



CSE487:Computer and Cybersecurity

[Fall23]

[Group 309]

Mini Project 01

Securing a Network System with PKI and Configure Firewall and IDS

Submitted for

Rashedul Amin Tuhin

Department of Computer Science and Engineering

Submitted by

Name: Md. Abdul Ahad Rifat

ID:2020-1-60-215

Name: Niaz Ahmed

ID:2020-2-60-192

Name:Sudipta Poddar

ID:2020-2-60-196

Download Kali Linux Operating System

Kali linux iso download link

<https://www.kali.org/get-kali/#kali-installer-images>

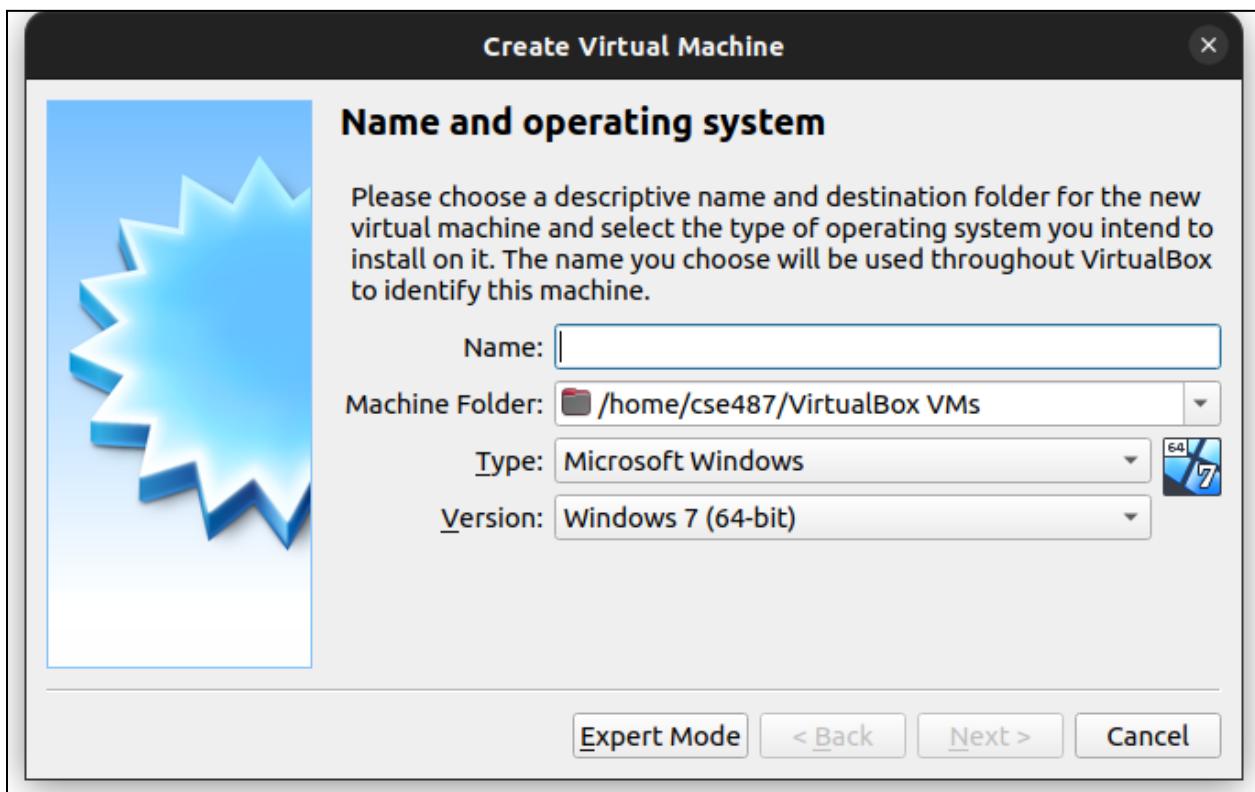
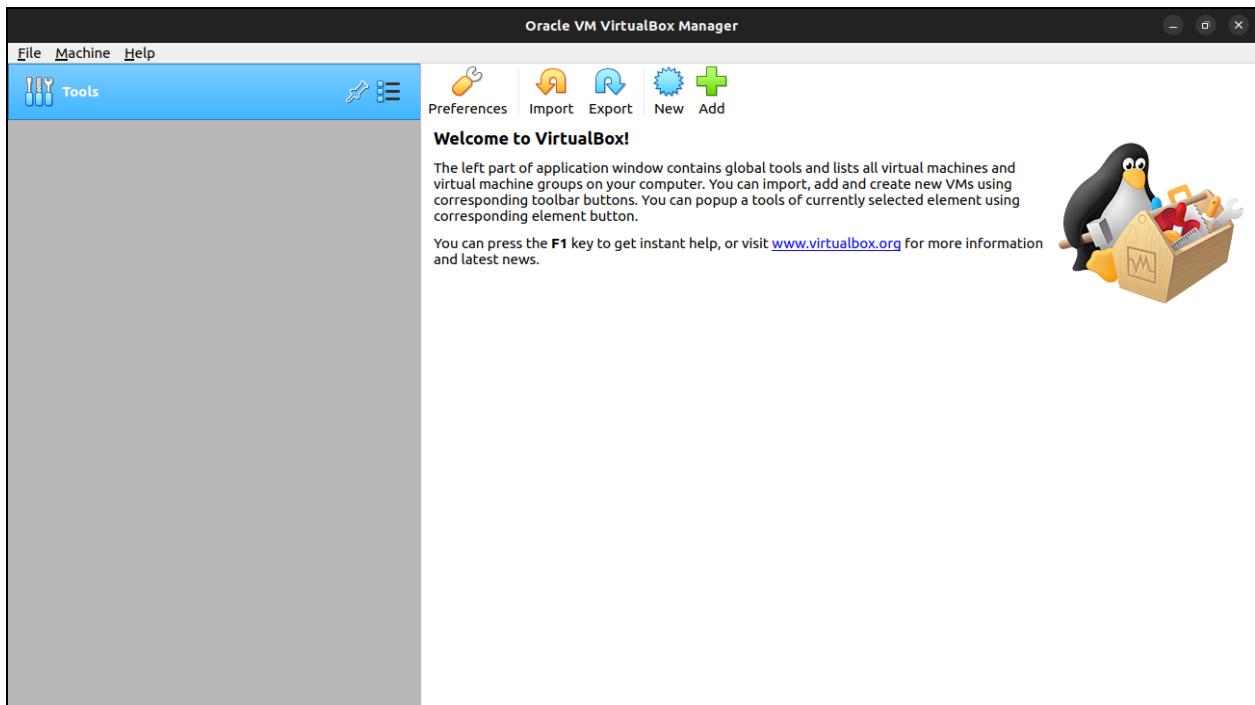
In our project, Kali Linux is the preferred operating system. However, you have the flexibility to opt for any Linux-based OS, ensuring that the commands align with the Debian-based structure. If utilizing a different Linux distribution, adhere to their specific guidelines when executing commands. This ensures a meaningful and seamless execution of tasks across various Linux environments.

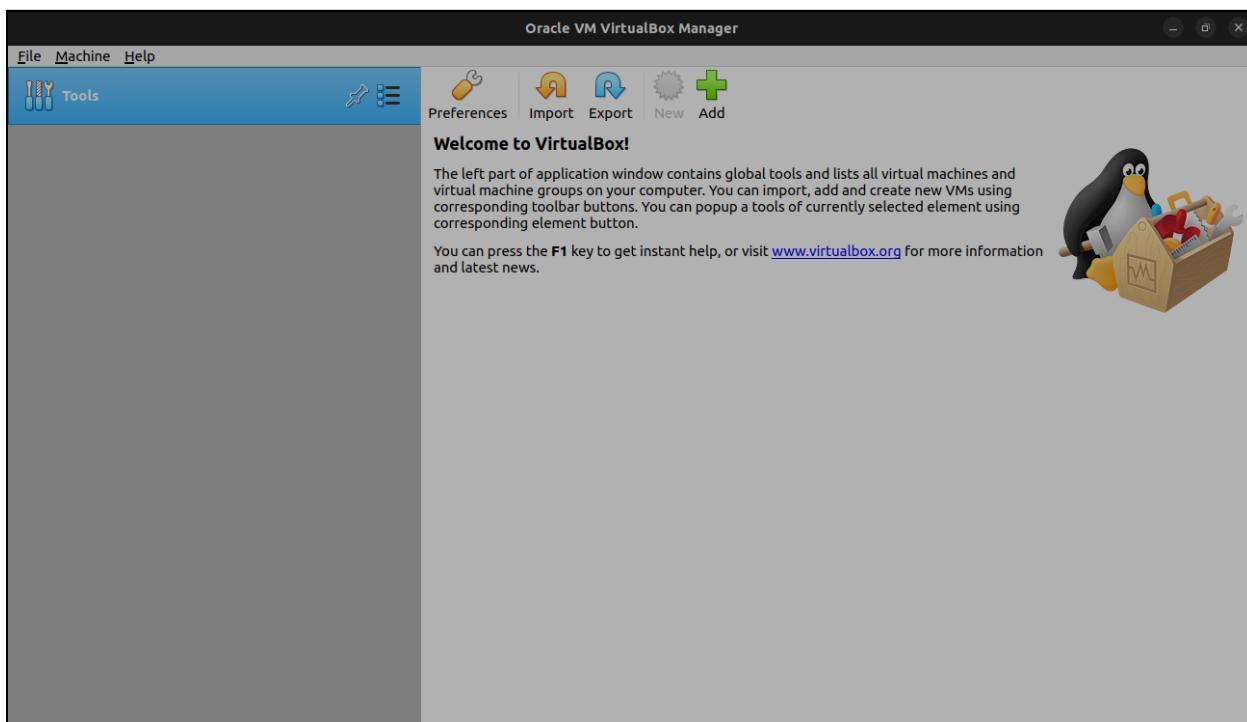
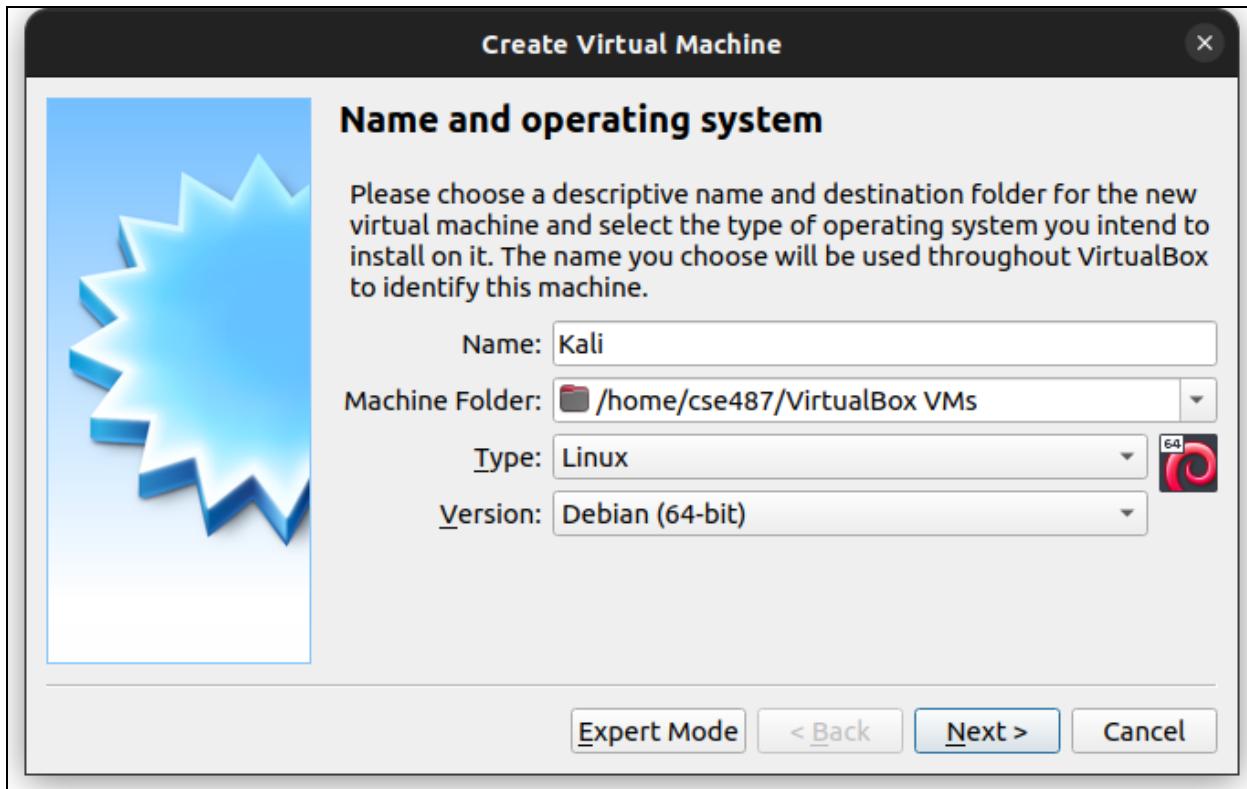
Installation Kali Linux in Virtual Box

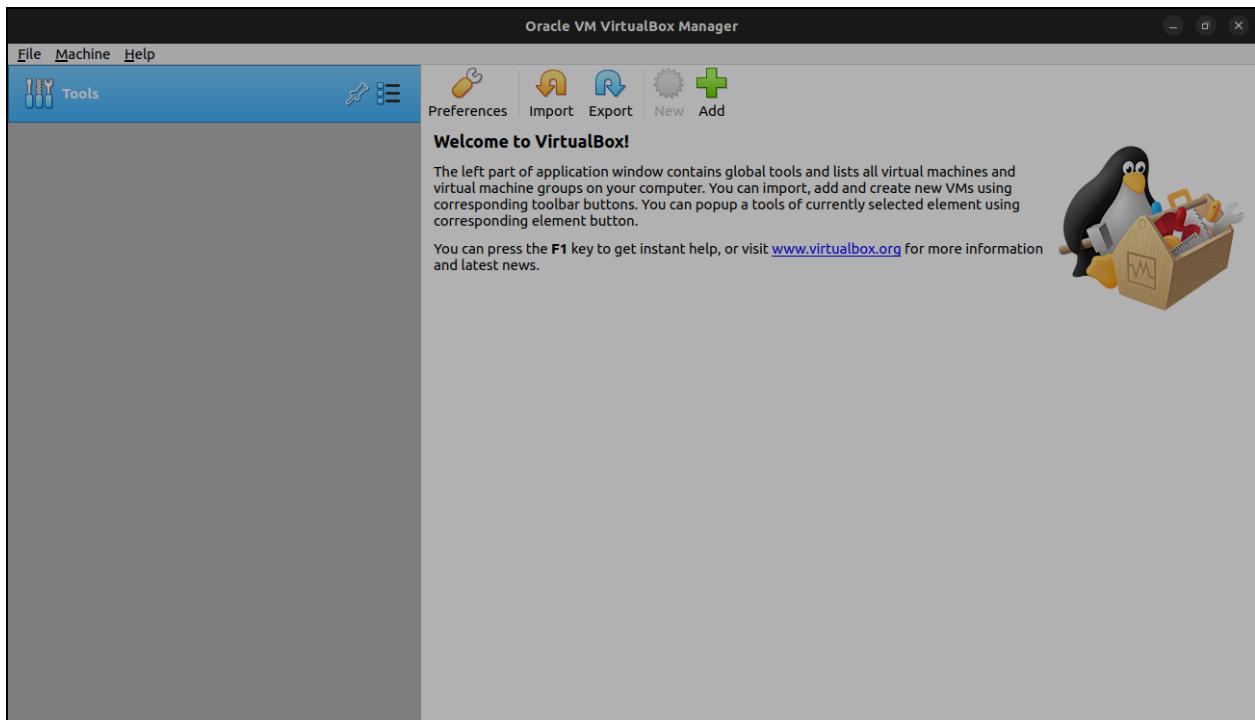
VirtualBox download link

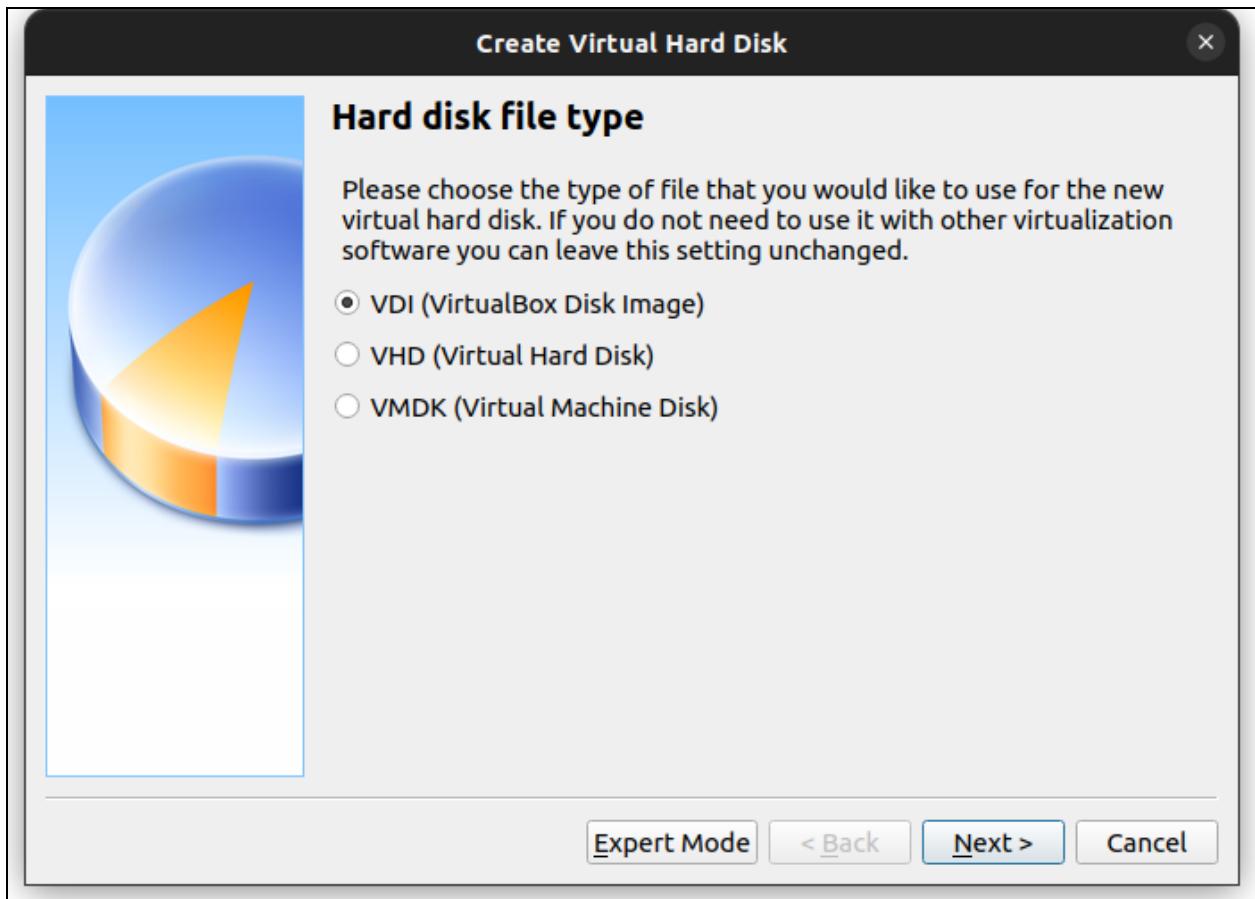
<https://www.virtualbox.org/wiki/Downloads>

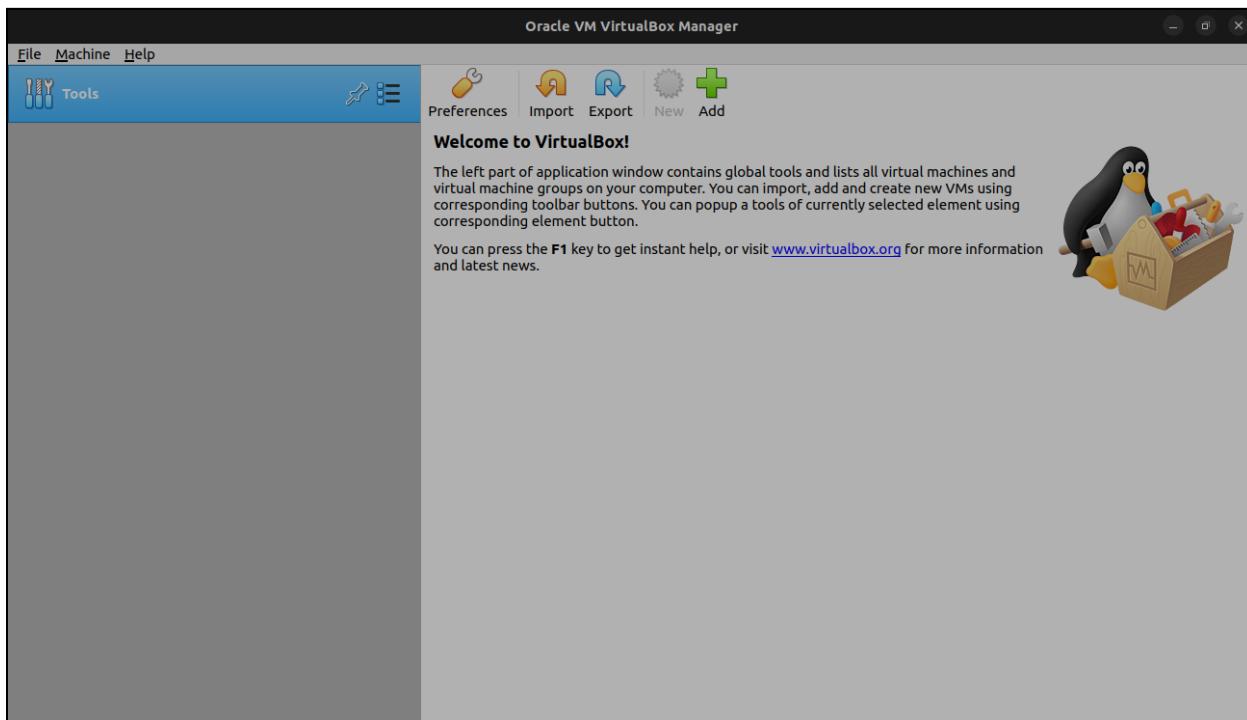
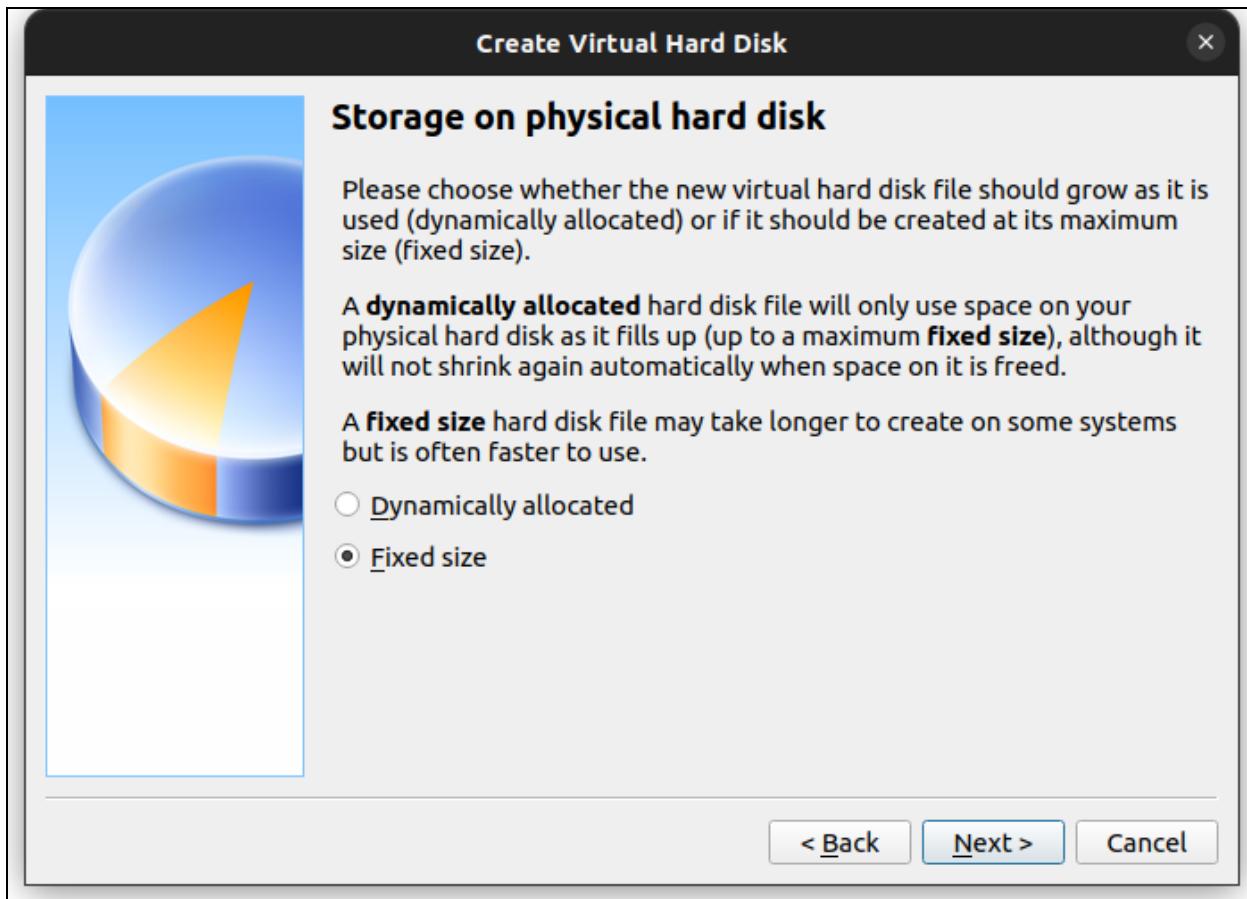
VirtualBox is a popular virtualization software that allows you to run multiple operating systems on a single physical machine.

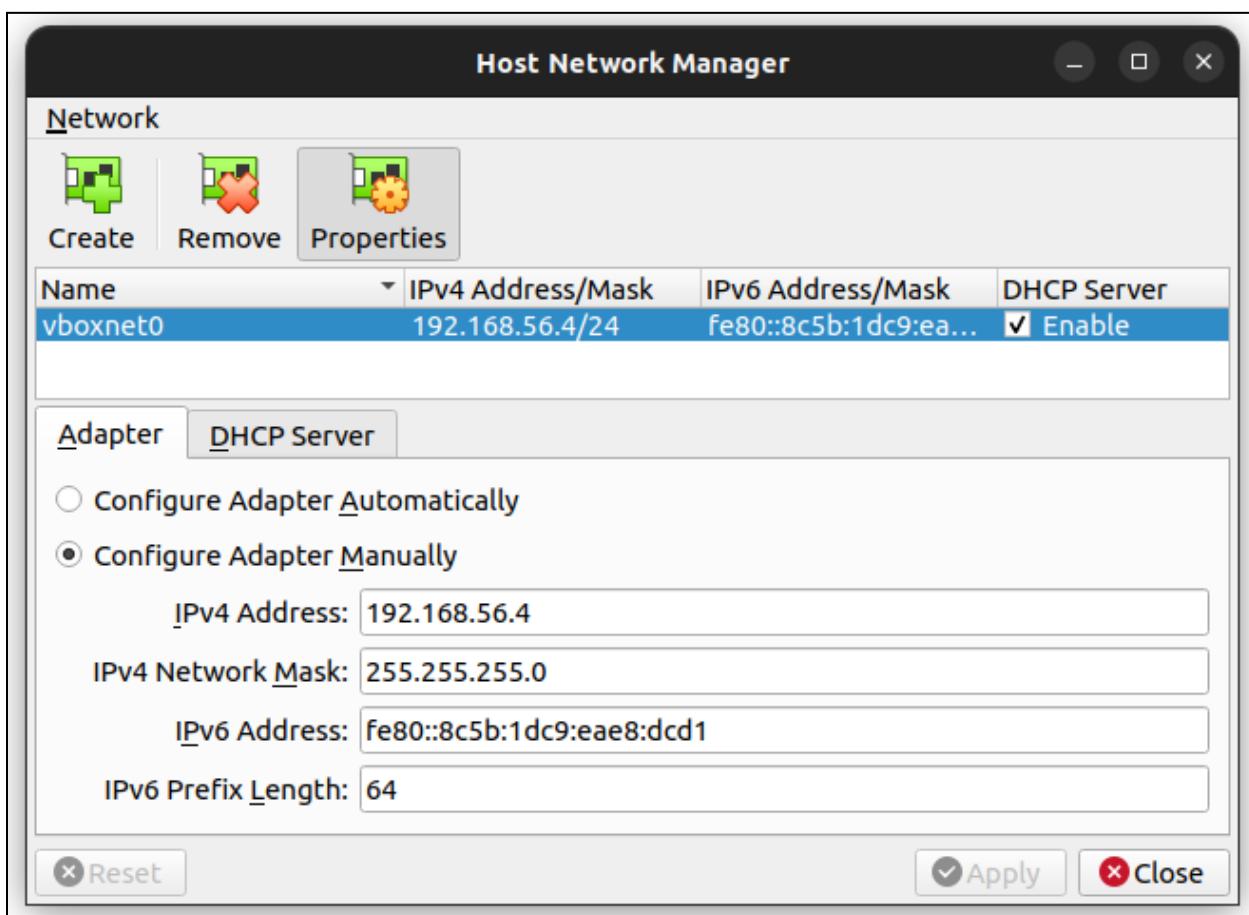
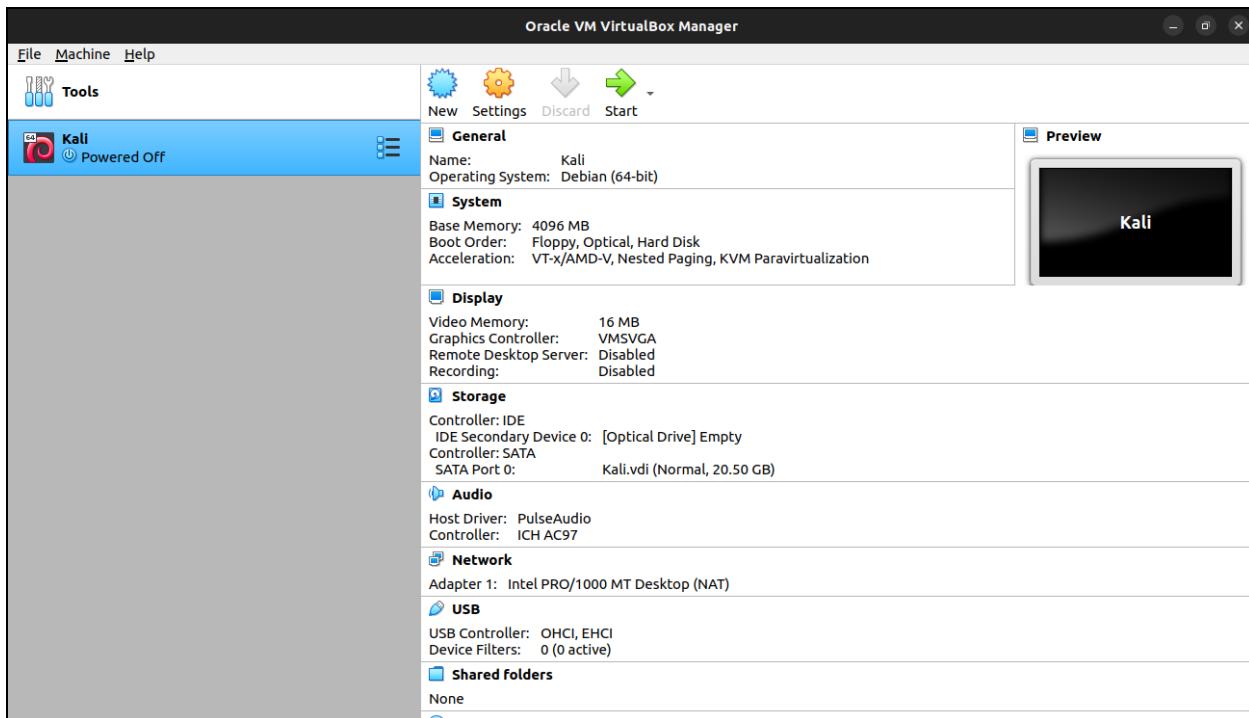


