Exercise 1 - Create a Self-signed Certificate

A certificate is a technique of safeguarding communication between two entities or between users and a Web server. It is difficult to interpret the information once a certificate, such as an SSL or TLS certificate, encrypts the communication during transmission. capturing the moment If a certificate is not used, information sent over the Internet is sent in an unencrypted format. clear-text format that can be readily intercepted SSL is no longer in use and has been phased out. TLS has taken its place. You have the option of using a third-party certificate or creating a self-signed certificate.

In this exercise, you will learn to create a self-signed certificate.

Topology

DOMAIN = networktute.com

NTKALIVM1 = Kali 2022.1 - Standalone Server

Prerequisite

- *VMware Workstation 16 Pro*
    - When making this tutorial, we used the “Windows Server 2019” VM Template and “Windows 10 & later” VM Template. Since VMware didn’t have the updated templates.
- *Kali Linux 2022.1*

Task 1: Create a Self-signed Certificate

A self-signed certificate can be produced by anybody and is utilized for individual or internal use in an organization. Web browsers, in any case, do not trust self-signed certificates.

Now Let's, create a self-signed certificate.

NOTE: Since this is Test environment we will use a common password "toor". But Please make sure you always your complex password to prevent problems.

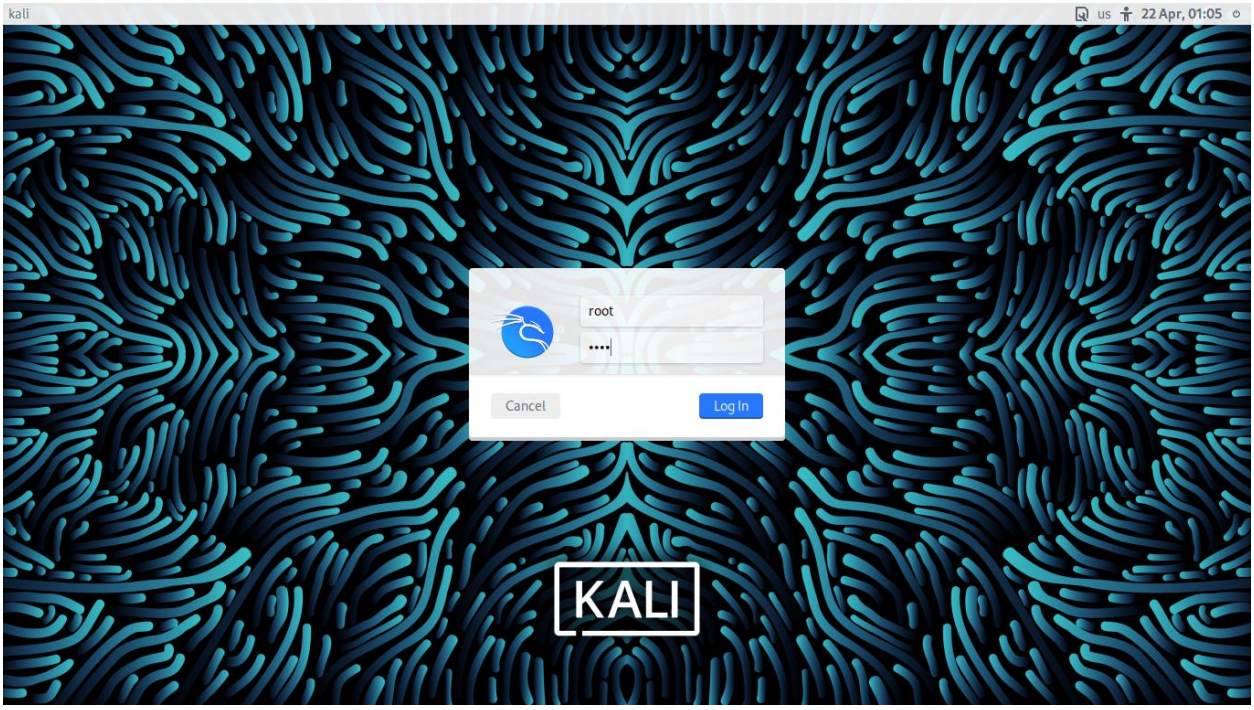
Step 1:

Connect to NTKALIVM1.

