Project 1

Creating a Secure Network

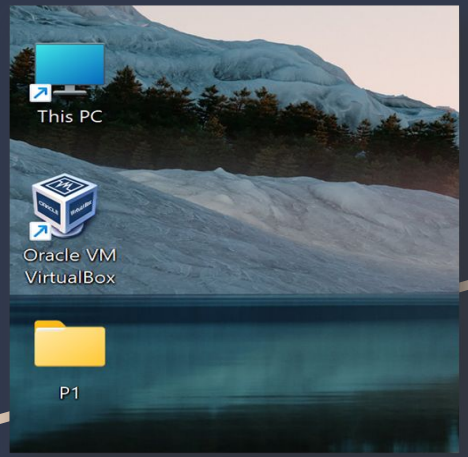
Summary

- **Install VirtualBox and Extensions**
  - Download VirtualBox
  - Install Extension Pack
- **Set Up Virtual Machines**
  - Import Virtual Machines
- **Access www.seclab.net from CEO PC**
  - Browser Access
- **Document Network Information**
- **FTP Download**
- **Create a New User Account on Web server**
- **Port Scanning with Nmap**
- **Network Security Verification**
- **Capture FTP Traffic with Wireshark**

- **Virtual Machine Deployment and Configuration**
  Installed and configured VirtualBox and necessary extensions. Deployed virtual machines: Router-FW, DNS Server, Web Server, CEO PC, and three Kali Linux machines.
- **Network Troubleshooting**
  For the CEO PC ensuring proper and correct configuration of the IP address and network integration without altering the existing network setup.
- **System Information Discovery**
  Documenting system information for the CEO PC, Web Server, and DNS Server, including OS versions, IP addresses, subnet masks, default gateway addresses.
- **Secure File Transfer**
  Successfully transferred the “Social-Media-Security-Policy” document from the Web Server to the CEO PC using FTP.
- **User Account Management**
  Created a new user account on the Web Server
- **Security Assessments**
  Using Nmap scans open ports on both the DNS Server and Web Server
- **Network Security Verification**
  Verified the segmentation and protection of the Trusted network from the Untrusted network
- **Traffic Monitoring**
  Utilized Wireshark on Kali Linux to capture FTP file transfer traffic between the CEO PC and Web Server.
- **Policy Documentation**
  Documented the “Social-Media-Security-Policy,” feature key areas such as access management, privacy provisions, and security monitoring.