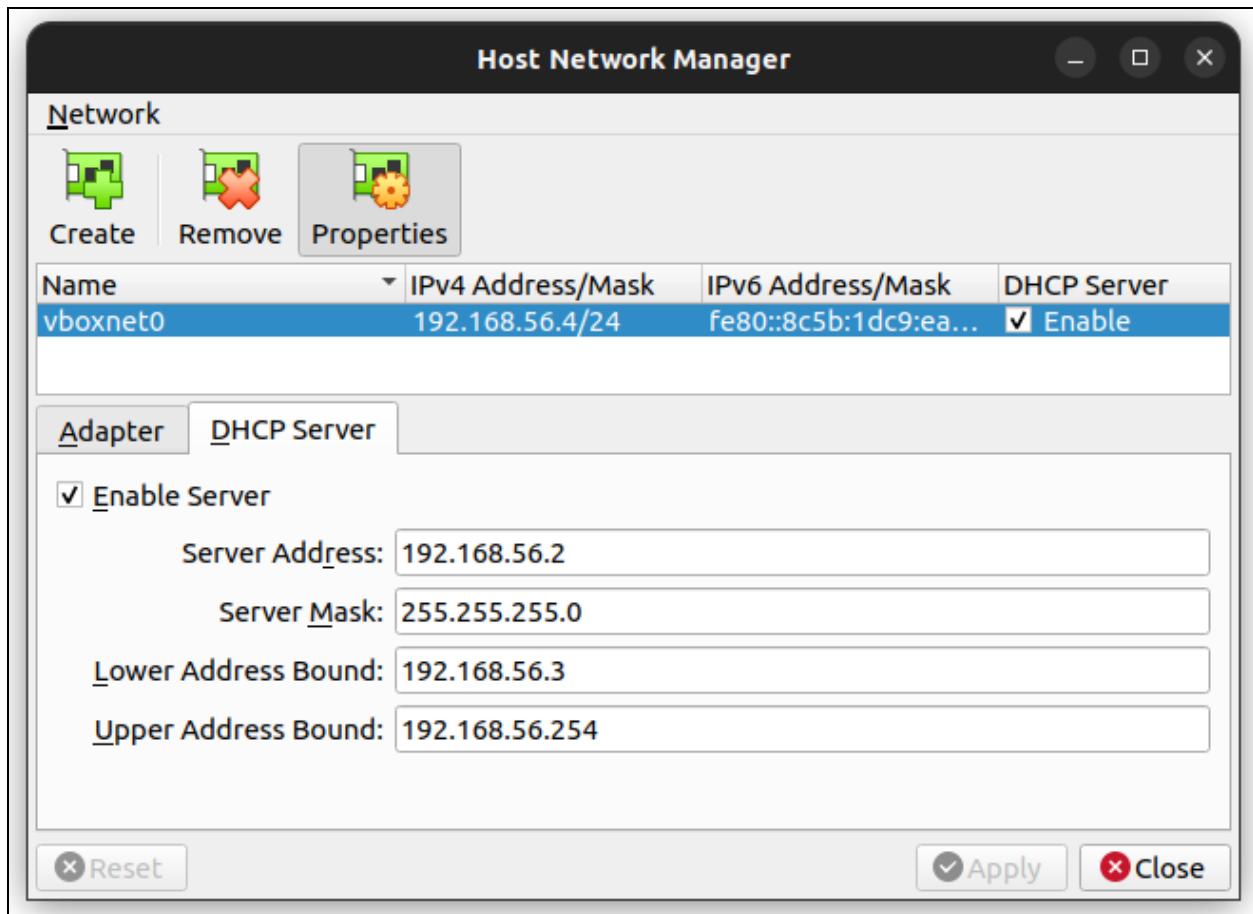


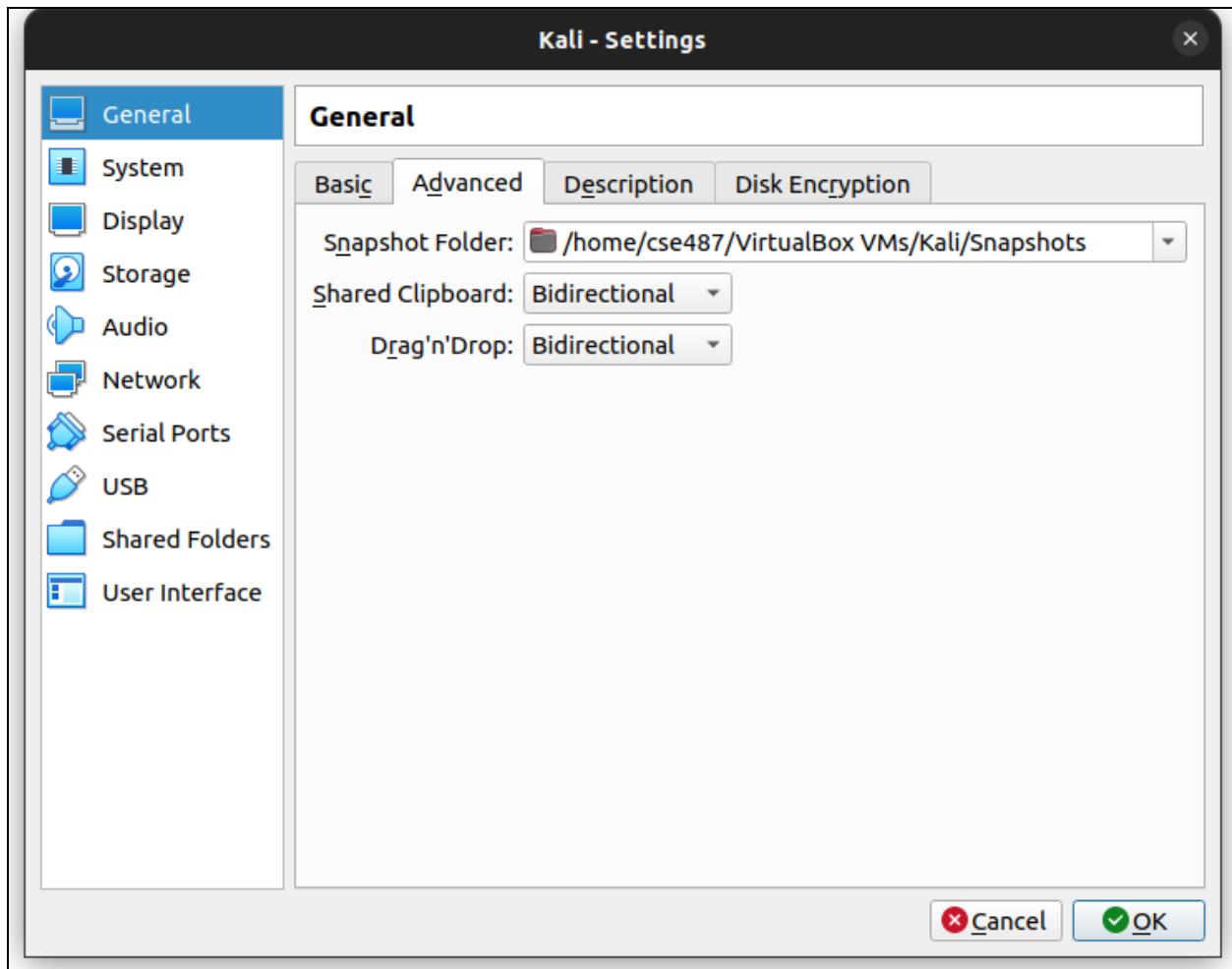


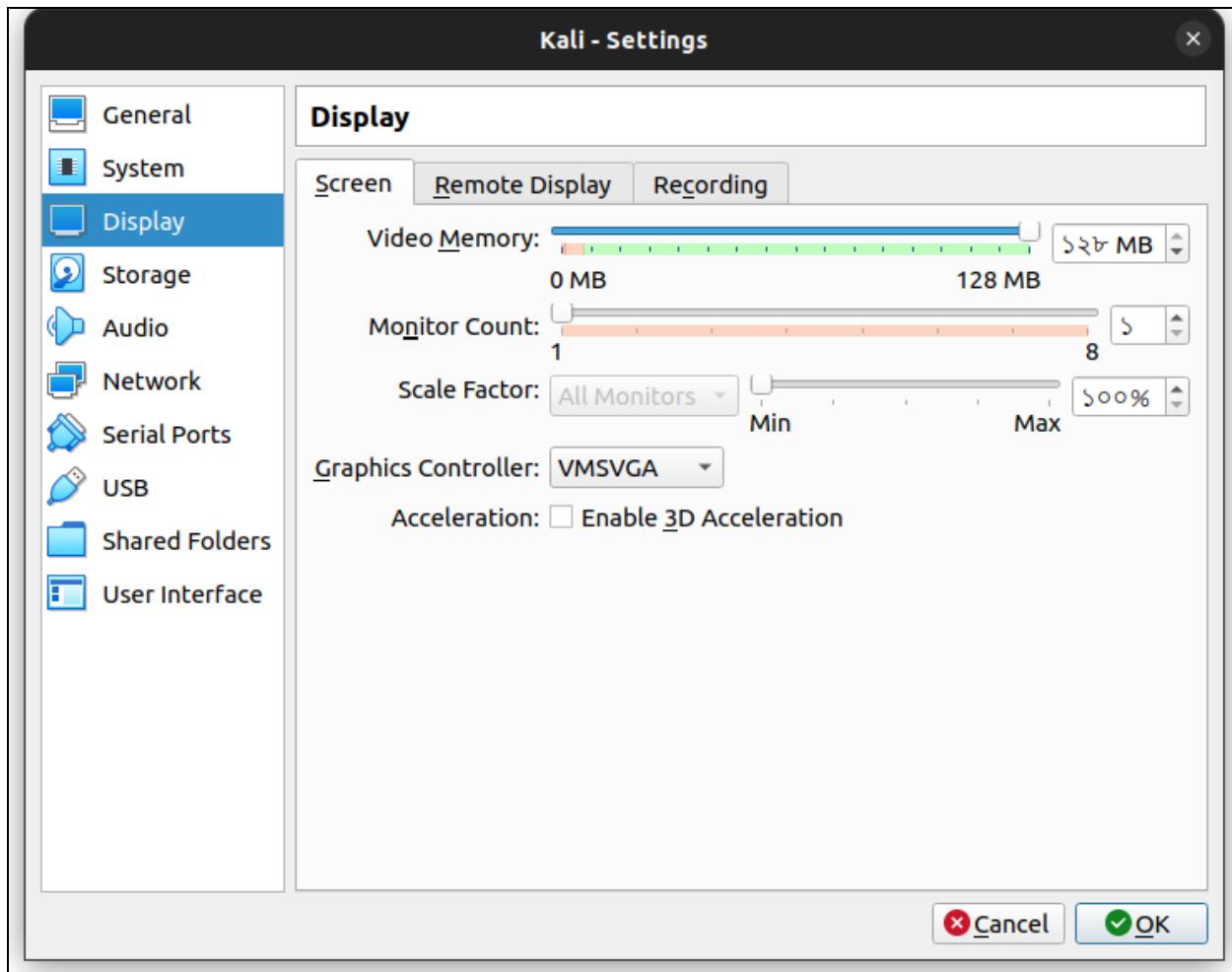


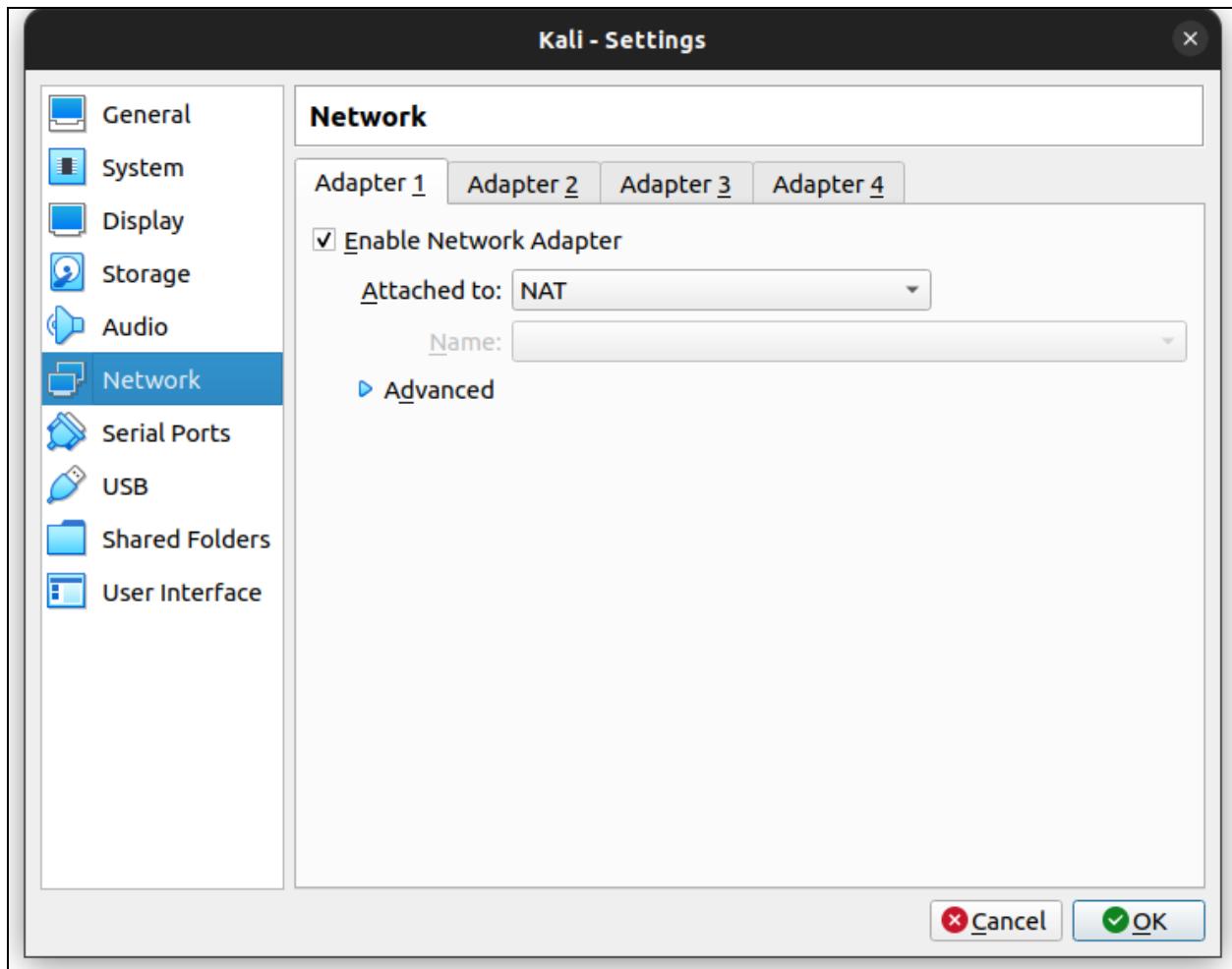


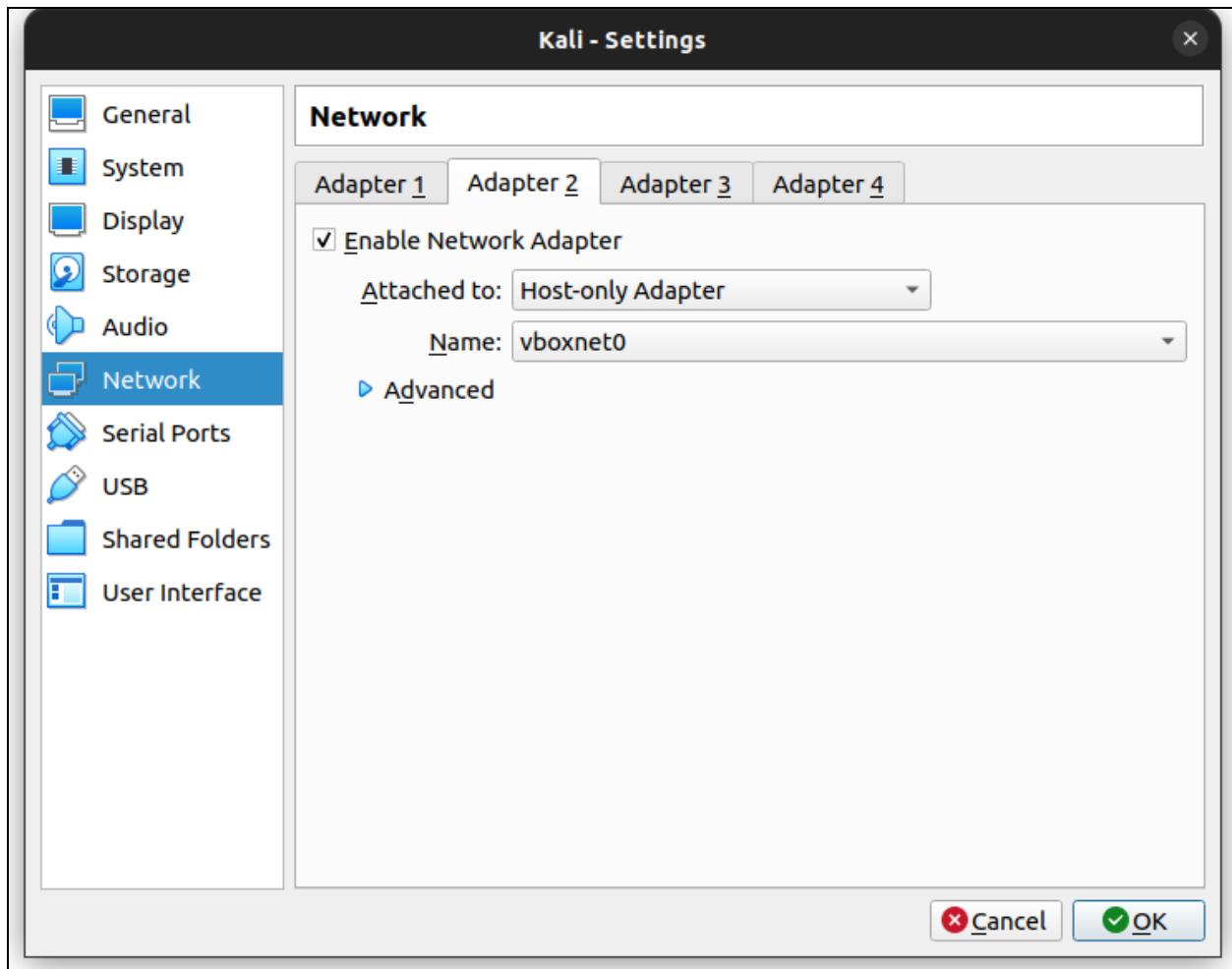


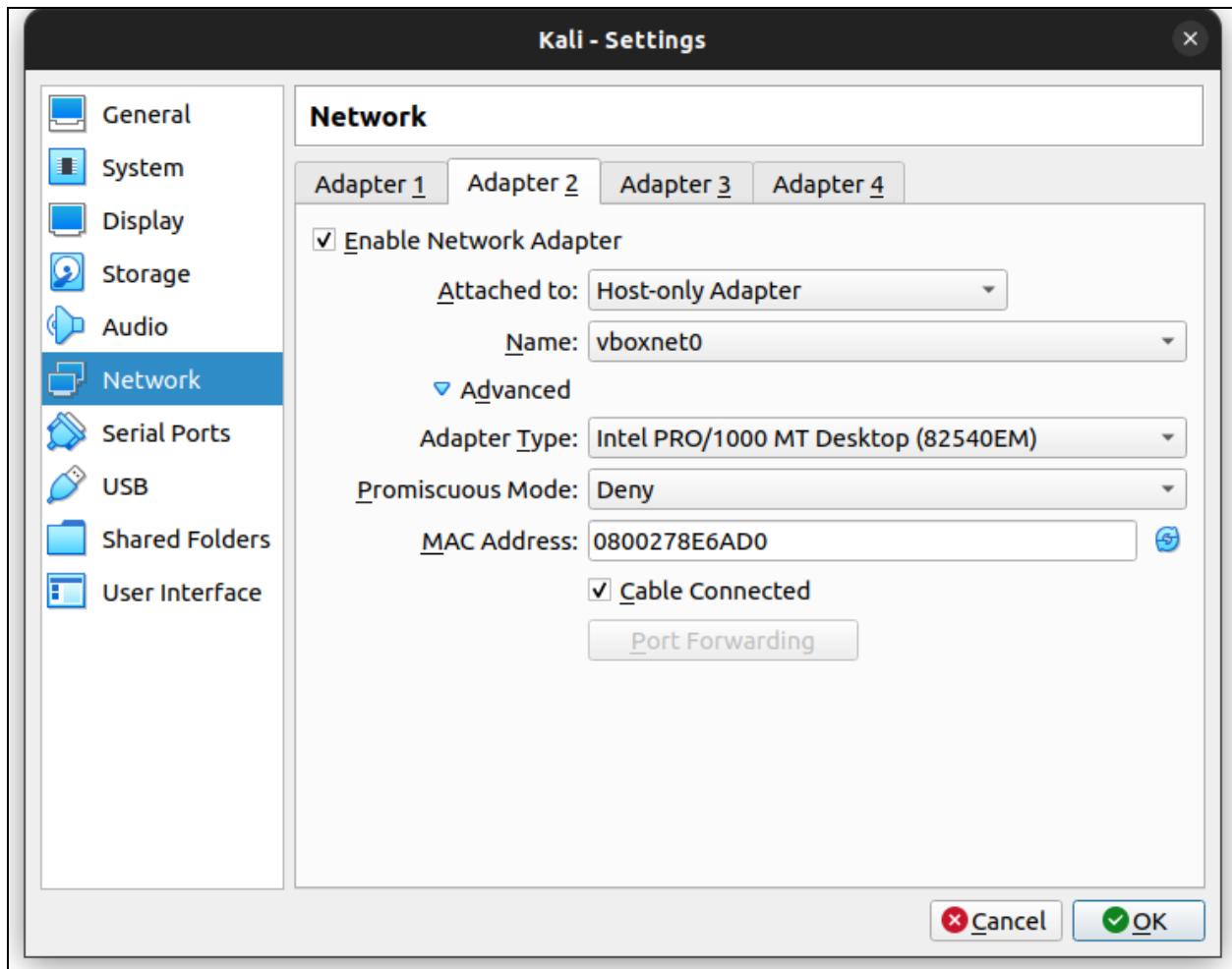


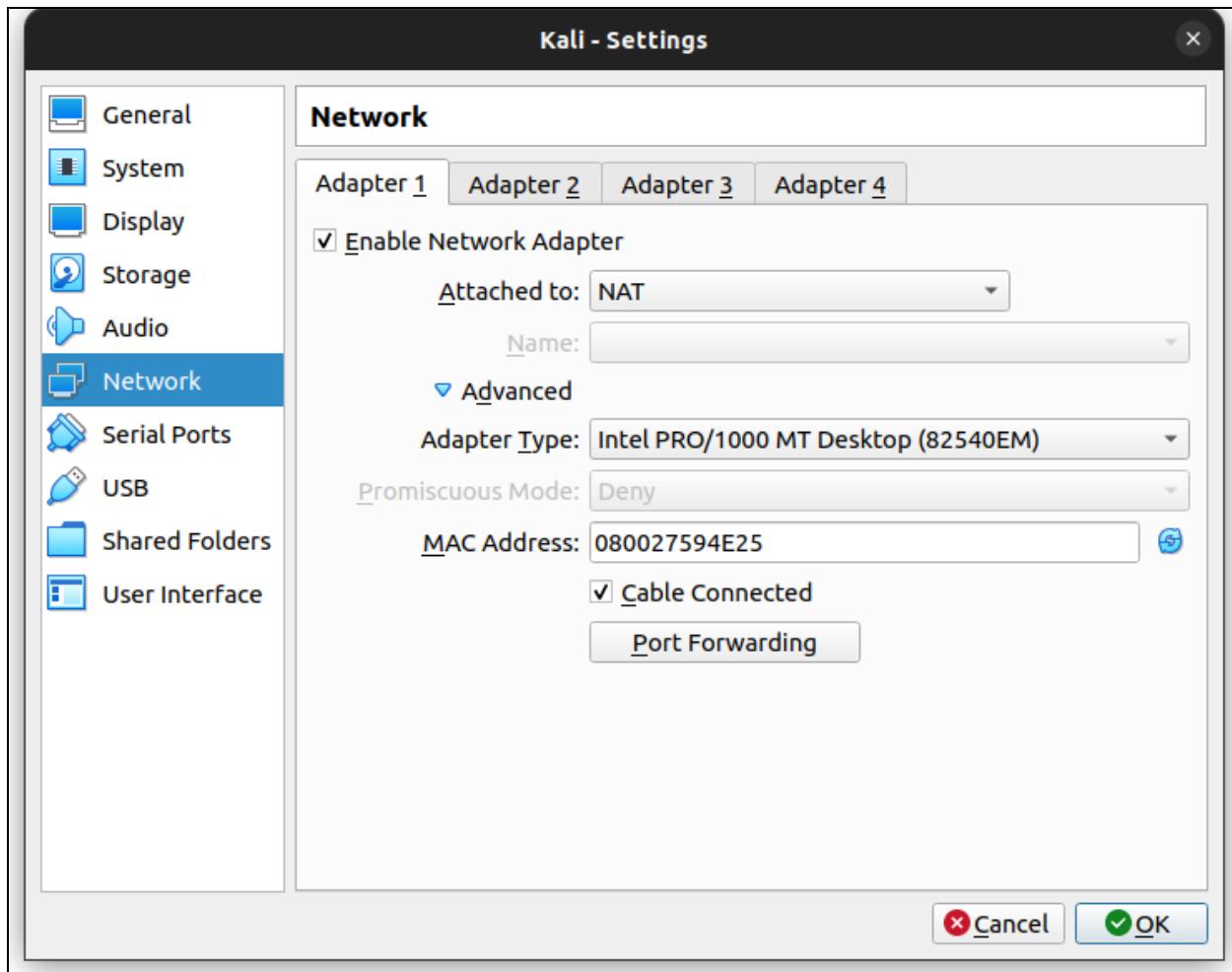


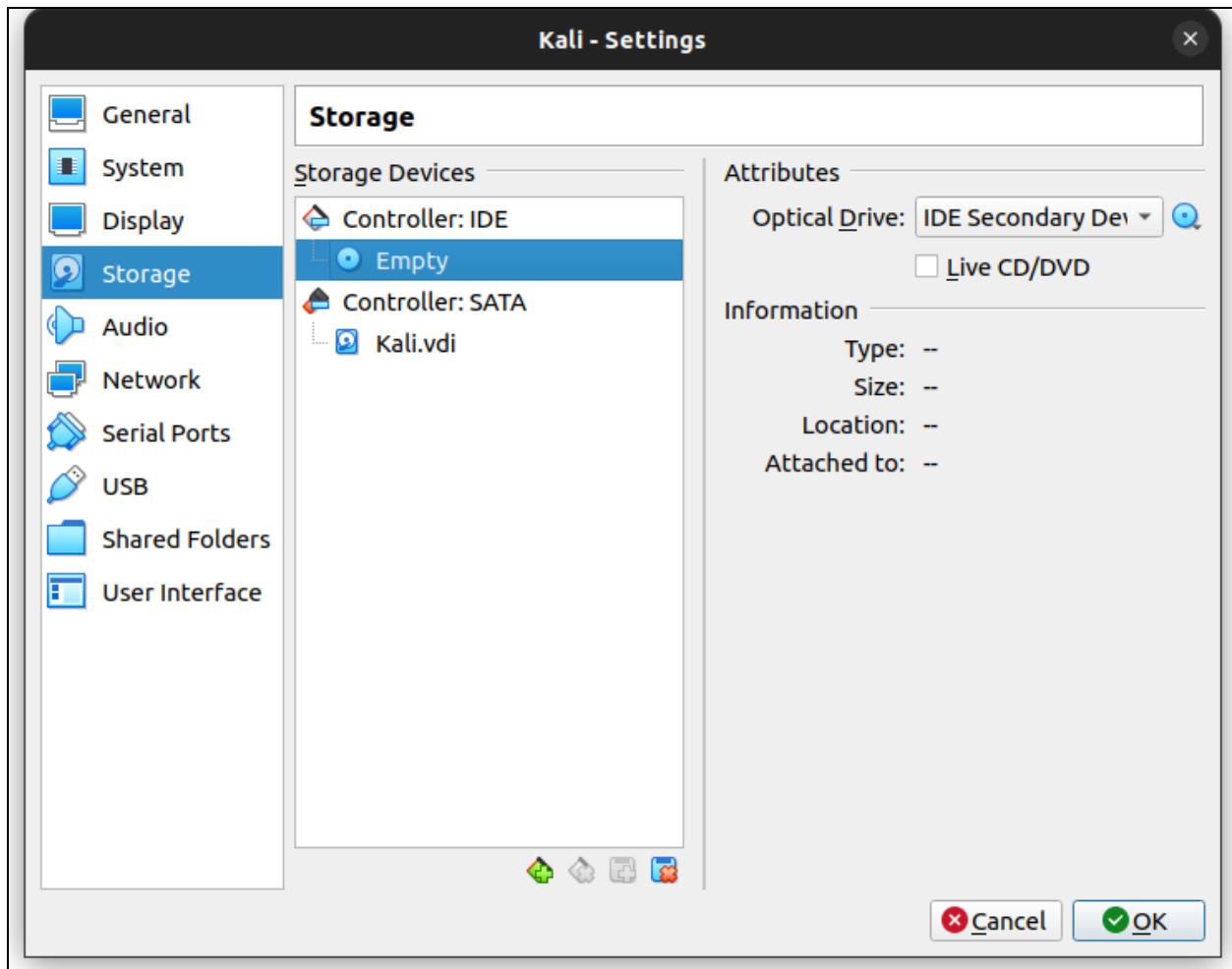


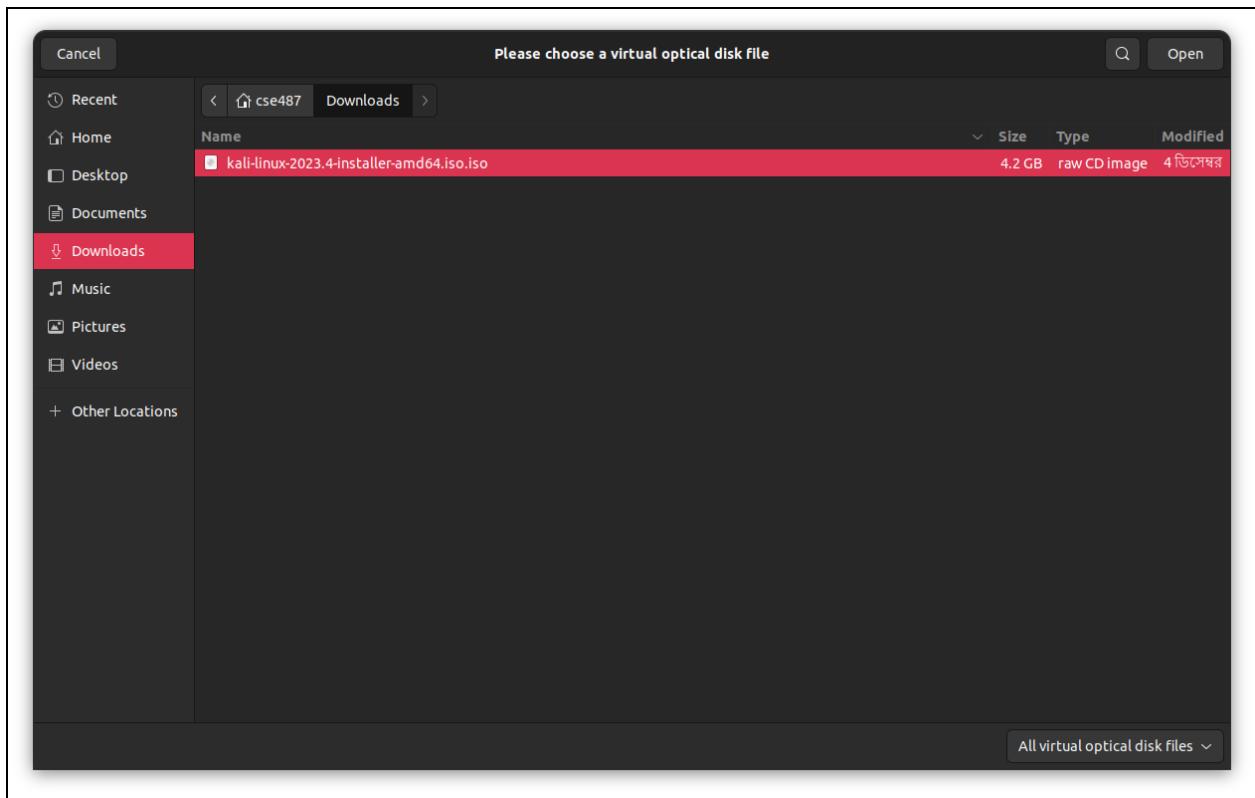


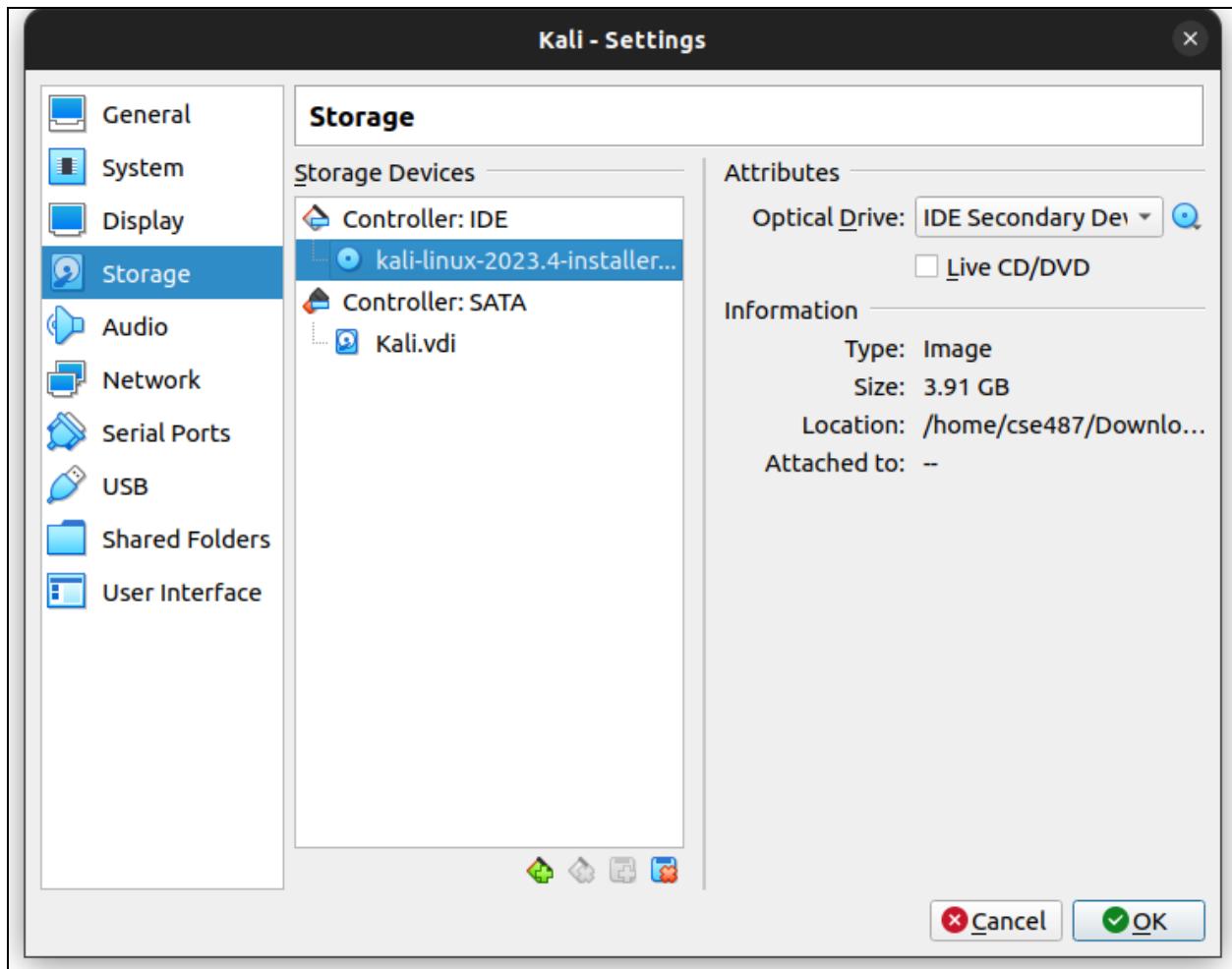


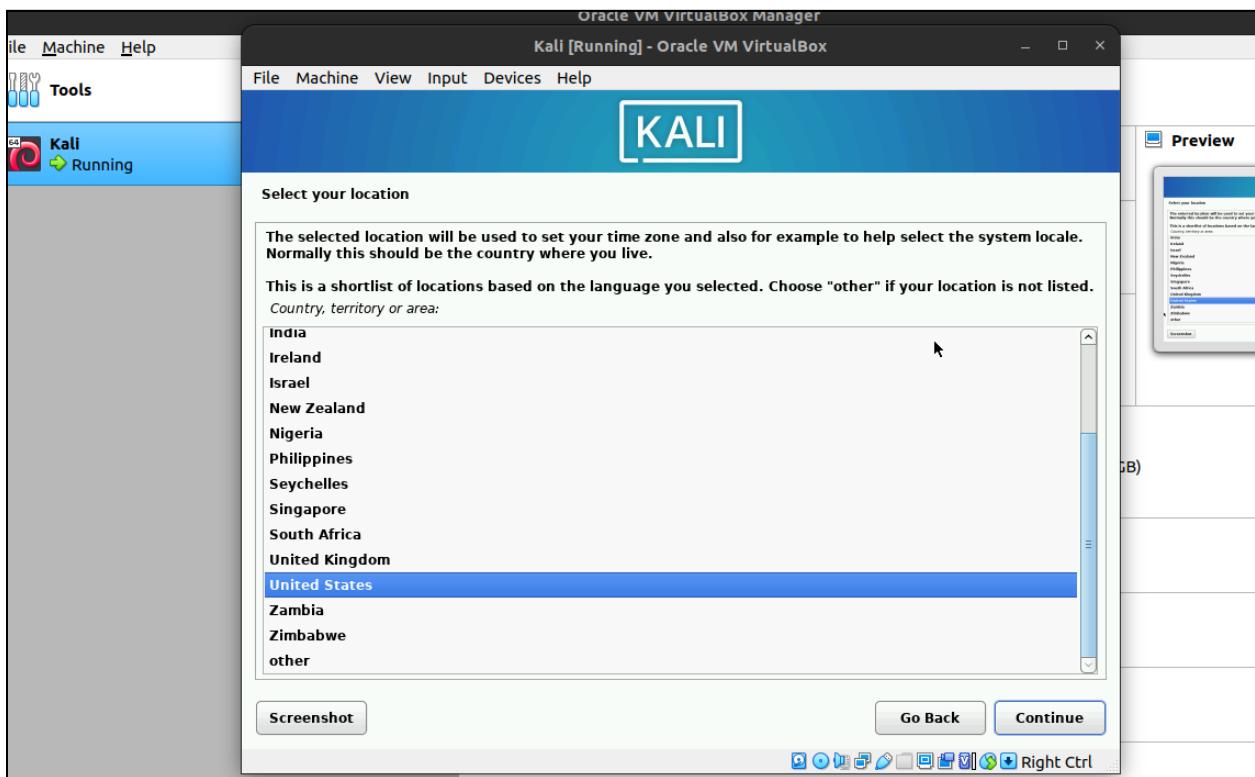
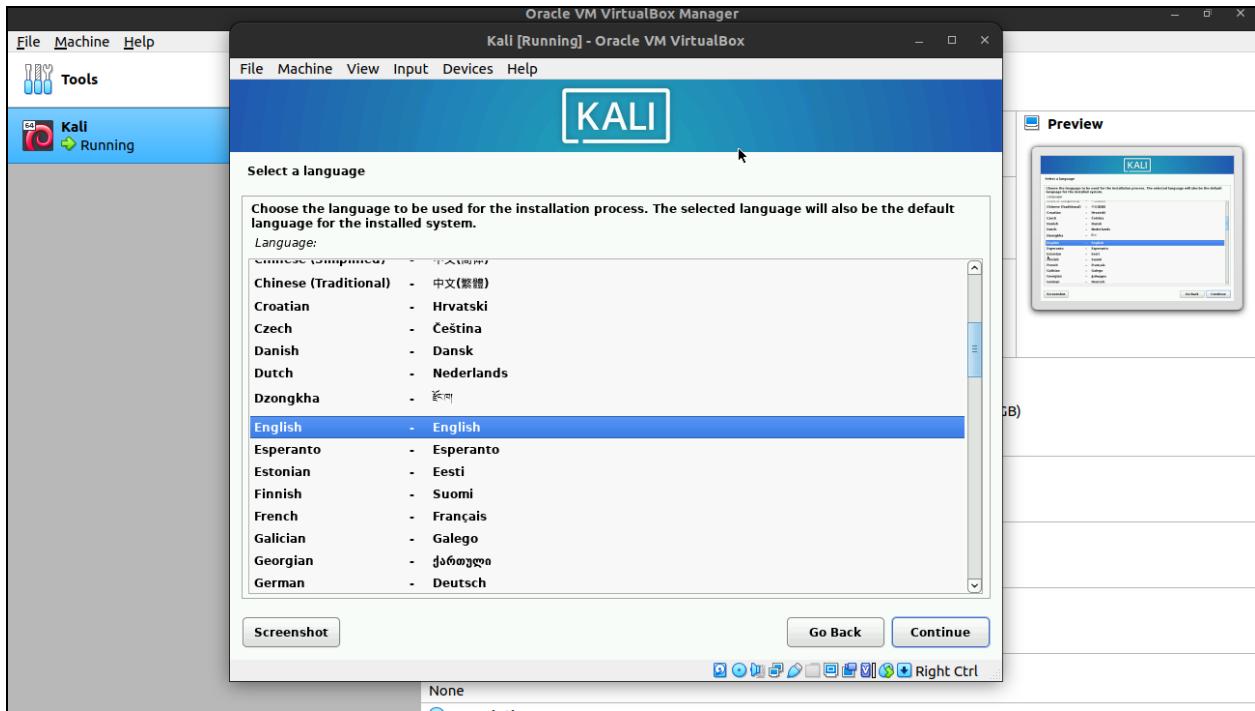


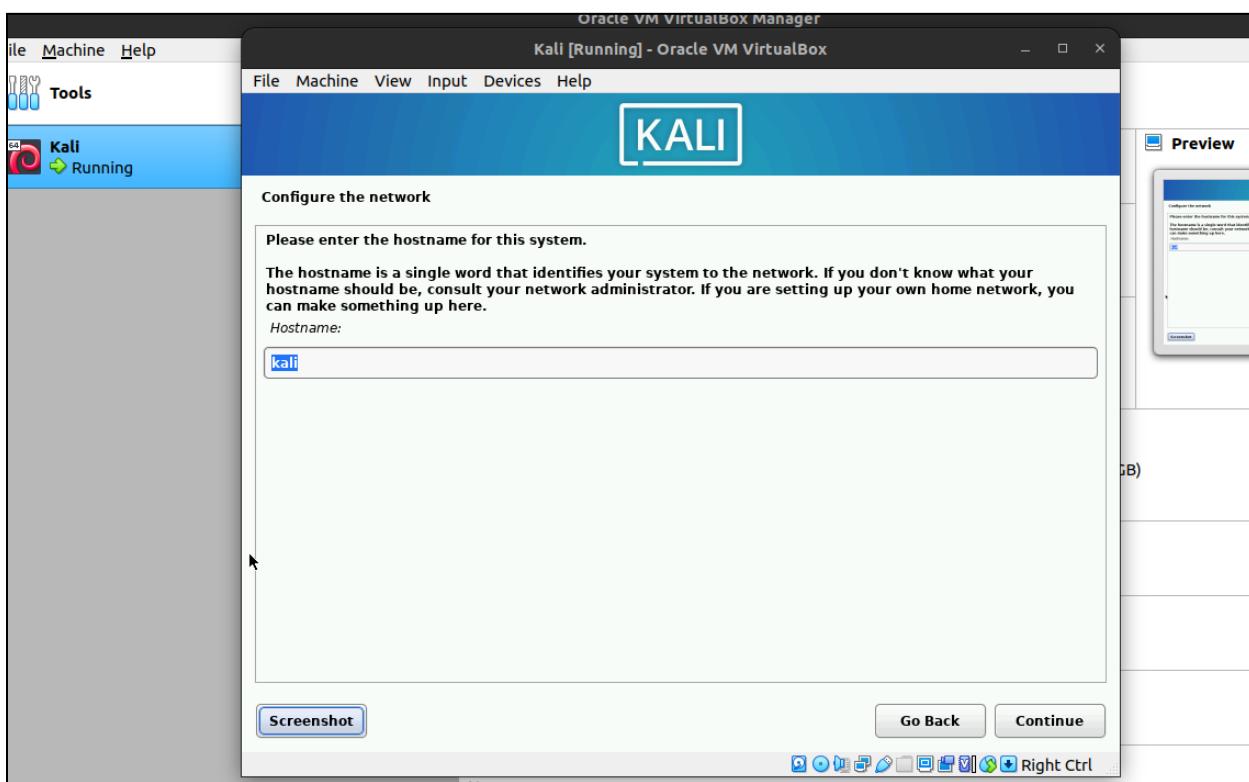
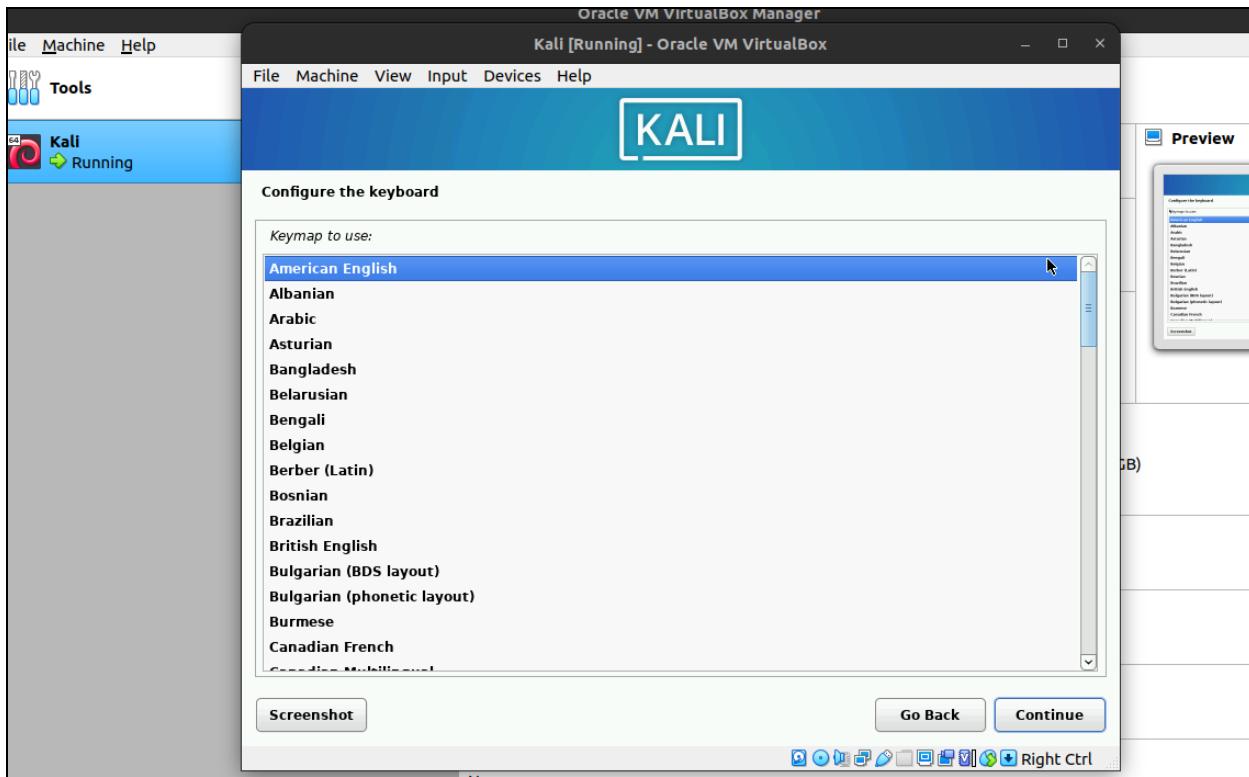