In the **Enter your username** text box, type the following: ***root***

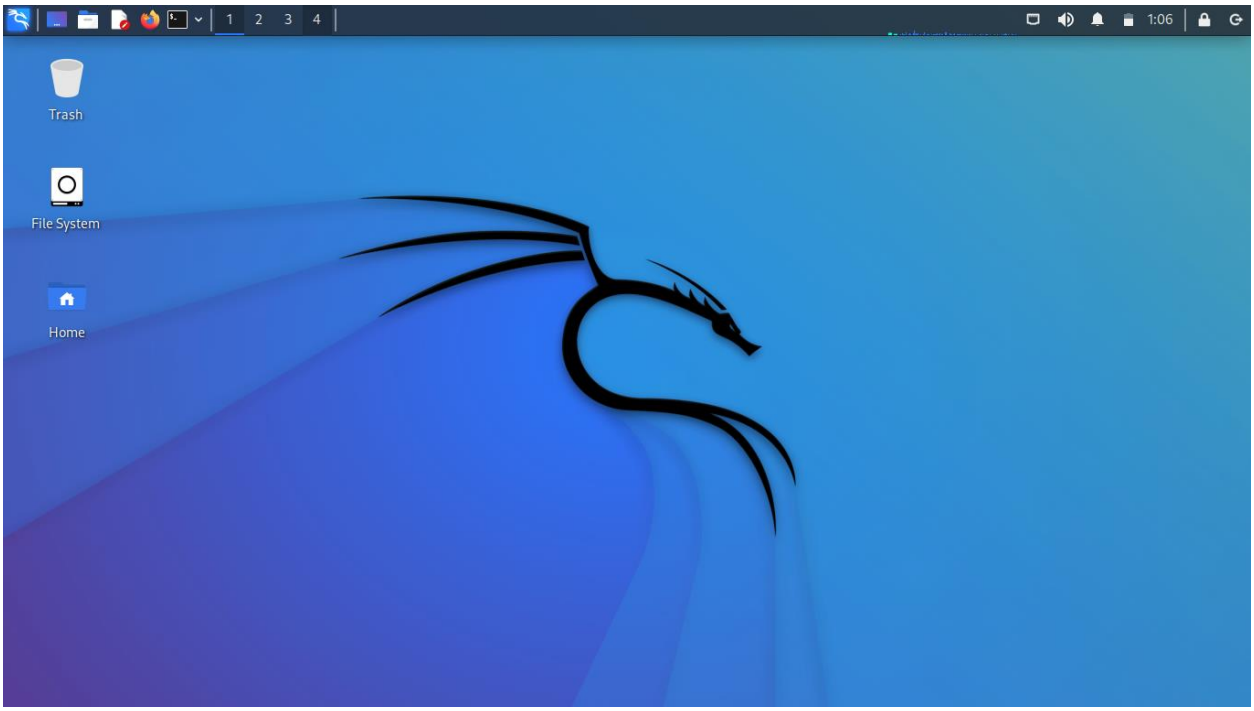
In the **Enter your password** text box, type the following: ***toor***

Click **Log In** or press **Enter**.