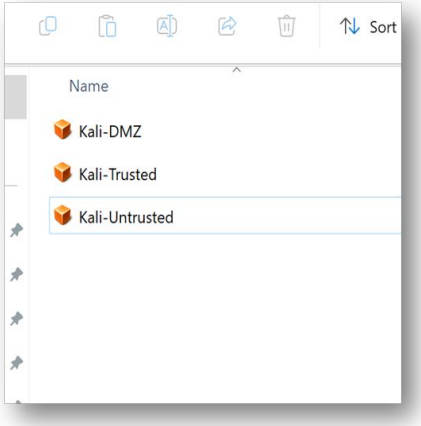
Services for Customer

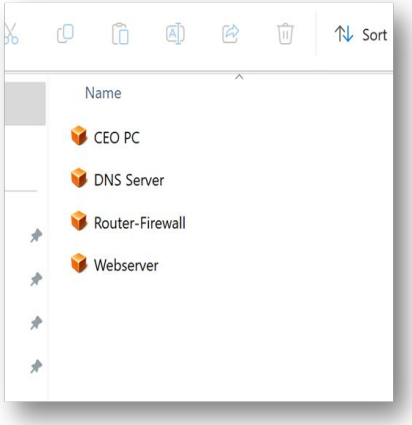
Install virtualBox and extension



Installed Vm

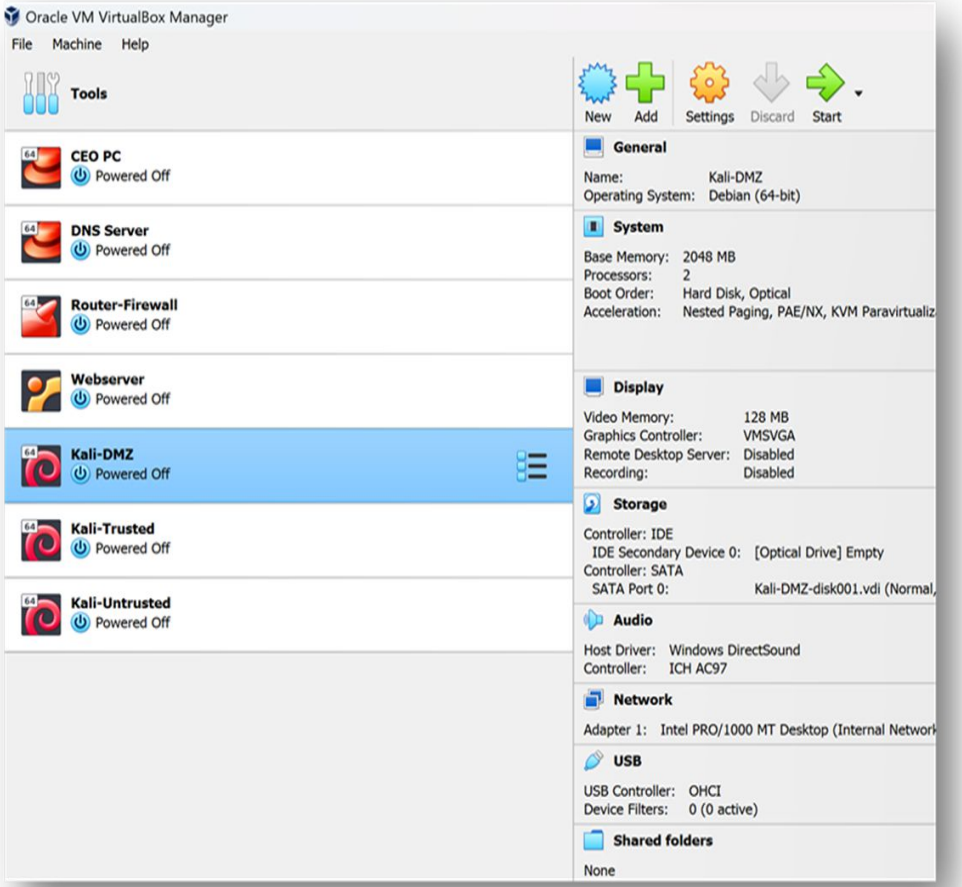
Installed Extension





All the machine are installed

- Router-FW
- DNS Server
- Webserver
- CEO PC
- 3 Kali Linux machines



Troubleshoot and resolve issues in CEO PC

```
root@PC1:~
File  Edit  View  Search  Terminal  Help
Release:        6.4
Codename:       Final
[root@PC1 ~]# ifconfig /all
/all: error fetching interface information: Device not found
[root@PC1 ~]# ifconfig -a
eth2      Link encap:Ethernet  HWaddr 08:00:27:24:68:E3
          inet addr:203.0.113.69  Bcast:203.0.113.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe24:68e3/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:5 errors:0 dropped:0 overruns:0 frame:0
          TX packets:931 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:570 (570.0 b)  TX bytes:39414 (38.4 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:630 errors:0 dropped:0 overruns:0 frame:
          TX packets:630 errors:0 dropped:0 overruns:0 carrie
          collisions:0 txqueuelen:0
          RX bytes:59337 (57.9 KiB)  TX bytes:59337 (57.9 KiB

[root@PC1 ~]#
```

```
Applications  Places  System                    Sat May 25, 4:07 PM  root
root@PC1:~/Desktop
File  Edit  View  Search  Terminal  Help
eth2      Link encap:Ethernet  HWaddr 08:00:27:24:68:E3
          inet addr:192.168.0.15  Bcast:192.168.0.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe24:68e3/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:13 errors:0 dropped:0 overruns:0 frame:0
          TX packets:80 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1792 (1.7 KiB)  TX bytes:4564 (4.4 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:46 errors:0 dropped:0 overruns:0 frame:0
          TX packets:46 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:3752 (3.6 KiB)  TX bytes:3752 (3.6 KiB)

[root@PC1 Desktop]# ping -c4 10.200.0.11
10.200.0.11) 56(84) bytes of data.
00.0.11: icmp_seq=1 ttl=63 time=3.77 ms
00.0.11: icmp_seq=2 ttl=63 time=12.0 ms
00.0.11: icmp_seq=3 ttl=63 time=12.3 ms
00.0.11: icmp_seq=4 ttl=63 time=10.6 ms

ng statistics ---
ted, 4 received, 0% packet loss, time 3046ms
ev = 3.771/9.730/12.398/3.504 ms
#
sktop   [Cybersecurity Bootca...
```

```
Applications  Places  System                    Sat May 25, 4:03 PM  root
Cybersecurity Bootcamp Server - Mozilla Firefox
File  Edit  View  History  Bookmarks  Tools  Help
Welcome to CentOS   Cybersecurity Bootcamp Ser...
www.seclab.net                                  Google

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.

[root@PC1:~/Desktop]   Cybersecurity Bootca...
```

```
root@webserver:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:90:2f:9a
          inet addr:10.200.0.12  Bcast:10.200.0.15  Mask:255.255.255.248
          inet6 addr: fe80::a00:27ff:fe90:2f9a/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1068 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1109 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:78849 (77.0 KB)  TX bytes:70808 (69.1 KB)
          Interrupt:9 Base address:0xd020

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:625 errors:0 dropped:0 overruns:0 frame:0
          TX packets:625 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:281209 (274.6 KB)  TX bytes:281209 (274.6 KB)
