

CS6500 - Network Security

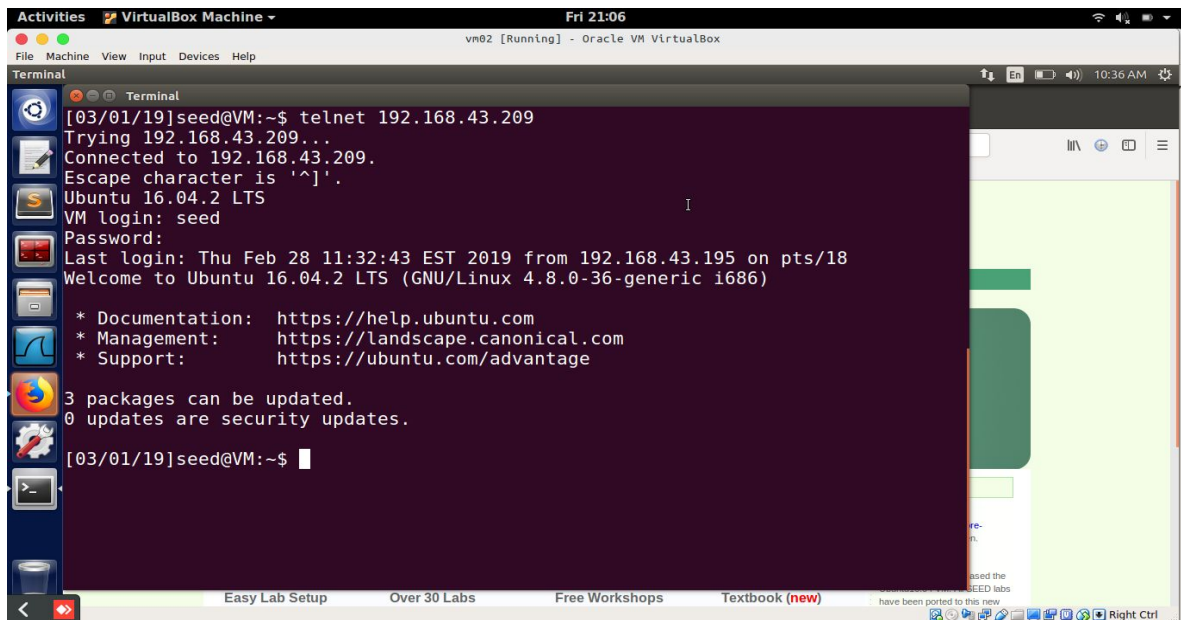
Tutorial - 3a : Report

- CS18M036 & CS18M050

Basics :

1. Implementing firewall rules using default system firewall to block incoming and outgoing telnet services :

sudo ufw deny from any to any port 23



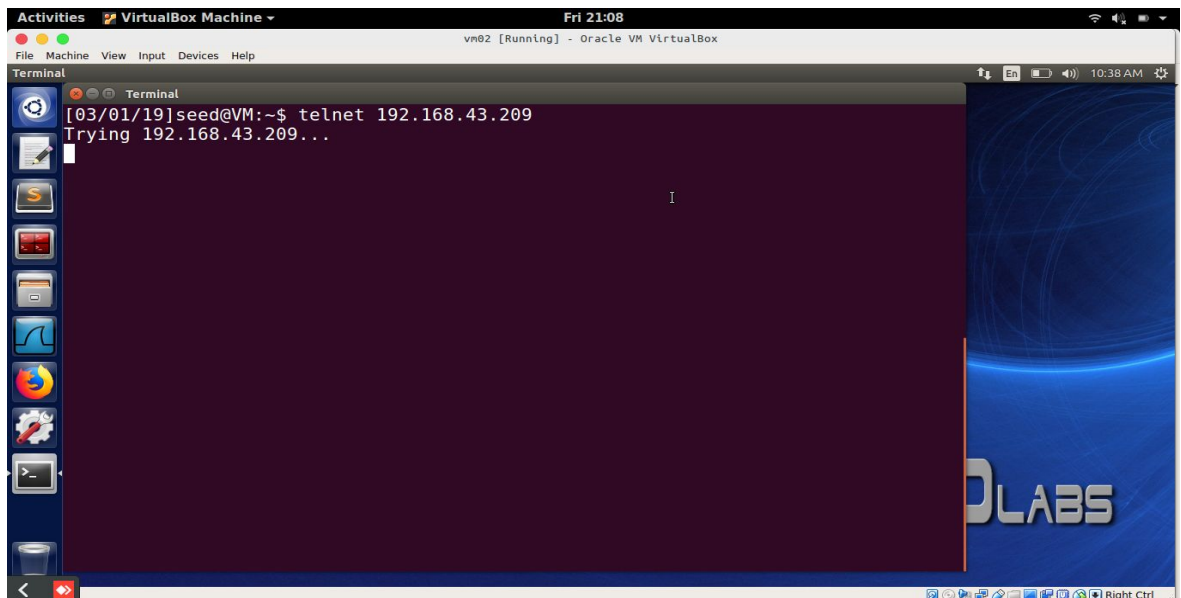
The screenshot shows a VirtualBox window titled 'vm02 [Running] - Oracle VM VirtualBox'. Inside, a terminal window is open with the following text:

```
[03/01/19]seed@VM:~$ telnet 192.168.43.209
Trying 192.168.43.209...
Connected to 192.168.43.209.
Escape character is '^['.
Ubuntu 16.04.2 LTS
VM login: seed
Password:
Last login: Thu Feb 28 11:32:43 EST 2019 from 192.168.43.195 on pts/18
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-generic i686)

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

3 packages can be updated.
0 updates are security updates.

[03/01/19]seed@VM:~$
```