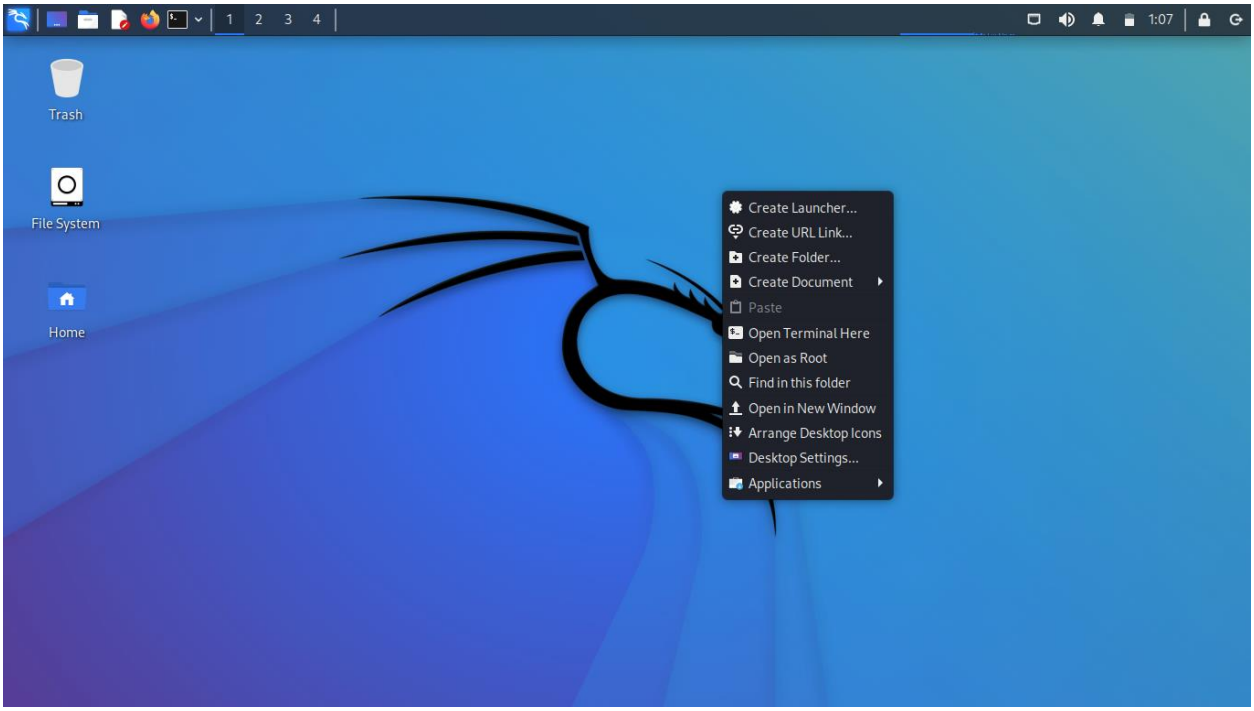
Step 2:

After a successful login, the desktop is displayed.



Step 3:

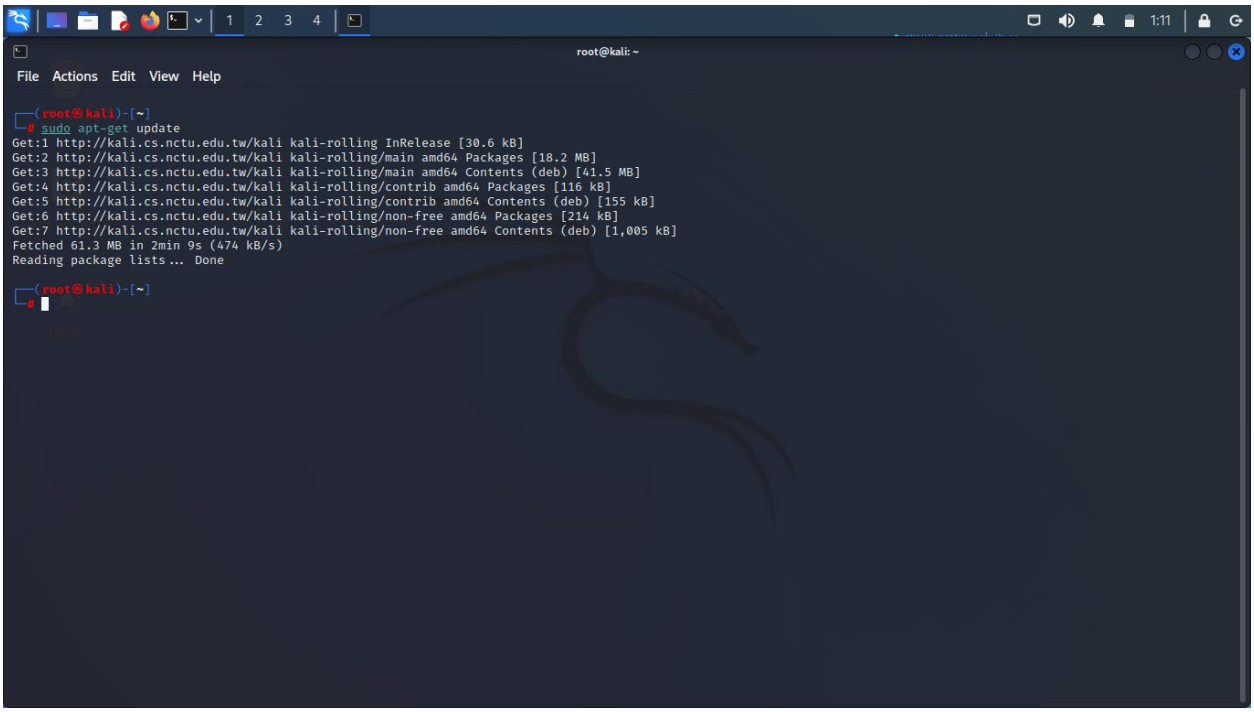
On the desktop, right-click and select **Open Terminal Here**.



