

Creating A Secure Network

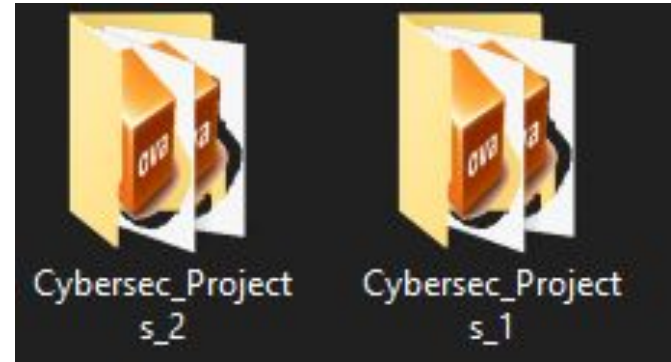
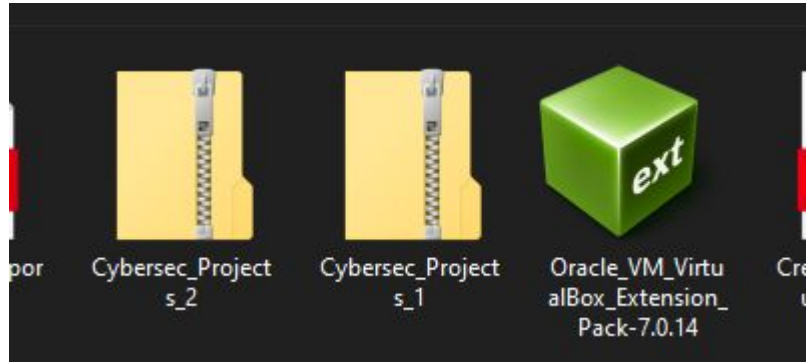
By: Nadem Sahial

Executive Summary

Greetings and welcome to our lecture on building a secure virtual network. As data is essential to success in today's changing corporate environment. We'll go into detail in this slideshow about the process of creating and setting up a safe virtual network that is customized to your company's specific requirements. Our goal has been to create an environment where your data is not only stored but also protected against emerging cyber threats, starting with strategic planning and ending with solid implementation. You will learn about every aspect of our approach as we go through the slides, showcasing our dedication to improving your digital safety.



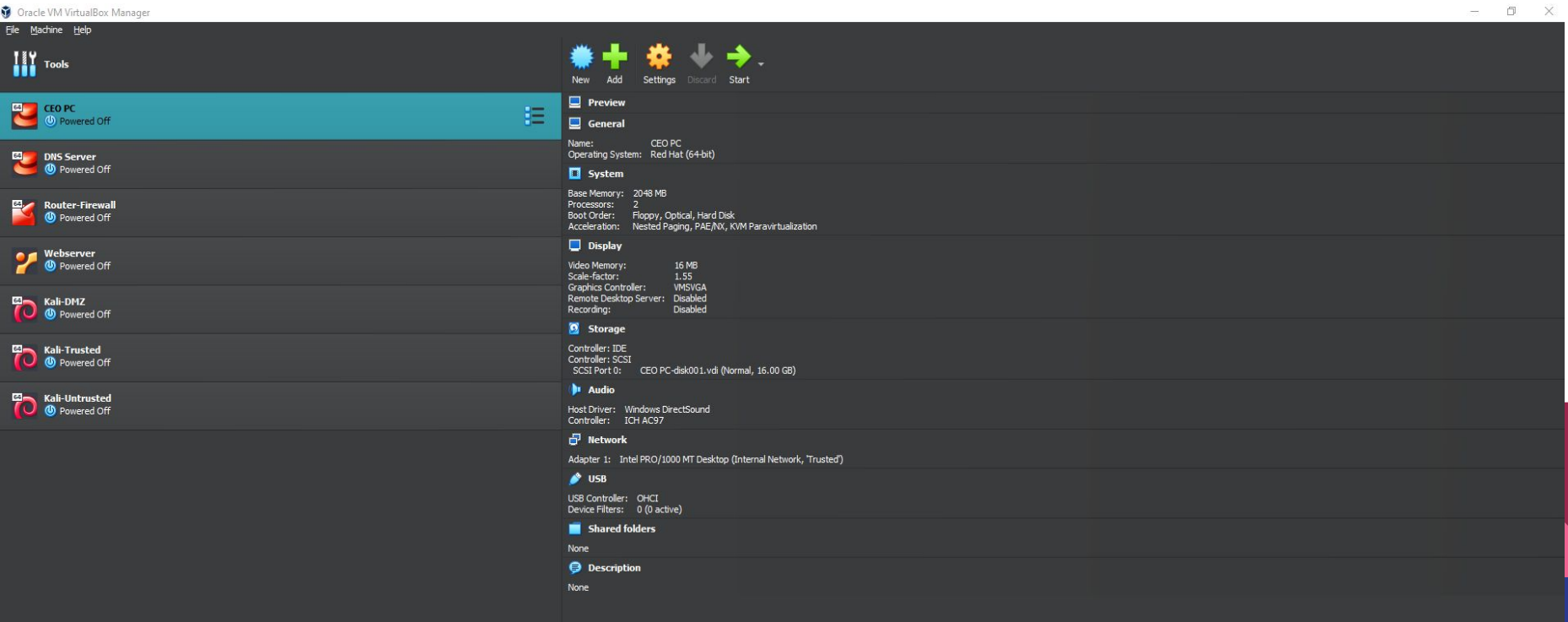
Step 1: Install VirtualBox and Extensions