```

```
[root@localhost ~]# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:50:56:00:11:01
          inet addr:10.200.0.11  Bcast:10.200.0.15  Mask:255.255.255.248
          inet6 addr: fe80::250:56ff:fe00:1101/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:6570 errors:0 dropped:0 overruns:0 frame:0
          TX packets:6560 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:682824 (666.8 KiB)  TX bytes:537859 (525.2 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:63 errors:0 dropped:0 overruns:0 frame:0
          TX packets:63 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:5727 (5.5 KiB)  TX bytes:5727 (5.5 KiB)

[root@localhost ~]#
```

```
root@webserver:/etc# lsb_release
No LSB modules are available.
root@webserver:/etc# ls -l | grep -i os
-rw-r--r--  1 root     root       92 2007-10-20 07:51 host.conf
-rw-r--r--  1 root     root       10 2014-10-07 07:54 hostname
-rw-r--r--  1 root     root      267 2014-10-07 07:55 hosts
-rw-r--r--  1 root     root      588 2012-05-20 14:29 hosts.allow
-rw-r--r--  1 root     root      878 2010-03-16 19:01 hosts.deny
-rw-r--r--  1 root     root      121 2012-05-20 14:31 hosts.equiv
drwxr-xr-x  3 root     root     4096 2014-10-07 07:58 postfix
drwxr-xr-x  3 root     root     4096 2010-03-17 10:08 postgresql
drwxr-xr-x  3 root     root     4096 2010-03-17 10:08 postgresql-common
root@webserver:/etc# ls -l | grep -i release
-rw-r--r--  1 root     root       96 2008-04-15 01:04 lsb-release
root@webserver:/etc# cat lsb-release
DISTRIB_ID=Ubuntu
DISTRIB_RELEASE=8.04
DISTRIB_CODENAME=hardy
DISTRIB_DESCRIPTION="Ubuntu 8.04"
root@webserver:/etc# cd ..
```

```
drwxr-xr-x.  2 root root    4096 Oct  9  2014 postfix
lrwxrwxrwx.  1 root root      14 Oct  9  2014 redhat-release -> centos-release
lrwxrwxrwx.  1 root root      14 Oct  9  2014 system-release -> centos-release
drwxr-xr-x.  2 root root    4096 Oct  9  2014 yum.repos.d
[root@localhost etc]# ls -l| grep -i release
-rw-r--r--.  1 root root      27 Feb 25  2013 centos-release
lrwxrwxrwx.  1 root root      14 Oct  9  2014 redhat-release -> centos-release
lrwxrwxrwx.  1 root root      14 Oct  9  2014 system-release -> centos-release
-rw-r--r--.  1 root root      25 Feb 25  2013 system-release-cpe
[root@localhost etc]# cat centos -release
cat: invalid option -- 'r'
Try `cat --help' for more information.
[root@localhost etc]# cat centos-release
CentOS release 6.4 (Final)
[root@localhost etc]#
```

```
root@PC1:~
File  Edit  View  Search  Terminal  Help
eth2      Link encap:Ethernet  HWaddr 08:00:27:24:68:E3
          inet addr:203.0.113.69  Bcast:203.0.113.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe24:68e3/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:4 errors:0 dropped:0 overruns:0 frame:0
          TX packets:62 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:510 (510.0 b)  TX bytes:2916 (2.8 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:36 errors:0 dropped:0 overruns:0 frame:0
          TX packets:36 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:2972 (2.9 KiB)  TX bytes:2972 (2.9 KiB)

[root@PC1 ~]# ^C
[root@PC1 ~]# lsb_release -a
LSB Version:    :base-4.0-amd64:base-4.0-noarch:core-4.0-amd64:core-4.0-noarch:g
raphics-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
```