Step 4:

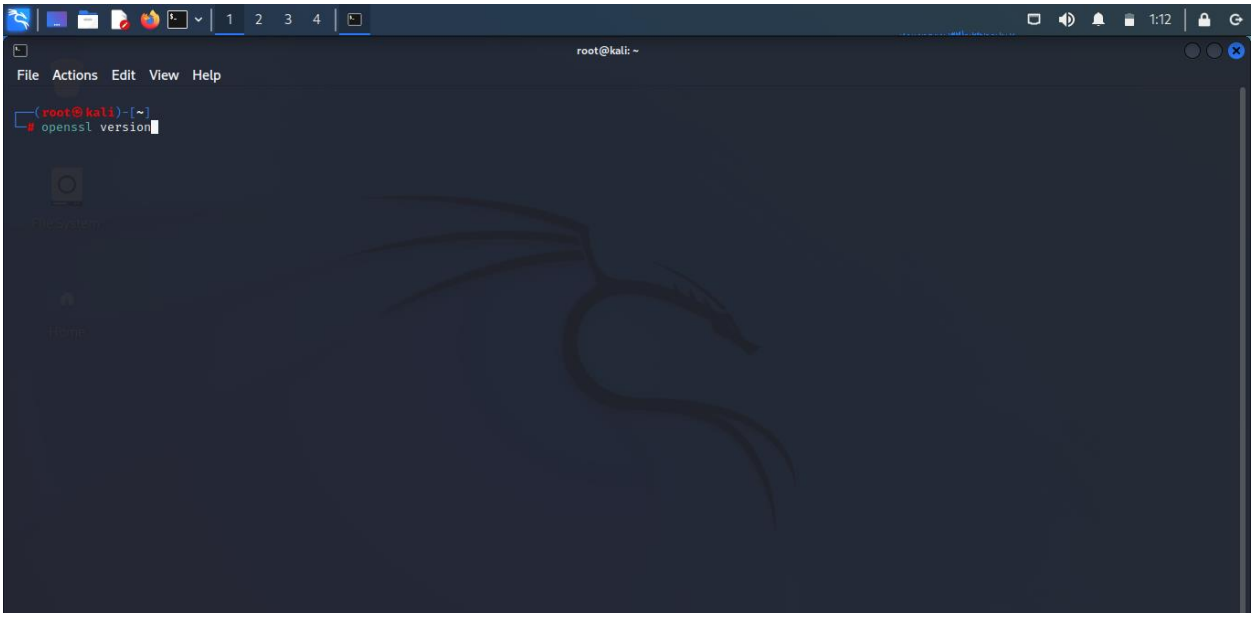
To create a self-signed certificate, you need to install the **openssl** package

Before proceeding with the installation, Let's do a system update by Typing: ***sudo apt-get update***