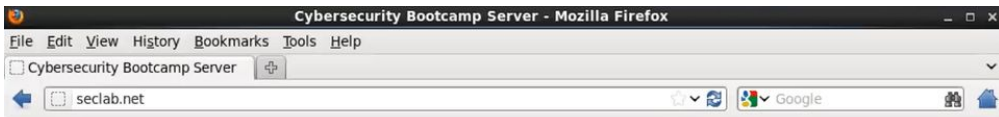
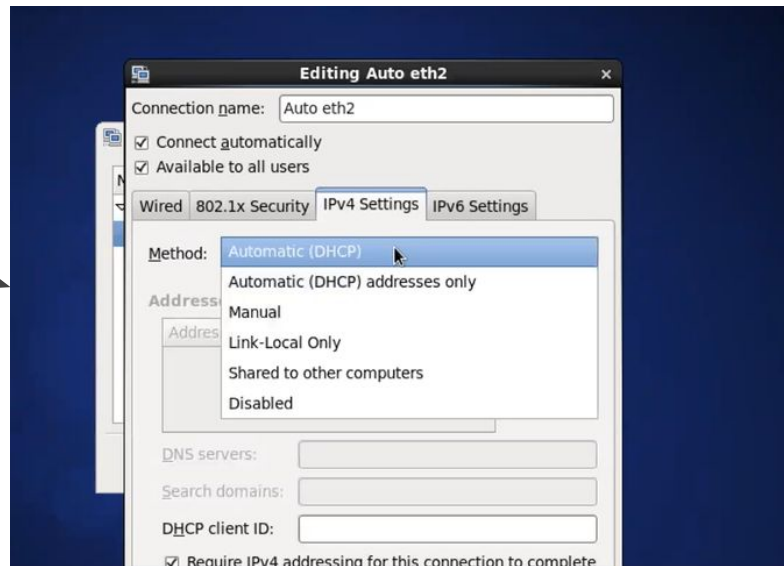
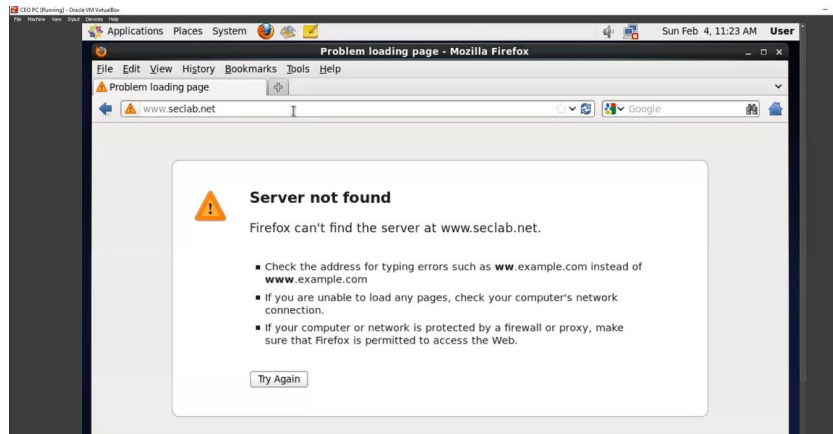
I installed Virtualbox and the extensions. I then unzipped the large sized project files.