CEO PC

WEB SERVER

DNS SERVER

CEO PC [Running] - Oracle VM VirtualBox

Applications Places System Sun May 26, 9:34 AM root

root@PC1:~

File Edit View Search Terminal Help

```
150 Here comes the directory listing.
-rw-r--r--    1 1003     1003          447 Apr 17  2020 Candidate-List
-rw-r--r--    1 1003     1003         1524 Apr 16  2020 Social-Media-Security-Po
licy
226 Directory send OK.
ftp> get Social-Media-Security-Policy
local: Social-Media-Security-Policy remote: Social-Media-Security-Policy
227 Entering Passive Mode (10,200,0,12,158,52).
150 Opening BINARY mode data connection for Social-Media-Security-Policy (1524 b
ytes).
226 Transfer complete.
1524 bytes received in 3.3e-05 secs (46181.82 Kbytes/sec)
ftp> bye
221 Goodbye.
[root@PC1 ~]# ls -l
total 104
-rw-------. 1 root root  1670 Feb  4  2014 anaconda-ks.cfg
drwxr-xr-x. 2 root root  4096 Mar 19  2023 Desktop
drwxr-xr-x. 2 root root  4096 Apr 17  2020 Documents
drwxr-xr-x. 2 root root  4096 Apr 17  2020 Downloads
-rw-r--r--. 1 root root 47503 Feb  4  2014 install.log
-rw-r--r--. 1 root root 10033 Feb  4  2014 install.log.syslog
drwxr-xr-x. 2 root root  4096 Apr 17  2020 Music
drwxr-xr-x. 2 root root  4096 Apr 17  2020 Pictures
drwxr-xr-x. 2 root root  4096 Apr 17  2020 Public
-rw-r--r--. 1 root root  1524 May 26 09:33 Social-Media-Security-Policy
drwxr-xr-x. 2 root root  4096 Apr 17  2020 Templates
drwxr-xr-x. 2 root root  4096 Apr 17  2020 Videos
[root@PC1 ~]#
```

root@PC1:~ Cybersecurity Bootca...