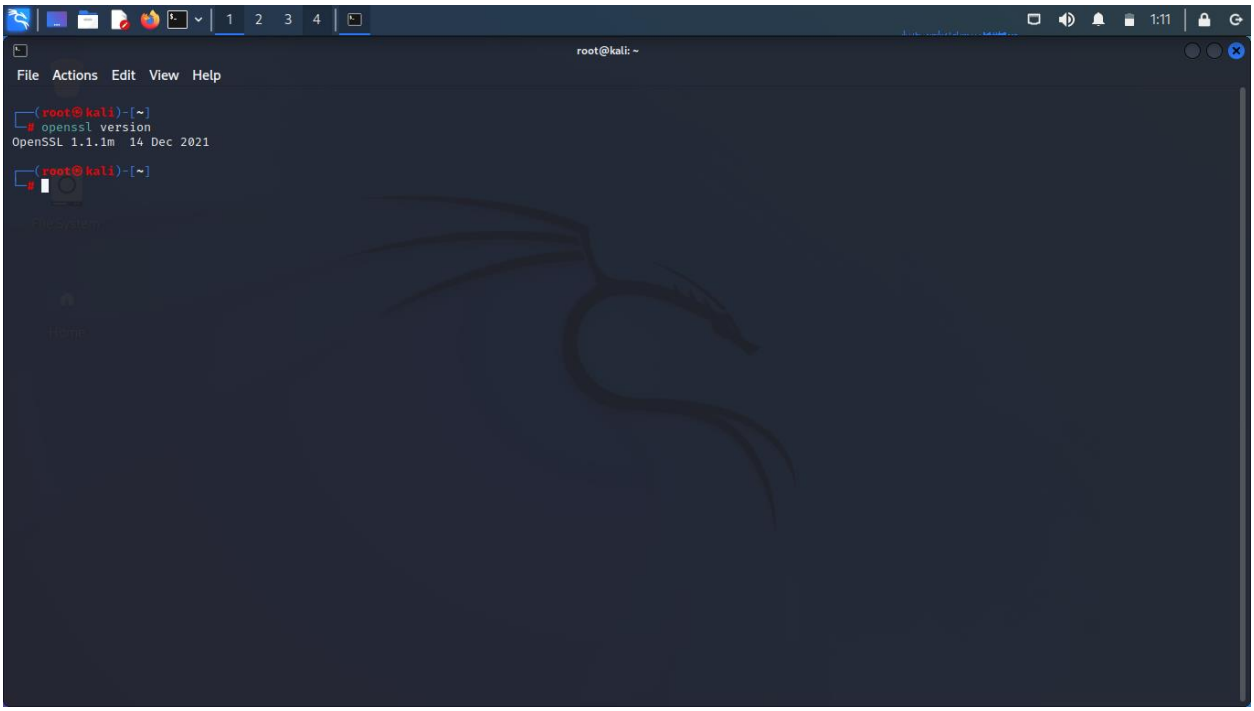
Step 5:

You can check if **openssl** is already installed. Type the following command: ***openssl version***



Step 6:

Notice that the output displays the openssl version.



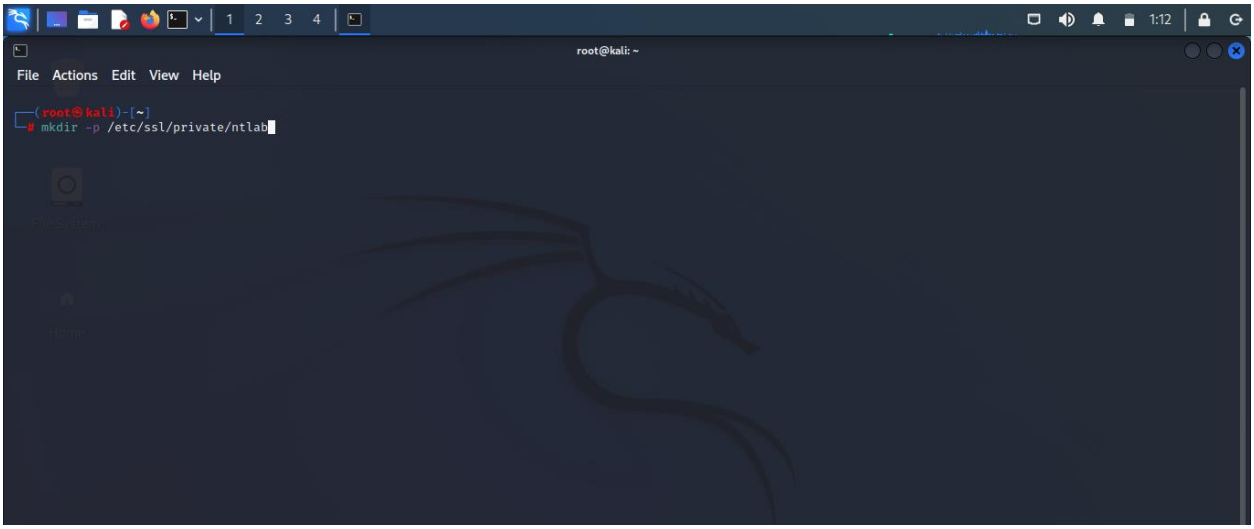
Step 7:

