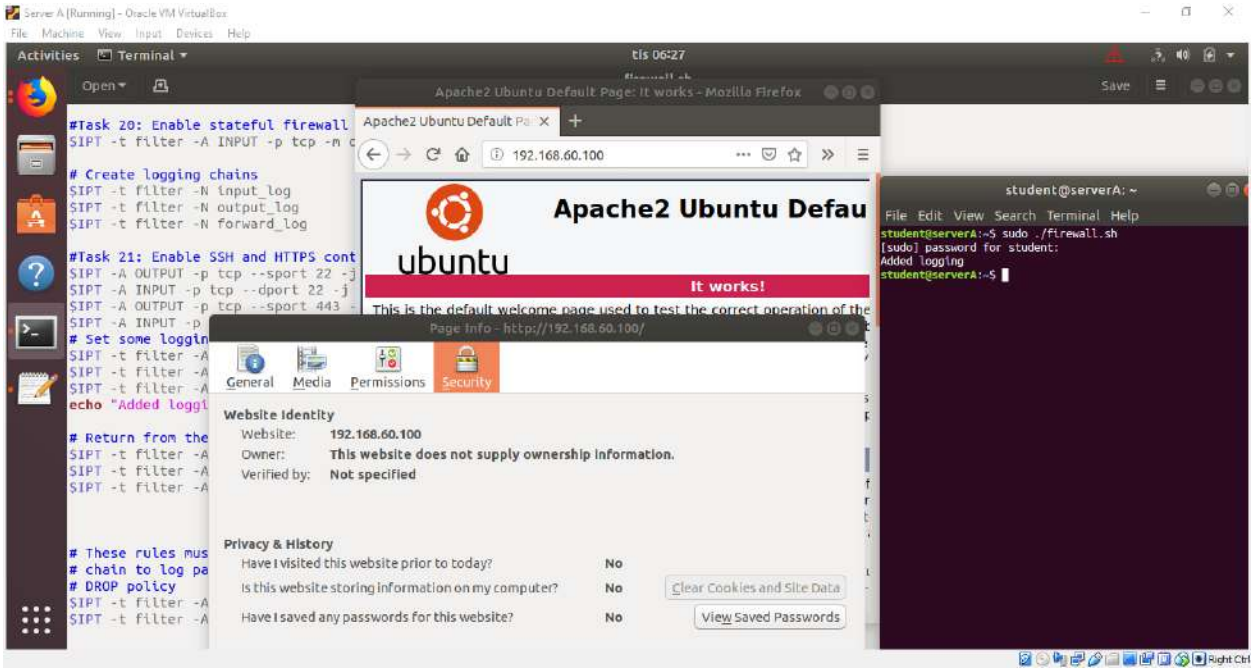
$IPT -A OUTPUT -p tcp --sport 443 -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT

$IPT -A INPUT -p tcp --dport 443 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT

After that enable SSH and HTTPS content from apache2 server.




Server A [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Firefox Web Browser
tis 06:25
Open
Save
#Task 20: Enable stateful firewall
SIPT -t filter -A INPUT -p tcp -m c
Create logging chains
SIPT -t filter -N input_log
SIPT -t filter -N output_log
SIPT -t filter -N forward_log
#Task 21: Enable SSH and HTTPS cont
SIPT -A OUTPUT -p tcp --sport 22 -j
SIPT -A INPUT -p tcp --dport 22 -j
SIPT -A OUTPUT -p tcp --sport 443 -
SIPT -A INPUT -p tcp --dport 443 -m
Set some logging targets for DROP
Apache2 Ubuntu Default Page: It works - Mozilla Firefox
Apache2 Ubuntu Default Pa
https://192.168.60.100
Apach
ubuntu
This is the default welcome page used
installation on Ubuntu systems
Apache packaging is derived.
student@serverA: ~
File Edit View Search Terminal Help
student@serverA:~$ sudo ./firewall.sh
[sudo] password for student:
Added logging
student@serverA:~$
Page Info - https://192.168.60.100/
General
Media
Permissions
Security
Website Identity
Website: 192.168.60.100
Owner: This website does not supply ownership information.
Verified by: CN=ubuntu
Expires on: November 7, 2028
View Certificate
Privacy & History
Have I visited this website prior to today? No
Is this website storing information on my computer? No
Clear Cookies and Site Data
student@serverA: ~
login as: student
student@192.168.60.100's password:
Welcome to Ubuntu 18.04.1 LTS (GNU/Linux 4.15.0-38-generic x86_64)
* Documentation: https://help.ubuntu.com
* Management: https://landscape.canonical.com
* Support: https://ubuntu.com/advantage
* Canonical Livepatch is available for installation.
- Reduce system reboots and improve kernel security. Activate at:
https://ubuntu.com/livepatch
0 packages can be updated.
0 updates are security updates.
Last login: Tue Dec 18 05:12:32 2018 from 127.0.0.1
student@serverA:~$
Right Ctrl