CEO PC [Running] - Oracle VM VirtualBox

Applications Places System Mon May 27

root@PC1:~

File Edit View Search Terminal Help

```
drwxr-xr-x. 2 root root  4096 Apr 17  2020 Videos
[root@PC1 ~]# cat Social-Media-Security-Policy
Draft Social Media Policy
Robot Parts, Inc.

Our company recognized that social media has become an integral part of our busi
ness and a key tool in our marketing strategy.  It has expanded our ability to i
nteract with our customers at a personal level, provides us with a platform to s
pread brand awareness,and gives our company a unique voice in the world of Robot
 Parts and Maintenance.  For these reasons, we want to continue the use of our c
orporate social media accounts; however, the social  media threat landscape is e
xpanding rapidly.  To protect our reputation, customers, and employees from thes
e threats, we are implementing this corporate social media security police, whic
h will hold us accountable to cyber security best practices as they pertain to t
he realm of social media.

Members of both the social media and cyber security teams are required to review
 this policy on an annual basis and make updates ad needed.  In the event of a s
ecurity incident, the is policy should be reviewed as s soon as possible to i id
entify any opportunities for improvement.

Access Management
[we need to specify what tools we will use and who the authorized users will be
by job title.  Also address the use of mobile device tools.}

Social Media Privacy Provision
[state we must address the corporate privacy policy when using social media.]

Social Media Security Monitoring
[Address who will monitor the corporate social media streams and hashtags.  Addr
ess how often to review and how to deal with specific events.}
```

Social-Media-Security-Policy

```
Changing the user information for oggy
Enter the new value, or press ENTER for the default
        Full Name []: oggy
        Room Number []: 123
        Work Phone []: 12345
        Home Phone []: 54321
        Other []:
Is the information correct? [y/N] y
root@webserver:~# pwd
/root
root@webserver:~# ls -l
total 12
drwxr-xr-x 2 root root 4096 2012-05-20 15:08 Desktop
-rwx------ 1 root root  401 2012-05-20 15:55 reset_logs.sh
-rw-r--r-- 1 root root  128 2024-05-25 20:51 vnc.log
root@webserver:~# cd /home
root@webserver:/home# ls -l
total 24
drwxr-xr-x 7 admin   admin1  4096 2014-10-08 06:25 admin
drwxr-xr-x 2 root    nogroup 4096 2010-03-17 10:08 ftp
drwxr-xr-x 2 jasper  jasper  4096 2020-04-17 05:47 jasper
drwxr-xr-x 2 oggy    oggy    4096 2024-05-25 21:47 oggy
drwxr-xr-x 2 service service 4096 2010-04-16 02:16 service
drwxr-xr-x 3 user    user    4096 2010-05-07 14:38 user
root@webserver:/home# _
```