Clear the screen by entering the following command: ***clear***

First, you need to create a new directory for storing the private key. Type the following command:

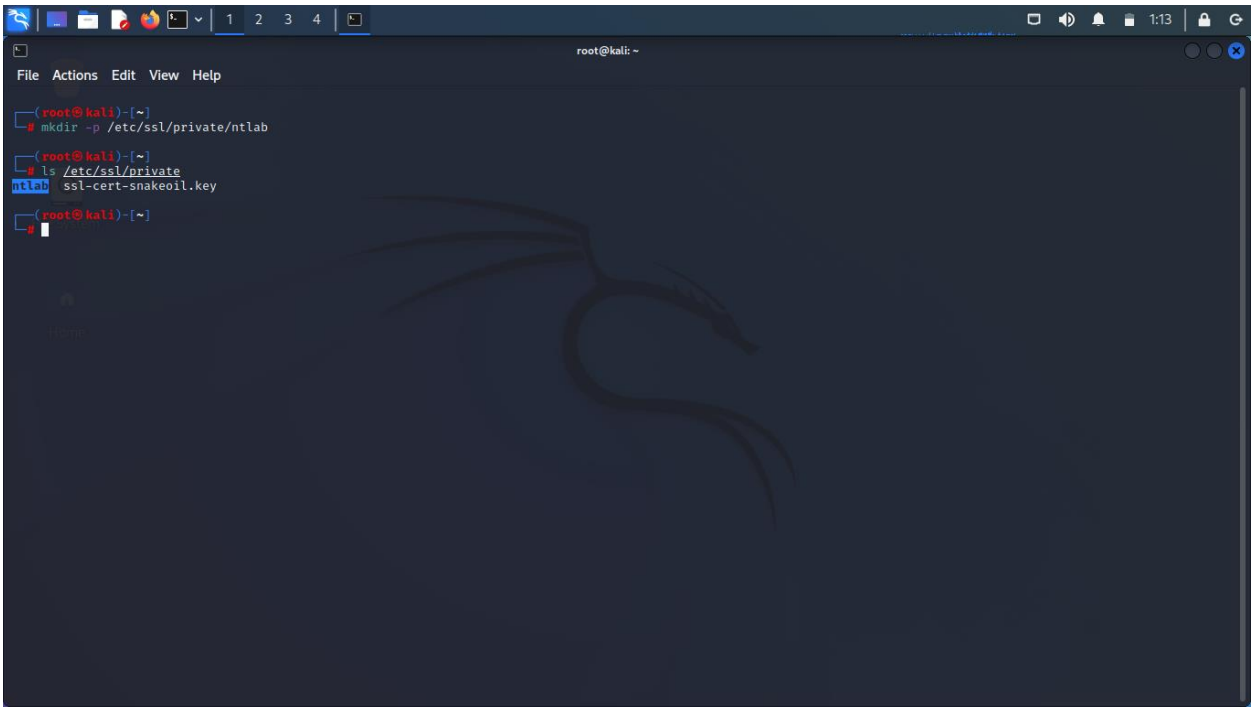
```
mkdir -p /etc/ssl/private/ntlab
```

Press **Enter**.



Step 8:

The directory is now created.