The screenshot shows the same VirtualBox window, but the terminal output is different, indicating a failed connection:

```
[03/01/19]seed@VM:~$ telnet 192.168.43.209
Trying 192.168.43.209...
```

2. Implementing firewall rules using default system firewall to block browsing of facebook.com :

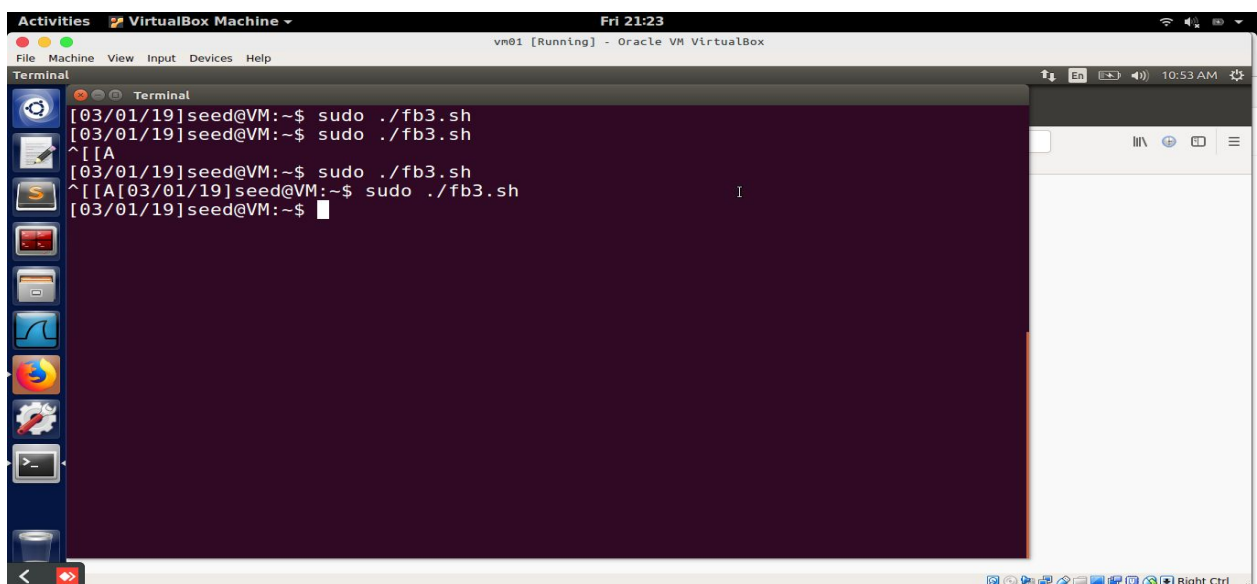
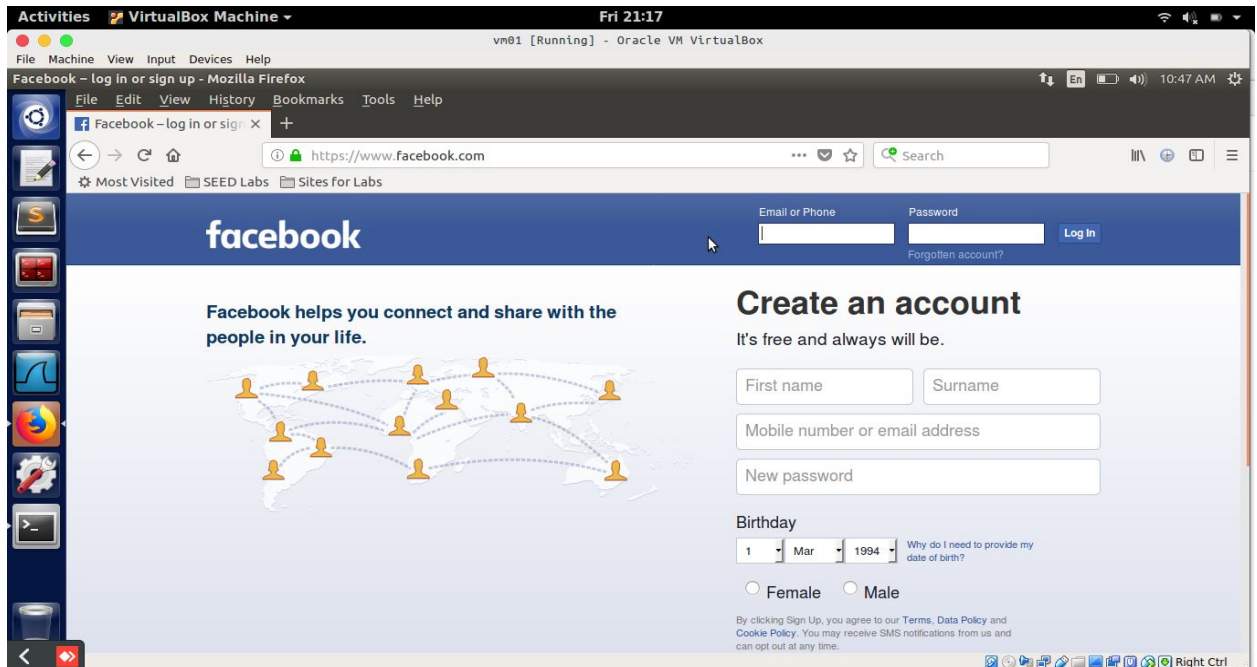
Created a shell script(fb3.sh) to block all the IP addresses generated by the facebook.com which is,