Step 2: Install Virtual Machines

Then I went ahead and installed each of the virtual machines successfully following the instructions from the PDF “Creating the Virtual Network”.



Step 3: Using seclab.net to Troubleshoot Issues



Congratulations Cybersecurity Bootcamper!

You are viewing this page because you have correctly installed Virtualbox, a firewall, a webserver, and a computer.

But your journey has just begun, padawan.....

Continue to develop this project and prepare your presentation.

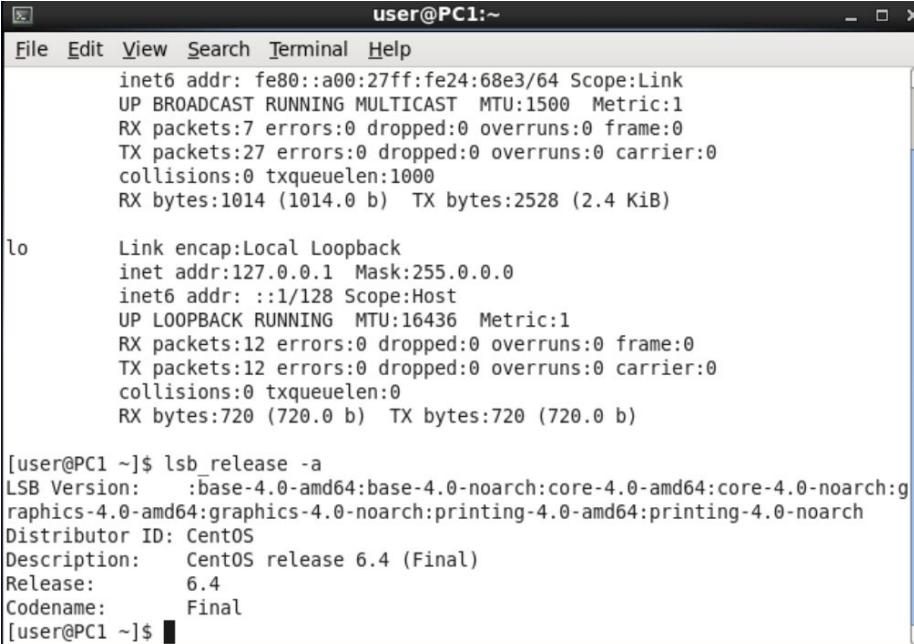
Then what I came to notice was that the reason why accessing seclab was unsuccessful was because of the DHCP Server. I set it from Manual to "Automatic DHCP" and the search was then successful.

Step 4: Discover & Document Information for the Servers

CEO PC OS Version -

OS Version was found through the
command “lsb_release -a”

Which is - CentOS release 6.4
(Final)



```
user@PC1:~  
File Edit View Search Terminal Help  
    inet6 addr: fe80::a00:27ff:fe24:68e3/64 Scope:Link  
    UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
    RX packets:7 errors:0 dropped:0 overruns:0 frame:0  
    TX packets:27 errors:0 dropped:0 overruns:0 carrier:0  
    collisions:0 txqueuelen:1000  
    RX bytes:1014 (1014.0 b)  TX bytes:2528 (2.4 KiB)  
  
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:12 errors:0 dropped:0 overruns:0 frame:0  
    TX packets:12 errors:0 dropped:0 overruns:0 carrier:0  
    collisions:0 txqueuelen:0  
    RX bytes:720 (720.0 b)  TX bytes:720 (720.0 b)  
  
[user@PC1 ~]$ lsb_release -a  
LSB Version:      :base-4.0-amd64;base-4.0-noarch:core-4.0-amd64:core-4.0-noarch:graph-  
ics-4.0-amd64:graphics-4.0-noarch:printing-4.0-amd64:printing-4.0-noarch  
Distributor ID:  CentOS  
Description:     CentOS release 6.4 (Final)  
Release:         6.4  
Codename:        Final  
[user@PC1 ~]$
```

Continue..