Server A [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Terminal
tis 06:27
Open
Save
#Task 20: Enable stateful firewall
SIPT -t filter -A INPUT -p tcp -m c
Create logging chains
SIPT -t filter -N input_log
SIPT -t filter -N output_log
SIPT -t filter -N forward_log
#Task 21: Enable SSH and HTTPS cont
SIPT -A OUTPUT -p tcp --sport 22 -j
SIPT -A INPUT -p tcp --dport 22 -j
SIPT -A OUTPUT -p tcp --sport 443 -
SIPT -A INPUT -p
Set some loggin
SIPT -t filter -A
SIPT -t filter -A
SIPT -t filter -A
echo "Added loggi
Return from the
SIPT -t filter -A
SIPT -t filter -A
SIPT -t filter -A
These rules mus
chain to log pa
DROP policy
SIPT -t filter -A
SIPT -t filter -A
Apache2 Ubuntu Default Page: It works - Mozilla Firefox
Apache2 Ubuntu Default Pa
192.168.60.100
Apache2 Ubuntu Defau
ubuntu
It works!
This is the default welcome page used to test the correct operation of the
Page Info - http://192.168.60.100/
General
Media
Permissions
Security
Website Identity
Website: 192.168.60.100
Owner: This website does not supply ownership information.
Verified by: Not specified
Privacy & History
Have I visited this website prior to today? No
Is this website storing information on my computer? No
Clear Cookies and Site Data
Have I saved any passwords for this website? No
View Saved Passwords
student@serverA: ~
File Edit View Search Terminal Help
student@serverA:~$ sudo ./firewall.sh
[sudo] password for student:
Added logging
student@serverA:~$
Right Ctrl