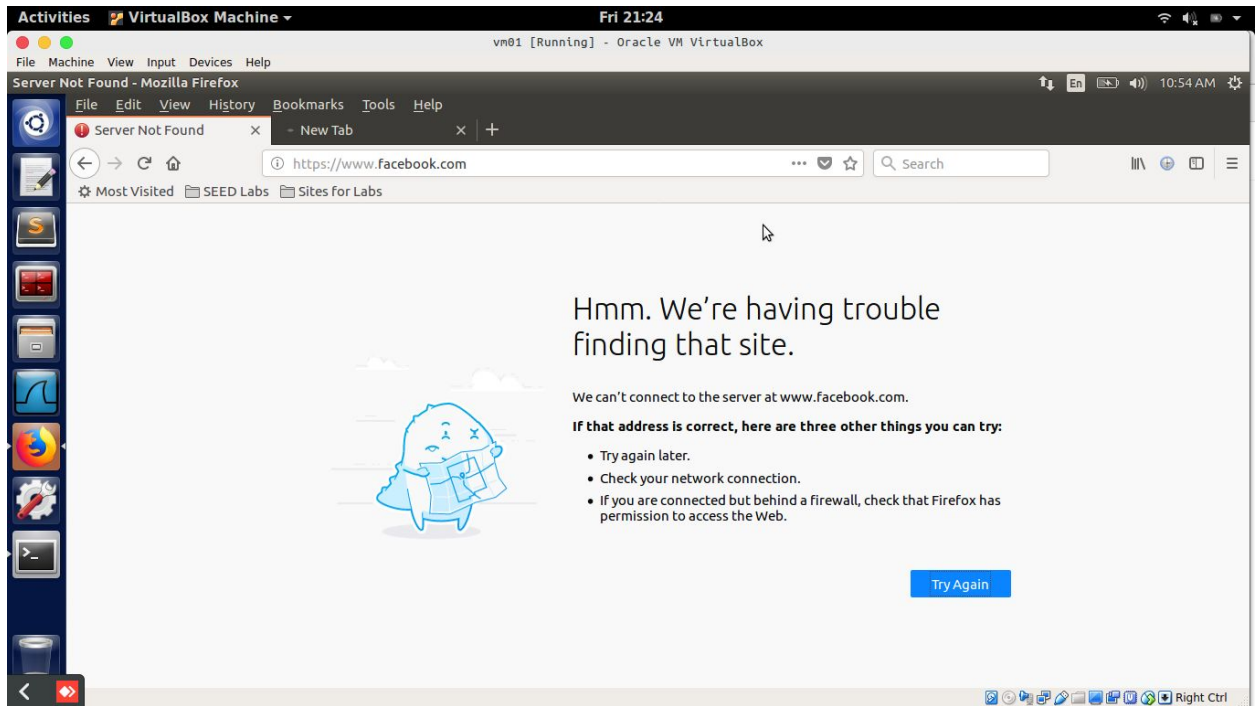
```
#!/bin/bash
```

```
for i in $(host facebook.com | grep "has address " | cut -d' ' -f4);
```

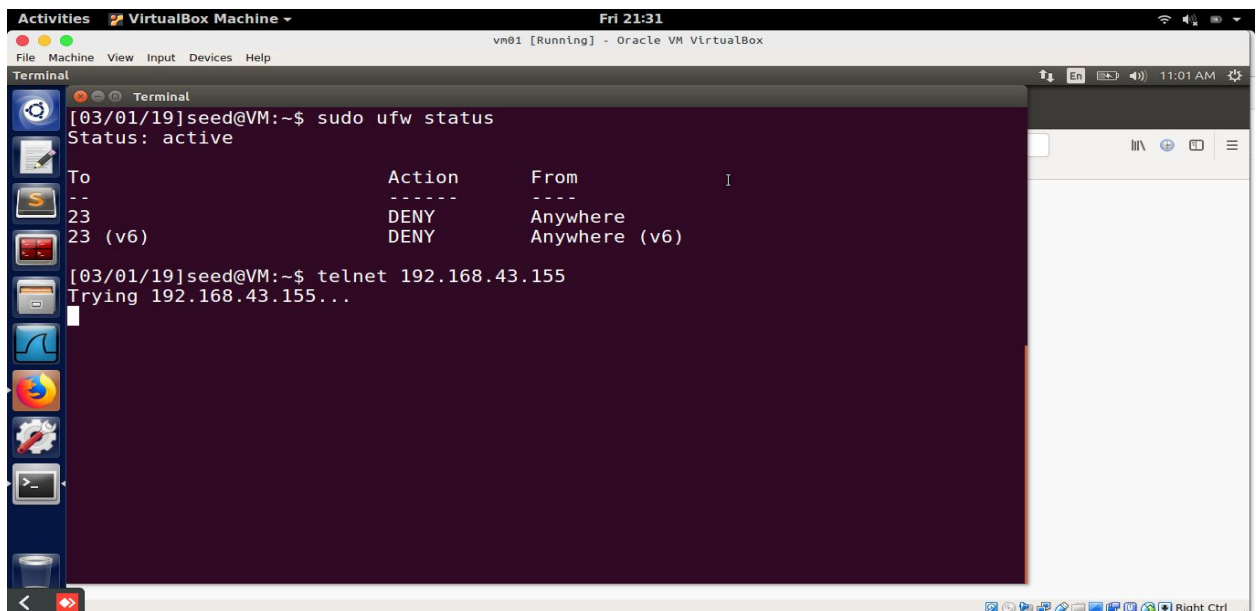
```
do iptables -A OUTPUT -p tcp -d $i --dport 443 -j REJECT
```

```
done
```