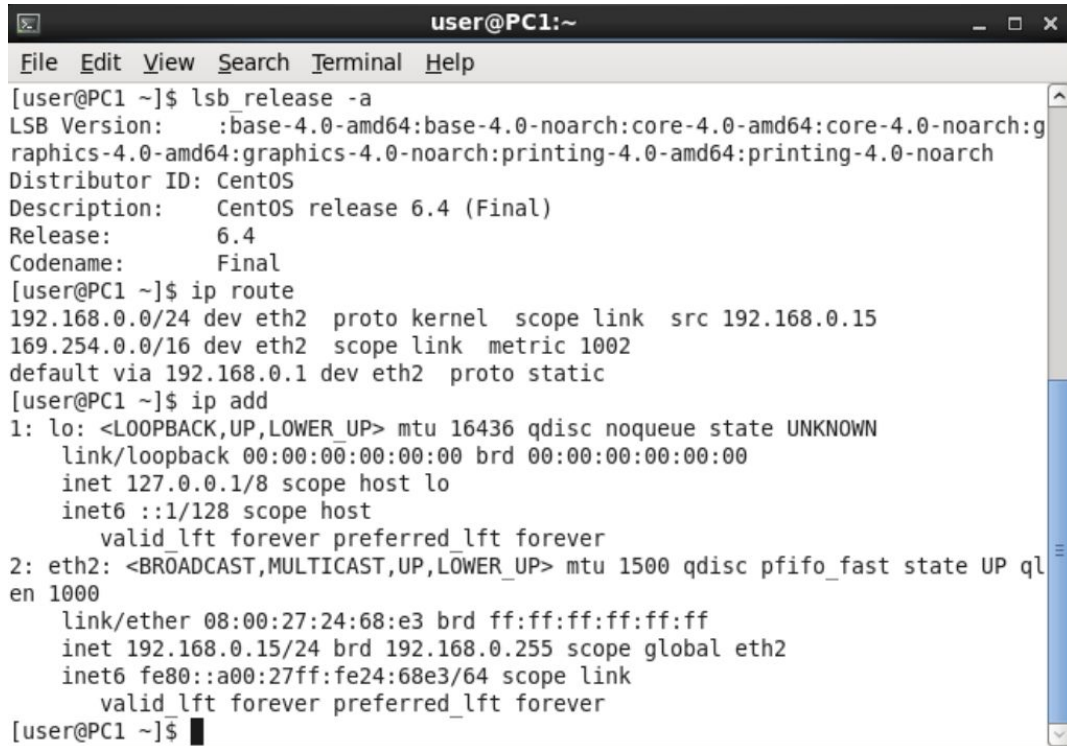
CEO PC - IP, Subnet Mask, Gateway, Server

IP/Subnet - 192.168.0.15/24

Gateway - 192.168.0.1

CEO PC Server - CentOS 6.4

This information was found through
utilizing the commands “ip route”
and “ip add”.



```
user@PC1:~  
File Edit View Search Terminal Help  
[user@PC1 ~]$ lsb_release -a  
LSB Version:      :base-4.0-amd64:base-4.0-noarch:core-4.0-amd64:core-4.0-noarch:graph  
  ics-4.0-amd64:graphics-4.0-noarch:printing-4.0-amd64:printing-4.0-noarch  
Distributor ID: CentOS  
Description:     CentOS release 6.4 (Final)  
Release:         6.4  
Codename:        Final  
[user@PC1 ~]$ ip route  
192.168.0.0/24 dev eth2  proto kernel  scope link    src 192.168.0.15  
169.254.0.0/16 dev eth2  scope link    metric 1002  
default via 192.168.0.1 dev eth2  proto static  
[user@PC1 ~]$ ip add  
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue state UNKNOWN  
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00  
    inet 127.0.0.1/8 scope host lo  
        inet6 ::1/128 scope host  
            valid_lft forever preferred_lft forever  
2: eth2: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP ql  
  en 1000  
    link/ether 08:00:27:24:68:e3 brd ff:ff:ff:ff:ff:ff  
    inet 192.168.0.15/24 brd 192.168.0.255 scope global eth2  
        inet6 fe80::a00:27ff:fe24:68e3/64 scope link  
            valid_lft forever preferred_lft forever  
[user@PC1 ~]$
```