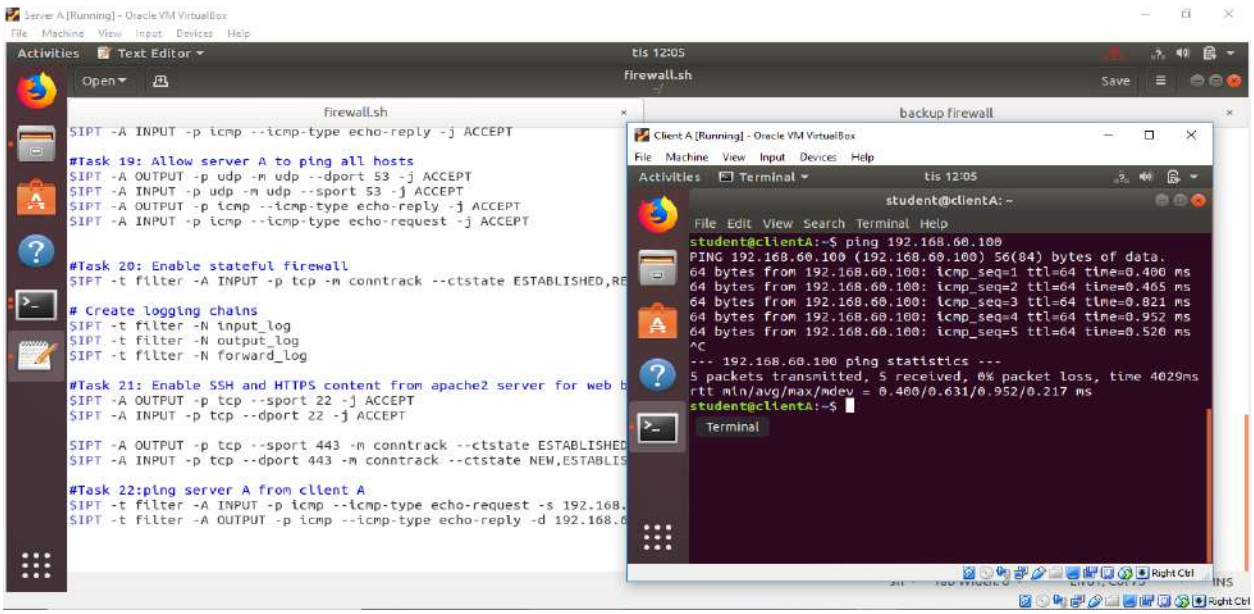
Task 22: Ping Server A from Client A

Modified my firewall script as per instruction and executed it. Commands-

$IPT -t filter -A INPUT -p icmp --icmp-type echo-request -s 192.168.60.111 -m conntrack --ctstate ESTABLISHED,RELATED,NEW -j ACCEPT

$IPT -t filter -A OUTPUT -p icmp --icmp-type echo-reply -d 192.168.60.111 -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT

After executing the firewall it's successfully done ping from client A

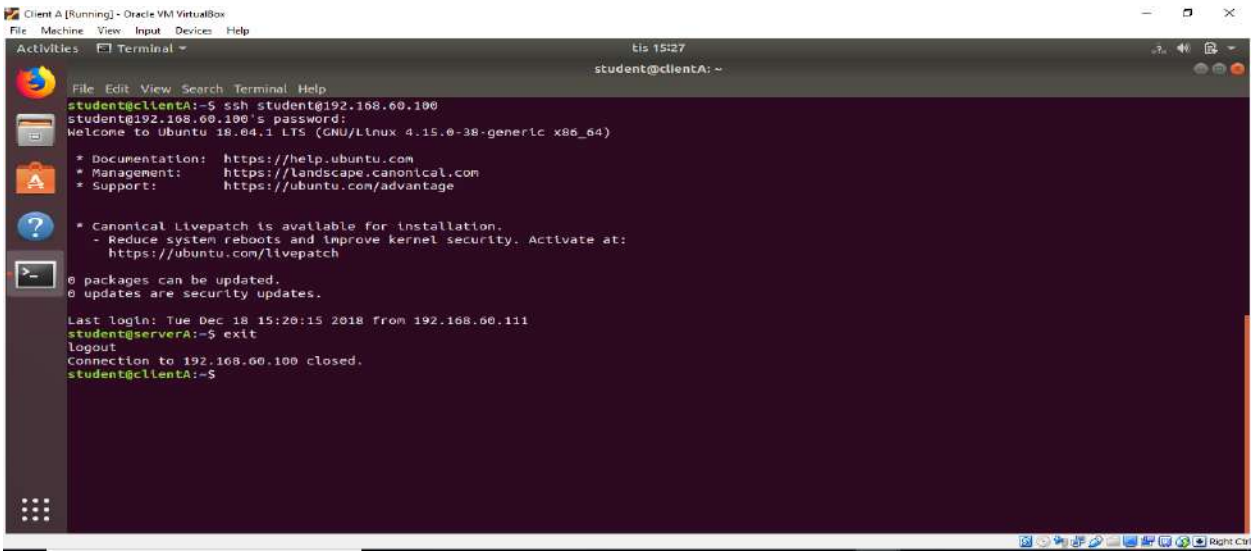


Task 23: SSH from Client A to Server A

By using this line

$IPT -A INPUT -p tcp -s 192.168.60.111 --dport 22 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT

SSH session to be established from Client A to Server A verify the password allow to access after that exit from server A.