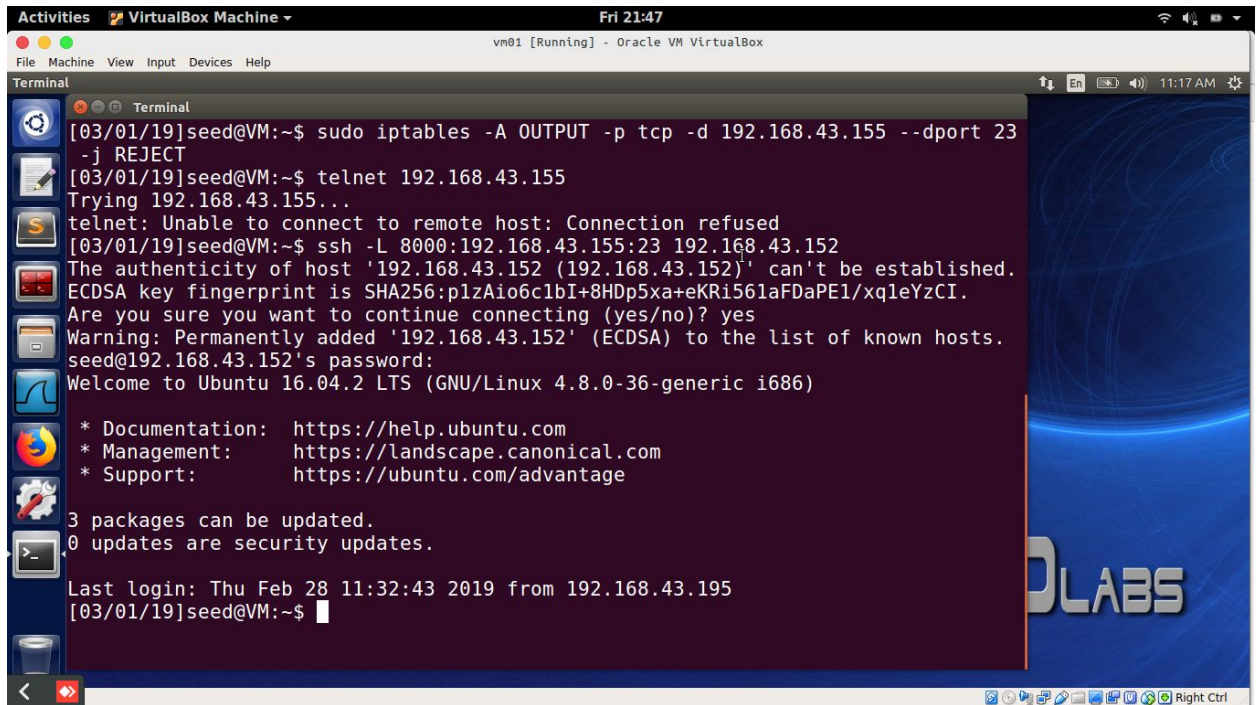


3. a) Evade the firewall to access telnet services using SSH tunneling using destination IP address :
- First block the telnet port from 192.168.43.195 machine using the command **sudo iptables -A OUTPUT -p tcp -d 192.168.43.195 --dport 23 -j REJECT**



Then we tried to telnet from the above machine to 192.168.43.155 but we couldn't succeed so now we use **SSH tunneling** technique as follow,