New User in Web Server

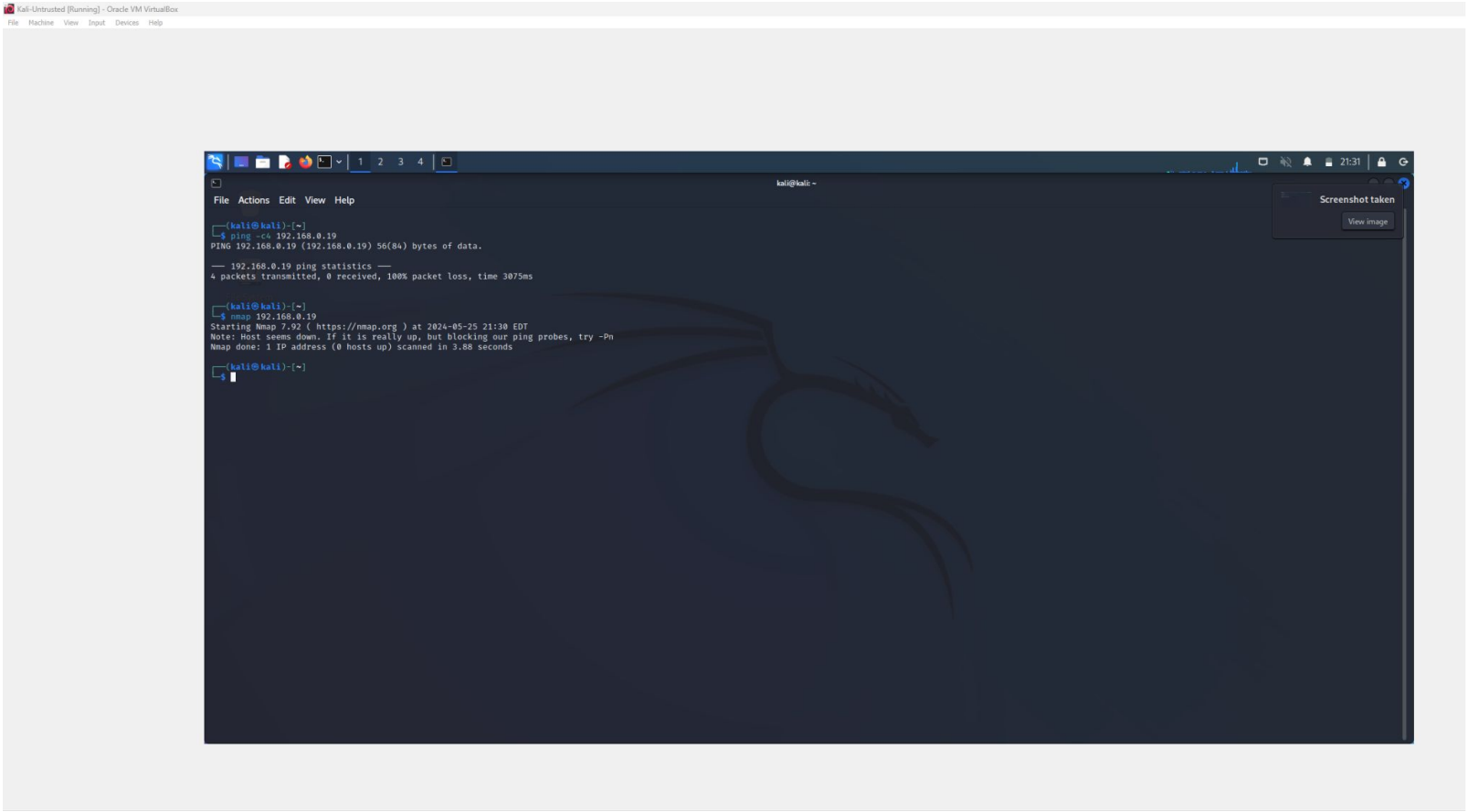
Open Ports

```
┌──(kali㉿kali)-[~]
└─$ nmap 10.200.0.12
Starting Nmap 7.92 ( https://nmap.org ) at 2024-05-25 15:53 EDT
Nmap scan report for www.seclab.net (10.200.0.12)
Host is up (0.034s 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 0.49 seconds
```