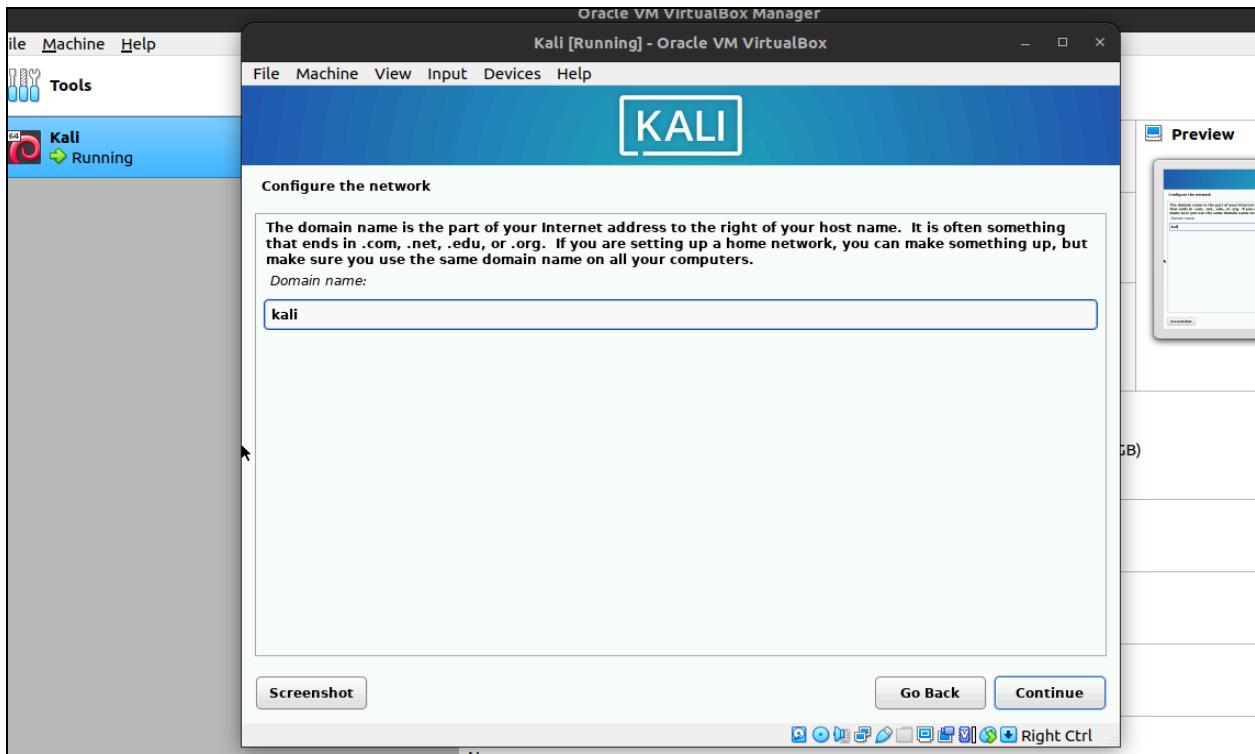


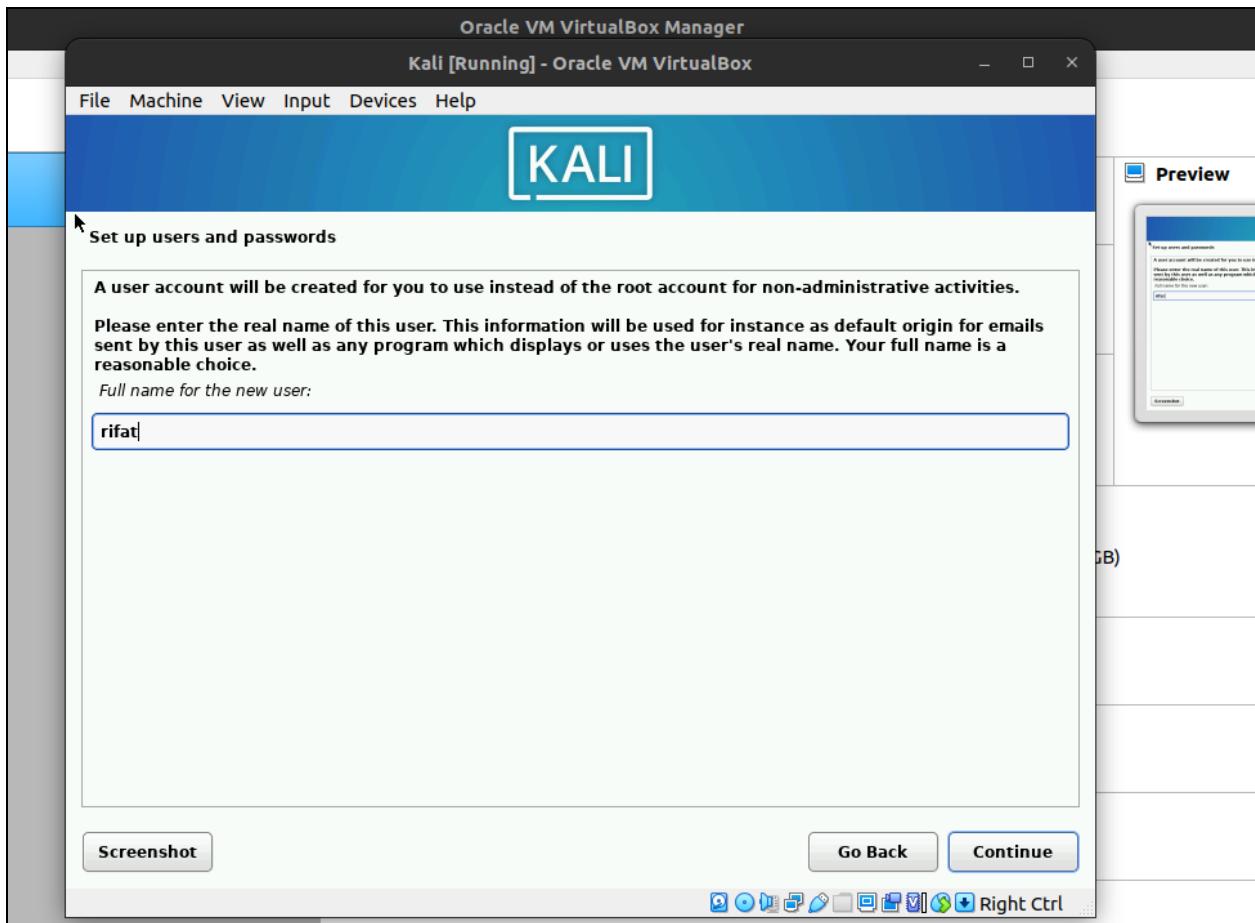


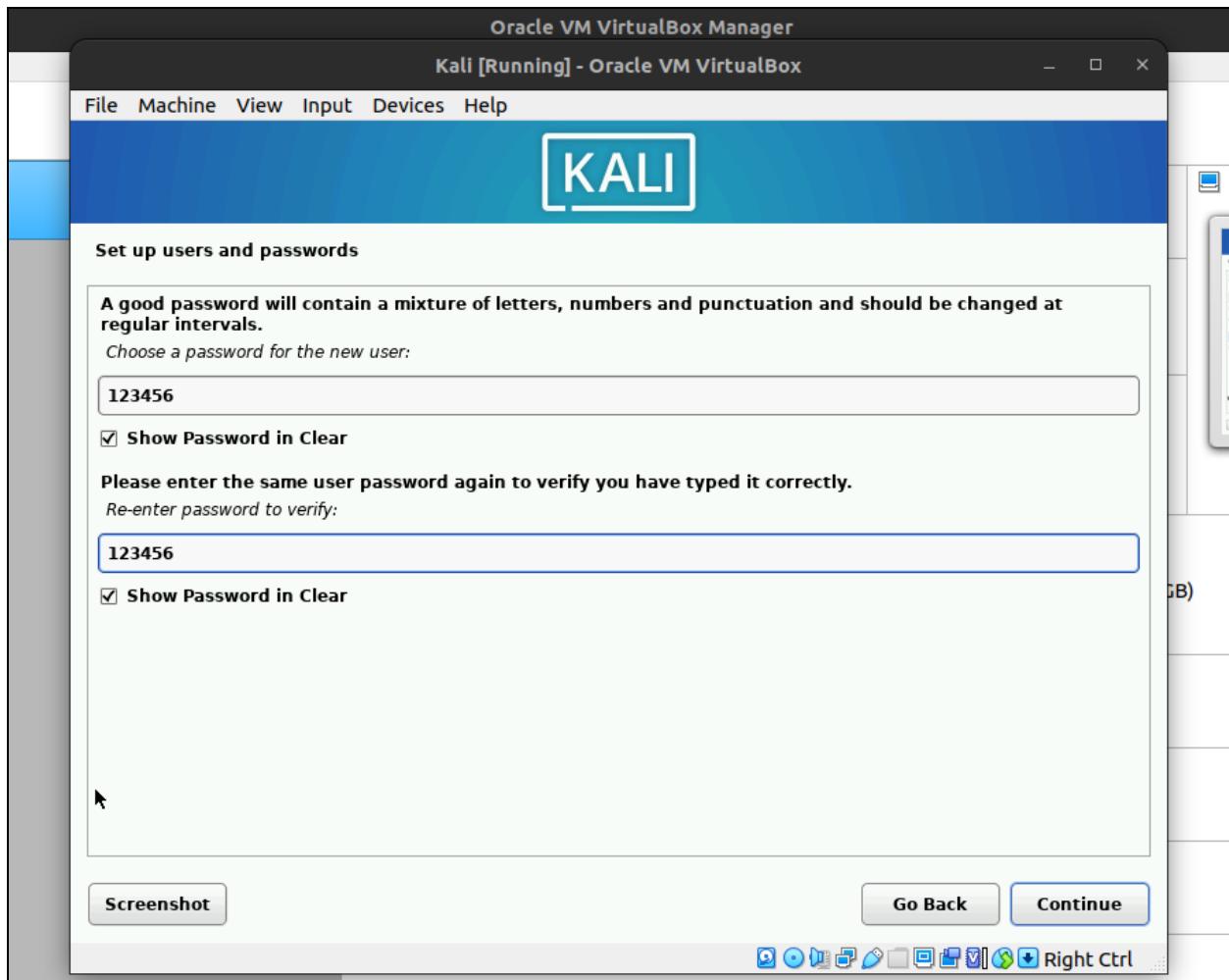


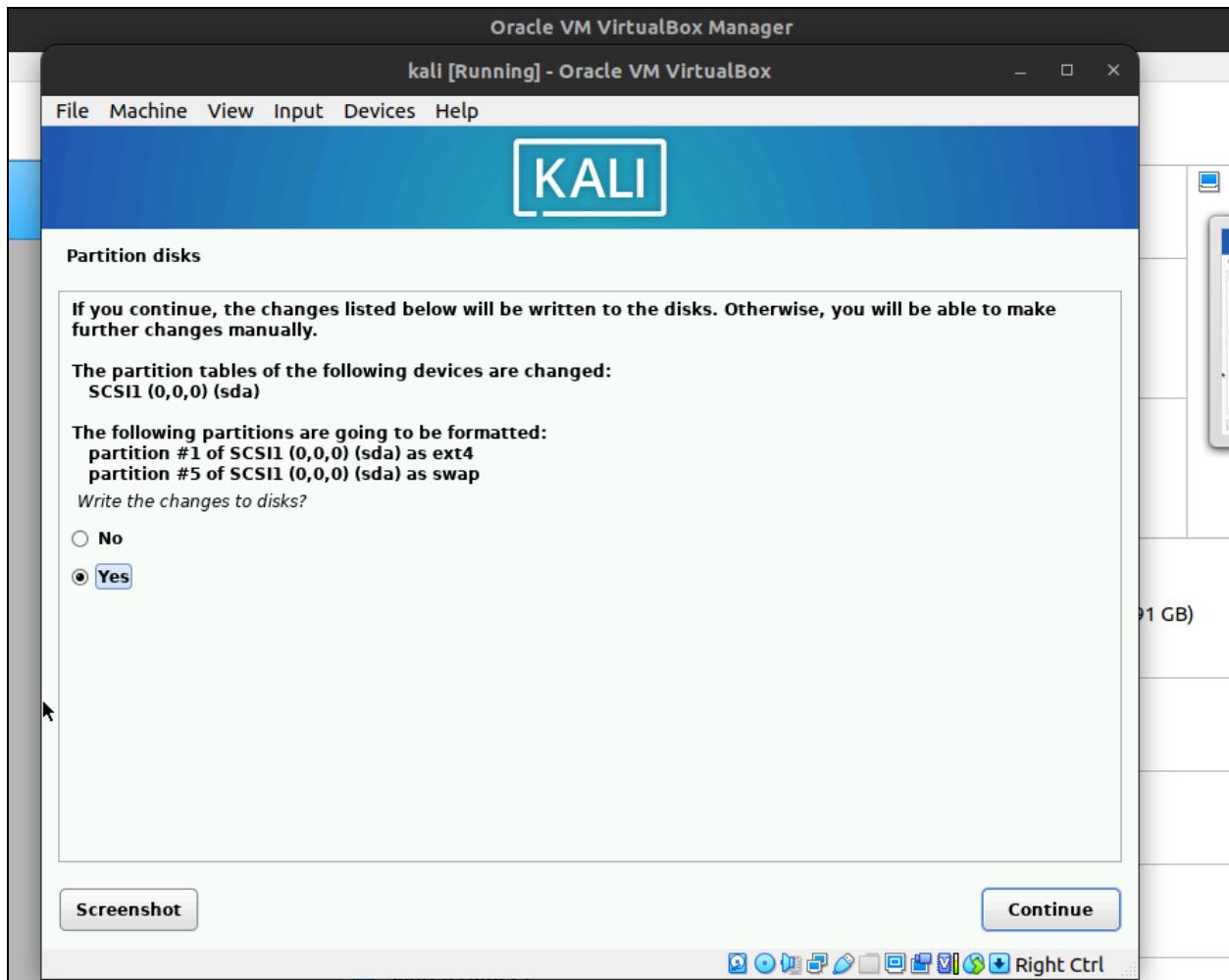


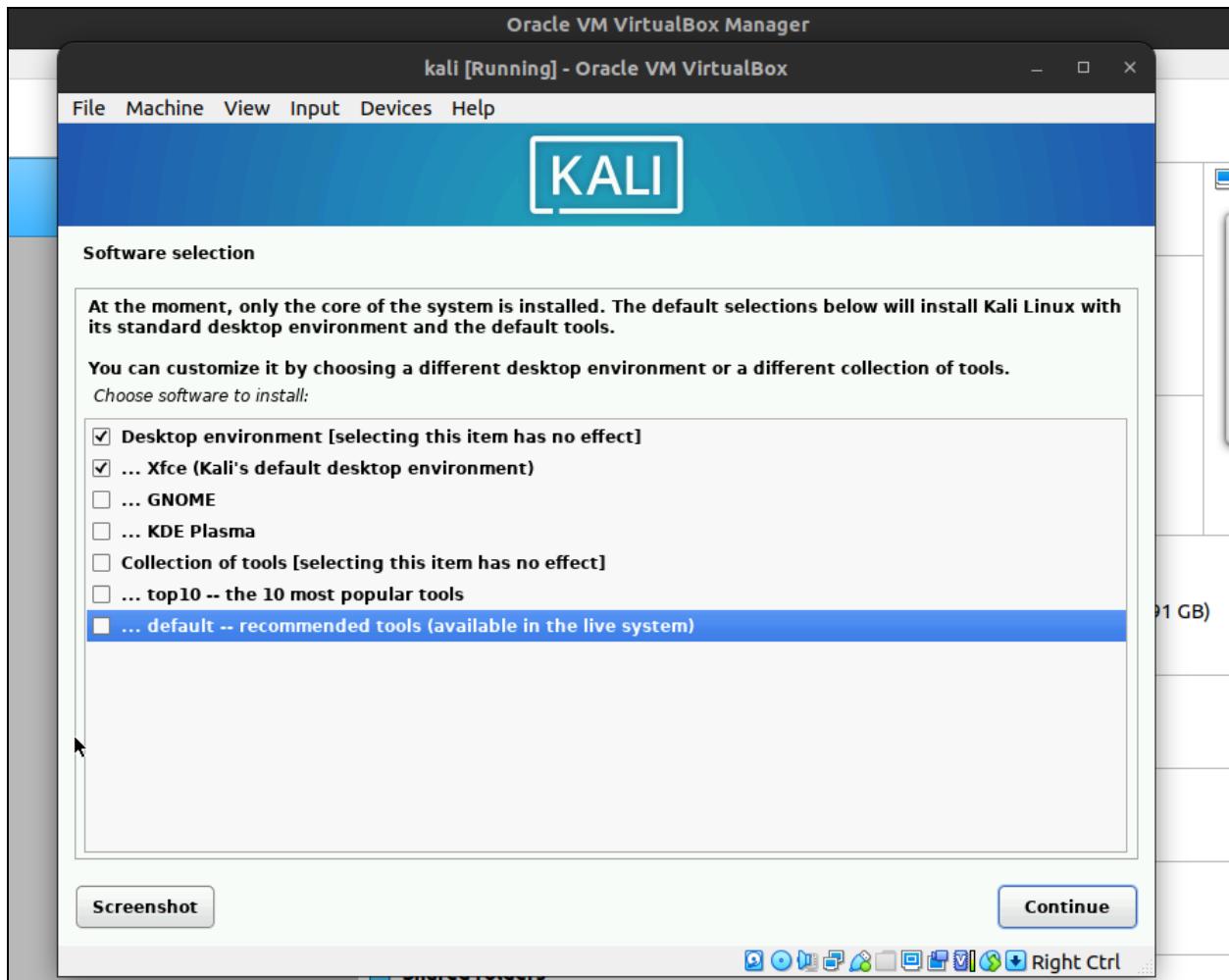


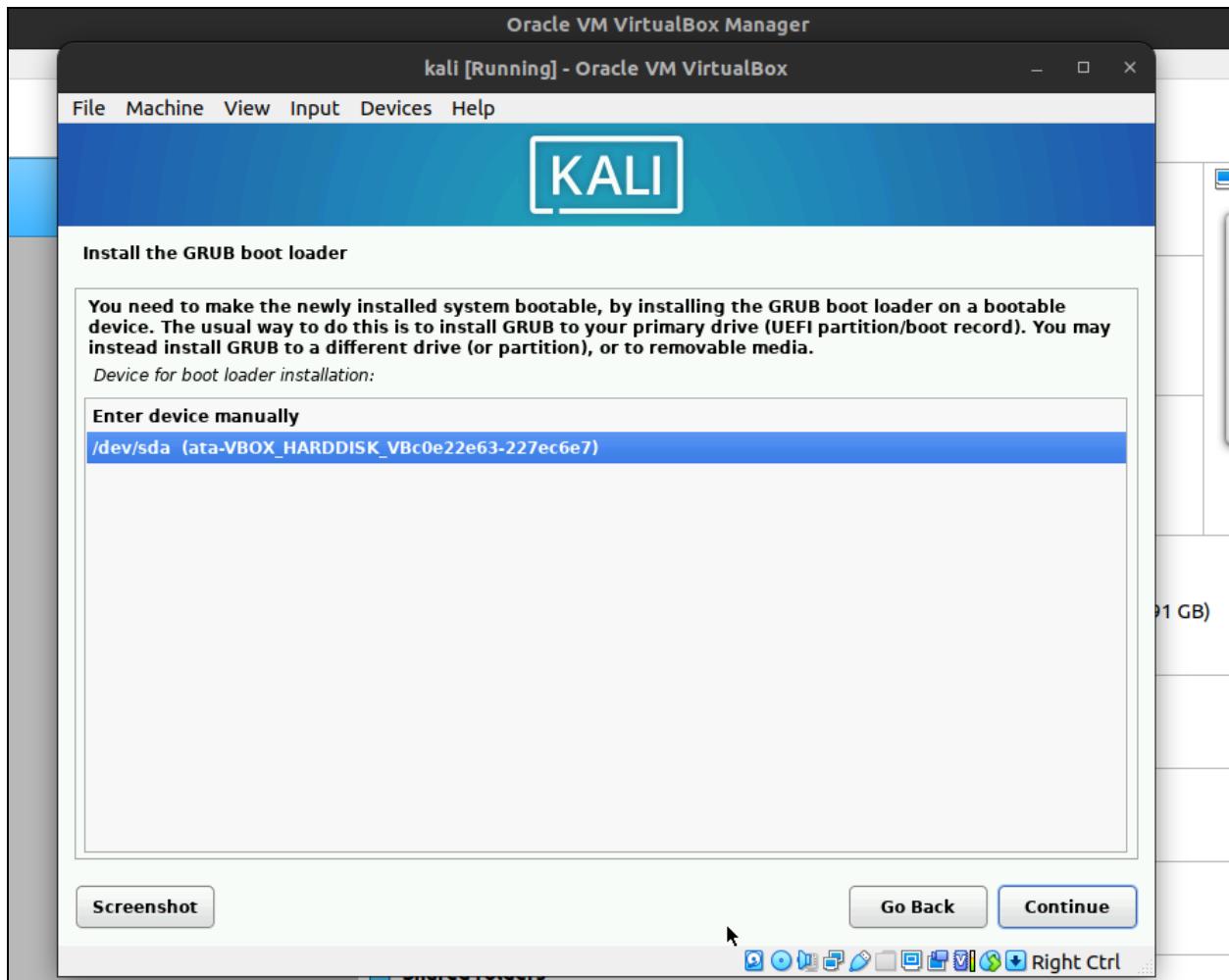


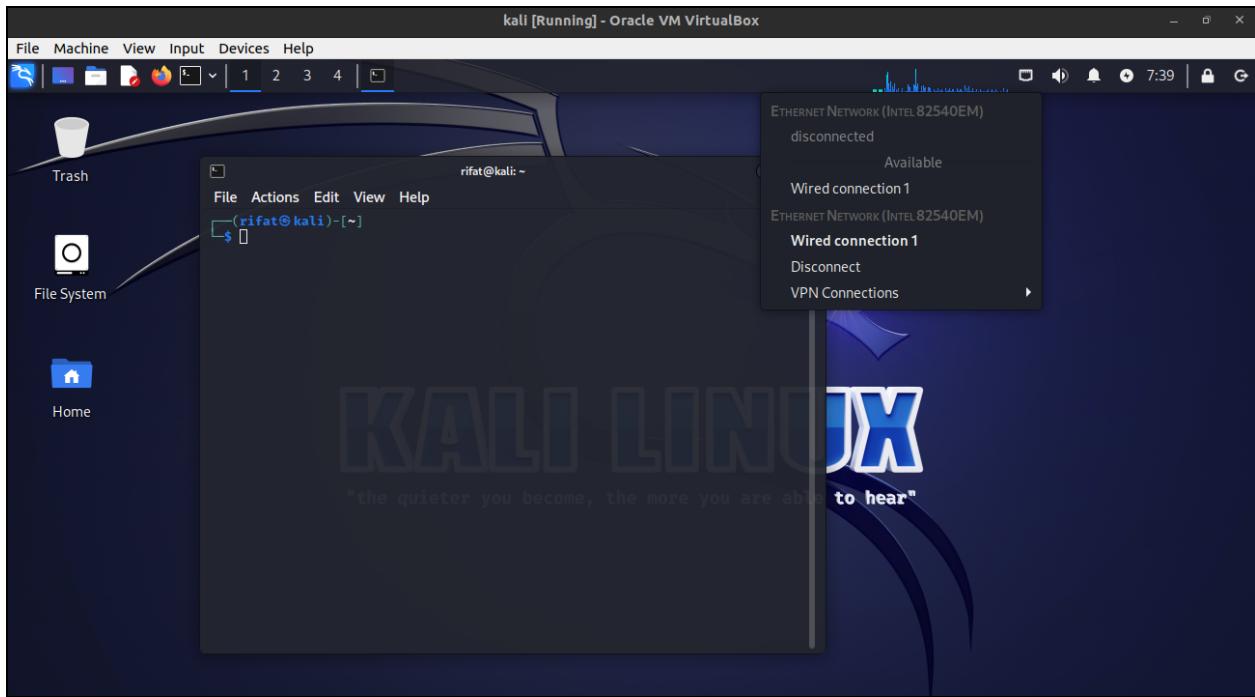




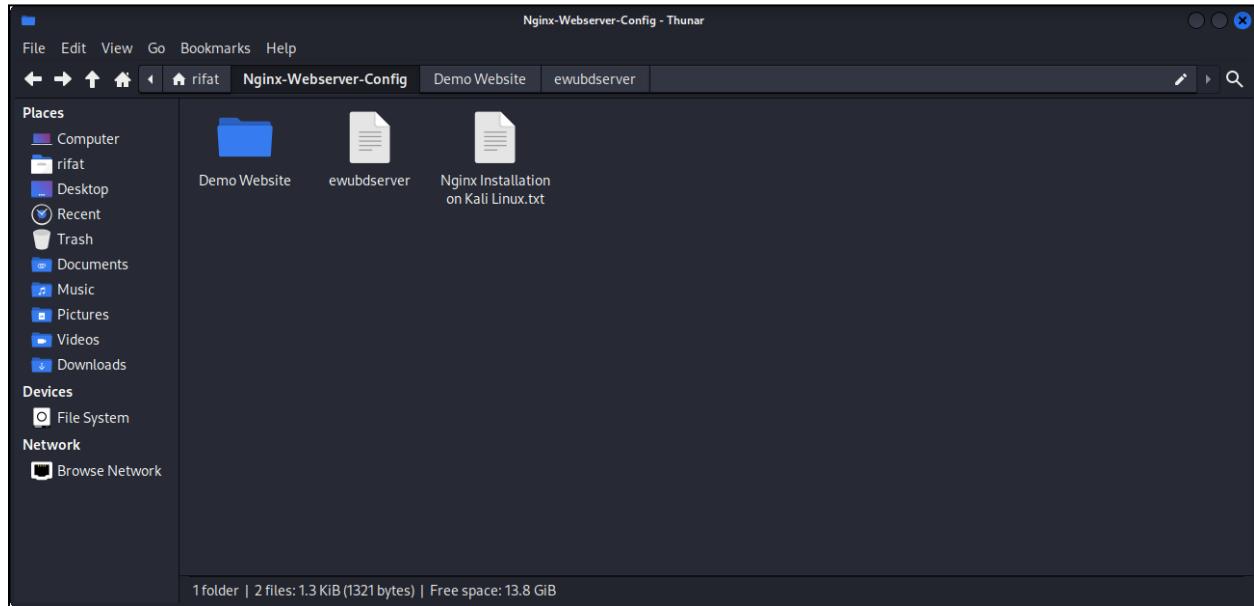








Gedit Text Editor Installation



SSL Certificate Configuration

```
#Bash
#!/bin/bash

# 1. Setting up the directory structure:

mkdir -p
{root-ca,sub-ca,server}/{private,certs,index,serial,pem,crl,csr}
mkdir generated

# Create empty files to track certificate issuance and serial
numbers:
touch root-ca/index/index
touch sub-ca/index/index

# Generate random numbers for unique certificate serial numbers:
openssl rand -hex 16 > root-ca/serial/serial
openssl rand -hex 16 > sub-ca/serial/serial
```

```

# Secure private key directories with read/write/execute
permissions for owner only:
chmod -v 700 {root-ca,sub-ca,server}/private

# Copy configuration files for Root CA and Sub CA:
cp root-ca.conf root-ca
cp sub-ca.conf sub-ca

# 2. Generating Root CA and Sub CA Certificates:

# Generate a strong encryption key (4096 bits) for the Root CA:
openssl genrsa -aes256 -out root-ca/private/ca.key 4096

# Generate a strong encryption key (4096 bits) for the Sub CA:
openssl genrsa -aes256 -out sub-ca/private/sub-ca.key 4096

# Generate a strong encryption key (2048 bits) for the server:
openssl genrsa -out server/private/server.key 2048

# Create a self-signed Root CA certificate valid for 20 years
(7305 days):
openssl req -config root-ca/root-ca.conf -key
root-ca/private/ca.key -new -x509 -days 7305 -sha256 -extensions
v3_ca -out root-ca/certs/ca.crt

# Create a certificate signing request (CSR) for the Sub CA:
openssl req -config sub-ca/sub-ca.conf -new -key
sub-ca/private/sub-ca.key -sha256 -out sub-ca/csr/sub-ca.csr

# Sign the Sub CA CSR using the Root CA, creating a valid Sub CA
certificate for one year (365 days):
openssl ca -config root-ca/root-ca.conf -extensions
v3_intermediate_ca -days 365 -notext -in sub-ca/csr/sub-ca.csr
-out sub-ca/certs/sub-ca.crt

# 3. Generating Server SSL Certificate:

# Create a CSR for the server:
openssl req -key server/private/server.key -new -sha256 -out
server/csr/server.csr

```

```
# Sign the server CSR using the Sub CA, creating a server
certificate valid for one year (365 days):
openssl ca -config sub-ca/sub-ca.conf -extensions server_cert
-days 365 -notext -in server/csr/server.csr -out
server/certs/server.crt

# Create a PKCS#12 (PFX) bundle containing the server's
certificate and private key for easy deployment:
openssl pkcs12 -inkey server/private/server.key -in
server/certs/server.crt -export -out server/certs/server.pfx

# 4. Organizing generated files:

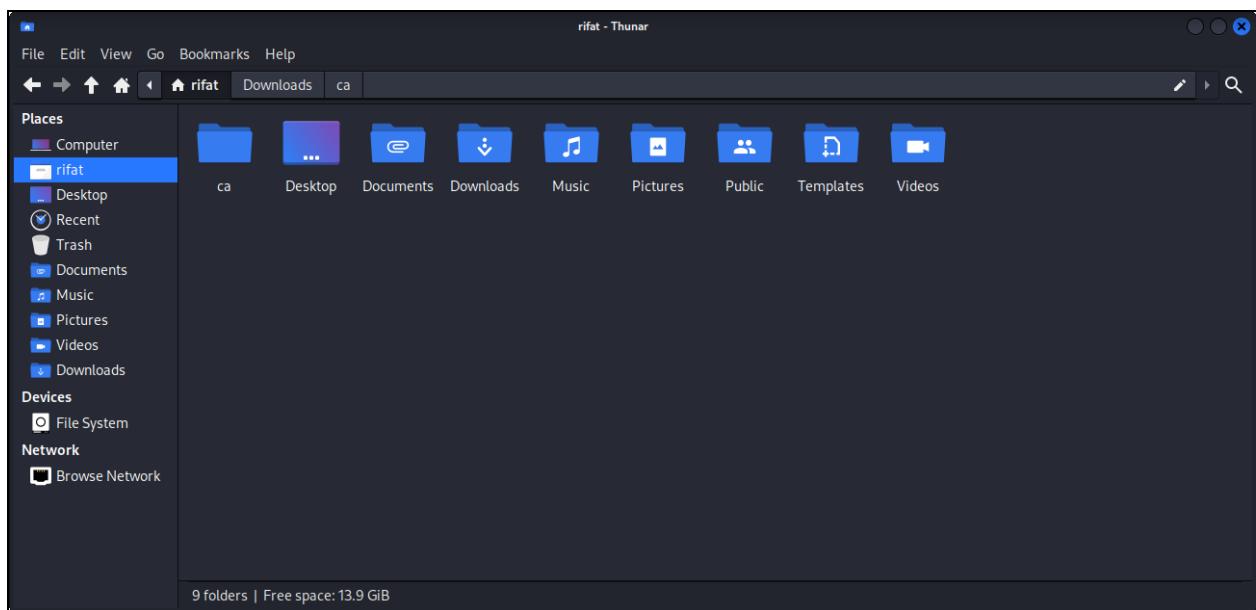
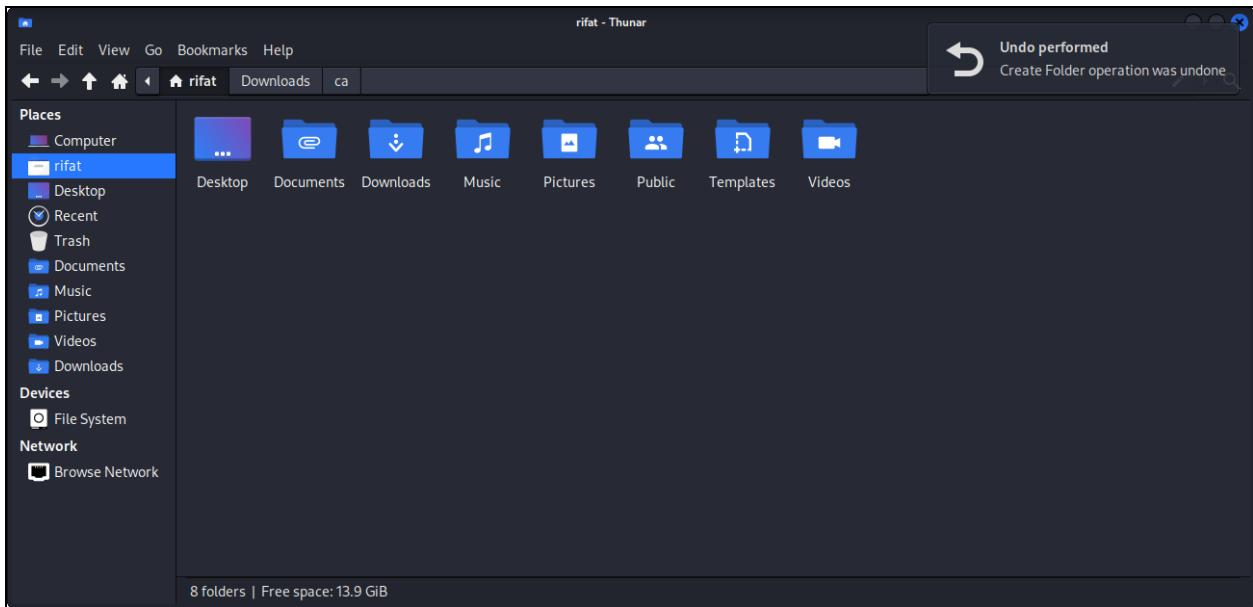
# Copy the Root CA, Sub CA, and server certificates to the
"generated" directory for easy access:
cp root-ca/certs/ca.crt generated
cp sub-ca/certs/sub-ca.crt generated
cp server/certs/server.crt generated

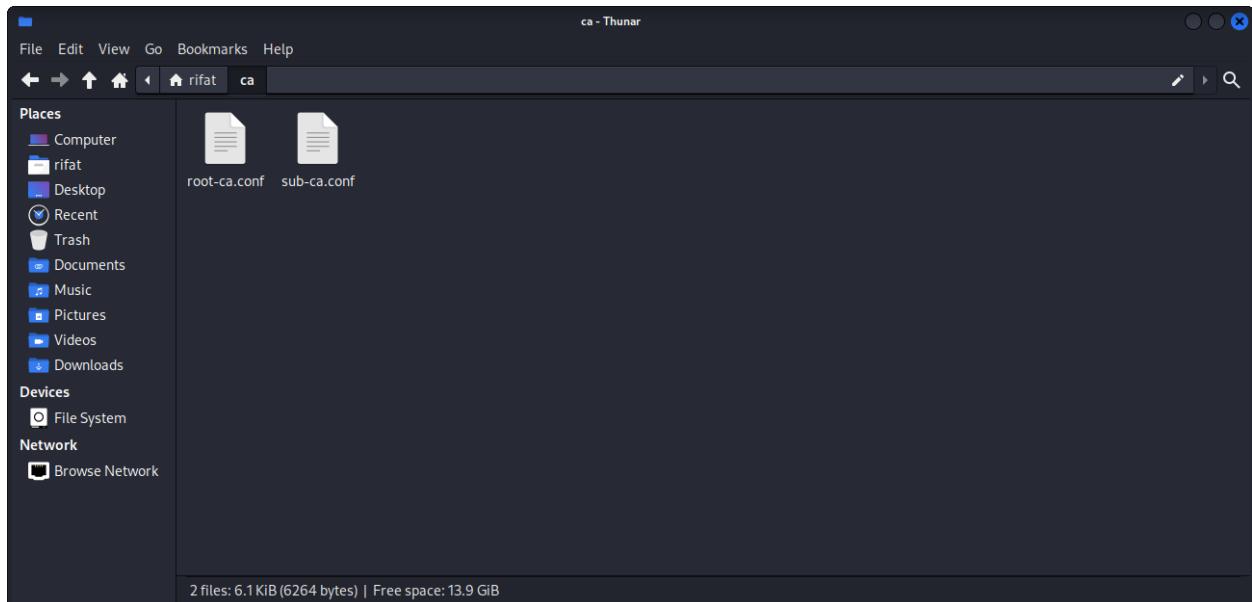
# Copy the server's private key to the "generated" directory:
cp server/private/server.key generated

# Copy the server's PFX bundle to the "generated" directory:
cp server/certs/server.pfx generated

# Move to the "generated" directory and combine the server, Sub
CA, and Root CA certificates into a single file for easier
installation:
cd generated
cat server.crt sub-ca.crt ca.crt > chained.crt

# This script has now generated all the necessary certificates
and organized them for easy deployment.
```





A screenshot of the Mousepad text editor window. The title bar says "~/ca/root-ca.conf - Mousepad". The menu bar includes File, Edit, Search, View, Document, and Help. The toolbar has icons for new, open, save, cut, copy, paste, find, and others. The main text area displays the following configuration file content:

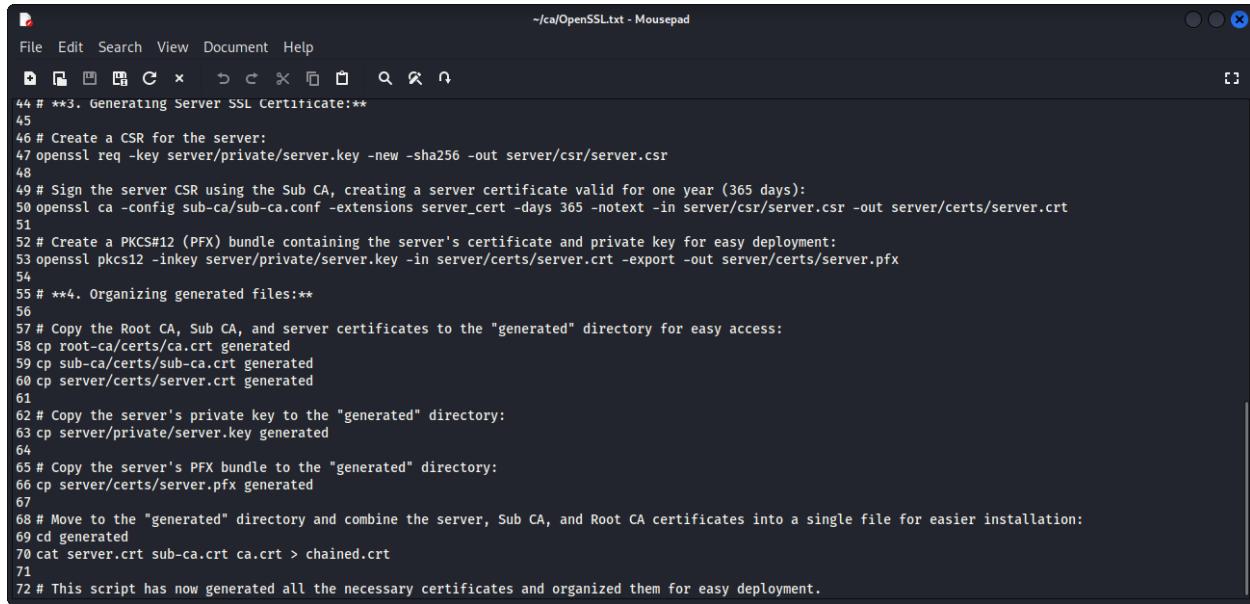
```
1 #root-ca.conf
2 [ca]
3
4 default_ca = CA_default
5
6
7 [CA_default]
8
9 dir = root-ca
10 certs = $dir/certs
11
12 crl_dir = $dir/crl
13
14 new_certs_dir = $dir/pem
15
16 database = $dir/index/index
17
18 serial = $dir/serial/serial
19
20 RANDFILE = $dir/private/.rand
21
22
23
24
25
26 private_key = $dir/private/ca.key
27
28 certificate = $dir/certs/ca.crt
29
```

```
File Edit Search View Document Help  
+/ca/sub-ca.conf - Mousepad  
1 #sub-ca.conf  
2  
3 [ca]  
4 default_ca = CA_default  
5  
6  
7 [CA_default]  
8  
10 dir = sub-ca  
11  
12 certs = $dir/certs  
13 |  
14 crl_dir = $dir/crl  
15  
16 new_certs_dir = $dir/pem  
17  
18 database = $dir/index/index  
19  
20 serial = $dir/serial/serial  
21  
22 RANDFILE = $dir/private/.rand  
23  
24  
25  
26 private_key = $dir/private/sub-ca.key  
27  
28 certificate = $dir/certs/sub-ca.crt  
29
```

```
File Edit Search View Document Help  
+/ca/sub-ca.conf - Mousepad  
1// nsCertType = server  
178 nsComment = "OpenSSL Generated Server Certificate"  
179 subjectKeyIdentifier = hash  
180 authorityKeyIdentifier = keyid,issuer:always  
181 keyUsage = critical, digitalSignature, keyEncipherment  
182 extendedKeyUsage = serverAuth  
183 [ server_cert ]  
184 # Extensions for server certificates  
185 basicConstraints = CA:FALSE  
186 nsCertType = server  
187 nsComment = "OpenSSL Generated Server Certificate"  
188 subjectKeyIdentifier = hash  
189 authorityKeyIdentifier = keyid,issuer:always  
190 keyUsage = critical, digitalSignature, keyEncipherment  
191 extendedKeyUsage = serverAuth  
192 subjectAltName = @alt_names  
193  
194 [alt_names]  
195 DNS.1 = ewubdserver.com  
196 DNS.2 = *.ewubdserver.com  
197 DNS.3 = www.ewubdserver.com  
198  
199  
200  
201  
202  
203  
204  
205
```

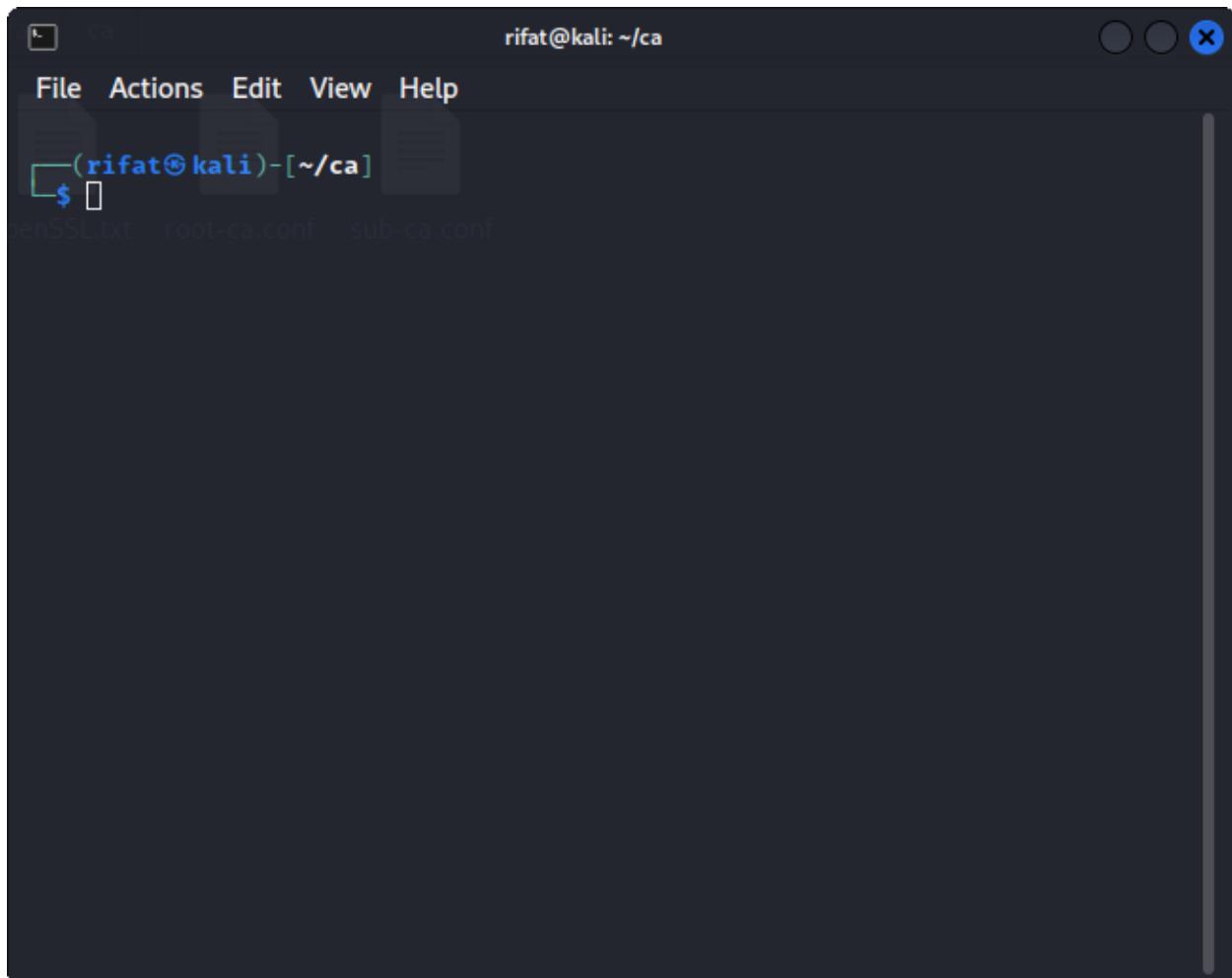
```
File Edit Search View Document Help
+/ca/OpenSSL.txt - Mousepad
1 Bash
2 #!/bin/bash
3
4 # **1. Setting up the directory structure:**
5
6 mkdir -p {root-ca,sub-ca,server}/{private,certs,index,serial,pem,crl,csr}
7 mkdir generated
8
9 # Create empty files to track certificate issuance and serial numbers:
10 touch root-ca/index/index
11 touch sub-ca/index/index
12
13 # Generate random numbers for unique certificate serial numbers:
14 openssl rand -hex 16 > root-ca/serial/serial
15 openssl rand -hex 16 > sub-ca/serial/serial
16
17 # Secure private key directories with read/write/execute permissions for owner only:
18 chmod -v 700 ca/{root-ca,sub-ca,server}/private
19
20 # Copy configuration files for Root CA and Sub CA:
21 cp root-ca.conf root-ca
22 cp sub-ca.conf sub-ca
23
24 # **2. Generating Root CA and Sub CA Certificates:**
25
26 # Generate a strong encryption key (4096 bits) for the Root CA:
27 openssl genrsa -aes256 -out root-ca/private/ca.key 4096
28
29 # Generate a strong encryption key (4096 bits) for the Sub CA:
30 openssl genrsa -aes256 -out sub-ca/private/sub-ca.key 4096
31
32 # Generate a strong encryption key (2048 bits) for the server:
33 openssl genrsa -out server/private/server.key 2048
34
35 # Create a self-signed Root CA certificate valid for 20 years (7305 days):
36 openssl req -config root-ca/root-ca.conf -key root-ca/private/ca.key -new -x509 -days 7305 -sha256 -extensions v3_ca -out root-ca/certs/ca.crt
37
38 # Create a certificate signing request (CSR) for the Sub CA:
39 openssl req -config sub-ca/sub-ca.conf -new -key sub-ca/private/sub-ca.key -sha256 -out sub-ca/csr/sub-ca.csr
40
41 # Sign the Sub CA CSR using the Root CA, creating a valid Sub CA certificate for one year (365 days):