ssh -L 8000:192.168.43.155:23 192.168.43.152



```
Activities VirtualBox Machine Fri 21:47
vm01 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal
[03/01/19]seed@VM:~$ sudo iptables -A OUTPUT -p tcp -d 192.168.43.155 --dport 23 -j REJECT
[03/01/19]seed@VM:~$ telnet 192.168.43.155
Trying 192.168.43.155...
telnet: Unable to connect to remote host: Connection refused
[03/01/19]seed@VM:~$ ssh -L 8000:192.168.43.155:23 192.168.43.152
The authenticity of host '192.168.43.152 (192.168.43.152)' can't be established.
ECDSA key fingerprint is SHA256:plzAio6clbI+8HDp5xa+eKRi561aFDaPEl/xqleYzCI.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.43.152' (ECDSA) to the list of known hosts.
seed@192.168.43.152's password:
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-generic i686)

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

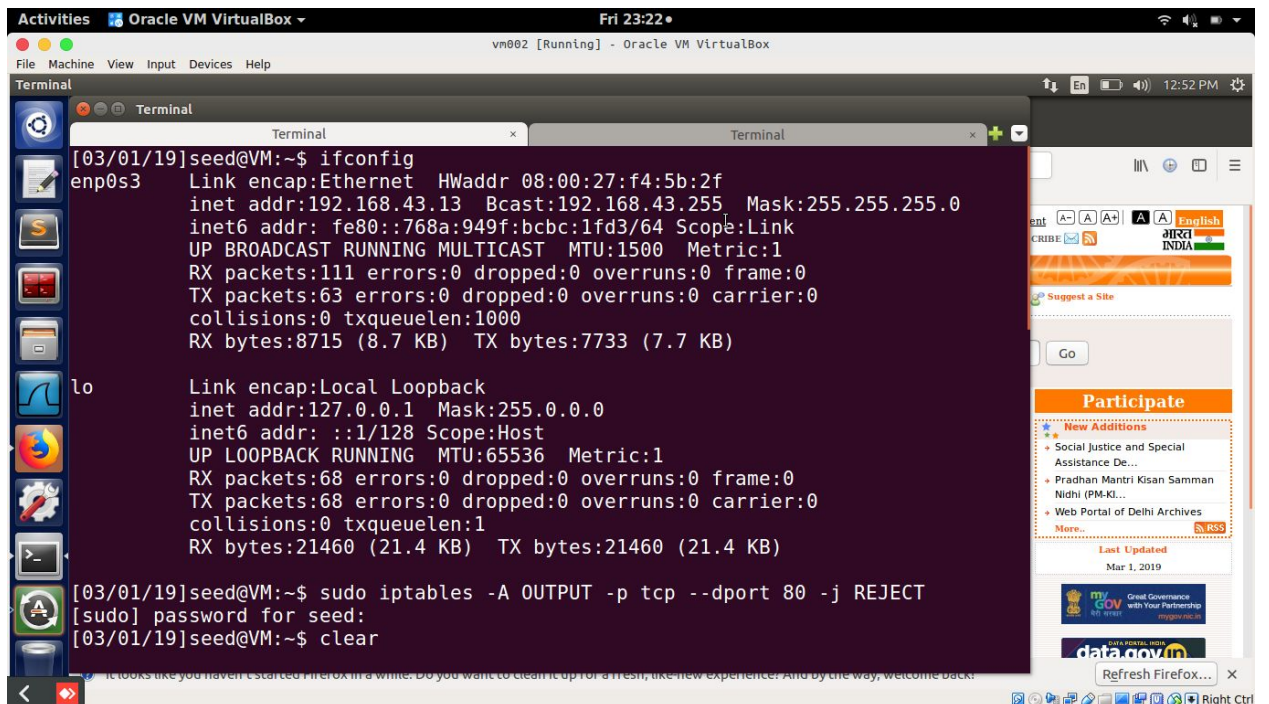
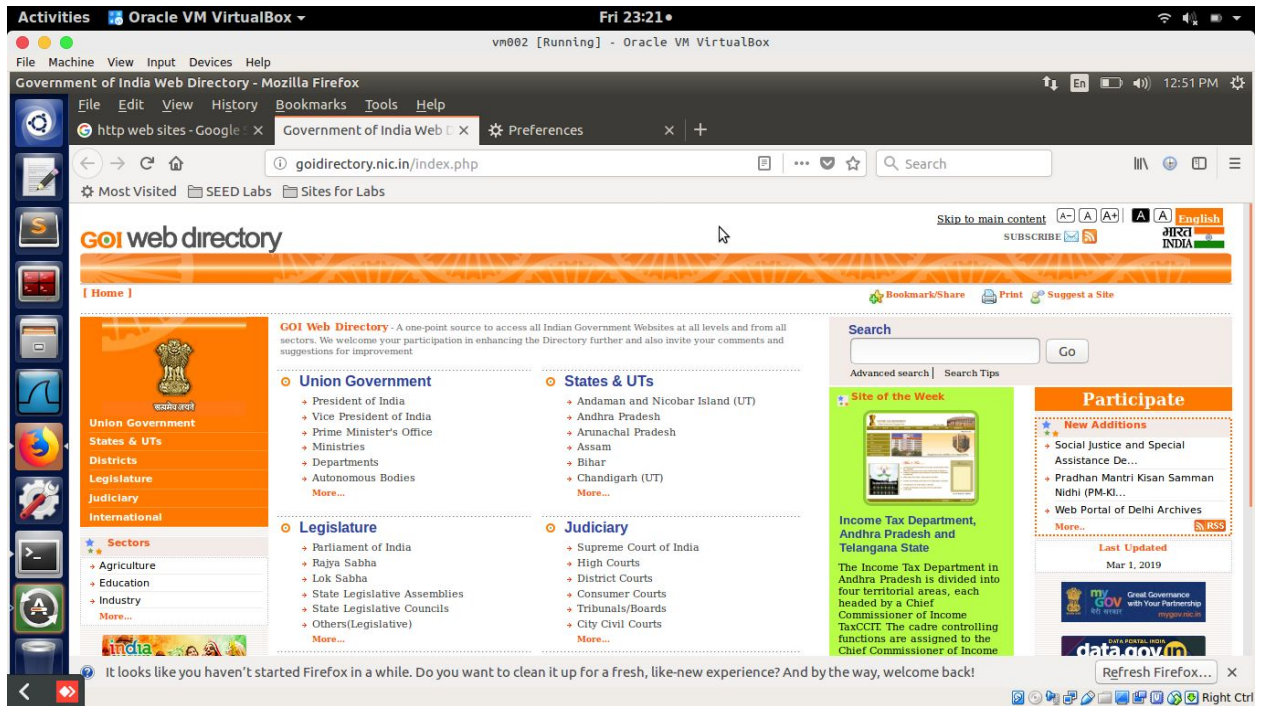
3 packages can be updated.
0 updates are security updates.

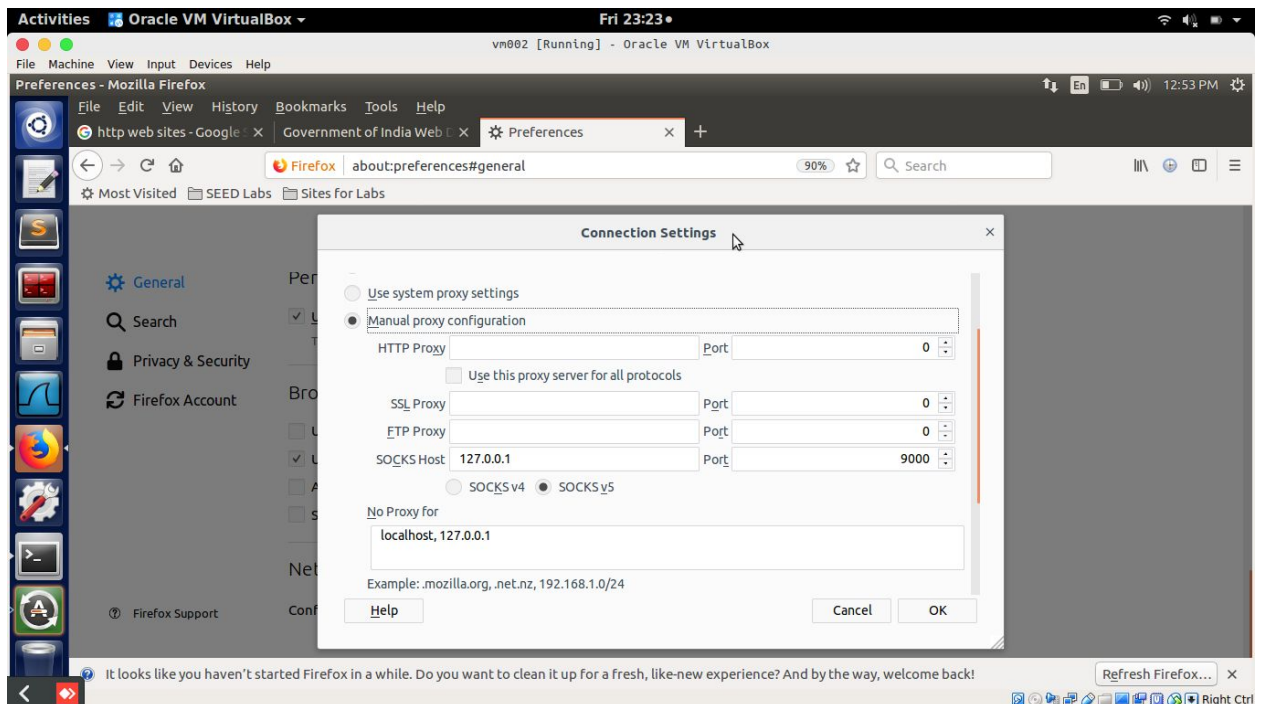
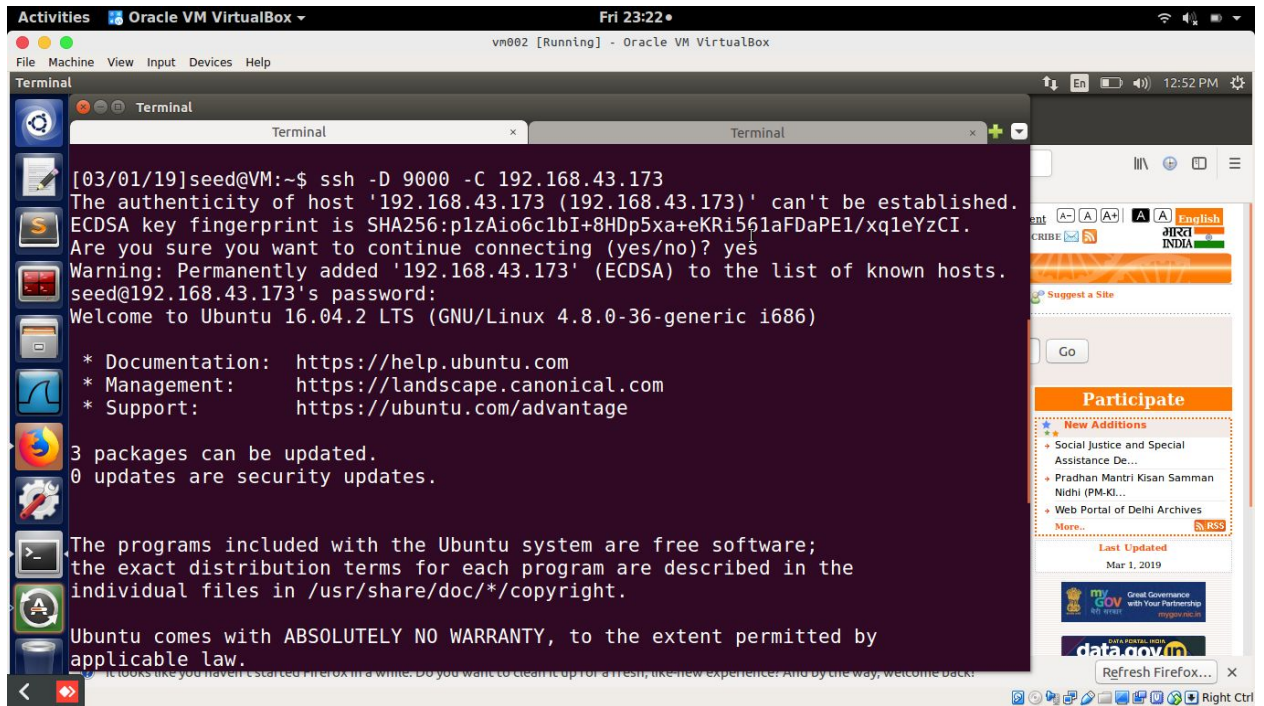
Last login: Thu Feb 28 11:32:43 2019 from 192.168.43.195
[03/01/19]seed@VM:~$
```