Web Server - OS Version

OS Version was found

through the command

“lsb_release -a”

Which is - Ubuntu 8.04

```
webserver login: admin
Password:

Login incorrect
webserver login: admin
Password:
Last login: Thu Oct 27 16:10:42 EDT 2022 on tty1
Linux webserver 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 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/
admin@webserver:~$ lsb_release -a
No LSB modules are available.
Distributor ID: Ubuntu
Description:    Ubuntu 8.04
Release:        8.04
Codename:       hardy
admin@webserver:~$ _
```


Web Server - IP, Subnet Mask, Gateway, Server

IP/Subnet - 10.200.0.12/29

Gateway - 10.200.0.9

Web Server - Ubuntu 8.04

This information was found
through utilizing the commands
“ip route” and “ip add”.

```
applicable law.  
  
To access official Ubuntu documentation, please visit:  
http://help.ubuntu.com/  
admin@webserver:~$ lsb_release -a  
No LSB modules are available.  
Distributor ID: Ubuntu  
Description:    Ubuntu 8.04  
Release:        8.04  
Codename:       hardy  
admin@webserver:~$ ip route  
10.200.0.8/29 dev eth0 proto kernel scope link src 10.200.0.12  
default via 10.200.0.9 dev eth0 metric 100  
admin@webserver:~$ ip add  
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue  
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00  
    inet 127.0.0.1/8 scope host lo  
    inet6 ::1/128 scope host  
        valid_lft forever preferred_lft forever  
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000  
    link/ether 08:00:27:90:2f:9a brd ff:ff:ff:ff:ff:ff  
    inet 10.200.0.12/29 brd 10.200.0.15 scope global eth0  
    inet6 fe80::a00:27ff:fe90:2f9a/64 scope link  
        valid_lft forever preferred_lft forever  
admin@webserver:~$
```

DNS Server - OS Version

OS Version was found
through the command “cat
/etc/redhat-release”.

Which is - CentOS release
6.4

```
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo
inet6 ::1/128 scope host
    valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP ql
en 1000
    link/ether 00:50:56:00:11:01 brd ff:ff:ff:ff:ff:ff
    inet 10.200.0.11/29 brd 10.200.0.15 scope global eth0
    inet6 fe80::250:56ff:fe00:1101/64 scope link
        valid_lft forever preferred_lft forever
[root@localhost ~]# lsb_release -a
-bash: lsb_release: command not found
[root@localhost ~]# lsb release -a
-bash: lsb: command not found
[root@localhost ~]# os version
-bash: os: command not found
[root@localhost ~]# lsb_release
-bash: lsb_release: command not found
[root@localhost ~]# cat /etc/os-release
cat: /etc/os-release: No such file or directory
[root@localhost ~]# hostnamectl
-bash: hostnamectl: command not found
[root@localhost ~]# cat /etc/redhat-release
CentOS release 6.4 (Final)
[root@localhost ~]# _
```

DNS Server - IP, Subnet Mask, Gateway, Server

IP/Subnet - 10.200.0.11/29

Gateway - 10.200.0.9

DNS Server - CentOS 6.4

This information was found through utilizing the commands “ip route” and “ip add”.

```
-bash: .OSVersion: command not found
[root@localhost ~]# uname-a
-bash: uname-a: command not found
[root@localhost ~]# uname -a
Linux localhost.localdomain 2.6.32-358.el6.x86_64 #1 SMP Fri Feb 22 00:31:26 UTC
2013 x86_64 x86_64 x86_64 GNU/Linux
[root@localhost ~]# cat /etc/lsb-release
cat: /etc/lsb-release: No such file or directory
[root@localhost ~]# ip route
10.200.0.8/29 dev eth0 proto kernel scope link src 10.200.0.11
169.254.0.0/16 dev eth0 scope link metric 1002
default via 10.200.0.9 dev eth0
[root@localhost ~]# ip add
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue state UNKNOWN
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP ql
en 1000
    link/ether 00:50:56:00:11:01 brd ff:ff:ff:ff:ff:ff
    inet 10.200.0.11/29 brd 10.200.0.15 scope global eth0
    inet6 fe80::250:56ff:fe00:1101/64 scope link
        valid_lft forever preferred_lft forever
[root@localhost ~]# S_
```