42 openssl ca -config root-ca/root-ca.conf -extensions v3_intermediate_ca -days 365 -notext -in sub-ca/csr/sub-ca.csr -out sub-ca/certs/sub-ca.crt
43
44 # **3. Generating Server SSL Certificate:**
45
46 # Create a CSR for the server:
47 openssl req -key server/private/server.key -new -sha256 -out server/csr/server.csr
48
49 # Sign the server CSR using the Sub CA, creating a server certificate valid for one year (365 days):
50 openssl ca -config sub-ca/sub-ca.conf -extensions server_cert -days 365 -notext -in server/csr/server.csr -out server/certs/server.crt
```

```
File Edit Search View Document Help
+/ca/OpenSSL.txt - Mousepad
22 cp sub-ca.conf sub-ca
23
24 # **2. Generating Root CA and Sub CA Certificates:**
25
26 # Generate a strong encryption key (4096 bits) for the Root CA:
27 openssl genrsa -aes256 -out root-ca/private/ca.key 4096
28
29 # Generate a strong encryption key (4096 bits) for the Sub CA:
30 openssl genrsa -aes256 -out sub-ca/private/sub-ca.key 4096
31
32 # Generate a strong encryption key (2048 bits) for the server:
33 openssl genrsa -out server/private/server.key 2048
34
35 # Create a self-signed Root CA certificate valid for 20 years (7305 days):
36 openssl req -config root-ca/root-ca.conf -key root-ca/private/ca.key -new -x509 -days 7305 -sha256 -extensions v3_ca -out root-ca/certs/ca.crt
37
38 # Create a certificate signing request (CSR) for the Sub CA:
39 openssl req -config sub-ca/sub-ca.conf -new -key sub-ca/private/sub-ca.key -sha256 -out sub-ca/csr/sub-ca.csr
40
41 # Sign the Sub CA CSR using the Root CA, creating a valid Sub CA certificate for one year (365 days):
42 openssl ca -config root-ca/root-ca.conf -extensions v3_intermediate_ca -days 365 -notext -in sub-ca/csr/sub-ca.csr -out sub-ca/certs/sub-ca.crt
43
44 # **3. Generating Server SSL Certificate:**
45
46 # Create a CSR for the server:
47 openssl req -key server/private/server.key -new -sha256 -out server/csr/server.csr
48
49 # Sign the server CSR using the Sub CA, creating a server certificate valid for one year (365 days):
50 openssl ca -config sub-ca/sub-ca.conf -extensions server_cert -days 365 -notext -in server/csr/server.csr -out server/certs/server.crt
```



The screenshot shows a terminal window titled "Mousepad" with the file path "/ca/OpenSSL.txt". The content of the file is a shell script for generating SSL certificates. The script includes comments, command-line arguments, and file paths related to OpenSSL operations like generating a CSR, signing it with a CA, and creating a PKCS#12 bundle.

```
44 # **3. Generating Server SSL Certificate:**  
45  
46 # Create a CSR for the server:  
47 openssl req -key server/private/server.key -new -sha256 -out server/csr/server.csr  
48  
49 # Sign the server CSR using the Sub CA, creating a server certificate valid for one year (365 days):  
50 openssl ca -config sub-ca/sub-ca.conf -extensions server_cert -days 365 -notext -in server/csr/server.csr -out server/certs/server.crt  
51  
52 # Create a PKCS#12 (PFX) bundle containing the server's certificate and private key for easy deployment:  
53 openssl pkcs12 -inkey server/private/server.key -in server/certs/server.crt -export -out server/certs/server.pfx  
54  
55 # **4. Organizing generated files:**  
56  
57 # Copy the Root CA, Sub CA, and server certificates to the "generated" directory for easy access:  
58 cp root-ca/certs/ca.crt generated  
59 cp sub-ca/certs/sub-ca.crt generated  
60 cp server/certs/server.crt generated  
61  
62 # Copy the server's private key to the "generated" directory:  
63 cp server/private/server.key generated  
64  
65 # Copy the server's PFX bundle to the "generated" directory:  
66 cp server/certs/server.pfx generated  
67  
68 # Move to the "generated" directory and combine the server, Sub CA, and Root CA certificates into a single file for easier installation:  
69 cd generated  
70 cat server.crt sub-ca.crt ca.crt > chained.crt  
71  
72 # This script has now generated all the necessary certificates and organized them for easy deployment.
```



The screenshot shows a terminal window with the title bar "rifat@kali: ~/ca". The window displays a file tree and a command line interface. The file tree shows files like "OpenSSL.txt", "root-ca.conf", and "sub-ca.conf". The command line shows the user's prompt "(rifat㉿kali)-[~/ca]".

rifat@kali: ~/ca

```
File Actions Edit View Help Help
(rifat@kali)-[~/ca]
$ sudo apt install tree
[sudo] password for rifat:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages will be upgraded:
  tree          OpenSSL1.0.2-root-ca.conf  sub-ca.conf
1 upgraded, 0 newly installed, 0 to remove and 668 not upgraded.
Need to get 54.6 kB of archives.
After this operation, 0 B of additional disk space will be used.
Get:1 http://kali.cs.nycu.edu.tw/kali kali-rolling/main amd64 tree amd64 2.1.1-2 [54.6 kB]
Fetched 54.6 kB in 2s (24.7 kB/s)
(Reading database ... 143684 files and directories currently installed.)
Preparing to unpack .../tree_2.1.1-2_amd64.deb ...
Unpacking tree (2.1.1-2) over (2.1.1-1) ...
Setting up tree (2.1.1-2) ...
Processing triggers for man-db (2.11.2-3) ...
[ Downloads
  Devices
    File System
  Network
    Browse Network

Progress: [ 80%] [#########################################.....] 3 files, 9.2 KB (9419 bytes) | Free space: 13.9 GB
```

```
rifat@kali: ~/ca
File Actions Edit View Help Help
Reading state information ... Done
The following packages will be upgraded:
  tree
1 upgraded, 0 newly installed, 0 to remove and 668 not upgraded.
Need to get 54.6 kB of archives.
After this operation, 0 B of additional disk space will be used.
Get:1 http://kali.cs.nycu.edu.tw/kali kali-rolling/main amd64 tree amd64 2.1.
1-2 [54.6 kB]          OpenSSLBt root-ca.conf sub-ca.conf
Fetched 54.6 kB in 2s (24.7 kB/s)
(Reading database ... 143684 files and directories currently installed.)
Preparing to unpack .../tree_2.1.1-2_amd64.deb ...
Unpacking tree (2.1.1-2) over (2.1.1-1) ...
Setting up tree (2.1.1-2) ...
Processing triggers for man-db (2.11.2-3) ...
Processing triggers for kali-menu (2023.4.3) ...

└─(rifat㉿kali)-[~/ca]
$ sudo apt install openssl
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following additional packages will be installed:
  libssl3
The following packages will be upgraded:
  libssl3 openssl
2 upgraded, 0 newly installed, 0 to remove and 666 not upgraded.
Need to get 3432 kB of archives.
After this operation, 43.0 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://kali.cs.nycu.edu.tw/kali kali-rolling/main amd64 libssl3 amd64 3
.0.11-1 [2016 kB]
Get:2 http://kali.cs.nycu.edu.tw/kali kali-rolling/main amd64 openssl amd64 3
.0.11-1 [1416 kB]
57% [2 openssl 0 B/1416 kB 0%] 3 files, 32 kB (9419 bytes) | Free space: 13.9 GiB
```

```
rifat@kali: ~/ca
File Actions Edit View Help
Places
Computer
Documents
Downloads
Pictures
Videos
OpenSSL
-(rifat@kali)-[~/ca]
$ mkdir -p {root-ca,sub-ca,server}/{private,certs,index,serial,pem,crl,csr}
-(rifat@kali)-[~/ca]
$ mkdir generated
-(rifat@kali)-[~/ca]
$ touch root-ca/index/index
-(rifat@kali)-[~/ca]
$ touch sub-ca/index/index
-(rifat@kali)-[~/ca]
$ openssl rand -hex 16 > root-ca/serial/serial
-(rifat@kali)-[~/ca]
$ openssl rand -hex 16 > sub-ca/serial/serial
-(rifat@kali)-[~/ca]
$ chmod -v 700 ca/{root-ca,sub-ca,server}/private
chmod: cannot access 'ca/root-ca/private': No such file or directory
'ca/root-ca/private' could not be accessed
chmod: cannot access 'ca/sub-ca/private': No such file or directory
'ca/sub-ca/private' could not be accessed
chmod: cannot access 'ca/server/private': No such file or directory
'ca/server/private' could not be accessed
-(rifat@kali)-[~/ca]
$ 
```