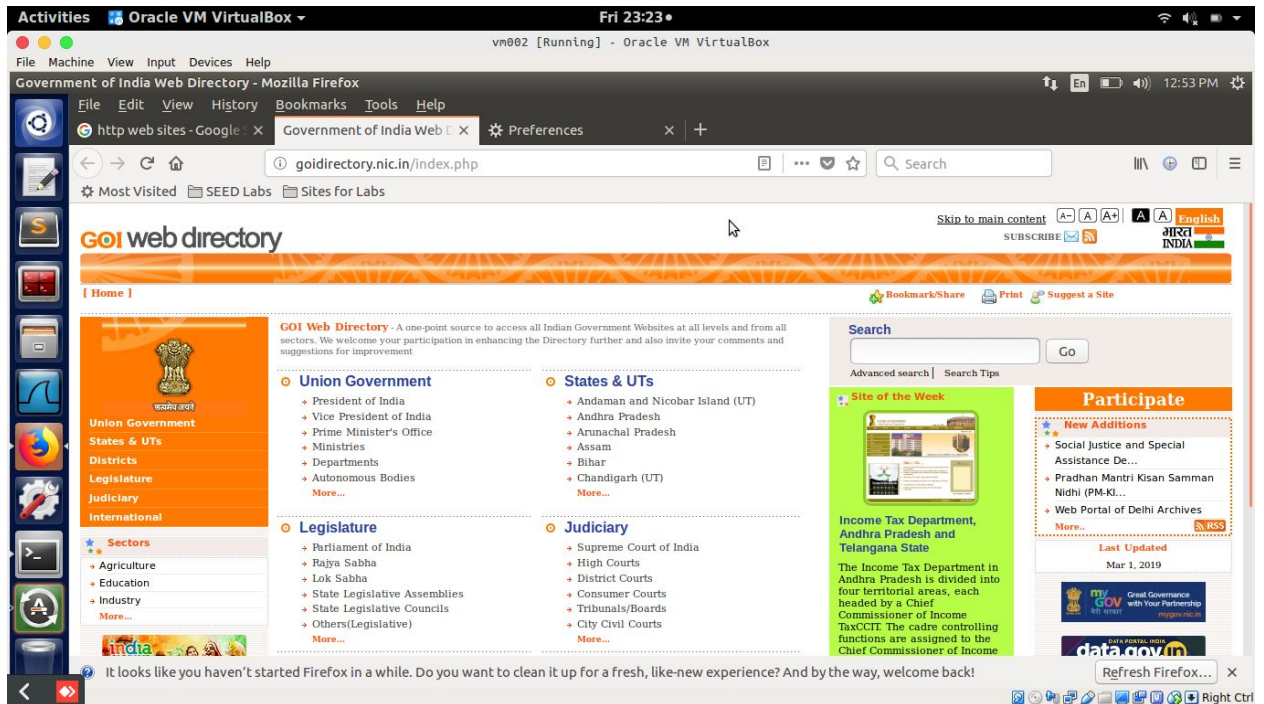
b)Evade the firewall to access http services using SSH tunneling without using destination IP address :