Step 5: Use FTP to Download the “Social-Media-Security-Policy”

```
Password:
Login incorrect
webserver login:
Password:
Login incorrect
webserver login: root
Password:
Last login: Sun Feb  4 22:08:43 EST 2024 from :0.0 on pts/0
Linux webserver 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 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/
You have new mail.
root@webserver:~# find / -name Social-Media-Security-Policy
/home/jasper/Social-Media-Security-Policy
root@webserver:~#
```

I located the policy in the Web Server then headed to the CEO PC and I connected the FTP, logged in, then was able to locate and transfer the file successfully.

```
user@PC1:~
File Edit View Search Terminal Help
?Invalid command
ftp> quit
221 Goodbye.
[user@PC1 ~]$ ftp 10.200.0.12
Connected to 10.200.0.12 (10.200.0.12).
220 (vsFTPd 2.3.4)
Name (10.200.0.12:user): jasper
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> cd /home
250 Directory successfully changed.
ftp> cd jasper
250 Directory successfully changed.
ftp> get Social-Media-Security-Policy
local: Social-Media-Security-Policy remote: Social-Media-Security-Policy
227 Entering Passive Mode (10,200,0,12,140,187).
150 Opening BINARY mode data connection for Social-Media-Security-Policy (1524 bytes).
226 Transfer complete.
1524 bytes received in 2.6e-05 secs (58615.38 Kbytes/sec)
ftp>
```

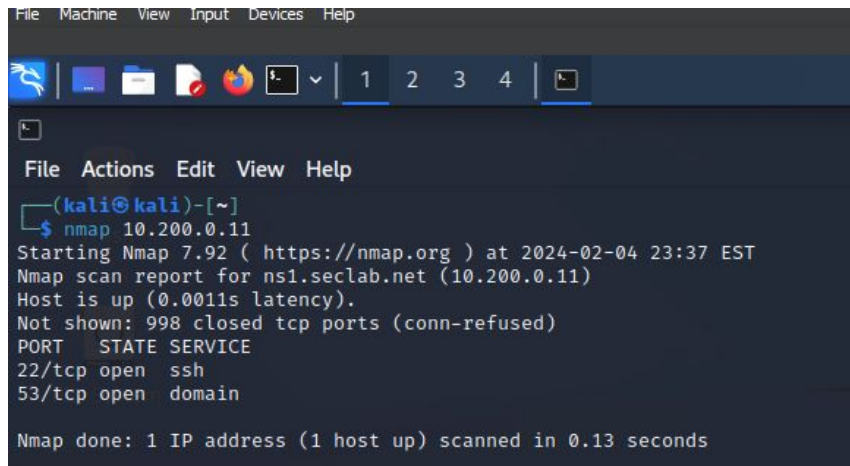
Step 6: Create a New User Account on the Web Server

I created an account
on the Web Server
named “orange2”
and signed in also.

```
adduser: Please enter a username matching the regular expression configured
via the NAME_REGEX[_SYSTEM] configuration variable. Use the '--force-badname'
option to relax this check or reconfigure NAME_REGEX or NAME_REGEX_SYSTEM.
root@webserver:~# Orange2
-bash: Orange2: command not found
root@webserver:~# sudo adduser orange2
Adding user `orange2' ...
Adding new group `orange2' (1005) ...
Adding new user `orange2' (1005) with group `orange2' ...
Creating home directory `/home/orange2' ...
Copying files from `/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for orange2
Enter the new value, or press ENTER for the default
    Full Name []: Orange Sahial
    Room Number []:
    Work Phone []:
    Home Phone []:
    Other []:
Is the information correct? [y/N] y
root@webserver:~# su - orange2
orange2@webserver:~$
```