4 folders | 3 files: 9.2 KiB (9419 bytes) | Free space: 13.9 GiB

rifat@kali: ~/ca

```
File Actions Edit View Help Help

(rifat@kali)-[~/ca]
$ chmod -v 700 {root-ca,sub-ca,server}/private
mode of 'root-ca/private' changed from 0755 (rwxr-xr-x) to 0700 (rwx-----)
mode of 'sub-ca/private' changed from 0755 (rwxr-xr-x) to 0700 (rwx-----)
mode of 'server/private' changed from 0755 (rwxr-xr-x) to 0700 (rwx-----)

(rifat@kali)-[~/ca] generated root-ca server sub-ca OpenSSL
$ cp root-ca.conf root-ca

(rifat@kali)-[~/ca]
$ cp sub-ca.conf sub-ca

(rifat@kali)-[~/ca]
$ 

Music
Pictures
Videos
Downloads

Devices
File System

Network
Browse Network

4 folders | 3 files: 9.2 KiB (9419 bytes) | Free space: 13.9 GiB
```

```
rifat@kali: ~/ca
File Actions Edit View Help Help

(rifat@kali)-[~/ca]
$ chmod -v 700 {root-ca,sub-ca,server}/private
mode of 'root-ca/private' changed from 0755 (rwxr-xr-x) to 0700 (rwx-----)
mode of 'sub-ca/private' changed from 0755 (rwxr-xr-x) to 0700 (rwx-----)
mode of 'server/private' changed from 0755 (rwxr-xr-x) to 0700 (rwx-----)

(rifat@kali)-[~/ca] generated root-ca server sub-ca OpenSSL
$ cp root-ca.conf root-ca

(rifat@kali)-[~/ca]
$ cp sub-ca.conf sub-ca

(rifat@kali)-[~/ca]
$ openssl genrsa -aes256 -out root-ca/private/ca.key 4096
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:

(rifat@kali)-[~/ca]
$ openssl genrsa -aes256 -out sub-ca/private/sub-ca.key 4096
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:

(rifat@kali)-[~/ca]
$ openssl genrsa -out server/private/server.key 2048

(rifat@kali)-[~/ca]
$ 
```

4 folders | 3 files: 9.2 KiB (9419 bytes) | Free space: 13.9 GiB

rifat@kali: ~/ca

File Actions Edit View Help Help

```
└─(rifat㉿kali)-[~/ca]
$ openssl req -config root-ca/root-ca.conf -key root-ca/private/ca.key -new
-x509 -days 7305 -sha256 -extensions v3_ca -out root-ca/certs/ca.crt
Enter pass phrase for root-ca/private/ca.key:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
Country Name (2 letter code) [BD]:
State or Province Name [DHK]:
Locality Name [RAMPURA]:
Organization Name [EWUBD]:
Organizational Unit Name [ADMIN]:
Common Name [rootCA]:
Email Address []:
└── Downloads
└─(rifat㉿kali)-[~/ca]
$ [ ]
```

File System

Network

Browse Network

4 folders | 3 files: 9.2 KiB (9419 bytes) | Free space: 13.9 GiB

```
rifat@kali: ~/ca
File Actions Edit View Help Help

What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.

Country Name (2 letter code) [BD]: 
State or Province Name [DHK]: 
Locality Name [RAMPURA]: 
Organization Name [EWUBD]: 
Organizational Unit Name [ADMIN]: 
Common Name [rootCA]: 
Email Address []:

└─(rifat㉿kali)-[~/ca]
$ openssl req -config sub-ca/sub-ca.conf -new -key sub-ca/private/sub-ca.key -sha256 -out sub-ca/csr/sub-ca.csr
Enter pass phrase for sub-ca/private/sub-ca.key:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.

Country Name (2 letter code) [BD]: 
State or Province Name [DHK]: 
Locality Name [RAMPURA]: 
Organization Name [EWUBD]: 
Organizational Unit Name [SUBADMIN]: 
Common Name [subCA]: 
Email Address []:

└─(rifat㉿kali)-[~/ca]
$ 
```

```
rifat@kali: ~/ca
└─(rifat㉿kali)-[~/ca]
$ openssl ca -config root-ca/root-ca.conf -extensions v3_intermediate_ca -days 365 -notext -in sub-ca/csr/sub-ca.csr -out sub-ca/certs/sub-ca.crt
Using configuration from root-ca/root-ca.conf
Enter pass phrase for root-ca/private/ca.key:
Check that the request matches the signature
Signature ok
Certificate Details:
    Serial Number: 87:4a:28:87:05:e6:66:ca:9e:8e:9d:2b:9f:95:ad:18
    Validity
        Not Before: Dec 24 13:13:13 2023 GMT
        Not After : Dec 23 13:13:13 2024 GMT
    Subject:
        countryName = BD
        stateOrProvinceName = DHK
        organizationName = EWUBD
        organizationalUnitName = SUBADMIN
        commonName = subCA
    X509v3 extensions:
        X509v3 Subject Key Identifier:
        Devices DD:ED:DD:AC:0F:3B:0A:B1:20:37:B1:B8:D9:64:C8:4E:AD:37:BE:3C
        X509v3 Authority Key Identifier:
        File System B4:7A:60:39:9B:06:27:E9:3C:F6:76:EA:81:99:28:DE:E2:EB:75:07
        Network X509v3 Basic Constraints: critical
            CA:TRUE, pathlen:0
        Browser X509v3 Key Usage: critical
            Digital Signature, Certificate Sign, CRL Sign
Certificate is to be certified until Dec 23 13:13:13 2024 GMT (365 days)
Sign the certificate? [y/n]:y

1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
4 folders | 3 files: 9.2 KiB (9419 bytes) | Free space: 13.9 GiB
```

```
rifat@kali: ~/ca
File Actions Edit View Help Help
X509v3 Key Usage: critical
Digital Signature, Certificate Sign, CRL Sign
Certificate is to be certified until Dec 23 13:13:13 2024 GMT (365 days)
Sign the certificate? [y/n]:y
Computer root-ca server sub-ca OpenSSL.txt
1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Database updated
Recent
(rifat@kali)-[~/ca]
$ openssl req -key server/private/server.key -new -sha256 -out server/csr/server.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.

Country Name (2 letter code) [AU]:BD
State or Province Name (full name) [Some-State]:DHK
Locality Name (eg, city) []:RAMPURA
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Server Ltd
Organizational Unit Name (eg, section) []:ADMIN
Common Name (e.g. server FQDN or YOUR name) []:www.ewubdserver.com
Email Address []:rifat39200@gmail.com
Browse Network
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:123456
An optional company name []:Server Ltd

(rifat@kali)-[~/ca]
$ 
```

rifat@kali: ~/ca

File Actions Edit View Help Help

```
1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Database updated

[(rifat㉿kali)-[~/ca]]
$ openssl pkcs12 -inkey server/private/server.key -in server/certs/server.crt -export
-out server/certs/server.pfx generated
root-ca server sub-ca chained.crt
Enter Export Password:
Verifying - Enter Export Password:

[(rifat㉿kali)-[~/ca]]
$ cp root-ca/certs/ca.crt generated
Documents Pictures Downloads
[(rifat㉿kali)-[~/ca]]
$ cp sub-ca/certs/sub-ca.crt generated
[(rifat㉿kali)-[~/ca]]
$ cp server/certs/server.crt generated
[(rifat㉿kali)-[~/ca]]
$ cp server/private/server.key generated
[(rifat㉿kali)-[~/ca]]
$ cp server/certs/server.pfx generated
[(rifat㉿kali)-[~/ca]]
$ cat server.crt sub-ca.crt ca.crt > chained.crt
cat: server.crt: No such file or directory
cat: sub-ca.crt: No such file or directory
cat: ca.crt: No such file or directory

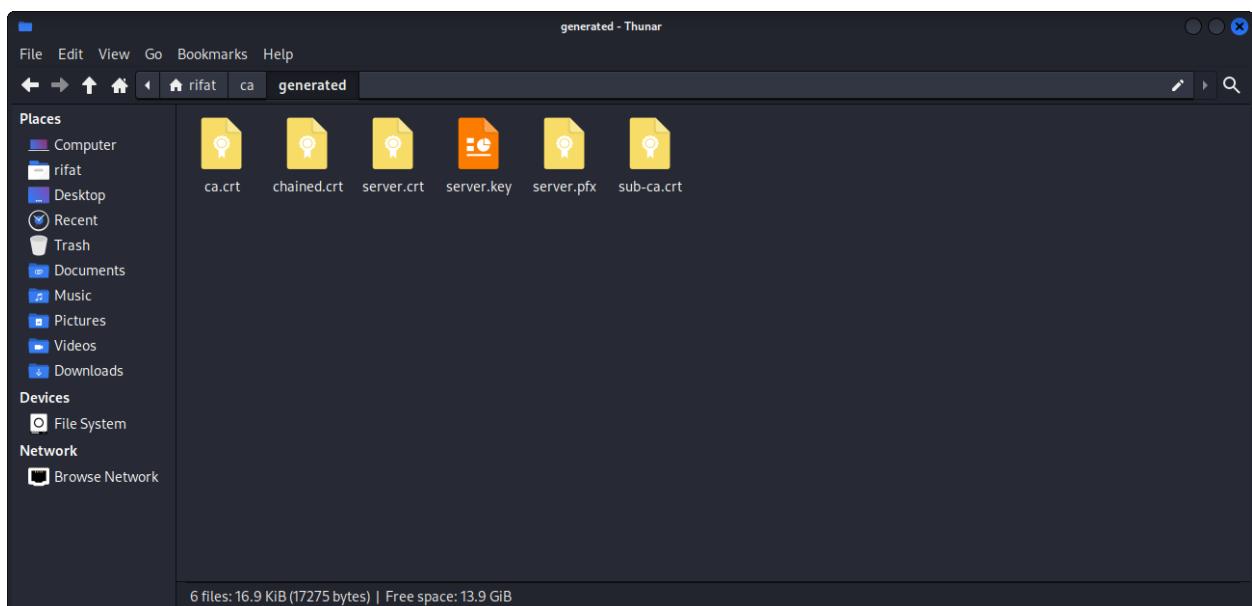
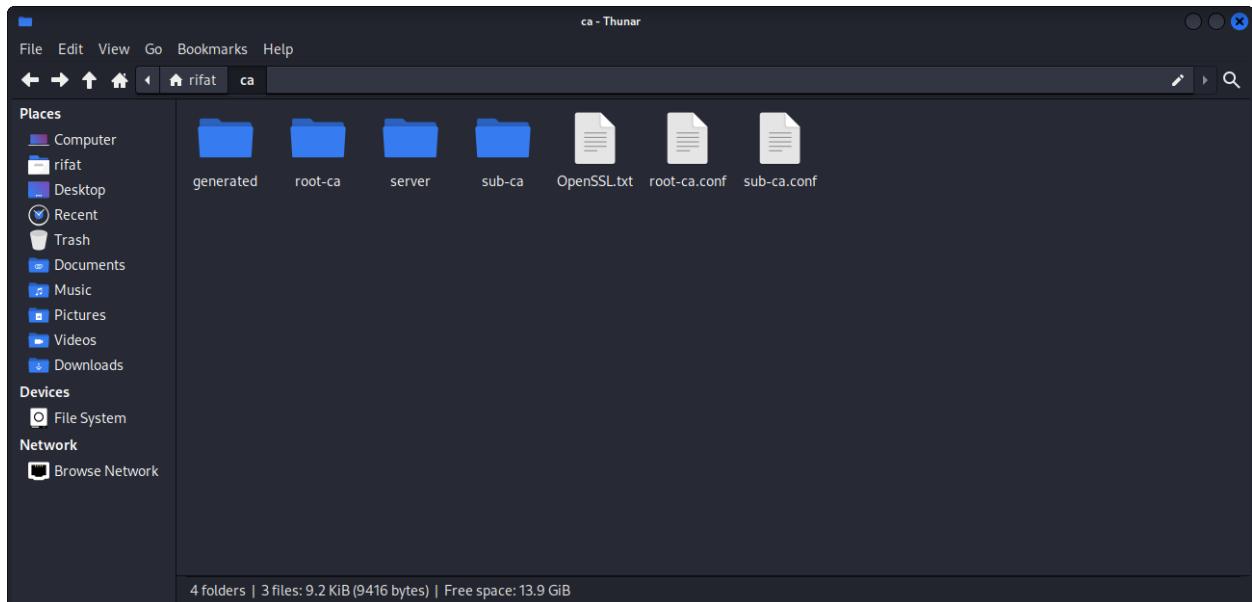
[(rifat㉿kali)-[~/ca]]
$ 
```

4 folders | 4 files: 9.2 KiB (9419 bytes) | Free space: 13.9 GiB

```
rifat@kali: ~/ca/generated
File Actions Edit View Help Help
(rifat㉿kali)-[~/ca]
$ cd generated
Places
(rifat㉿kali)-[~/ca/generated]
$ cat server.crt sub-ca.crt ca.crt > chained.crt
ted root-ca server sub-ca chained.crt
$ Desktop
Recent
Trash
Documents
Music
Pictures
Videos
Downloads
Devices
File System
Network
Browse Network
4 folders | 4 files: 9.2 KiB (9419 bytes) | Free space: 13.9 GiB
```

```
rifat@kali: ~/ca/generated
File Actions Edit View Help Help
(rifat㉿kali)-[~/ca] rifat@kali: ~
$ cd generated
Places
(rifat㉿kali)-[~/ca/generated]
$ cat server.crt sub-ca.crt ca.crt > chained.crt
(rifat㉿kali)-[~/ca/generated] ed root-ca server sub-ca chained.c
$ tree
.
├── ca.crt
├── chained.crt
├── server.crt
├── server.key
├── server.pfx
└── sub-ca.crt
  └── Pictures
  └── Videos
1 directory, 6 files
(rifat㉿kali)-[~/ca/generated]
$ 
Devices
File System
Network
Browse Network
4 folders | 4 files: 9.2 KiB (9419 bytes) | Free space: 13.9 GiB
```

```
(rifat㉿kali)-[~/ca/generated]
$ cd ..
Places
(rifat㉿kali)-[~/ca]
$ tree
.
├── OpenSSL.txt
├── chained.crt
└── generated
    ├── ca.crt
    ├── chained.crt
    ├── server.crt
    ├── server.key
    ├── server.pfx
    └── sub-ca.crt
.
├── root-ca
    ├── certs
    │   └── ca.crt
    ├── crl
    ├── csr
    ├── index
    │   ├── index
    │   ├── index.attr
    │   └── index.old
    ├── pem
    │   └── 874A288705E666CA9E8E9D2B9F95AD18.pem
    ├── private
    │   └── ca.key
    ├── root-ca.conf
    └── serial
        ├── serial
        └── serial.old
root-ca.conf
4 folders | 4 files: 9.2 KiB (9419 bytes) | Free space: 13.9 GiB
```



Nginx Web Server Configuration

#Open a terminal on Kali Linux and use the following command.

```
sudo apt update  
sudo apt install nginx
```

#After installing, try entering the local IP or localhost. If the installation is successful, a successful display will appear.

ifconfig

#Now trying to turn on the service.

```
sudo systemctl status nginx  
sudo systemctl enable nginx  
sudo systemctl start nginx
```

#If you want to turn off the service, use this command.

```
sudo systemctl status nginx  
sudo systemctl stop nginx  
sudo systemctl disable nginx
```

#copy folder

```
sudo cp -r ewubdserver /var/www  
cd ~  
cd /var/www
```

#permission changes

```
sudo chmod -R 755 ewubdserver
```

#gedit install

```
sudo apt install gedit
```

```
#To set up a virtual host, we need to create a file in  
/etc/nginx/sites-enabled/ directory.
```

```
cd /etc/nginx/sites-enabled  
sudo rm default
```

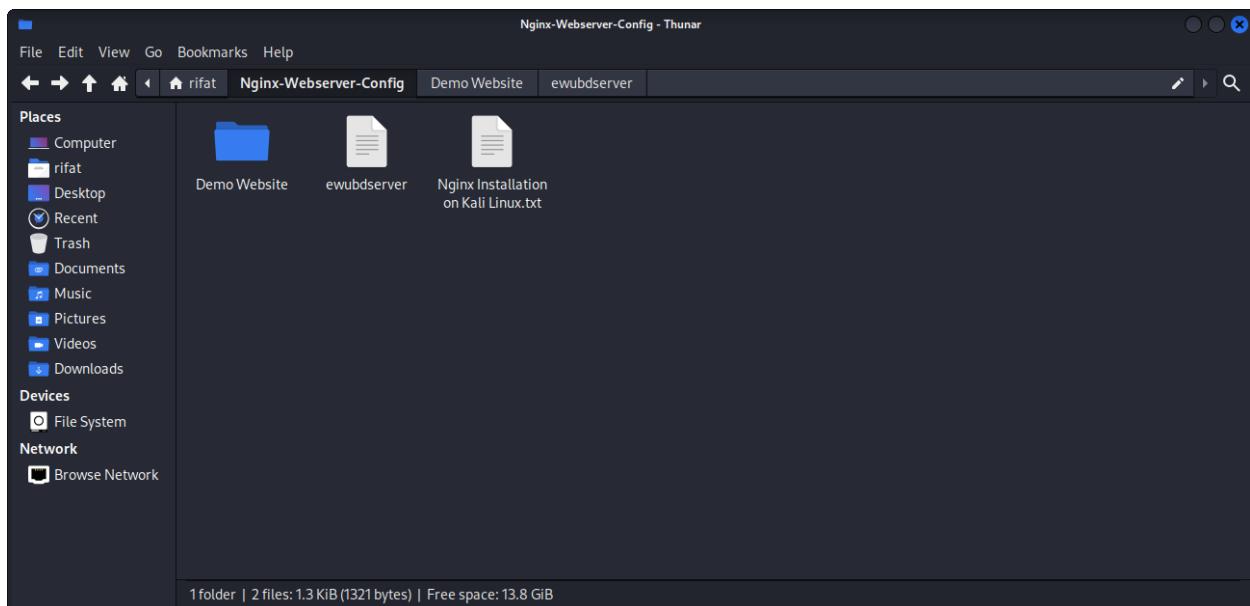
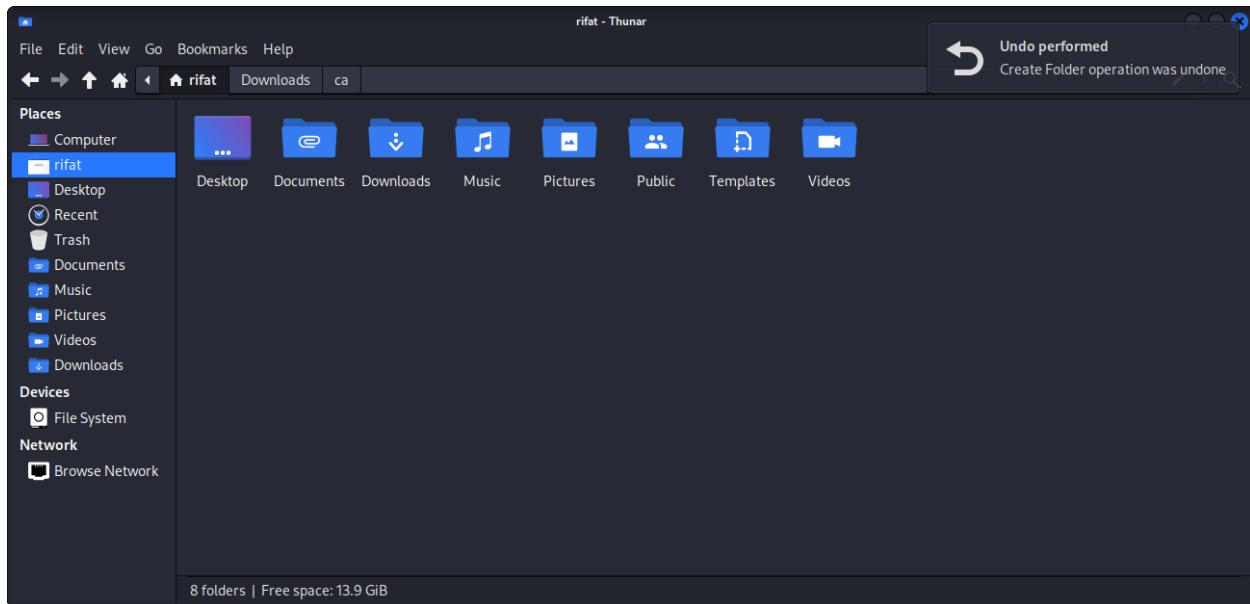
```
#check ewubdserver file  
sudo gedit ewubdserver
```

```
#To make our site work, simply restart the Nginx service.
```

```
sudo service nginx restart  
sudo service nginx status
```

```
rifat@kali: ~
File Actions Edit View Help
└─(rifat㉿kali)-[~]
$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
        inet6 ::1/128 scope host noprefixroute
            valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:77:ce:ea brd ff:ff:ff:ff:ff:ff
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:89:76:e9 brd ff:ff:ff:ff:ff:ff
    inet 192.168.56.5/24 brd 192.168.56.255 scope global dynamic noprefixroute
        valid_lft 561sec preferred_lft 561sec
        inet6 fe80::a00:27ff:fe89:76e9/64 scope link noprefixroute
            valid_lft forever preferred_lft forever
└─(rifat㉿kali)-[~]
$ 
```

```
rifat@kali: ~
File Actions Edit View Help
└─(rifat㉿kali)-[~]
$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
        inet6 ::1/128 scope host noprefixroute
            valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:77:ce:ea brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute eth0
        valid_lft 86349sec preferred_lft 86349sec
        inet6 fe80::a00:27ff:fe77:ceea/64 scope link noprefixroute
            valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:89:76:e9 brd ff:ff:ff:ff:ff:ff
$ 
```



```
(rifat㉿kali)-[~/Nginx-Webserver-Config]
$ tree
.
└── Demo Website
    └── ewubdserver
        ├── images
        │   ├── developer.png
        │   ├── hardy.png
        │   └── header_bg.png
        ├── icons
        │   ├── facebook.png
        │   ├── insta.png
        │   ├── js.png
        │   ├── mongo.png
        │   ├── nodejs.png
        │   ├── react.png
        │   └── twitter.png
        └── index.html
        └── styles
            └── style.css
    └── Nginx Installation on Kali Linux.txt
    └── ewubdserver

6 directories, 15 files

(rifat㉿kali)-[~/Nginx-Webserver-Config]
$
```

```
*Nginx Installation on Kali Linux.txt
~/Nginx-Webserver-Config
1 #Open a terminal on Kali Linux and use the following command.
2
3 sudo apt update
4 sudo apt install nginx
5
6 #After installing, try entering the local IP or localhost. If the installation is successful, a successful display will appear.
7
8 ifconfig
9
10 #Now trying to turn on the service.
11
12 sudo systemctl status nginx
13 sudo systemctl enable nginx
14 sudo systemctl start nginx
15
16 #If you want to turn off the service, use this command.
17
18 sudo systemctl status nginx
19 sudo systemctl stop nginx
20 sudo systemctl disable nginx
21
22
23 #copy folder
24
25 sudo cp -r ewubdserver /var/www
26 cd ~
27 cd /var/www
28
29 #permission changes
30
31 sudo chmod -R 777 ewubdserver
32
33
34 #gedit install
35
36 sudo apt install gedit
37
38
39 #To set up a virtual host, we need to create a file in /etc/nginx/sites-enabled/ directory.
40
41 cd /etc/nginx/sites-enabled
42 sudo rm default
43
44 #check ewubdserver file|
45 sudo gedit ewubdserver
46
47
48 #To make our site work, simply restart the Nginx service.
49
50 sudo service nginx restart
51 sudo service nginx status
52
53
54
```

Plain Text ▾ Tab Width: 8 ▾ Ln 31, Col 18 INS

```
Nginx Installation on Kali Linux.txt
~/Nginx-Webserver-Config
25 sudo cp -r ewubdserver /var/www
26 cd ~
27 cd /var/www
28
29 #permission changes
30
31 sudo chmod -R 700 ewubdserver
32
33
34 #gedit install
35
36 sudo apt install gedit
37
38
39 #To set up a virtual host, we need to create a file in /etc/nginx/sites-enabled/ directory.
40
41 cd /etc/nginx/sites-enabled
42 sudo rm default
43
44 #check ewubdserver file|
45 sudo gedit ewubdserver
46
47
48 #To make our site work, simply restart the Nginx service.
49
50 sudo service nginx restart
51 sudo service nginx status
52
53
54
```

Plain Text ▾ Tab Width: 8 ▾ Ln 44, Col 24 INS

Kali Linux rifat@kali: ~

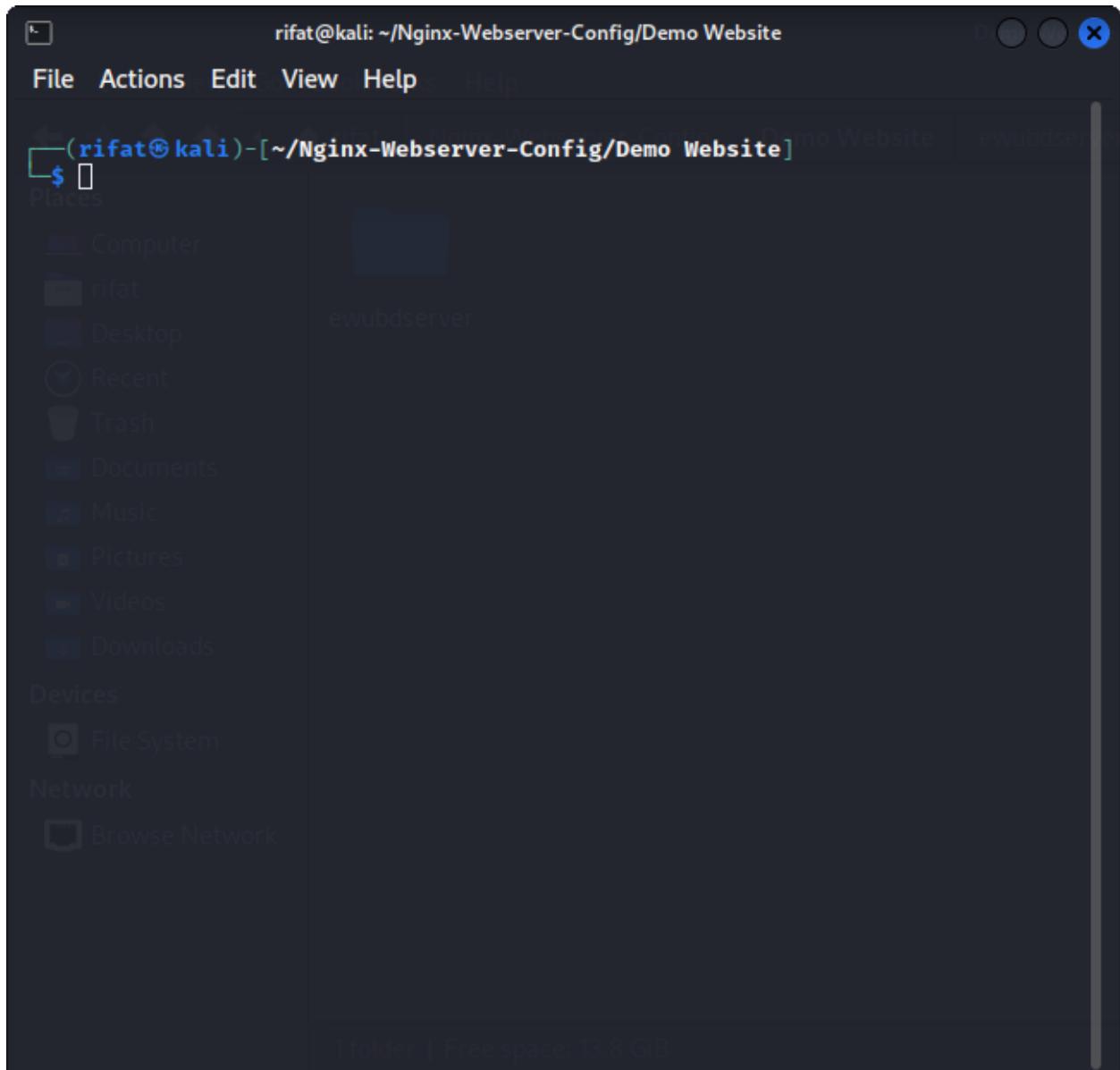
```
(rifat㉿kali)-[~]
$ sudo apt install nginx
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  nginx-common
Suggested packages:
  fcgiwrap nginx-doc ssl-cert
The following NEW packages will be installed:
  nginx nginx-common
0 upgraded, 2 newly installed, 0 to remove and 662 not upgraded.
Need to get 643 kB of archives.
After this operation, 1684 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://kali.cs.nycu.edu.tw/kali kali-rolling/main amd64 nginx-common all 1.24.0-2 [111 kB]
Get:2 http://kali.cs.nycu.edu.tw/kali kali-rolling/main amd64 nginx amd64 1.24.0-2 [532 kB]
Fetched 643 kB in 3s (207 kB/s)
Preconfiguring packages...
Selecting previously unselected package nginx-common.
(Reading database... 145686 files and directories currently installed.)
Preparing to unpack .../nginx-common_1.24.0-2_all.deb... to know more about Kali?
Unpacking nginx-common (1.24.0-2)...
Selecting previously unselected package nginx.
Preparing to unpack .../nginx_1.24.0-2_amd64.deb...
Unpacking nginx (1.24.0-2)...
Setting up nginx (1.24.0-2)...
Setting up nginx-common (1.24.0-2)...
update-rc.d: We have no instructions for the nginx init script.
update-rc.d: It looks like a network service, we disable it.
nginx.service is a disabled or a static unit, not starting it.
```

```
Kali Linux rifat@kali: ~
File Actions Edit View Help
(Reading database ... 145686 files and directories currently installed.)
Preparing to unpack .../nginx-common_1.24.0-2_all.deb ...
Unpacking nginx-common (1.24.0-2) ...
Selecting previously unselected package nginx.
Preparing to unpack .../nginx_1.24.0-2_amd64.deb ...
Unpacking nginx (1.24.0-2) ...
Setting up nginx (1.24.0-2) ...
Setting up nginx-common (1.24.0-2) ...
update-rc.d: We have no instructions for the nginx init script.
update-rc.d: It looks like a network service, we disable it.
nginx.service is a disabled or a static unit, not starting it.
Processing triggers for man-db (2.11.2-3) ...
Processing triggers for kali-menu (2023.4.3) ...

└─(rifat㉿kali)-[~]
$ sudo systemctl status nginx
● nginx.service - A high performance web server and a reverse proxy server
  Loaded: loaded (/lib/systemd/system/nginx.service; disabled; preset: d)
  Active: inactive (dead)
    Docs: man:nginx(8)

└─(rifat㉿kali)-[~]
$ sudo systemctl enable nginx
Synchronizing state of nginx.service with SysV service script with /lib/syst
emd/systemd-sysv-install.
Want to know more about Kali? Documentation
  Executing: /lib/systemd/systemd-sysv-install enable nginx
  Created symlink /etc/systemd/system/multi-user.target.wants/nginx.service →
/lib/systemd/system/nginx.service.

└─(rifat㉿kali)-[~]
$ 
```



```
rifat@kali: /var/www
File Actions Edit View Help Help
(rifat@kali)-[~/Nginx-Webserver-Config/Demo Website]
$ sudo cp -r ewubdserver /var/www
[sudo] password for rifat:
(rifat@kali)-[~/Nginx-Webserver-Config/Demo Website]
$ cd ~
(rifat@kali)-[~]
$ cd /var/www
(rifat@kali)-[/var/www]
$ sudo chmod -R 777 ewubdserver
(rifat@kali)-[/var/www]
$ tree
.
├── ewubdserver
│   ├── images
│   │   ├── developer.png
│   │   ├── hardy.png
│   │   ├── header_bg.png
│   │   └── icons
│   │       ├── facebook.png
│   │       ├── insta.png
│   │       ├── js.png
│   │       ├── mongo.png
│   │       ├── nodejs.png
│   │       ├── react.png
│   │       └── twitter.png
│   └── index.html
└── styles
    └── style.css
1 folder | Free space: 13.8 GB
```

rifat@kali: /etc/nginx/sites-enabled

File Actions Edit View Help Help

Places Nginx-Webserver-Config Demo Website

Con icon8-linkedin-90.png

mongo.png nodejs.png react.png twitter.png icons8-linkedin-90.png

index.html

styles style.css ewubdserver

html index.nginx-debian.html

6 directories, 14 files

```
└─(rifat㉿kali)-[/var/www]
$ cd /etc/nginx/sites-enabled

└─(rifat㉿kali)-[/etc/nginx/sites-enabled]
$ sudo rm default

└─(rifat㉿kali)-[/etc/nginx/sites-enabled]
$ gedit ewubdserver
Devices
Network
(gedit:55823): tepl-WARNING **: 09:21:14.889: Style scheme 'Kali-Dark' cannot be found, falling back to 'Kali-Dark' default style scheme.

(gedit:55823): tepl-WARNING **: 09:21:14.889: Default style scheme 'Kali-Dark' cannot be found, check your installation.

(gedit:55823): dconf-WARNING **: 09:21:16.762: failed to commit changes to dconf: Failed to execute child process "dbus-launch" (No such file or directory)

└─(rifat㉿kali)-[/etc/nginx/sites-enabled]
$
```

```
rifat@kali: /etc/nginx/sites-enabled
File Actions Edit View Help Help
(rifat@kali)-[/etc/nginx/sites-enabled] Config Demo Website
$ sudo gedit ewubdserver
Places Computer
rifat
Desktop ewubdserver
Recent
Trash
Documents
Music
Pictures
Videos
Downloads
Devices
File System
Network
Browse Network
1 folder | Free space: 13.8 GB
```