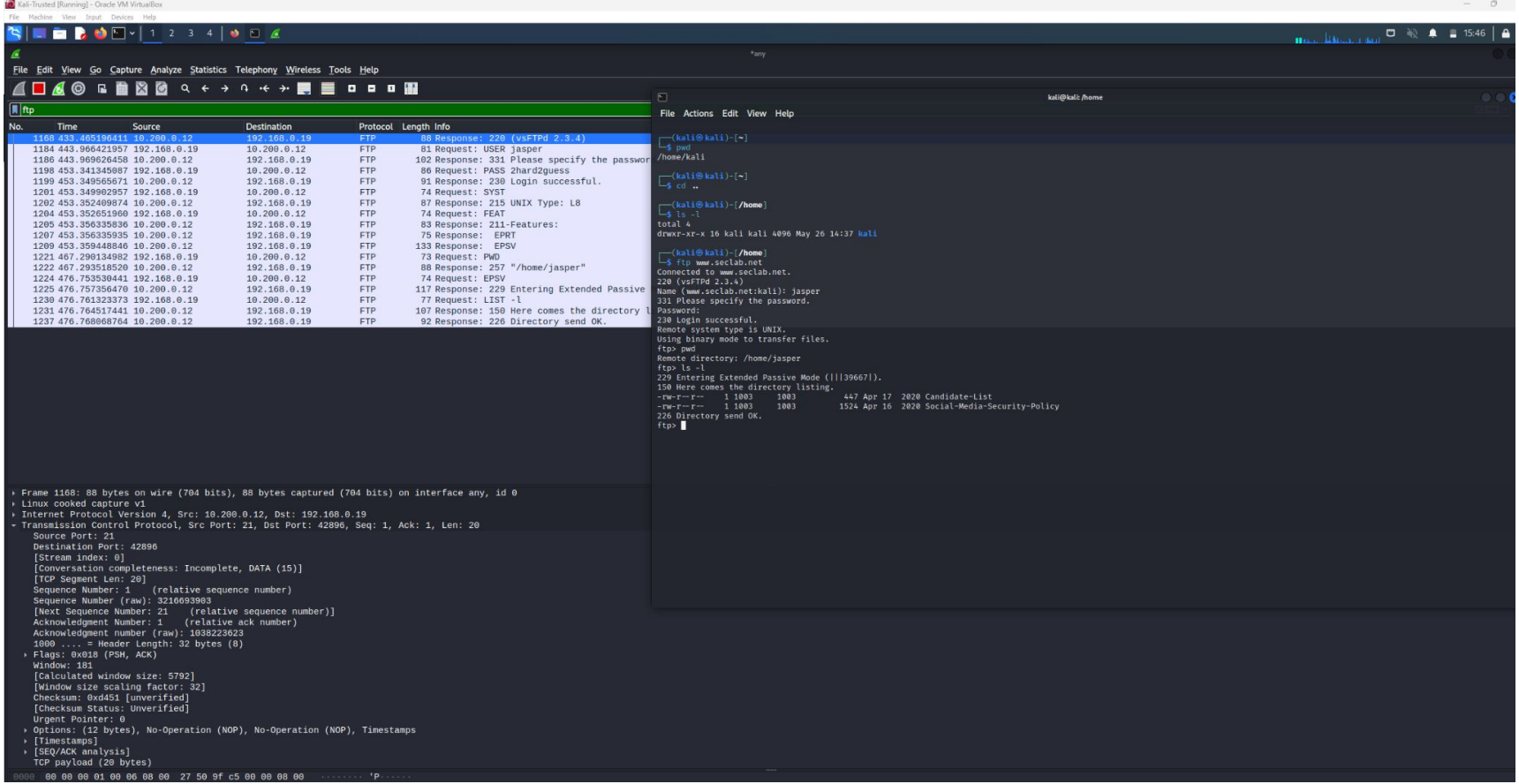
```
┌──(kali㉿kali)-[~]
└─$ nmap 10.200.0.11
Starting Nmap 7.92 ( https://nmap.org ) at 2024-05-25 15:52 EDT
Nmap scan report for ns1.seclab.net (10.200.0.11)
Host is up (0.035s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT   STATE SERVICE
22/tcp open  ssh
53/tcp open  domain

Nmap done: 1 IP address (1 host up) scanned in 0.48 seconds

┌──(kali㉿kali)-[~]
└─$
```