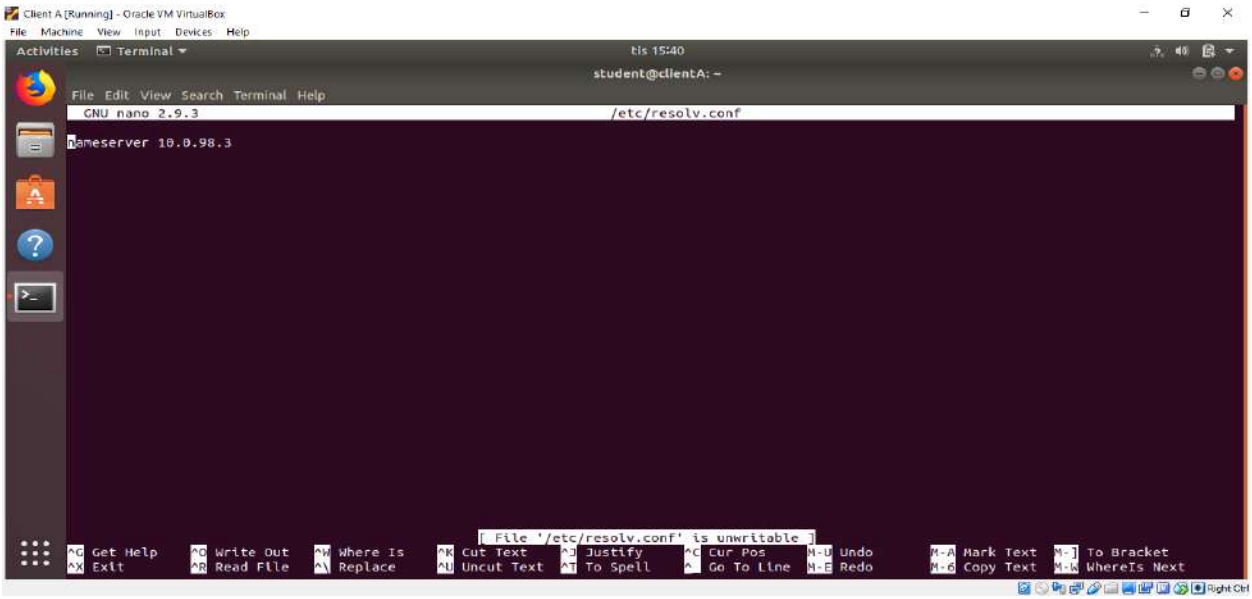


Task 24: Add gateway and DNS server to Client A

Modified the file /etc/resolv.conf on Client A and verify the 10.0.98.3 is listed as DNS server