The screenshot shows a terminal window with a dark theme. The title bar reads "ewubdserver /etc/nginx/sites-enabled". The main area contains the following Nginx configuration file:

```
1 server {
2     listen 80;
3     listen [::]:80;
4
5     listen 443 ssl;
6     listen [::]:443 ssl;
7
8     server_name ewubdserver;
9
10    ssl_certificate /home/rifat/ca/generated/chained.crt;
11    ssl_certificate_key /home/rifat/ca/generated/server.key;
12
13    root /var/www/ewubdserver;
14    index index.html;
15
16    location / {
17        try_files $uri $uri/ =404;
18    }
19 }
20 |
```

At the bottom of the terminal window, there is status information: "Saving file "/etc/nginx/sites-enabled/e... Plain Text ▾ Tab Width: 8 ▾ Ln 20, Col 1 INS".

```
rifat@kali: /etc/nginx/sites-enabled
File Actions Edit View Help
(gedit:56134): tepl-WARNING **: 09:21:44.288: Style scheme 'Kali-Dark' canno
t be found, falling back to 'Kali-Dark' default style scheme.

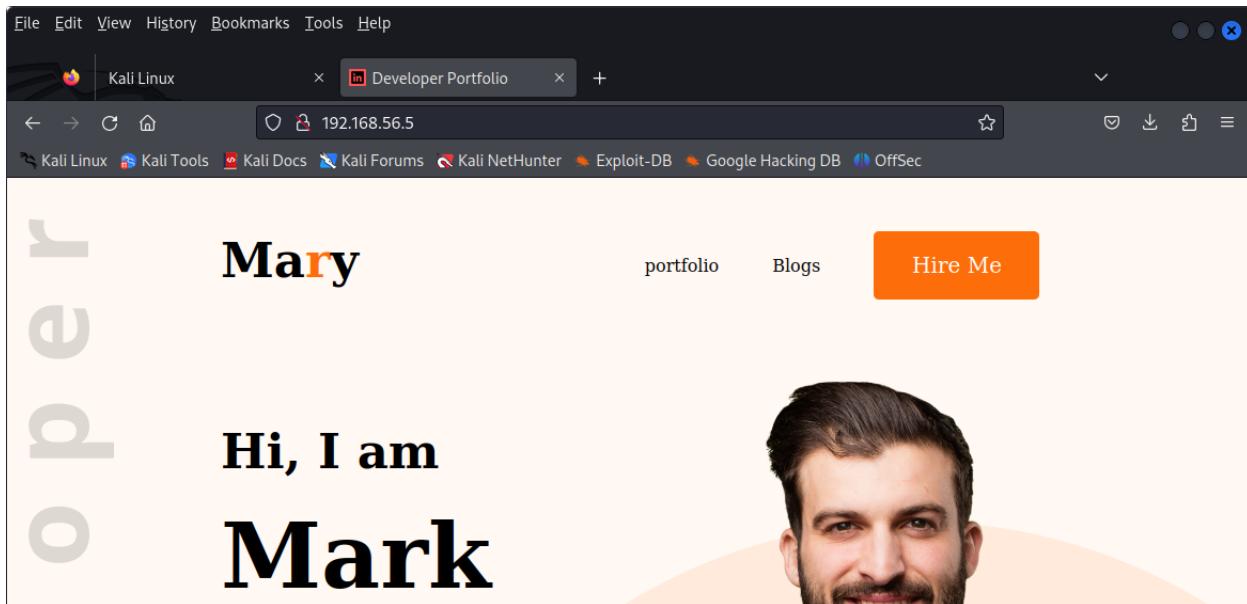
(gedit:56134): tepl-WARNING **: 09:21:44.288: Default style scheme 'Kali-Dar
k' cannot be found, check your installation.

(gedit:56134): dconf-WARNING **: 09:22:31.146: failed to commit changes to d
conf: Failed to execute child process "dbus-launch" (No such file or direc
tory)
File System
└─(rifat㉿kali)-[/etc/nginx/sites-enabled]
  └─$ sudo service nginx restart

└─(rifat㉿kali)-[/etc/nginx/sites-enabled]
  └─$ sudo service nginx status

● nginx.service - A high performance web server and a reverse proxy server
  Loaded: loaded (/lib/systemd/system/nginx.service; enabled; preset: di>
  Active: active (running) since Sun 2023-12-24 09:22:54 EST; 7s ago
    Docs: man:nginx(8)
  Process: 56758 ExecStartPre=/usr/sbin/nginx -t -q -g daemon on; master_>
  Process: 56760 ExecStart=/usr/sbin/nginx -g daemon on; master_process o>
  Main PID: 56761 (nginx)
    Tasks: 3 (limit: 4604)
   Memory: 2.8M
      CPU: 45ms
     CGroup: /system.slice/nginx.service
             ├─56761 "nginx: master process /usr/sbin/nginx -g daemon on; m>
             ├─56762 "nginx: worker process"
             └─56763 "nginx: worker process"

Dec 24 09:22:54 kali systemd[1]: Starting nginx.service - A high performanc>
Dec 24 09:22:54 kali systemd[1]: Started nginx.service - A high performance>
[lines 1-17/17 (END)]
```



Bind9 DNS Server Configuration

1. Navigate to the BIND configuration directory:

```
cd /etc/bind
```

2. Back up original configuration files (recommended):

```
sudo cp named.conf.options named.conf.options.original  
sudo cp named.conf.local named.conf.local.original
```

3. Create copies of zone files:

```
sudo cp db.local db.ewubdserver.com  
sudo cp db.127 db.56.168.192
```

4. Edit global options file:

```
sudo gedit named.conf.options
```

- Adjust settings as needed (consult BIND documentation for details).

5. Edit local zone definitions file:

```
sudo gedit named.conf.local
```

- Add entries for the new zones:

```
zone "ewubdserver.com" IN{  
    type master;  
    file "/etc/bind/db.ewubdserver.com";  
};  
  
zone "56.168.192.in-addr.arpa" IN{  
    type master;  
    file "/etc/bind/db.56.168.192";  
};
```

6. Edit forward zone file:

```
sudo gedit db.ewubdserver.com
```

- Add resource records (SOA, NS, A, MX, CNAME, etc.).
- Verify zone file syntax:

```
named-checkzone ewubdserver.com db.ewubdserver.com
```

7. Edit reverse zone file:

```
sudo gedit db.56.168.192
```

- Add PTR records for reverse lookups.
- Verify zone file syntax:

```
named-checkzone 56.168.192.in-addr.arpa db.56.168.192
```

8. Manage the BIND service:

In updated version **bind9** keyword replace with **named**

- Check service status:

```
sudo systemctl status named
```

- Start the service:

```
sudo systemctl start named
```

- Enable service at boot:

```
sudo systemctl enable named
```

- Verify service status

```
sudo systemctl status named
```

9. Configure local resolver:

```
sudo gedit /etc/resolv.conf
```

- Add the server's IP address as the first nameserver:

```
nameserver 192.168.56.5
```

10. Restart BIND:

```
sudo systemctl restart named
```

11. Test DNS resolution:

```
nslookup www.ewubdserver.com
```

Additional Notes:

- Replace placeholders with actual IP addresses and hostnames.
- Consult BIND documentation for advanced configuration options.
- Consider security implications and implement appropriate safeguards (e.g., access control lists).
- Regularly review and update DNS configuration as needed.

```
(rifat㉿kali)-[~]
$ sudo apt install bind9
[sudo] password for rifat:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  bind9-dnsutils bind9-host bind9-libs bind9-utils liburcu8
Suggested packages:
  bind-doc resolvconf ufw
The following NEW packages will be installed:
  bind9 bind9-utils liburcu8
The following packages will be upgraded:
  bind9-dnsutils bind9-host bind9-libs
3 upgraded, 3 newly installed, 0 to remove and 659 not upgraded.
Need to get 3099 kB of archives.
After this operation, 2964 kB disk space will be freed.
Do you want to continue? [Y/n] y
Get:1 http://http.kali.org/kali kali-rolling/main amd64 bind9-host amd64 1:9
.19.17-2~kali1 [310 kB]
Get:2 http://http.kali.org/kali kali-rolling/main amd64 bind9-dnsutils amd64
 1:9.19.17-2~kali1 [416 kB]
Get:3 http://kali.cs.nycu.edu.tw/kali kali-rolling/main amd64 liburcu8 amd64
 0.14.0-2 [72.6 kB]
Get:4 http://http.kali.org/kali kali-rolling/main amd64 bind9-libs amd64 1:9
.19.17-2~kali1 [1384 kB]
Get:5 http://http.kali.org/kali kali-rolling/main amd64 bind9-utils amd64 1:
9.19.17-2~kali1 [416 kB]
Get:6 http://http.kali.org/kali kali-rolling/main amd64 bind9 amd64 1:9.19.1
7-2~kali1 [499 kB]
Fetched 3099 kB in 8s (385 kB/s)
(Reading database ... 145736 files and directories currently installed.)
Preparing to unpack .../0-bind9-host_1%3a9.19.17-2~kali1_amd64.deb ...
```

```
rifat@kali: /etc/bind
File Actions Edit View Help
(rifat@kali)-[~]
$ cd /etc/bind

(rifat@kali)-[/etc/bind]
$ sudo cp named.conf.options named.conf.options.original
[sudo] password for rifat:

(rifat@kali)-[/etc/bind]
$ sudo cp named.conf.local named.conf.local.original
File System
(rifat@kali)-[/etc/bind]
$ sudo cp db.local db.ewubdserver.com

(rifat@kali)-[/etc/bind]
$ sudo cp db.127 db.56.168.192

(rifat@kali)-[/etc/bind]
$ gedit named.conf.options

(gedit:5864): tepl-WARNING **: 10:44:19.211: Style scheme 'Kali-Dark' cannot
be found, falling back to 'Kali-Dark' default style scheme.

(gedit:5864): tepl-WARNING **: 10:44:19.211: Default style scheme 'Kali-Dark'
' cannot be found, check your installation.

(gedit:5864): dconf-WARNING **: 10:46:37.595: failed to commit changes to dc
onf: Failed to execute child process "dbus-launch" (No such file or director
y)

(rifat@kali)-[/etc/bind]
$
```

The screenshot shows a terminal window with the following content:

```
named.conf.options
/etc/bind

1 options {
2     directory "/var/cache/bind";
3
4     // If there is a firewall between you and nameservers you want
5     // to talk to, you may need to fix the firewall to allow multiple
6     // ports to talk. See http://www.kb.cert.org/vuls/id/800113
7
8     // If your ISP provided one or more IP addresses for stable
9     // nameservers, you probably want to use them as forwarders.
10    // Uncomment the following block, and insert the addresses replacing
11    // the all-0's placeholder.
12
13    // forwarders {
14    //     0.0.0.0;
15    // };
16
17    //-
18    // If BIND logs error messages about the root key being expired,
19    // you will need to update your keys. See https://www.isc.org/bind-keys
20    //-
21 dnssec-validation auto;
22
23 listen-on-v6 { any; }|;
24 recursion yes;
25 listen-on{192.168.56.5;};
26 allow-transfer {none;};
27
28 forwarders {
29     192.168.56.0;
30 };
31
32 };
```

At the bottom of the terminal window, the status bar displays:

Loading file "/etc/bind/named.conf.options"...
Plain Text ▾ Tab Width: 8 ▾ Ln 23, Col 31 INS

The screenshot shows a terminal window with a dark theme. The title bar reads "named.conf.local" and "Save". The file content is as follows:

```
1 //
2 // Do any local configuration here
3 //
4
5 // Consider adding the 1918 zones here, if they are not used in your
6 // organization
7 //include "/etc/bind/zones.rfc1918";
8
9 zone "ewubdserver.com" IN{
10         type master;
11         file "/etc/bind/db.ewubdserver.com";
12 };
13 zone "56.168.192.in-addr.arpa" IN{
14         type master;
15         file "/etc/bind/db.56.168.192";
16 };
```

At the bottom of the terminal window, there are status indicators: "C ▾ Tab Width: 8 ▾ Ln 16, Col 3 INS".

Open ▾  db.56.168.192  /etc/bind  

```
1 ;
2 ; BIND reverse data file for local loopback interface
3 ;
4 $TTL    604800
5 @       IN      SOA     ns1.ewubdserver.com. root.ewubdserver.com. (
6                      1           ; Serial
7                      604800      ; Refresh
8                      86400       ; Retry
9                      2419200     ; Expire
10                     604800 )     ; Negative Cache TTL
11 ;
12 @      IN      NS      ns1.ewubdserver.com.
13 24    IN      PTR     ns1.ewubdserver.com.
14 24    IN      PTR     www.ewubdserver.com.
15 24    IN      PTR     ftp.ewubdserver.com.
16 24    IN      PTR     mail.ewubdserver.com.
17
```

Plain Text ▾ Tab Width: 8 ▾ Ln 17, Col 1 INS

```
rifat@kali: /etc/bind
```

File Actions Edit View Help

- o named.service - BIND Domain Name Server

```
  Loaded: loaded (/lib/systemd/system/named.service; disabled; preset: disabled)
  Active: inactive (dead)
    Docs: man:named(8)
```

```
(rifat@kali):~/etc/bind]$ sudo systemctl start named
```

```
(rifat@kali):~/etc/bind]$ sudo systemctl enable named
```

Synchronizing state of named.service with SysV service script with /lib/systemd/systemd-sysv-install.

```
Executing: /lib/systemd/systemd-sysv-install enable named
Created symlink /etc/systemd/system/bind9.service → /lib/systemd/system/named.service.
Created symlink /etc/systemd/system/multi-user.target.wants/named.service → /lib/systemd/system/named.service.
```

```
(rifat@kali):~/etc/bind]$ sudo systemctl status named
```

- named.service - BIND Domain Name Server

```
  Loaded: loaded (/lib/systemd/system/named.service; enabled; preset: disabled)
  Active: active (running) since Sun 2023-12-24 11:07:42 EST; 21s ago
    Docs: man:named(8)
    Main PID: 17555 (named)
      Status: "running"
        Tasks: 3 (limit: 4604)
       Memory: 27.5M
          CPU: 64ms
        Group: /system.slice/named.service
           └─17555 /usr/sbin/named -f -u bind
```

```
Dec 24 11:07:43 kali named[17555]: network unreachable resolving './NS/IN': 3
Dec 24 11:07:43 kali named[17555]: network unreachable resolving './NS/IN': 3
```

Verify zone file syntax:
named-checkzone 56.168.192.in-addr.arpa db.56.168.192
8. Manage the BIND service:

- Check service status:
sudo systemctl status named
- Start the service:
sudo systemctl start named
- Enable service at boot:
sudo systemctl enable named
- Verify service status:
sudo systemctl status named

9. Configure local resolver:
sudo gedit /etc/resolv.conf

```
Open ▾ + resolv.conf /etc
```

Save ⋮

```
1 # Generated by NetworkManager
2 nameserver 192.168.56.5
```

Plain Text ▾ Tab Width: 8 ▾ Ln 2, Col 24 INS


```
rifat@kali: /etc/bind
File Actions Edit View Help
~
~ Trash
~
~
~
~
~
(rifat@kali)-[~/etc/bind]
$ sudo gedit /etc/resolv.conf
(gedit:18275): tepl-WARNING **: 11:08:43.422: Style scheme 'Kali-Dark' cannot
be found, falling back to 'Kali-Dark' default style scheme.

(gedit:18275): tepl-WARNING **: 11:08:43.422: Default style scheme 'Kali-Dark'
' cannot be found, check your installation.

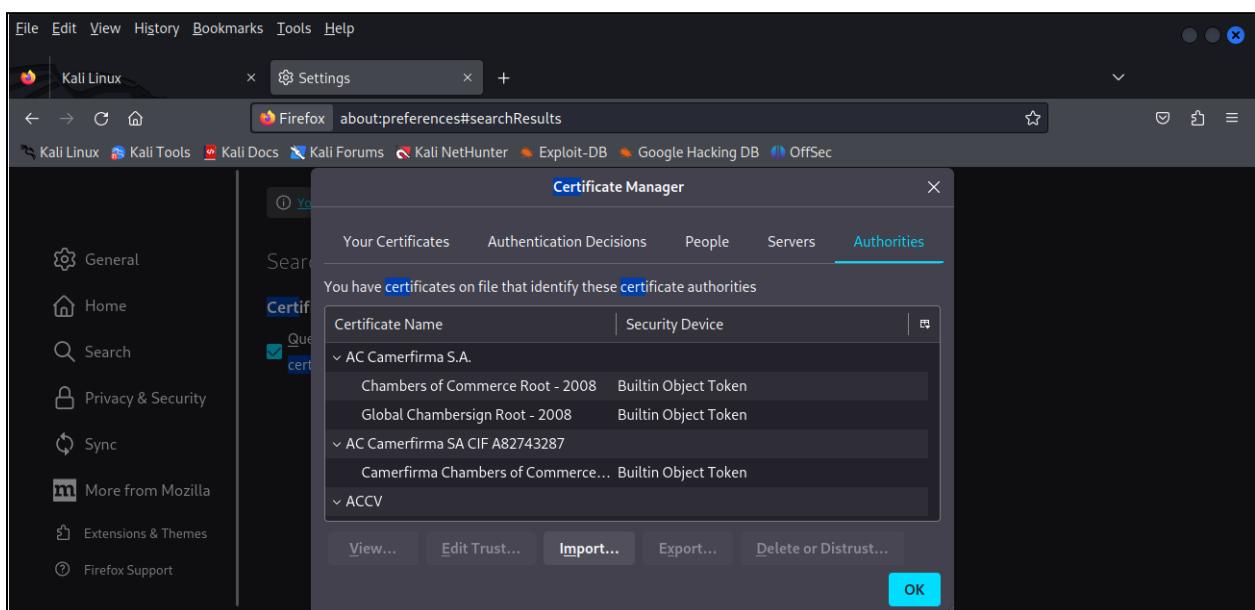
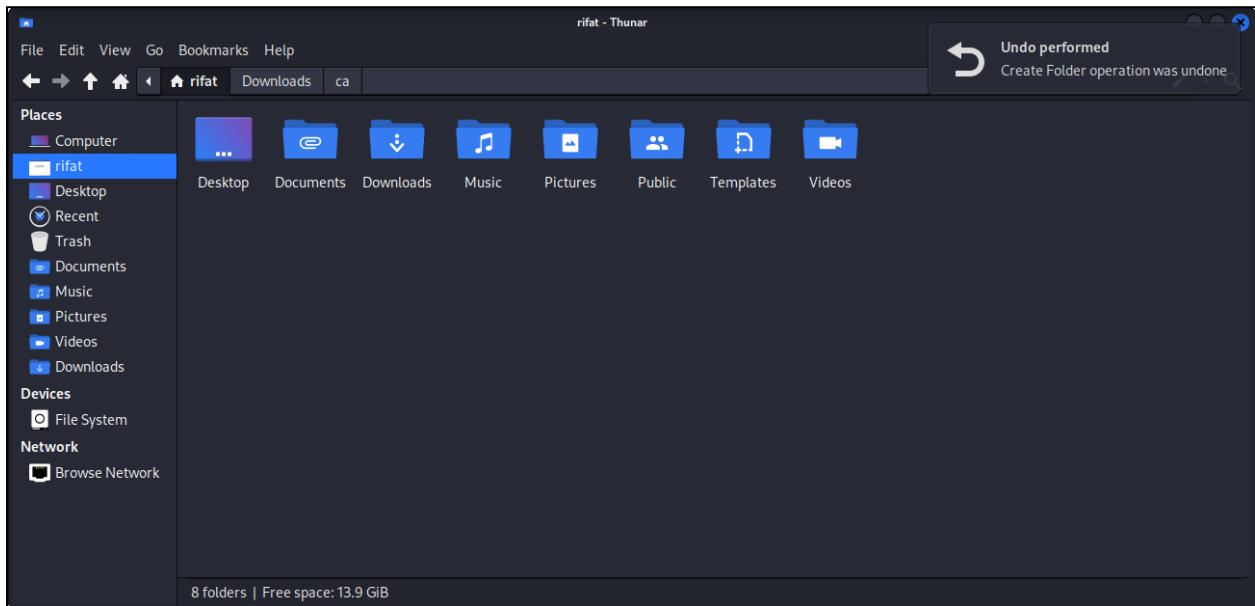
(gedit:18275): dconf-WARNING **: 11:09:24.969: failed to commit changes to dc
onf: Failed to execute child process "dbus-launch" (No such file or directory
)

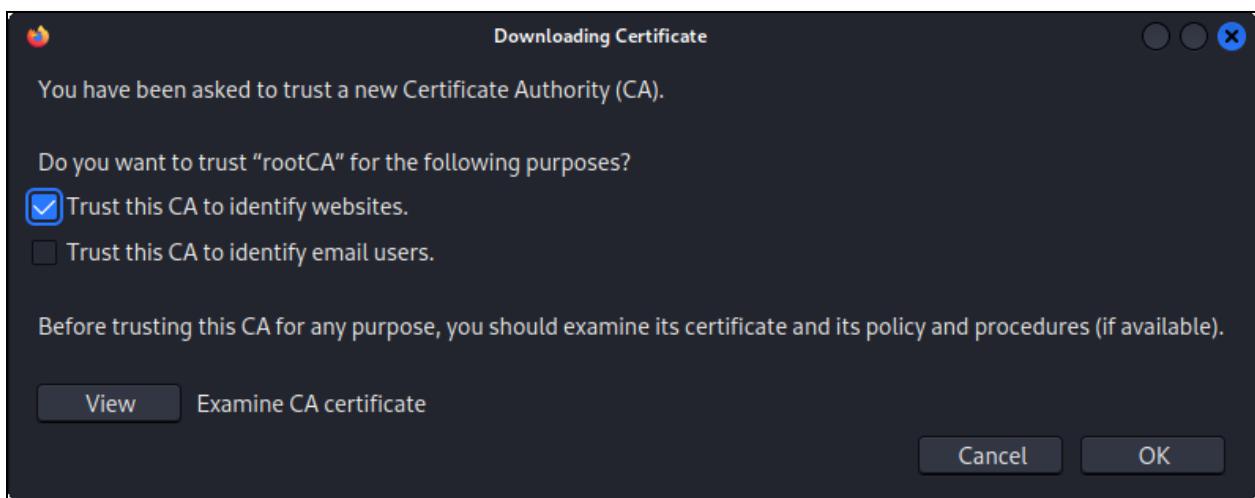
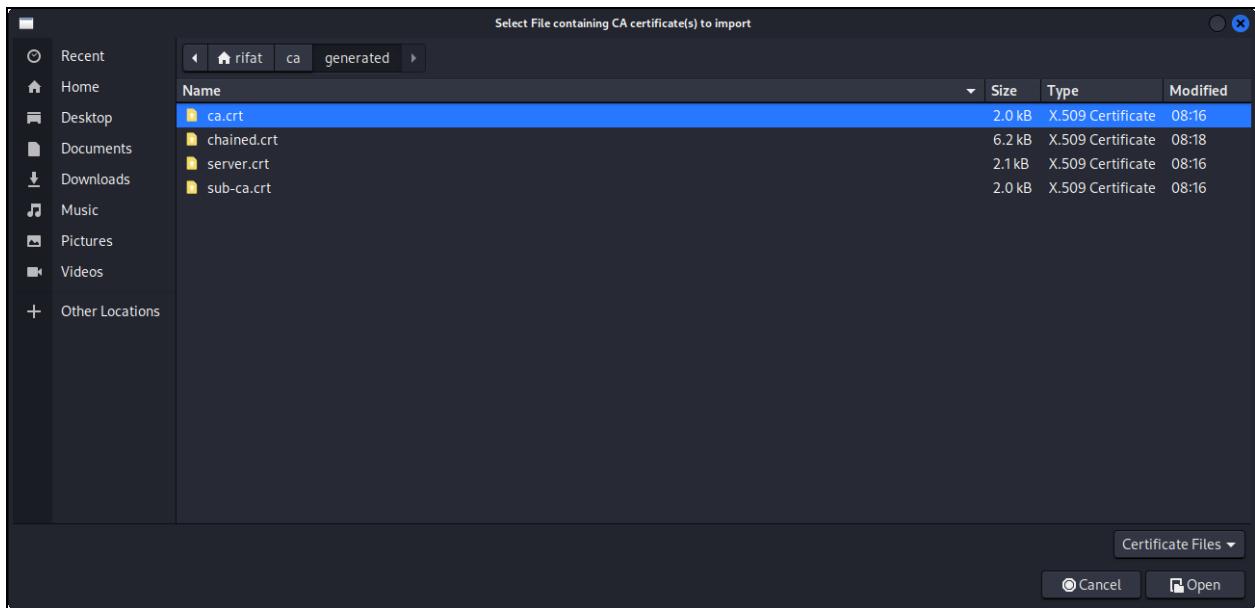
(rifat@kali)-[~/etc/bind]
$ sudo systemctl restart named
(rifat@kali)-[~/etc/bind]
$ nslookup www.ewubdserver.com
Server:          192.168.56.5
Address:         192.168.56.5#53

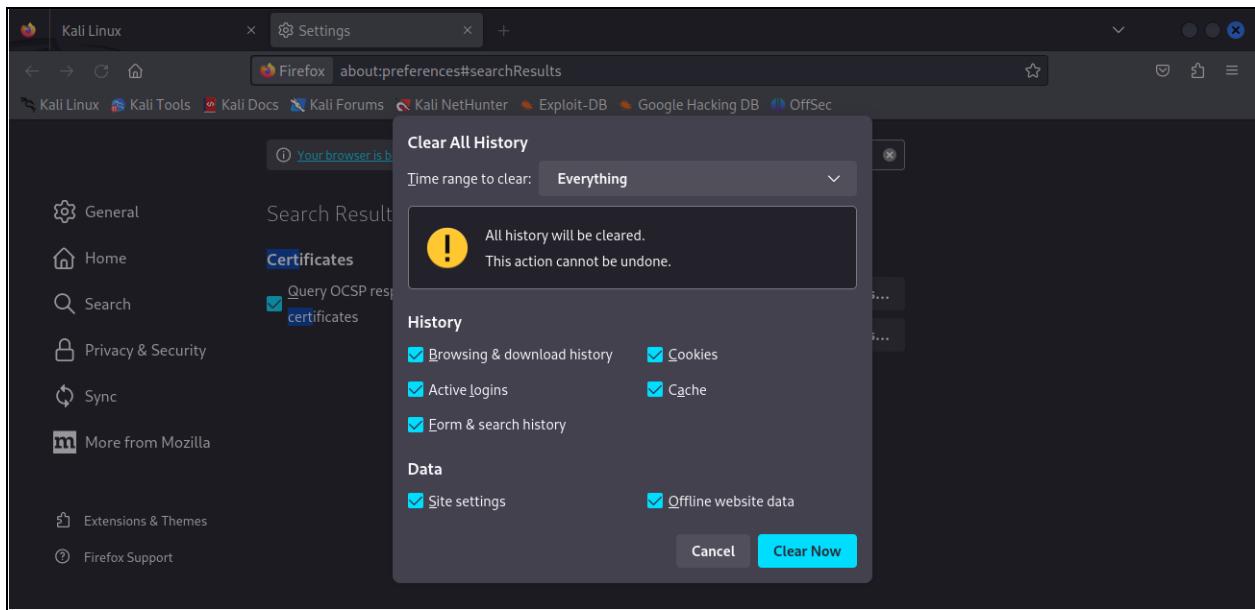
Name:    www.ewubdserver.com
Address: 192.168.56.5

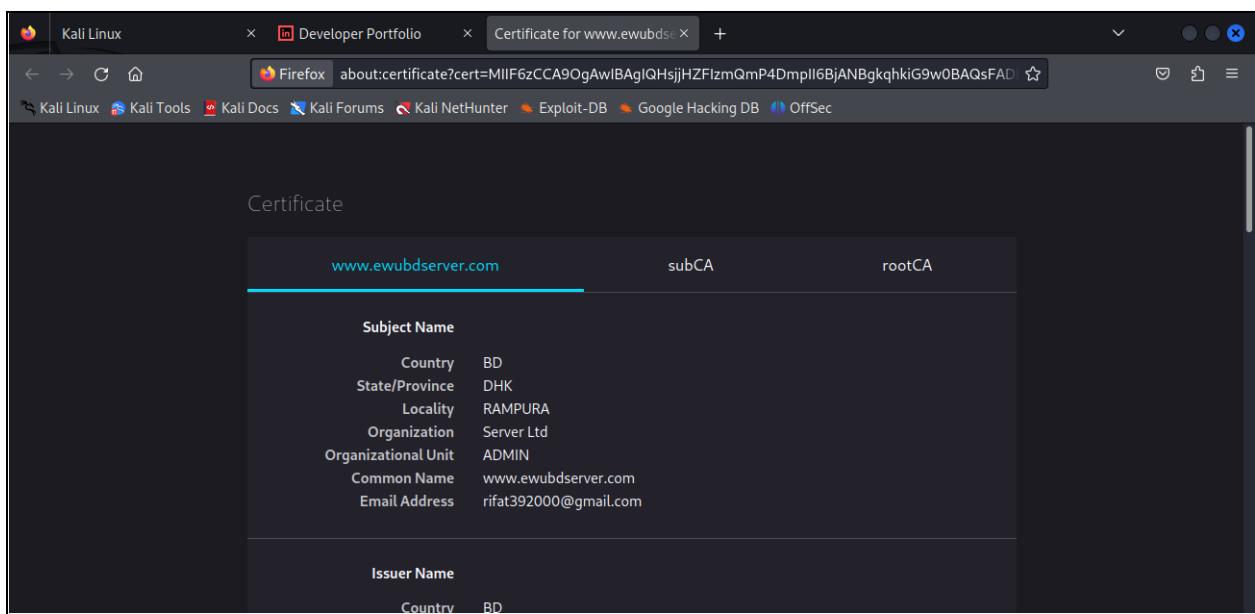
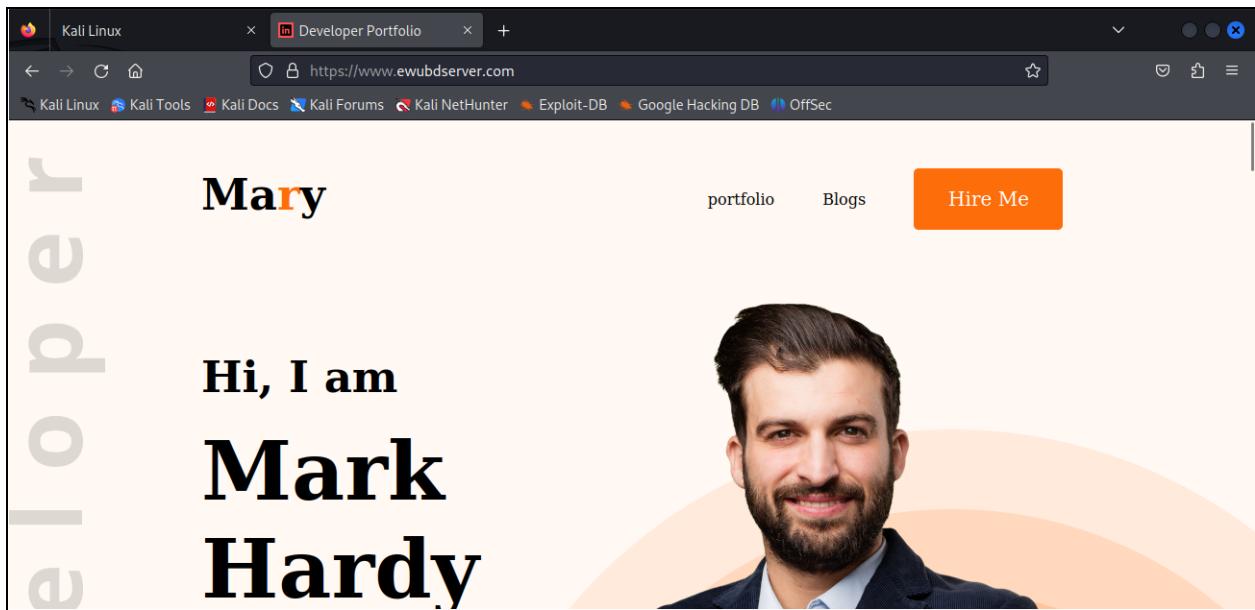
(rifat@kali)-[~/etc/bind]
$ 
```