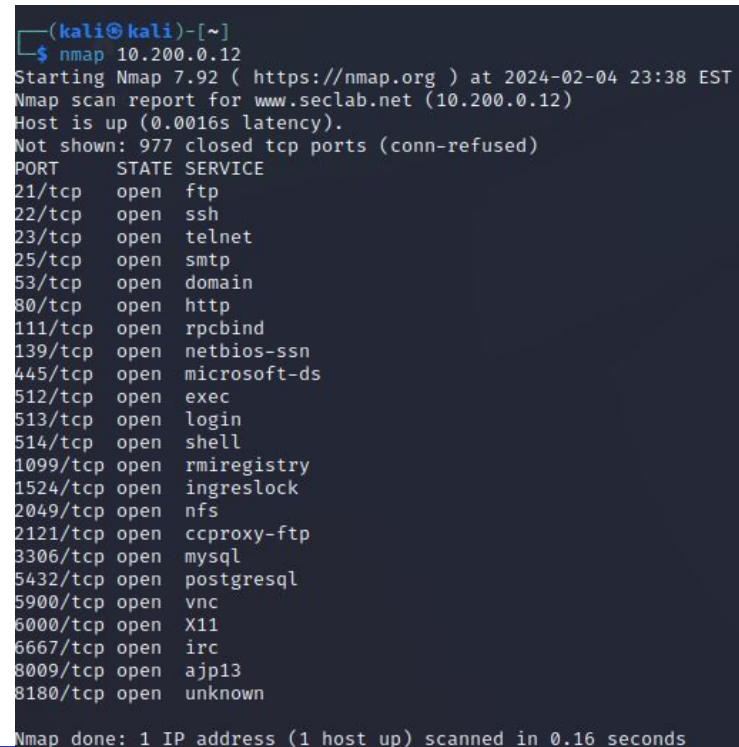
Step 7: Perform Port Scans Using NMAP

- Found 2 open ports for the IP 10.200.0.11
- Found 23 open ports for the IP 10.200.0.12



```
(kali@kali)-[~]
$ nmap 10.200.0.11
Starting Nmap 7.92 ( https://nmap.org ) at 2024-02-04 23:37 EST
Nmap scan report for ns1.seclab.net (10.200.0.11)
Host is up (0.0011s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh
53/tcp    open  domain

Nmap done: 1 IP address (1 host up) scanned in 0.13 seconds
```



```
(kali@kali)-[~]
$ nmap 10.200.0.12
Starting Nmap 7.92 ( https://nmap.org ) at 2024-02-04 23:38 EST
Nmap scan report for www.seclab.net (10.200.0.12)
Host is up (0.0016s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown

Nmap done: 1 IP address (1 host up) scanned in 0.16 seconds
```