DNS Server

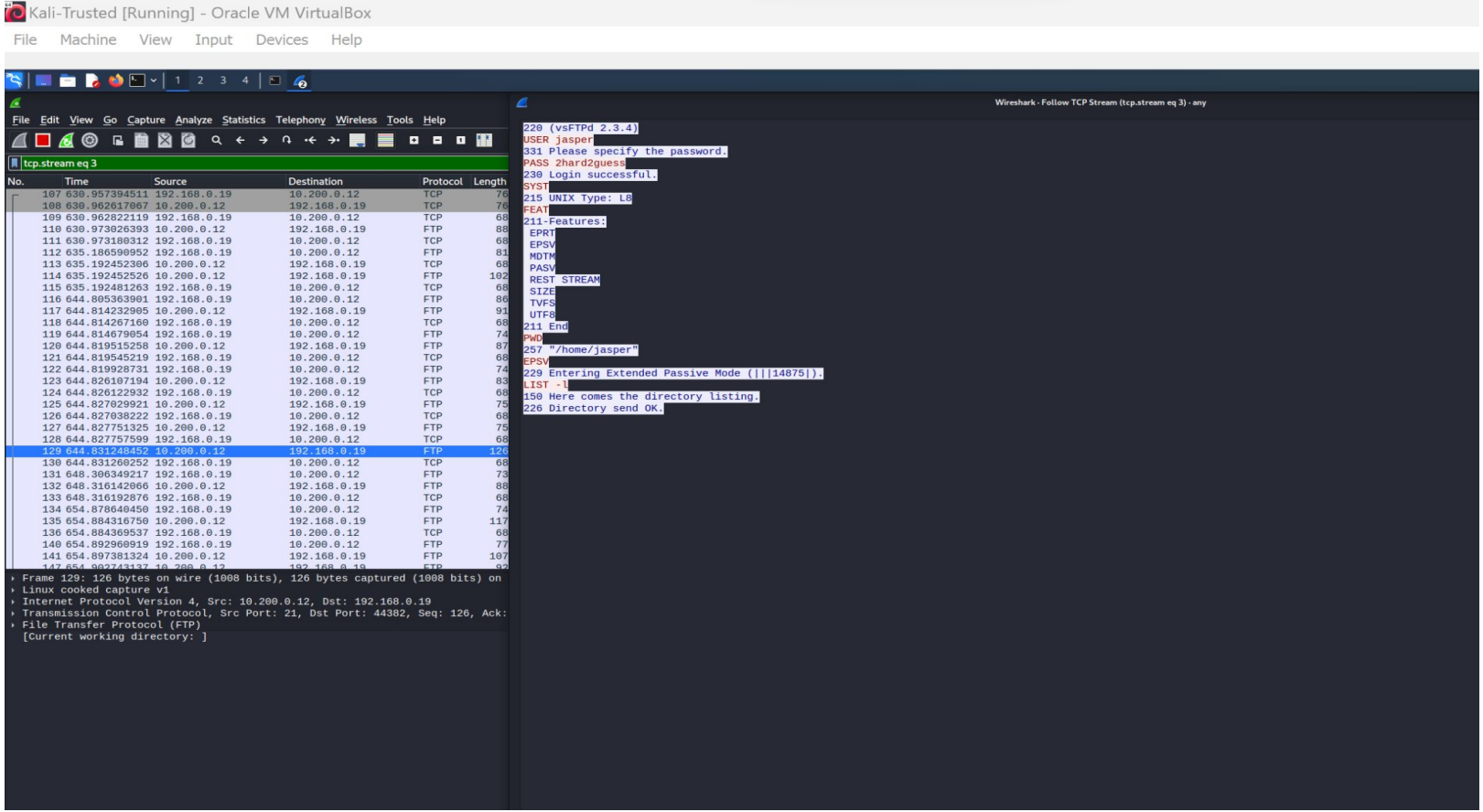
Web Server



Kali Trusted & Untrusted Security



Wireshark on Kali Linux



UserName and Password using FTP

Security Recommendations

- Security Awareness Training
- Backup and Disaster Recovery Planning
- Regular Security Audits and Updates

closing remarks

- The completion of this project has considerably improved the security aspect of the customer's infrastructure.
- By deploying a DMZ structure, conducting security assessment and building clear and useable security policies we have ensured that the network environment is secure and Strong against potential threats.
- Our work have showed the importance of network segmentation, regular security monitoring.
- This project is not for only current security aspect but for the future network security enhancements, we recommend the continued implementation of the security measures and improve the security of infrastructure.