nameserver 10.0.98.3

gateway 192.168.60.100

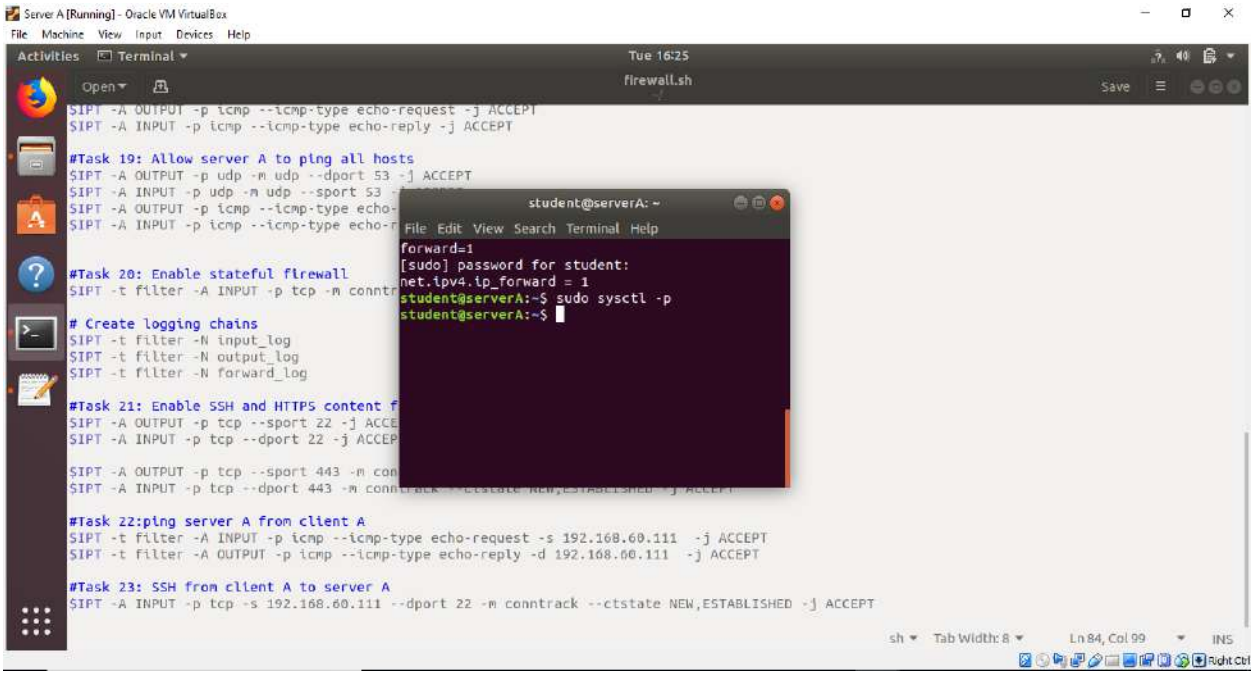


Task 25: Enable IP forwarding on Server A

For forwarding in server A executed the command in the terminal.