We first block the http service from the host machine by using the following command **sudo iptables -A OUTPUT -p tcp --dport 80 -j REJECT**

then we make **SSH tunneling** using the command **ssh -D 9000 -C 192.168.43.173** after this we make changes in **firefox network proxy setting** so that it gives http service to the clients.

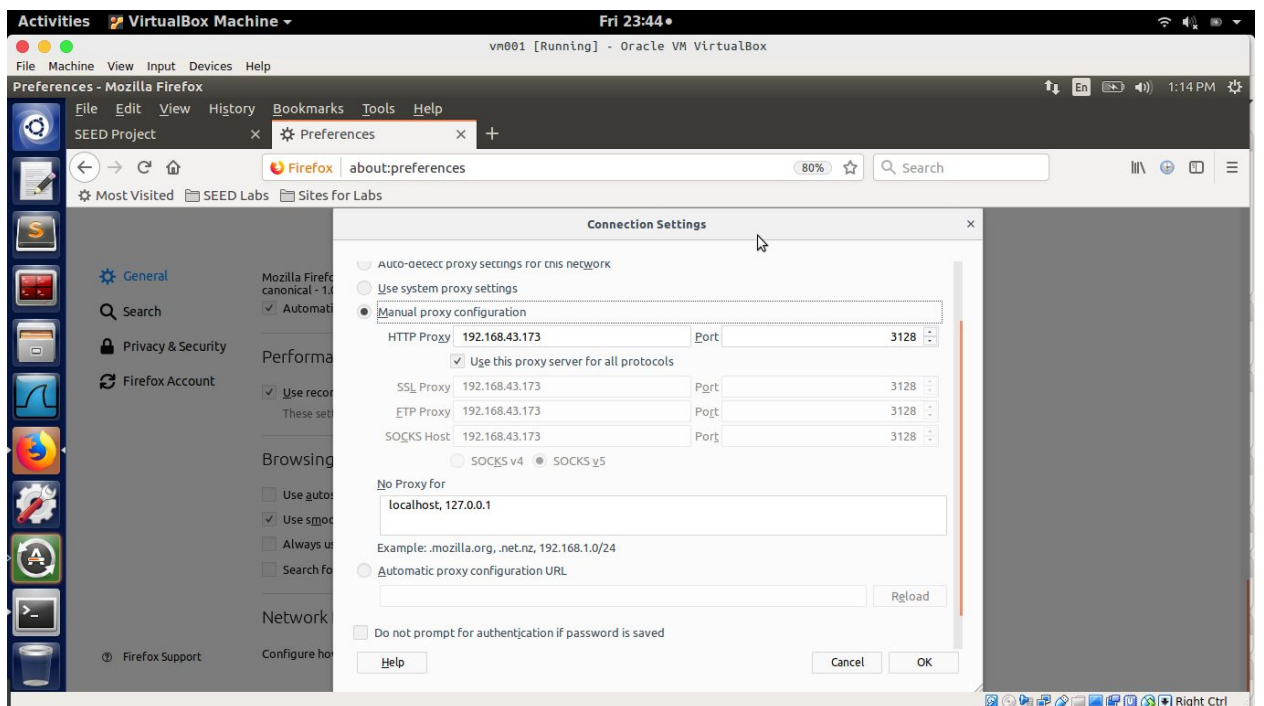
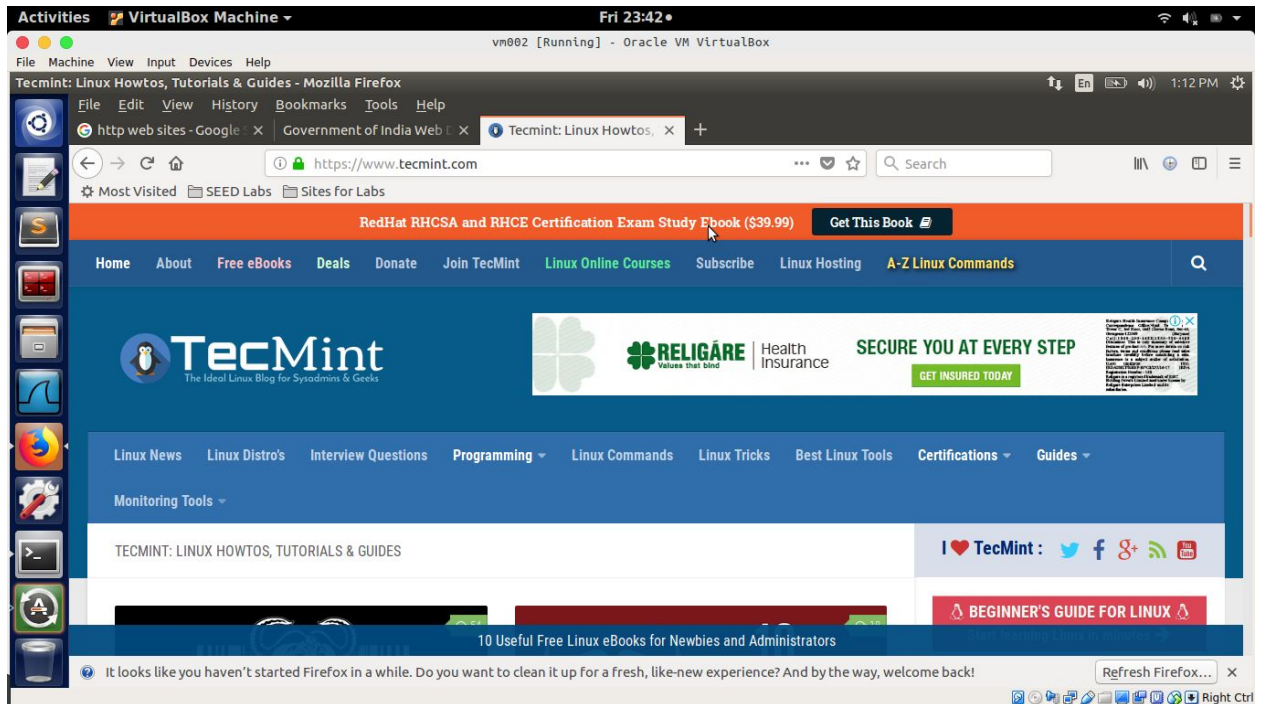






4. Implement a web proxy using squid services :

To implement web proxy using squid service we follow the following steps,
We first add ***acl localhost src 127.0.0.1/32*** and ***acl localnet src 192.168.0.0/24*** into the ***squid.conf*** file then we add ***http_access allow localhost*** and ***http_access allow localnet*** into the same file ***squid.conf*** now we are set with the configuration so now we make ***service squid restart*** and ***systemctl restart squid.service*** after this we go to firefox network proxy setting and make the following changes as shown in the below screenshots.



5. Evading firewall using squid as web proxy :

Here we follow the same thing as we did in the step number 4 only additional thing here we have to make is block **http service** from client

machine at this time there will be no http service all website will not be able to access and now set all the above stuff in server machine and now run the following command ***tail -f /var/log/squid/access.log*** and run the website again in the client machine all the http service will be available and websites will be accessible.