Server Side Website Validation Check









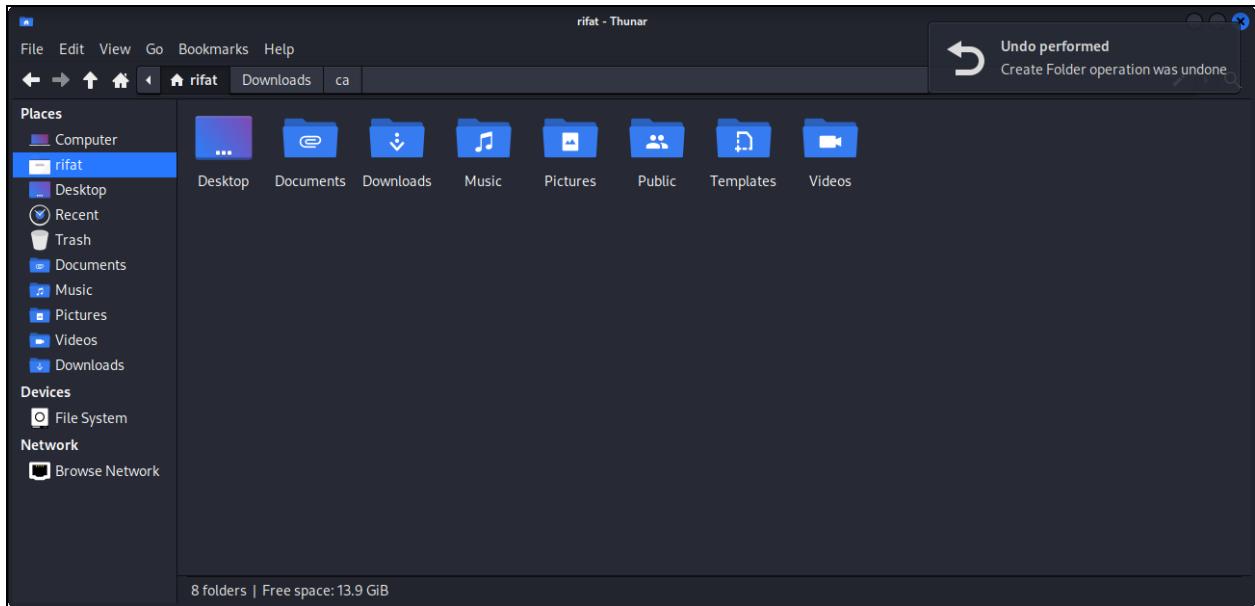
OpenSSH Configuration

```
#install  
sudo apt install openssh-server  
  
#configuration  
sudo gedit /etc/ssh/sshd_config  
  
sudo service ssh status  
sudo service ssh restart  
sudo service ssh status
```



The screenshot shows a terminal window titled 'rifat@kali: ~'. The command 'sudo apt install openssh-server' is run, and the terminal displays the package manager's output. It shows that the package is already installed (Status: installed), and it lists dependencies like 'libpam-ssh', 'monkeysphere', 'ssh-askpass', and 'molly-guard'. It also shows suggested packages like 'keychain' and 'libpam-ssh'. The terminal then lists upgraded packages ('openssh-client', 'openssh-server', 'openssh-sftp-server') and their details. It shows the download progress from three sources, totaling 1511 kB. The terminal then asks if the user wants to continue with the installation. It continues with the preconfiguration of packages, unpacking and preparing them. Finally, it installs the new version of the config file '/etc/ssh/sshd_config' and starts the 'sshd' service.

```
(rifat㉿kali)-[~] $ sudo apt install openssh-server  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
The following additional packages will be installed:  
  openssh-client openssh-sftp-server  
Suggested packages:  
  keychain libpam-ssh monkeysphere ssh-askpass molly-guard  
The following packages will be upgraded:  
  openssh-client openssh-server openssh-sftp-server  
3 upgraded, 0 newly installed, 0 to remove and 654 not upgraded.  
Need to get 1511 kB of archives.  
After this operation, 98.3 kB of additional disk space will be used.  
Do you want to continue? [Y/n] y  
Get:1 http://kali.cs.nycu.edu.tw/kali kali-rolling/main amd64 openssh-sftp-server amd64 1:9.4p1-1 [66.3 kB]  
Get:2 http://kali.cs.nycu.edu.tw/kali kali-rolling/main amd64 openssh-server amd64 1:9.4p1-1 [458 kB]  
Get:3 http://kali.cs.nycu.edu.tw/kali kali-rolling/main amd64 openssh-client amd64 1:9.4p1-1 [986 kB]  
Fetched 1511 kB in 5s (318 kB/s)  
Preconfiguring packages ...  
(Reading database ... 146158 files and directories currently installed.)  
Preparing to unpack .../openssh-sftp-server_1x3a9.4p1-1_amd64.deb ...  
Unpacking openssh-sftp-server (1:9.4p1-1) over (1:9.3p2-1) ...  
Preparing to unpack .../openssh-server_1x3a9.4p1-1_amd64.deb ...  
Unpacking openssh-server (1:9.4p1-1) over (1:9.3p2-1) ...  
Preparing to unpack .../openssh-client_1x3a9.4p1-1_amd64.deb ...  
Unpacking openssh-client (1:9.4p1-1) over (1:9.3p2-1) ...  
Setting up openssh-client (1:9.4p1-1) ...  
Installing new version of config file /etc/ssh/sshd_config ...  
Setting up openssh-sftp-server (1:9.4p1-1) ...  
Setting up openssh-server (1:9.4p1-1) ...  
Installing new version of config file /etc/ssh/moduli ...  
rescue-ssh.target is a disabled or a static unit not running, not starting it.
```

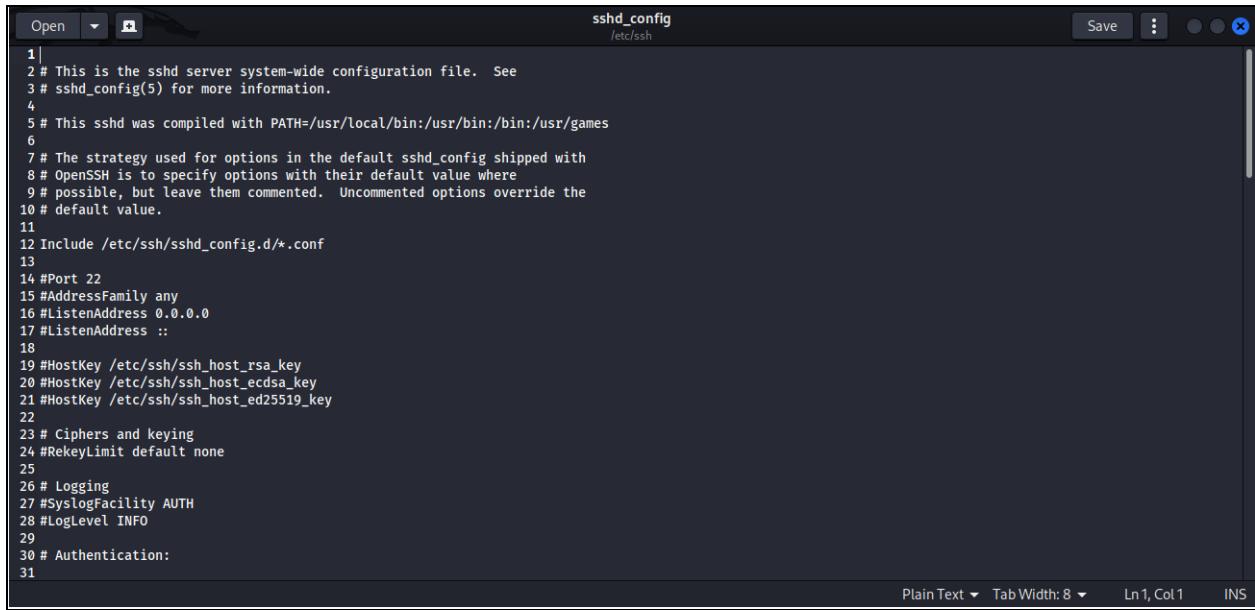


```
rifat@kali: ~
```

```
File Actions Edit View Help
```

```
Suggested packages:
  keychain libpam-ssh monkeysphere ssh-askpass molly-guard
The following packages will be upgraded:
  openssh-client openssh-server openssh-sftp-server
3 upgraded, 0 newly installed, 0 to remove and 654 not upgraded.
Need to get 1511 kB of archives.
After this operation, 98.3 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://kali.cs.nycu.edu.tw/kali kali-rolling/main amd64 openssh-sftp-server amd64 1:9.4p1-1 [66.3 kB]
Get:2 http://kali.cs.nycu.edu.tw/kali kali-rolling/main amd64 openssh-server amd64 1:9.4p1-1 [458 kB]
Get:3 http://kali.cs.nycu.edu.tw/kali kali-rolling/main amd64 openssh-client amd64 1:9.4p1-1 [986 kB]
Fetched 1511 kB in 5s (318 kB/s)
Preconfiguring packages ...
(Reading database... 146158 files and directories currently installed.)
Preparing to unpack .../openssh-sftp-server_1%3a9.4p1-1_amd64.deb ...
Unpacking openssh-sftp-server (1:9.4p1-1) over (1:9.3p2-1) ...
Preparing to unpack .../openssh-server_1%3a9.4p1-1_amd64.deb ...
Unpacking openssh-server (1:9.4p1-1) over (1:9.3p2-1) ...
Preparing to unpack .../openssh-client_1%3a9.4p1-1_amd64.deb ...
Unpacking openssh-client (1:9.4p1-1) over (1:9.3p2-1) ...
Setting up openssh-client (1:9.4p1-1) ...
Installing new version of config file /etc/ssh/sshd_config ...
Setting up openssh-sftp-server (1:9.4p1-1) ...
Setting up openssh-server (1:9.4p1-1) ...
Installing new version of config file /etc/ssh/moduli ...
rescue-ssh.target is a disabled or a static unit not running, not starting it.
ssh.service is a disabled or a static unit not running, not starting it.
ssh.socket is a disabled or a static unit not running, not starting it.
Processing triggers for man-db (2.11.2-3) ...
Processing triggers for kali-menu (2023.4.3) ...
Processing triggers for ufw (0.36.2-1) ...

(rifat@kali)-[~]
$ sudo gedit /etc/ssh/sshd_config
```

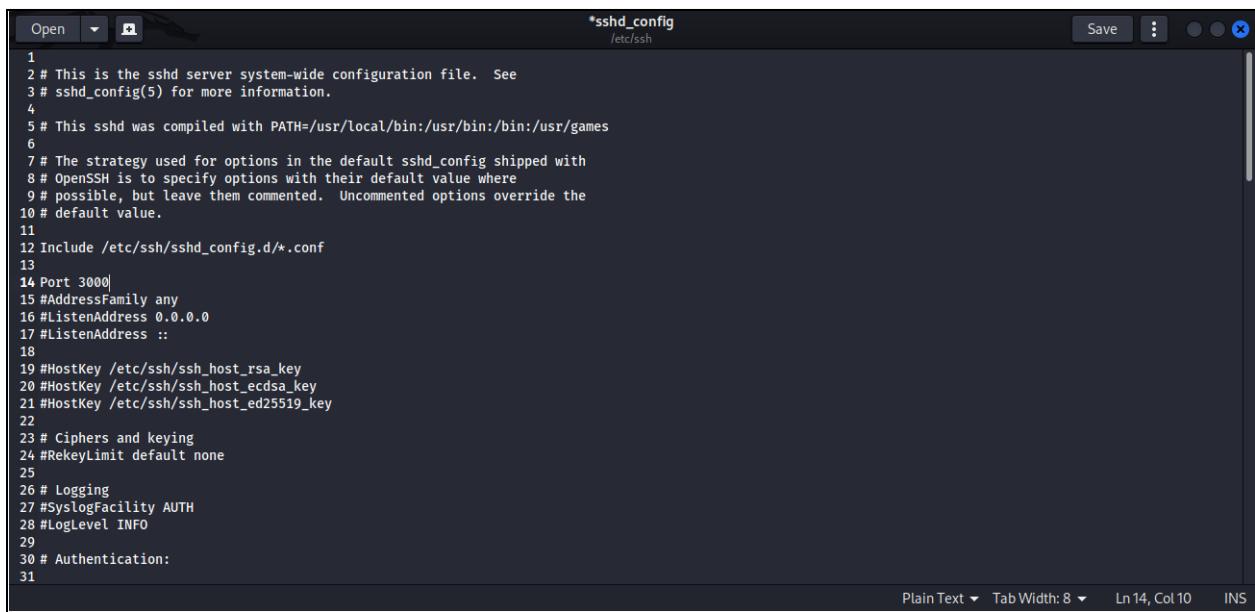


```
sshd_config
/etc/ssh

1 # This is the sshd server system-wide configuration file. See
2 # sshd_config(5) for more information.
4
5 # This sshd was compiled with PATH=/usr/local/bin:/usr/bin:/bin:/usr/games
6
7 # The strategy used for options in the default sshd_config shipped with
8 # OpenSSH is to specify options with their default value where
9 # possible, but leave them commented. Uncommented options override the
10 # default value.
11
12 Include /etc/ssh/sshd_config.d/*.conf
13
14 #Port 22
15 #AddressFamily any
16 #ListenAddress 0.0.0.0
17 #ListenAddress ::

18
19 #HostKey /etc/ssh/ssh_host_rsa_key
20 #HostKey /etc/ssh/ssh_host_ecdsa_key
21 #HostKey /etc/ssh/ssh_host_ed25519_key
22
23 # Ciphers and keying
24 #RekeyLimit default none
25
26 # Logging
27 #SyslogFacility AUTH
28 #LogLevel INFO
29
30 # Authentication:
31
```

Plain Text ▾ Tab Width: 8 ▾ Ln 1, Col 1 INS



```
*sshd_config
/etc/ssh

1 # This is the sshd server system-wide configuration file. See
2 # sshd_config(5) for more information.
4
5 # This sshd was compiled with PATH=/usr/local/bin:/usr/bin:/bin:/usr/games
6
7 # The strategy used for options in the default sshd_config shipped with
8 # OpenSSH is to specify options with their default value where
9 # possible, but leave them commented. Uncommented options override the
10 # default value.
11
12 Include /etc/ssh/sshd_config.d/*.conf
13
14 Port 3000
15 #AddressFamily any
16 #ListenAddress 0.0.0.0
17 #ListenAddress ::

18
19 #HostKey /etc/ssh/ssh_host_rsa_key
20 #HostKey /etc/ssh/ssh_host_ecdsa_key
21 #HostKey /etc/ssh/ssh_host_ed25519_key
22
23 # Ciphers and keying
24 #RekeyLimit default none
25
26 # Logging
27 #SyslogFacility AUTH
28 #LogLevel INFO
29
30 # Authentication:
31
```

Plain Text ▾ Tab Width: 8 ▾ Ln 14, Col 10 INS

```
*sshd_config  
/etc/ssh  
Open Save : X  
92 #X11UseLocalhost yes  
93 #PermitTTY yes  
94 PrintMotd no  
95 #PrintLastLog yes  
96 #TCPKeepAlive yes  
97 #PermitUserEnvironment no  
98 #Compression delayed  
99 ClientAliveInterval 10000000  
100 ClientAliveCountMax 3  
101 #UseDNS no  
102 #PidFile /run/sshd.pid  
103 #MaxStartups 10:30:100  
104 #PermitTunnel no  
105 #ChrootDirectory none  
106 #VersionAddendum none  
107  
108 # no default banner path  
109 #Banner none  
110  
111 # Allow client to pass locale environment variables  
112 AcceptEnv LANG LC_*
```

```
rifat@kali: ~
File Actions Edit View Help

(rifat@kali)-[~]
$ sudo service ssh status
● ssh.service - OpenBSD Secure Shell server
  Loaded: loaded (/lib/systemd/system/ssh.service; disabled; preset: disabled)
  Active: inactive (dead)
    Docs: man:sshd(8)
           man:sshd_config(5)

(rifat@kali)-[~]
$ sudo service ssh restart

(rifat@kali)-[~]
$ sudo service ssh status
● ssh.service - OpenBSD Secure Shell server
  Loaded: loaded (/lib/systemd/system/ssh.service; disabled; preset: disabled)
  Active: active (running) since Sun 2023-12-24 12:01:13 EST; 1s ago
    Docs: man:sshd(8)
           man:sshd_config(5)
      Process: 46475 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
 Main PID: 46476 (sshd)
   Tasks: 1 (limit: 4604)
  Memory: 1.6M
    CPU: 31ms
   CGroup: /system.slice/ssh.service
           └─46476 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Dec 24 12:01:12 kali systemd[1]: Starting ssh.service - OpenBSD Secure Shell server...
Dec 24 12:01:13 kali sshd[46476]: Server listening on 0.0.0.0 port 3000.
Dec 24 12:01:13 kali sshd[46476]: Server listening on :: port 3000.
Dec 24 12:01:13 kali systemd[1]: Started ssh.service - OpenBSD Secure Shell server.

(rifat@kali)-[~]
$
```

Firewall Configuration using UFW

Here, we implement **UFW** (Uncomplicated Firewall) as our Intrusion Prevention System (IPS). Our approach involves initially denying access to all ports, followed by selectively allowing specific ports to enhance security. Specifically, we permit traffic on port 80 for HTTP, port 443 for HTTPS, port 53 for DNS, and port 3000 for SSH. This meticulous configuration acts as a robust barrier against unauthorized access to other ports, fortifying the server's defenses effectively.

```
sudo apt install ufw
sudo ufw default allow outgoing
sudo ufw default deny incoming
sudo ufw enable
sudo ufw allow 80
sudo ufw allow 443
sudo ufw allow 53
sudo ufw allow 3000
```

```
rifat@kali: ~
File Actions Edit View Help

└─(rifat㉿kali)-[~]
$ sudo apt install ufw
[sudo] password for rifat:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  iptables libip4tc2 libip6tc2 libxtables12
Suggested packages:
  firewalld rsyslog
The following NEW packages will be installed:
  iptables libip6tc2 ufw
The following packages will be upgraded:
  libip4tc2 libxtables12
2 upgraded, 3 newly installed, 0 to remove and 657 not upgraded.
Need to get 600 kB of archives.
After this operation, 3414 kB of additional disk space will be used.
Do you want to continue? [Y/n] y\
Get:1 http://kali.cs.nycu.edu.tw/kali kali-rolling/main amd64 libip4tc2 amd6
4 1.8.10-1 [19.2 kB]
Get:2 http://kali.cs.nycu.edu.tw/kali kali-rolling/main amd64 libip6tc2 amd6
4 1.8.10-1 [19.6 kB]
Get:3 http://kali.cs.nycu.edu.tw/kali kali-rolling/main amd64 libxtables12 a
md64 1.8.10-1 [30.8 kB]
Get:4 http://kali.cs.nycu.edu.tw/kali kali-rolling/main amd64 iptables amd64
 1.8.10-1 [363 kB]
Get:5 http://kali.cs.nycu.edu.tw/kali kali-rolling/main amd64 ufw all 0.36.2
-1 [168 kB]
Fetched 600 kB in 3s (179 kB/s)
Preconfiguring packages...
(Reading database ... 145841 files and directories currently installed.)
Preparing to unpack .../libip4tc2_1.8.10-1_amd64.deb ...
Unpacking libip4tc2:amd64 (1.8.10-1) over (1.8.9-2) ...
```



"the quieter you become, the more you are heard"

```
rifat@kali: ~
File Actions Edit View Help
(rifat@kali)-[~]
$ sudo ufw default allow outgoing
Default outgoing policy changed to 'allow'
(be sure to update your rules accordingly)

(rifat@kali)-[~]
$ sudo ufw default deny incoming
Default incoming policy changed to 'deny'
(be sure to update your rules accordingly)

(rifat@kali)-[~]
$ sudo ufw enable
Firewall is active and enabled on system startup

(rifat@kali)-[~]
$ sudo ufw allow 80
Rule added
Rule added (v6)

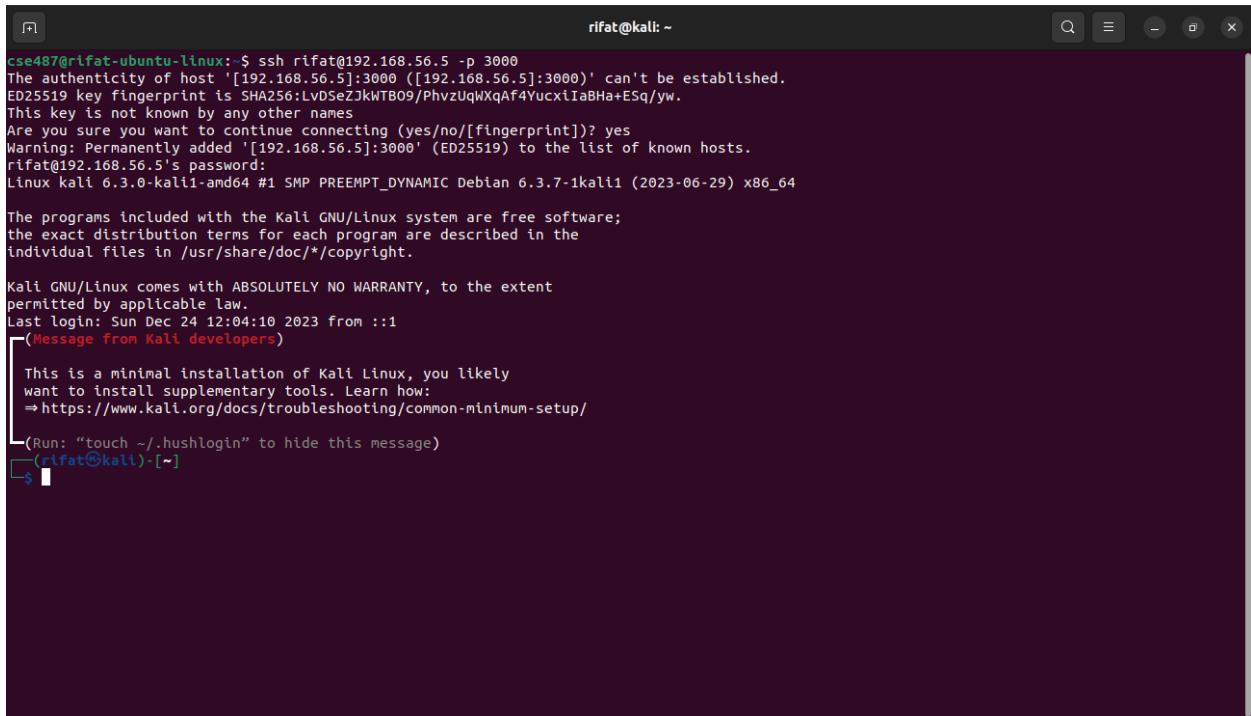
(rifat@kali)-[~]
$ sudo ufw allow 53
Rule added
Rule added (v6)

(rifat@kali)-[~]
$ sudo ufw allow 443
Rule added
Rule added (v6)

(rifat@kali)-[~]
$ sudo ufw allow 3000
Rule added
Rule added (v6)
```

Connect Client with SSH and Sharing Files

```
#copy file using ssh  
#syntax  
#scp -P port_number user@userAddress:copy_path destination_path  
scp -P 3000 rifat@192.168.56.5:/home/rifat/ca/generated/ca.crt  
/home/cse487/Downloads  
  
#copy directories  
scp -r -P 3000 rifat@192.168.56.5:/home/rifat/share  
/home/cse487/Downloads
```



The screenshot shows a terminal window titled 'rifat@kali: ~'. The session is initiated from a host with IP 192.168.56.5 (labeled 'cse487' in the title bar) to a host with IP 192.168.56.5 (labeled 'rifat@kali' in the title bar). The terminal displays the following text:

```
cse487@rifat-ubuntu-linux: $ ssh rifat@192.168.56.5 -p 3000  
The authenticity of host '[192.168.56.5]:3000 ([192.168.56.5]:3000)' can't be established.  
ED25519 key fingerprint is SHA256:LvDSeZJkWTB09/PhvzUqWXqAf4YucxiiABHa+ESq/yw.  
This key is not known by any other names  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Warning: Permanently added '[192.168.56.5]:3000' (ED25519) to the list of known hosts.  
rifat@192.168.56.5's password:  
Linux kali 6.3.0-kali1-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.3.7-1kali1 (2023-06-29) x86_64  
  
The programs included with the Kali GNU/Linux system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*copyright.  
  
Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent  
permitted by applicable law.  
Last login: Sun Dec 24 12:04:10 2023 from ::1  
[Message from Kali developers]  
  
This is a minimal installation of Kali Linux, you likely  
want to install supplementary tools. Learn how:  
⇒ https://www.kali.org/docs/troubleshooting/common-minimum-setup/  
  
(Run: "touch ~/.hushlogin" to hide this message)  
[rifat@kali: ~]
```

```
rifat@kali: ~/ca/generated
cse487@rifat-ubuntu-linux: $ ssh rifat@192.168.56.5 -p 3000
rifat@192.168.56.5's password:
Linux kali 6.3.0-kali1-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.3.7-1kali1 (2023-06-29) x86_64

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sun Dec 24 12:31:39 2023 from 192.168.56.4
(Message from Kali developers)

This is a minimal installation of Kali Linux, you likely
want to install supplementary tools. Learn how:
=>https://www.kali.org/docs/troubleshooting/common-minimum-setup/

(Run: "touch ~/.hushlogin" to hide this message)
[rifat@kali:~]
$ ls
Bind9-DNS-Config  Documents  Music      Pictures   Templates   Videos    openssh
Desktop          Downloads  Nginx-Webserver-Config  Public    'UFW Firewall'  ca

[rifat@kali:~]
$ cd ca
[rifat@kali:~/ca]
$ ls
OpenSSL.txt  generated  root-ca  root-ca.conf  server  sub-ca  sub-ca.conf

[rifat@kali:~/ca]
$ cd generated
[rifat@kali:~/ca/generated]
$ ls
ca.crt  chained.crt  server.crt  server.key  server.pfx  sub-ca.crt

[rifat@kali:~/ca/generated]
```

```
rifat@kali: ~/ca/generated
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sun Dec 24 12:31:39 2023 from 192.168.56.4
(Message from Kali developers)

This is a minimal installation of Kali Linux, you likely
want to install supplementary tools. Learn how:
=>https://www.kali.org/docs/troubleshooting/common-minimum-setup/

(Run: "touch ~/.hushlogin" to hide this message)
[rifat@kali:~]
$ ls
Bind9-DNS-Config  Documents  Music      Pictures   Templates   Videos    openssh
Desktop          Downloads  Nginx-Webserver-Config  Public    'UFW Firewall'  ca

[rifat@kali:~]
$ cd ca
[rifat@kali:~/ca]
$ ls
OpenSSL.txt  generated  root-ca  root-ca.conf  server  sub-ca  sub-ca.conf

[rifat@kali:~/ca]
$ cd generated
[rifat@kali:~/ca/generated]
$ ls
ca.crt  chained.crt  server.crt  server.key  server.pfx  sub-ca.crt

[rifat@kali:~/ca/generated]
$ pwd
/home/rifat/ca/generated

[rifat@kali:~/ca/generated]
$
```

```
cse487@rifat-ubuntu-linux: ~          cse487@rifat-ubuntu-linux: ~          cse487@rifat-ubuntu-linux: ~/Downloads
cse487@rifat-ubuntu-linux: $ scp -P 3000 rifat@192.168.56.5:/home/rifat/ca/generated/ca.crt /home/cse487/Downloads
rifat@192.168.56.5's password:
ca.crt
100% 2029    452.0KB/s   00:00
cse487@rifat-ubuntu-linux: $
```

```
cse487@rifat-ubuntu-linux: ~          cse487@rifat-ubuntu-linux: ~          cse487@rifat-ubuntu-linux: ~
cse487@rifat-ubuntu-linux: $ scp -P 3000 rifat@192.168.56.5:/home/rifat/ca/generated/ca.crt /home/cse487/Downloads
rifat@192.168.56.5's password:
ca.crt
100% 2029    452.0KB/s   00:00
cse487@rifat-ubuntu-linux: $ ls Downloads
Bind9.pdf
Bind9.txt
ca.crt
domain-powerhoster-com-some-interesting-facts-about-domain-name-system-.pdf
'how one user can copy other user file linux in a single machine .pdf'
How-The-Web-Works.webp
'IPS ( Intrusion Prevention System ).pdf'
kali-linux-2023.4-installer-amd64.iso.iso
OpenSSL.txt
Oracle_VM_VirtualBox_Extension_Pack-6.1.38-153438.vbox-extpack
PERFORMANCE.docx
Pictures-20231215T184714Z-001.zip
'Securing a Network System with PKI and Configure Firewall and IDS.pdf'
'Unconfirmed 330535.crdownload'
cse487@rifat-ubuntu-linux: $
```


Certificate import to the client browser

1. Adding the ca.crt File to Firefox:

- **Open Firefox Preferences:** Click the three-line menu in the top right corner, then select "Preferences" or "Options."
- **Navigate to Certificates:** Go to the "Privacy & Security" tab, scroll down to the "Certificates" section, and click the "View Certificates" button.
- **Import the Certificate:**
 - Under the "Authorities" tab, click the "Import" button.
 - Locate the ca.crt file on your computer and select it.
 - Check the box "Trust this CA to identify websites" and click "OK."

2. Clearing Browser Cache:

- **Access Cache Clearing:** In Firefox, go to "Preferences" or "Options" and find the "Privacy & Security" section.
- **Clear Cache and Data:** Look for options like "Clear history" or "Clear cache and cookies" and select the appropriate items to clear.

3. Checking Network Connection:

- **Verify Connection:** Ensure your device is connected to the correct network.
- **Check Network Settings:** Open your device's network settings and confirm that it's connected to the intended network.

4. Checking DNS Settings:

- **Automatic DNS:** If using automatic DNS, ensure it's configured correctly in your network settings.
- **Manual DNS:** If using manual DNS, follow these steps:
 - **Access DNS Settings:** Locate the DNS settings in your network configuration.
 - **Enter DNS Server IP:** Enter the IP address of your Bind9 DNS server.