sudo sysctl -w net.ipv4.ip_forward=1

sudo syscltl -p

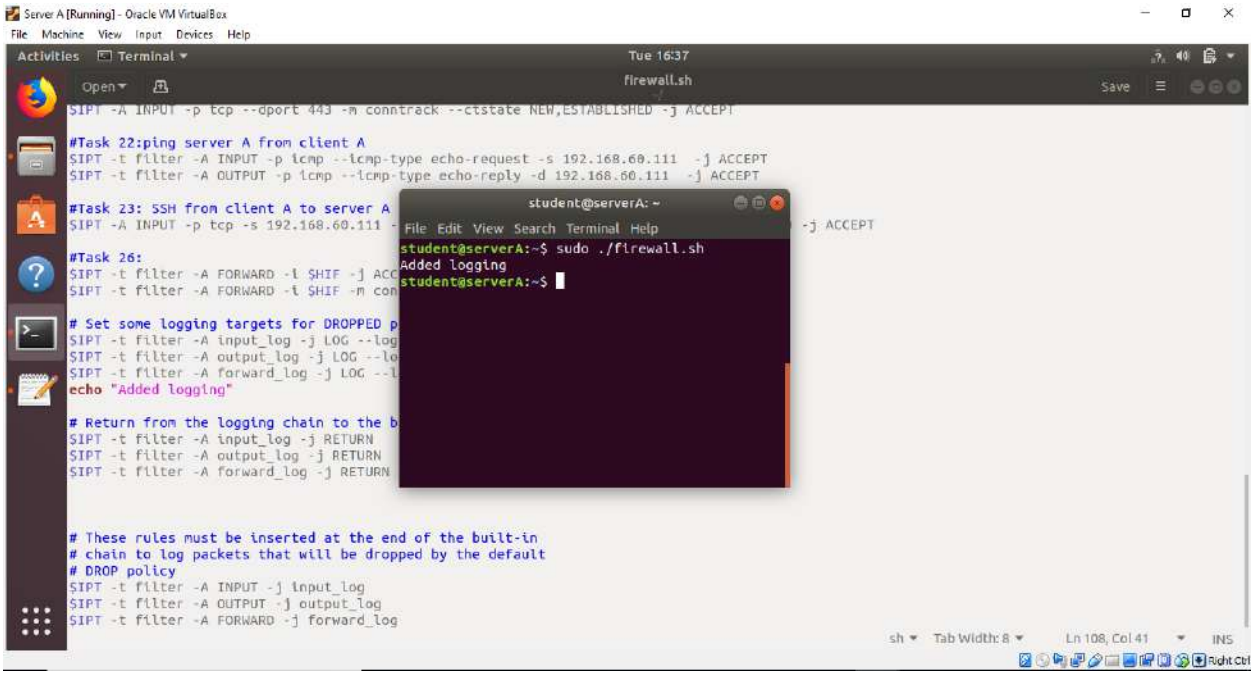


Task 26: Change iptables to forward packets

I have changed the rules for 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

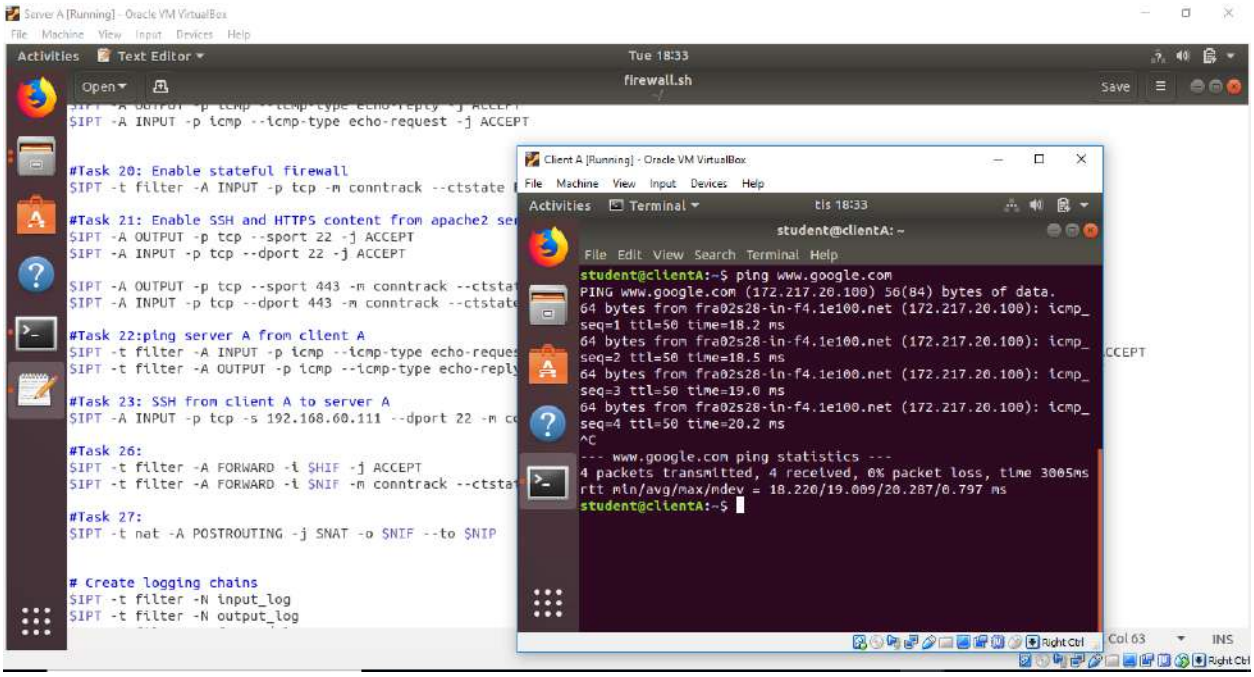


Task 27: Enable SNAT on Server A

After finished the forwarding rules then I edit my firewall.sh script

$IPT -t nat -A POSTROUTING -j SNAT -o $NIF --to $NIP

After executed the rules in server A then from client A. I can have managed to use the internet.



Reference:

- Lab 1: Linux networking and firewalls