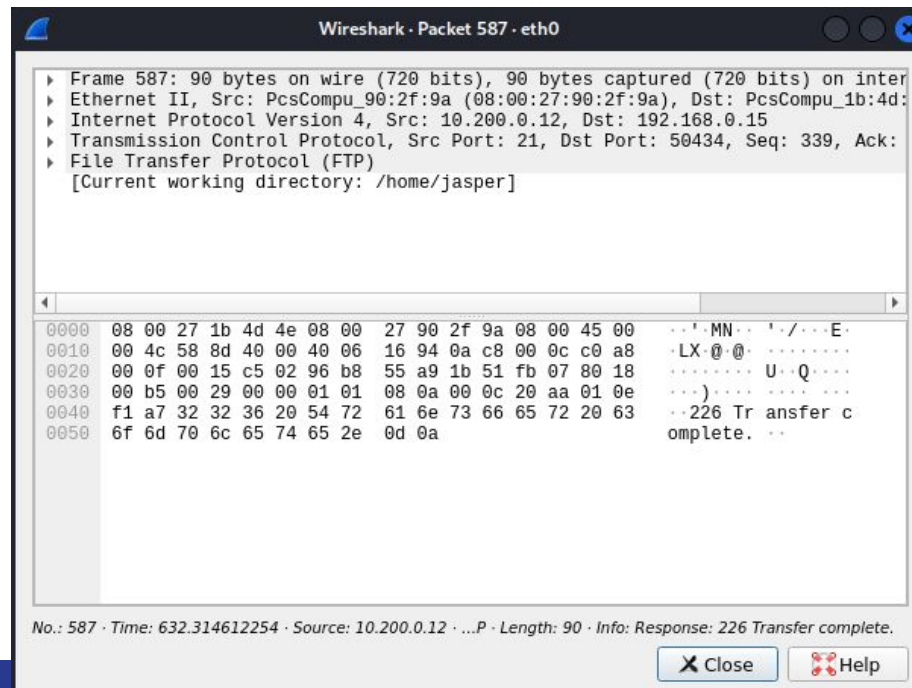
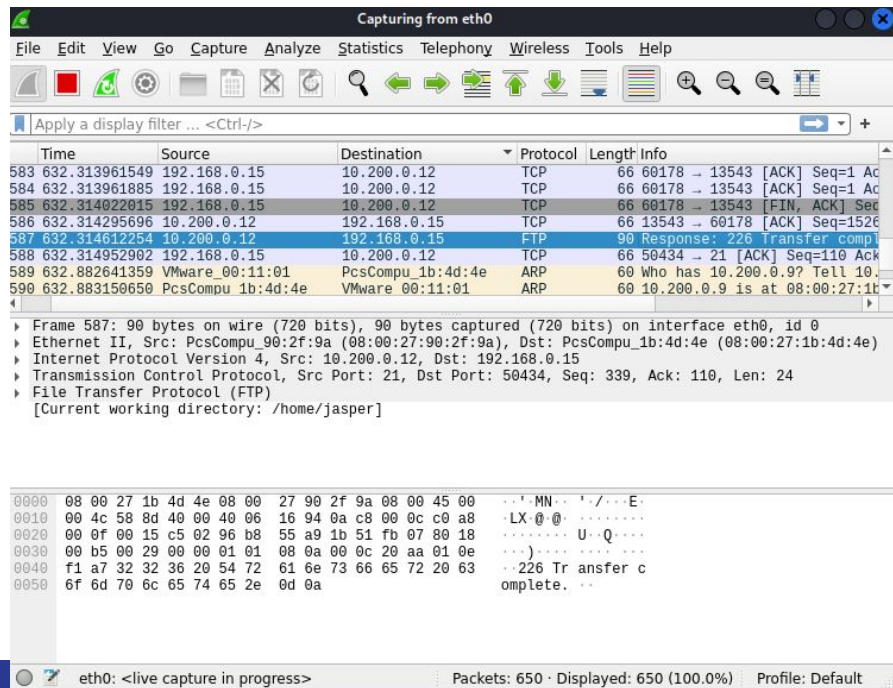
Step 8: Verify the Trusted Network is Protected From the Untrusted Network

I was able to ping from my untrusted network and transmit 4 packets with 100% packet loss which means the trusted network is successfully protected.

```
(kali㉿kali)-[~]  
$ ping -c 4 192.168.0.15  
PING 192.168.0.15 (192.168.0.15) 56(84) bytes of data.  
From 172.30.0.10 icmp_seq=1 Destination Host Unreachable  
From 172.30.0.10 icmp_seq=2 Destination Host Unreachable  
From 172.30.0.10 icmp_seq=3 Destination Host Unreachable  
From 172.30.0.10 icmp_seq=4 Destination Host Unreachable  
  
— 192.168.0.15 ping statistics —  
4 packets transmitted, 0 received, +4 errors, 100% packet loss, time 3054ms  
pipe 4
```


Step 9: Use Wireshark to Capture FTP File Transfer

I used wireshark to show the FTP file transfer with the IP 192.168.0.15.



Network Problems That Were Identified & How I Solved Them

I couldn't connect to the network and later came to find out the DHCP settings were set to manual. When I switched it to automatic DHCP settings, network was back to working normal.



Recommendations For Improvements

- Keep a lookout at all times for anything fishy in the network
- Build firewalls
- Have authentication
- Use VPN if needed
- Make sure software gets updated often because the latest updates most of the time have security patches