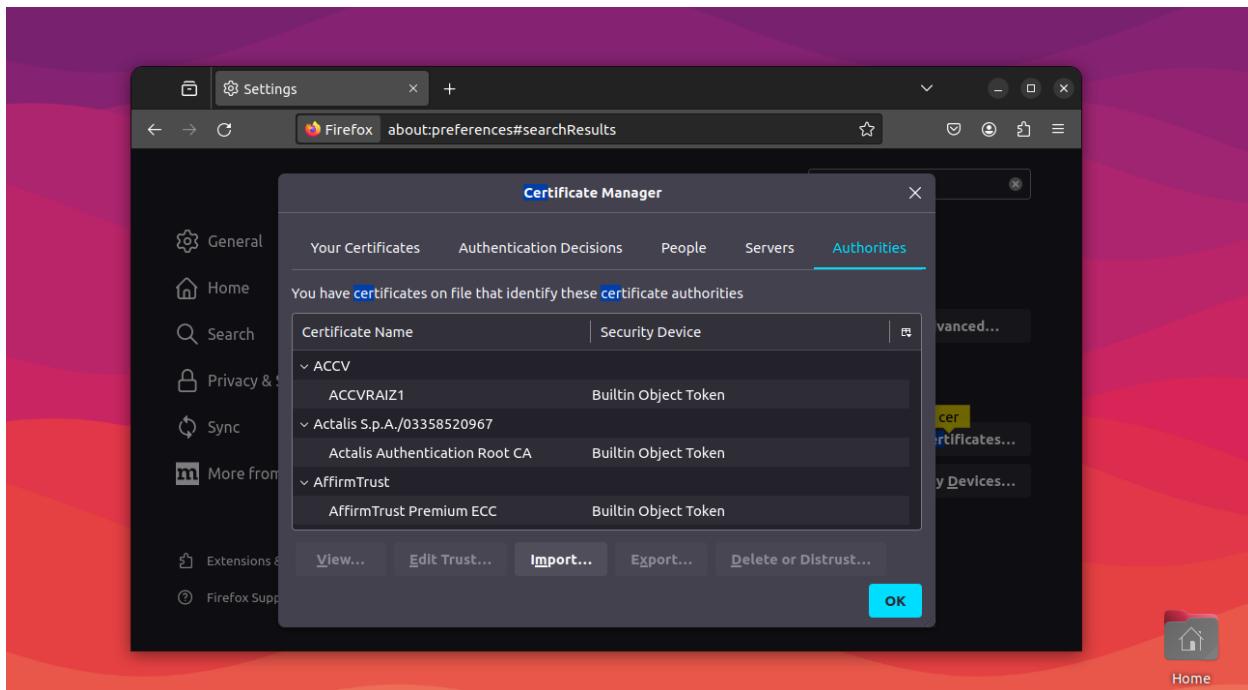
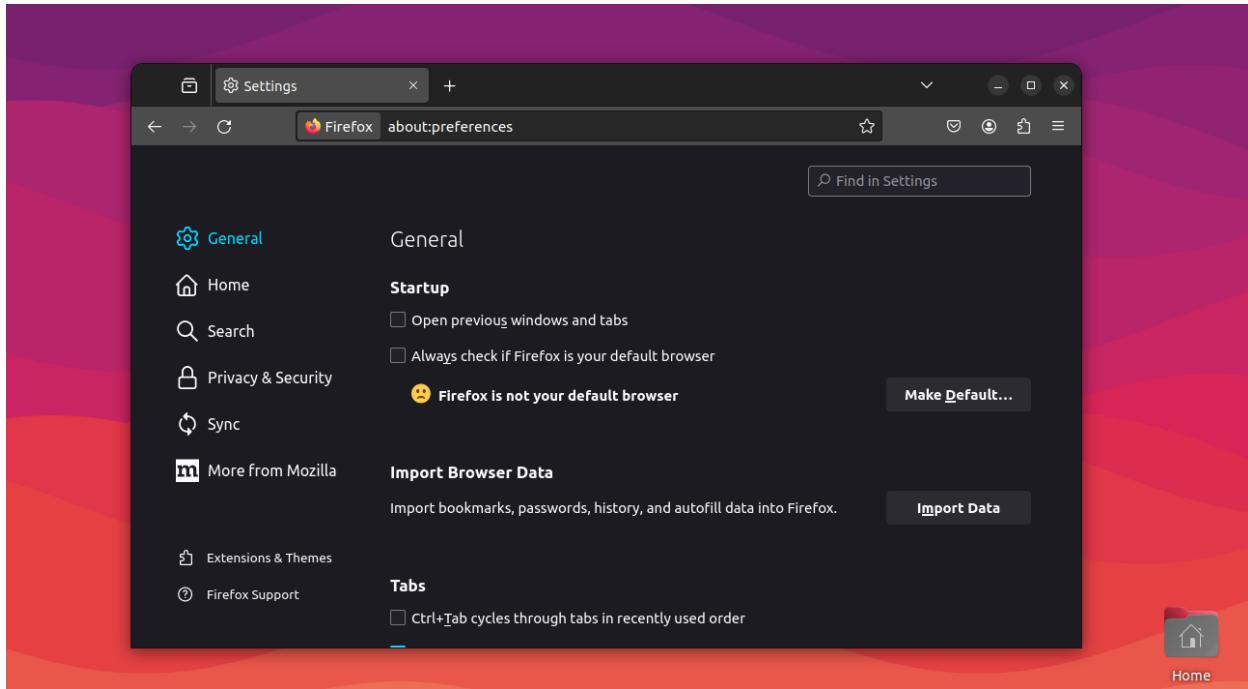
5. Restarting Network:

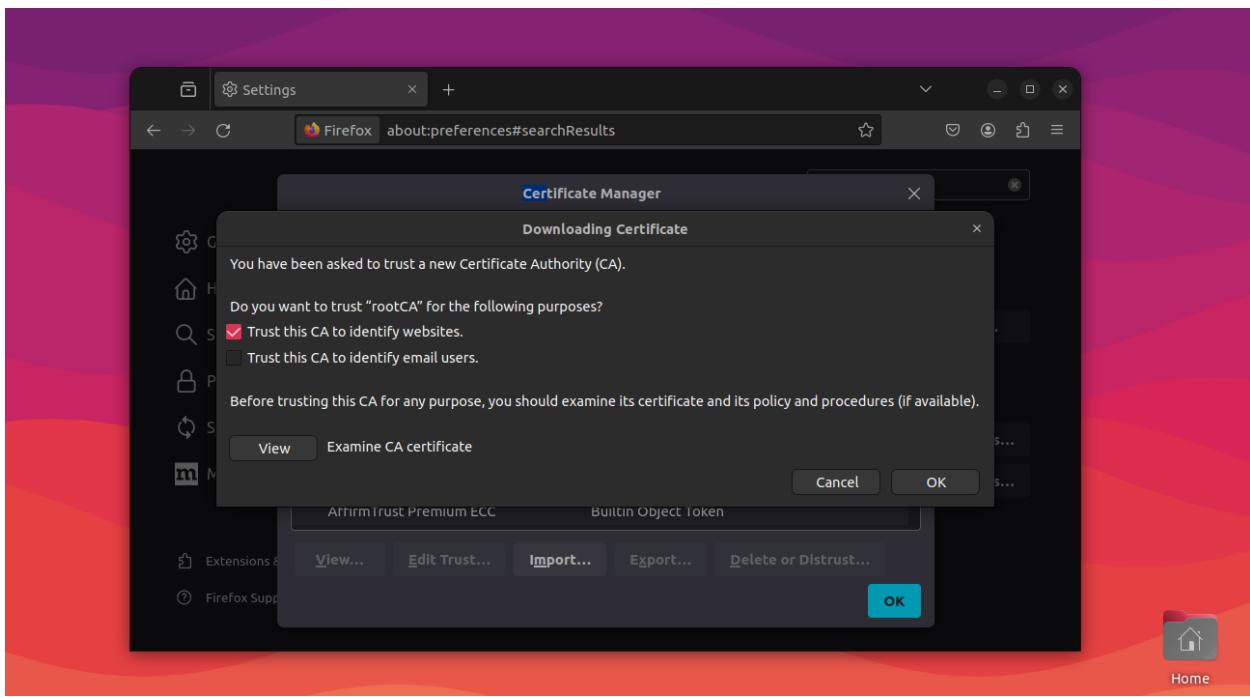
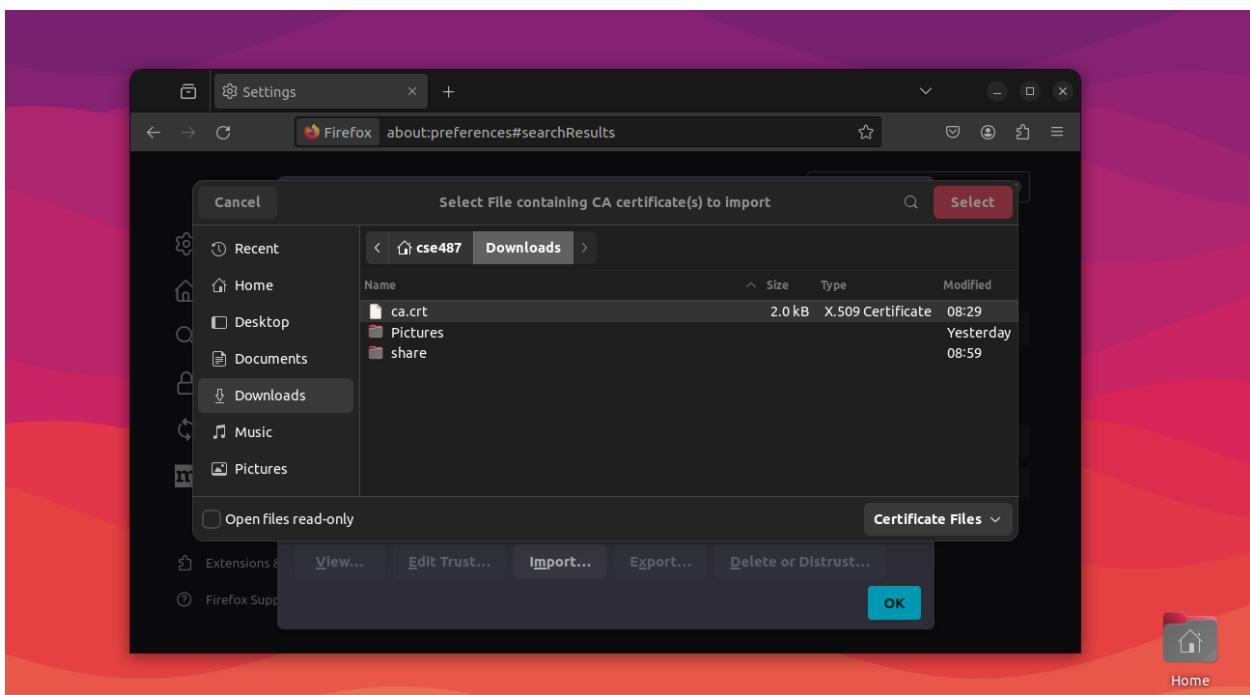
- **Restart Network:** Disconnect and reconnect to your network, or restart your network device.

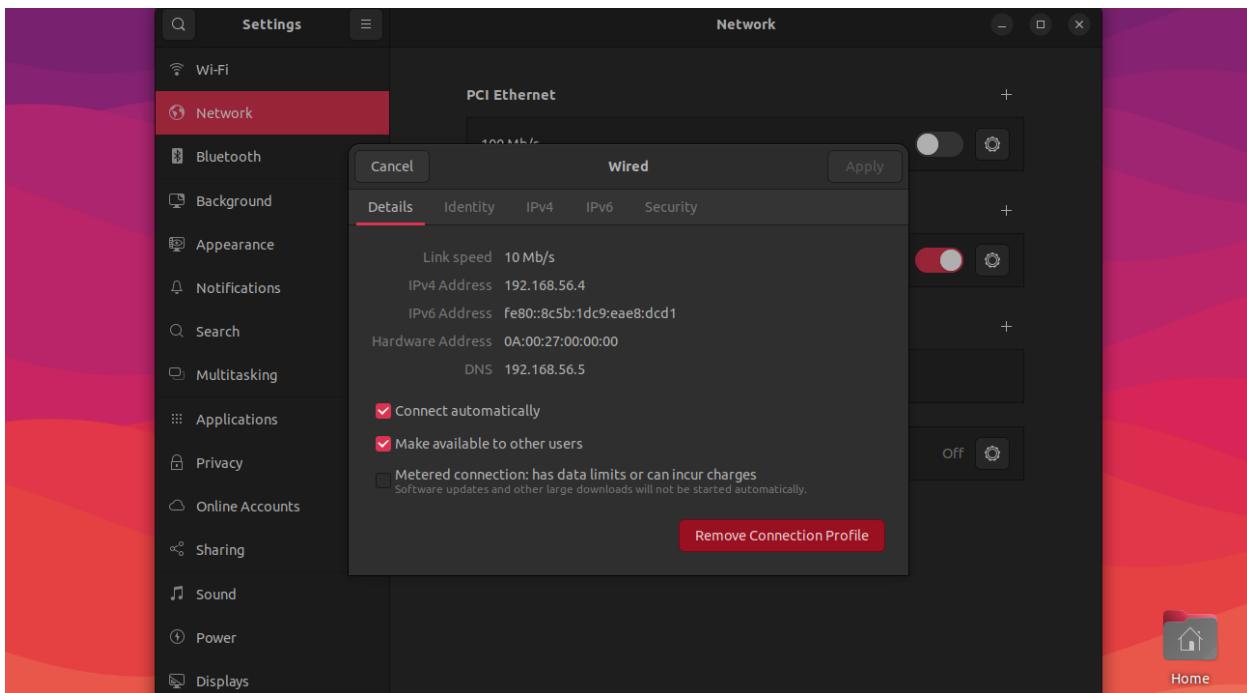
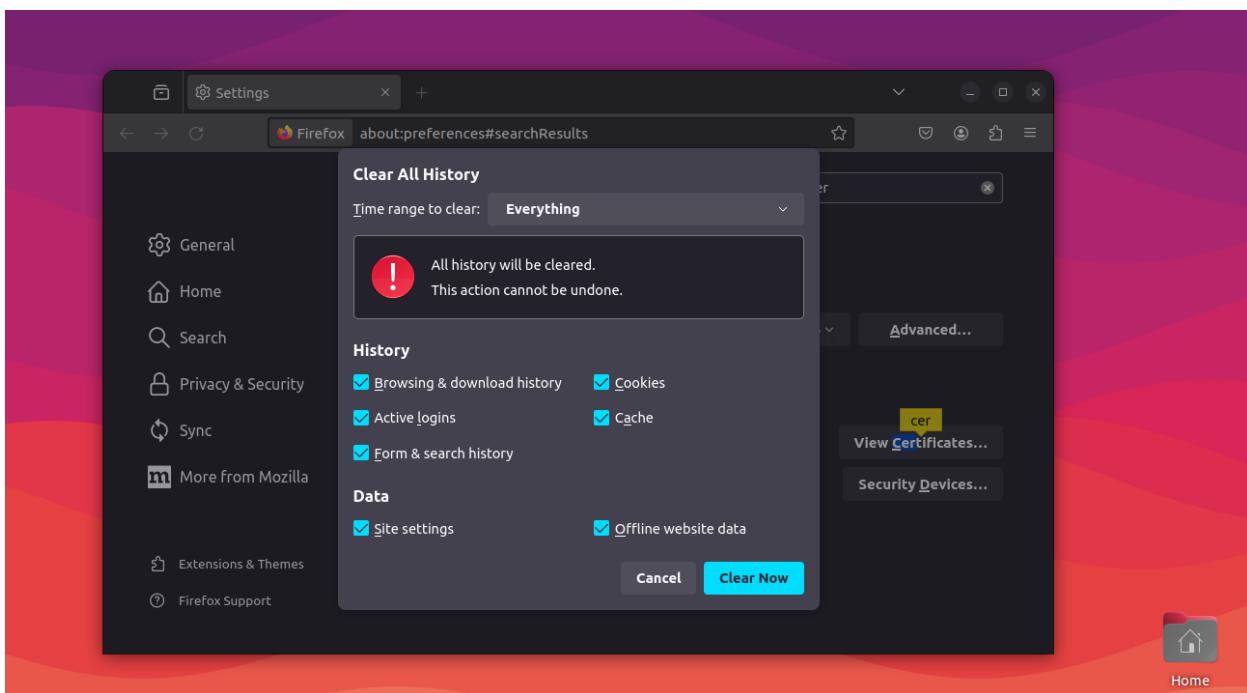
6. Accessing the Website:

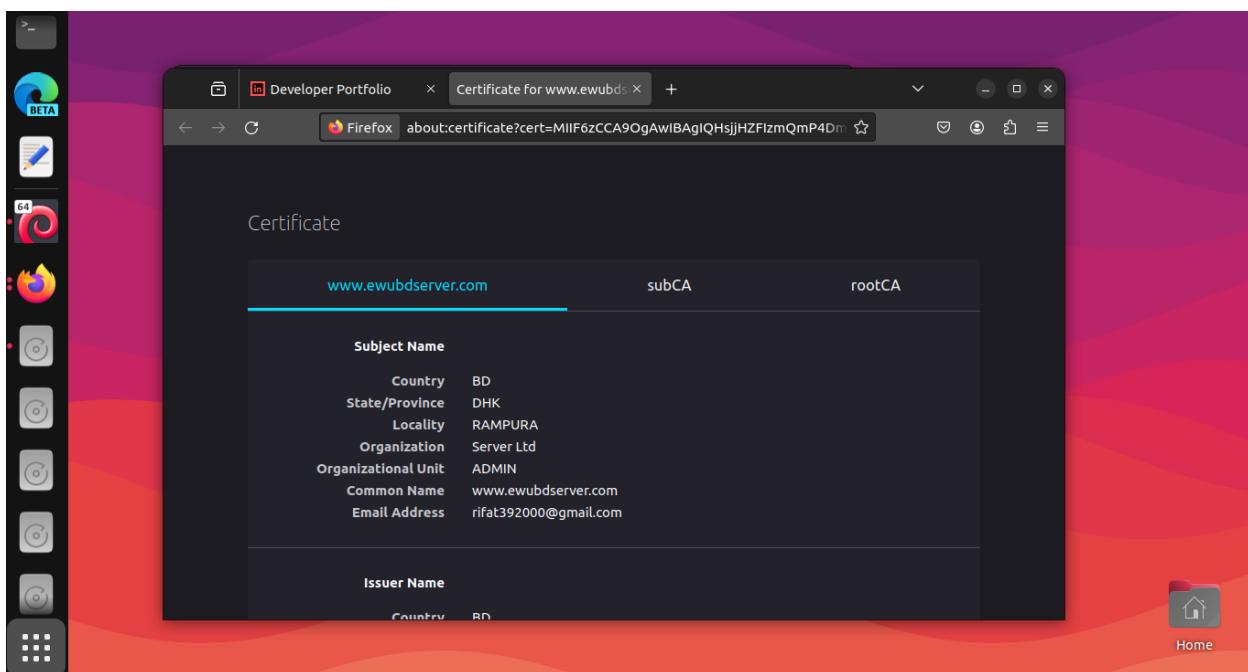
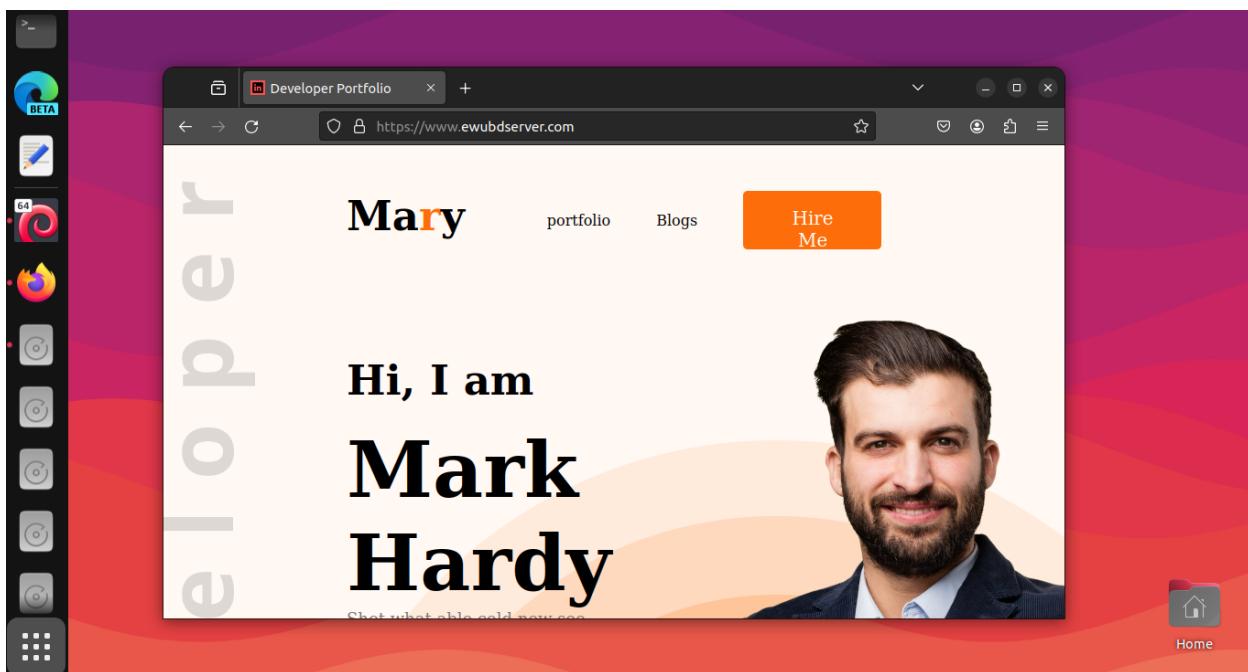
- **NSLOOKUP Command into Terminal:** nslookup www.ewubdserver.com

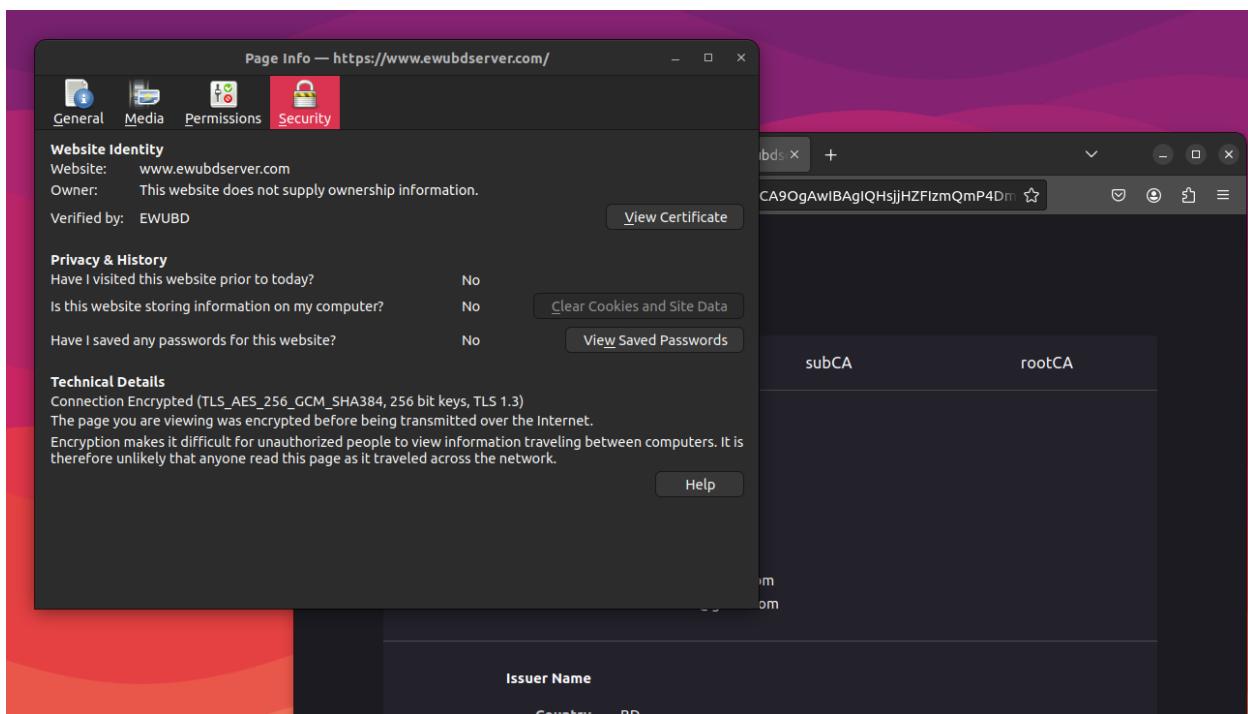
- **Enter Web Address:** After completing these steps, enter the web address of the website in your browser. You should now be able to access it securely with SSL.











SYN Flood and Smurf Attacks: A Responsible Approach

SYN Flood Attacks:

- **Mechanism:**
 - Attackers exploit the TCP three-way handshake by sending a large number of SYN (synchronization) packets to a target server.
 - The server allocates resources for each expected connection but never receives the final ACK (acknowledgement) packets to complete the handshakes.
 - This overwhelms the server's resources, potentially leading to service denial.
 - More information about SYN Flood attack read this article <https://www.cloudflare.com/learning/ddos/syn-flood-ddos-attack/>

Smurf Attacks:

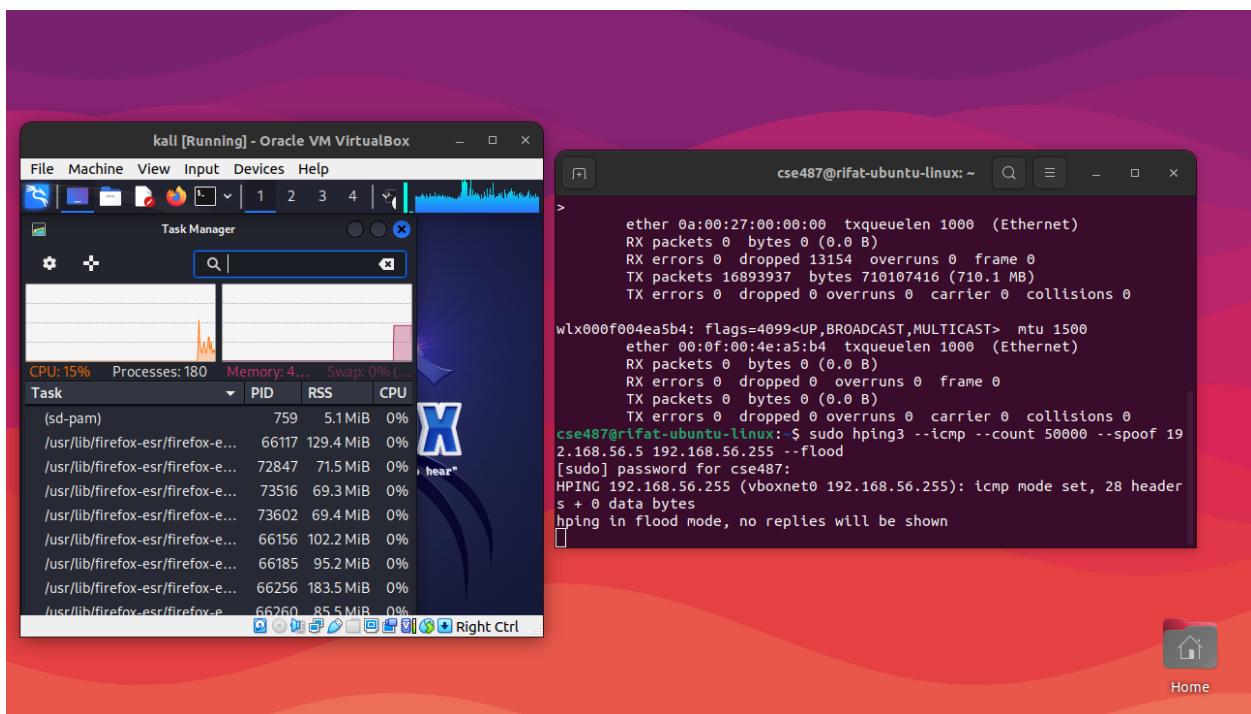
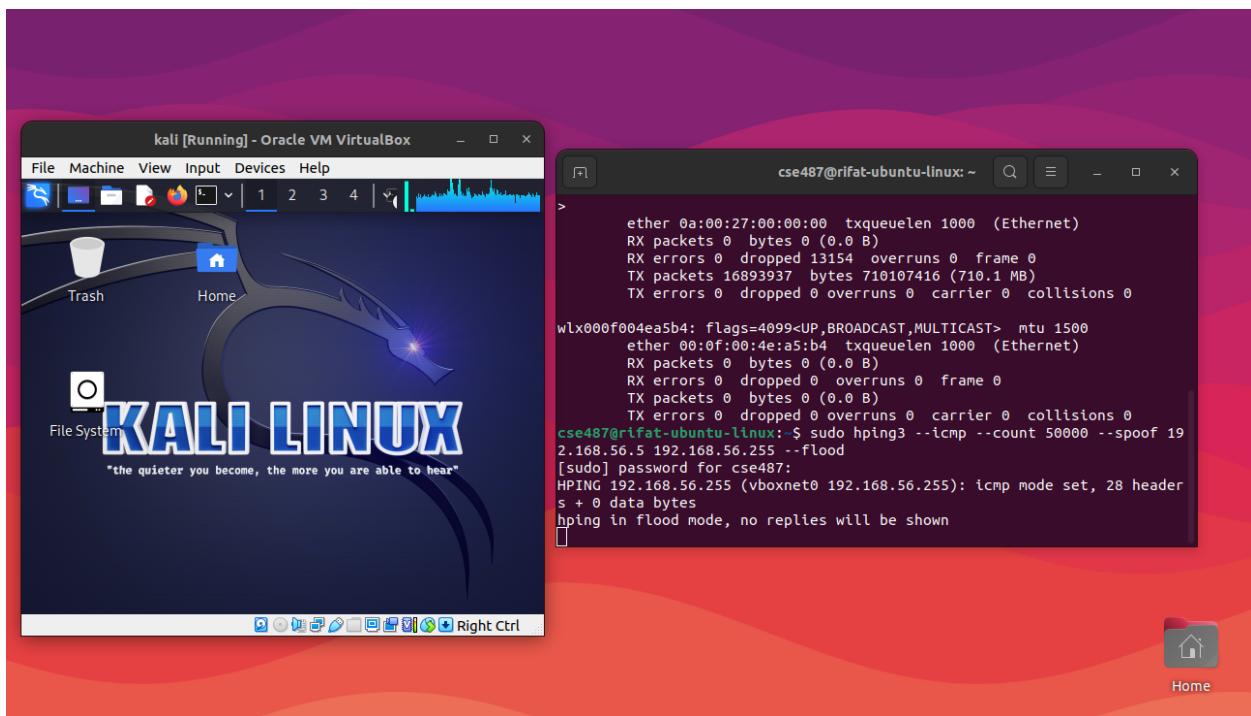
- **Mechanism:**
 - Attackers send spoofed ICMP (ping) packets to broadcast IP addresses on a network.
 - These packets appear to originate from the target victim's IP address.
 - Network devices respond to the pings, flooding the victim with a large volume of traffic, potentially overwhelming its resources.

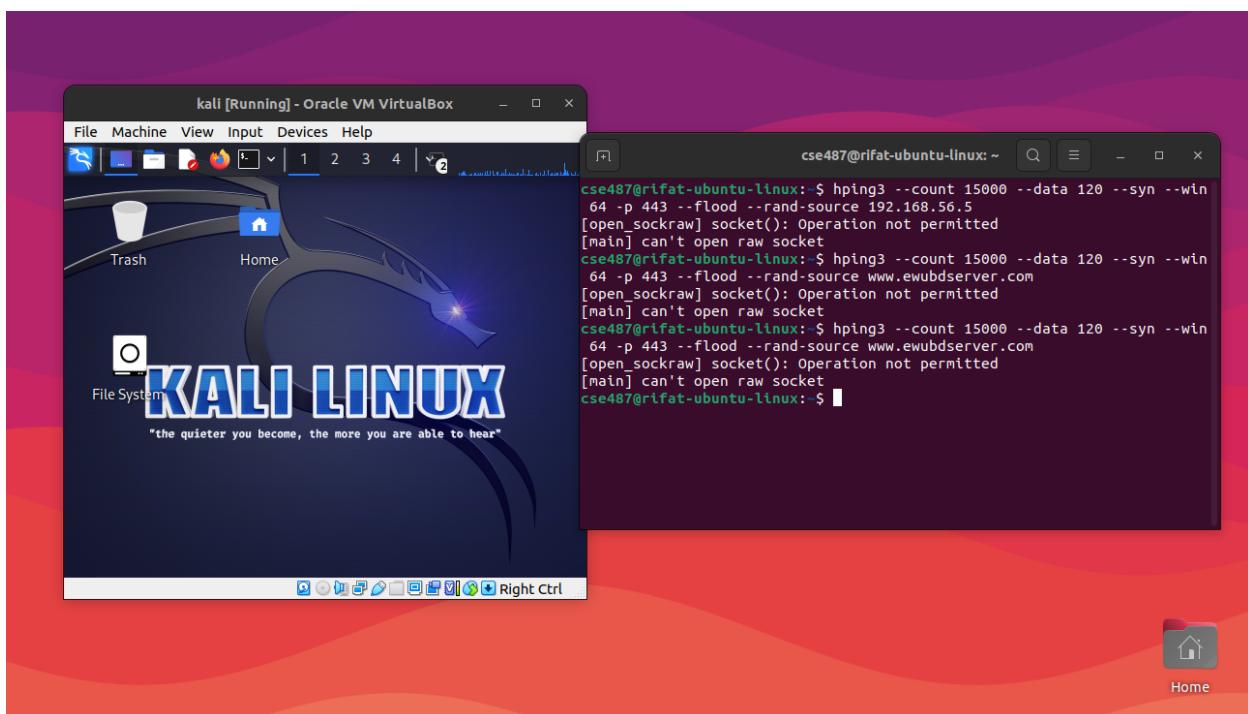
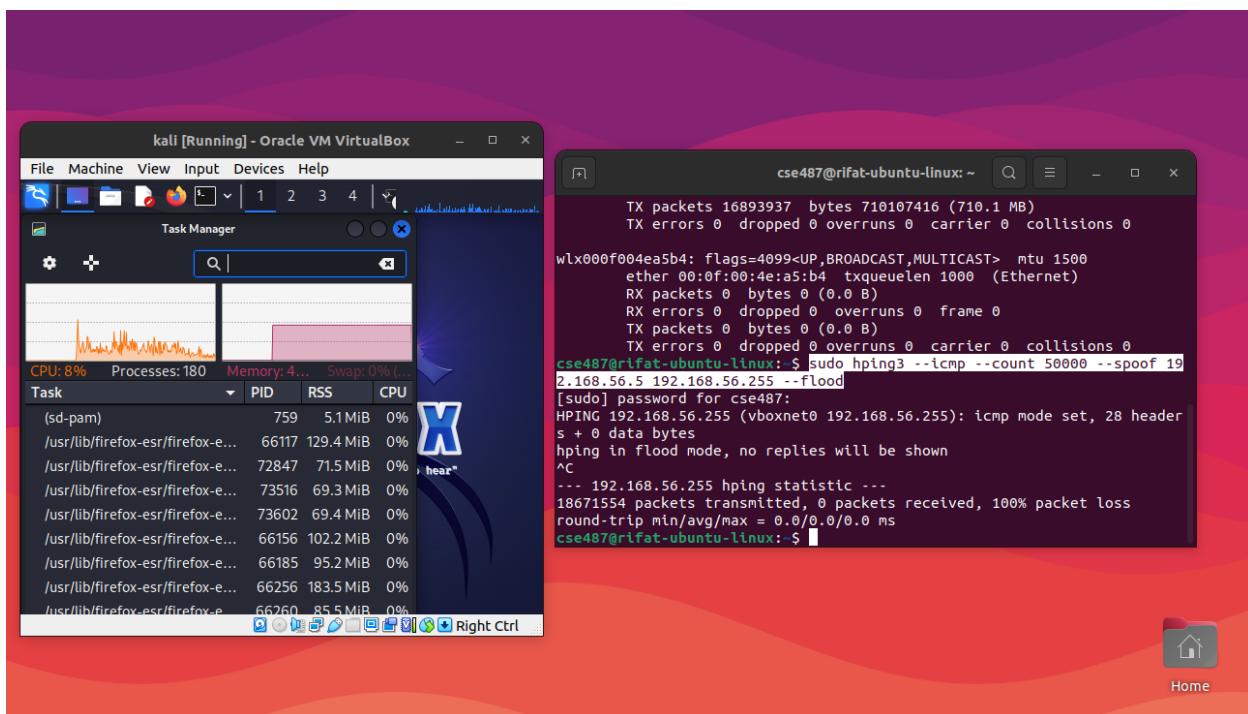
Remember:

- Unauthorized attacks can have severe legal and ethical consequences.
- Prioritize understanding and preventing attacks rather than conducting them.
- Use your knowledge responsibly to contribute to a more secure digital world.

Here we use **hping3**. hping3 is a command-line-oriented TCP/IP packet assembler/analyzer. It supports TCP, UDP, ICMP, and RAW-IP protocols, has a traceroute mode, the ability to send files between a covered channel, and many other features.

```
#SYN-FLOOD attacks
hping3 --count 15000 --data 120 --syn --win 64 -p 443 --flood
--rand-source www.ewubdserver.com
#Dos smurf attack
sudo hping3 --icmp --count 50000 --spoof 192.168.56.5
192.168.56.255 --flood
```





Github Link

<https://github.com/Rifat392000/SSLCertificatesGenerate>