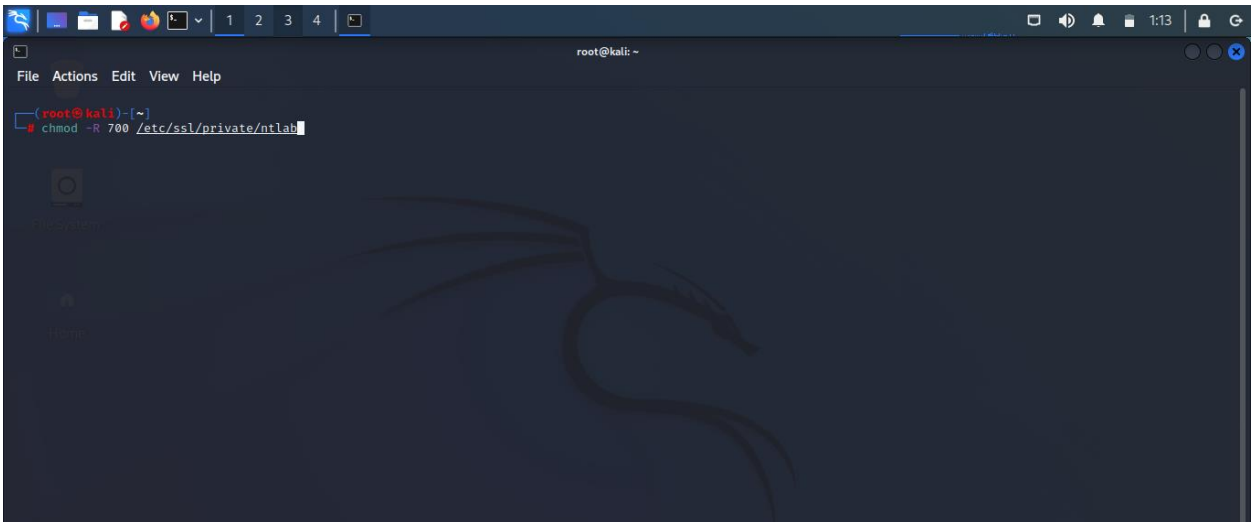


Step 9:

You need to ensure that the directory is not readable by anyone except the root user. Type the following command:

```
chmod -R 700 /etc/ssl/private/ntlab
```

Press **Enter**.



Step 10:

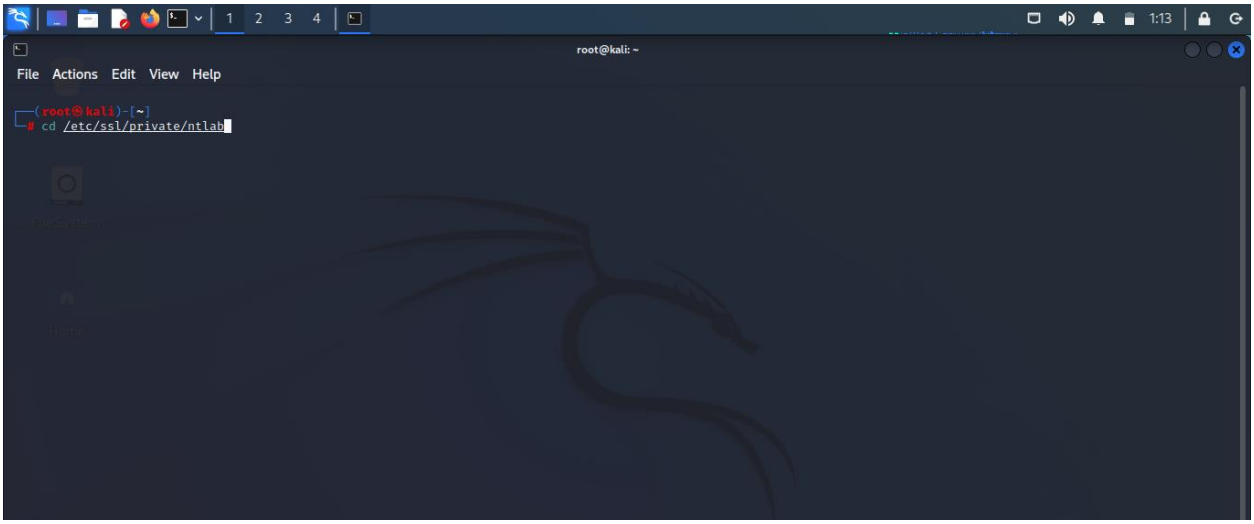
Only the root user now has read, write, and execute permissions on this directory. Other users do not have any permissions.

Step 11:

You need to now navigate to the newly-created directory. Type the following command:

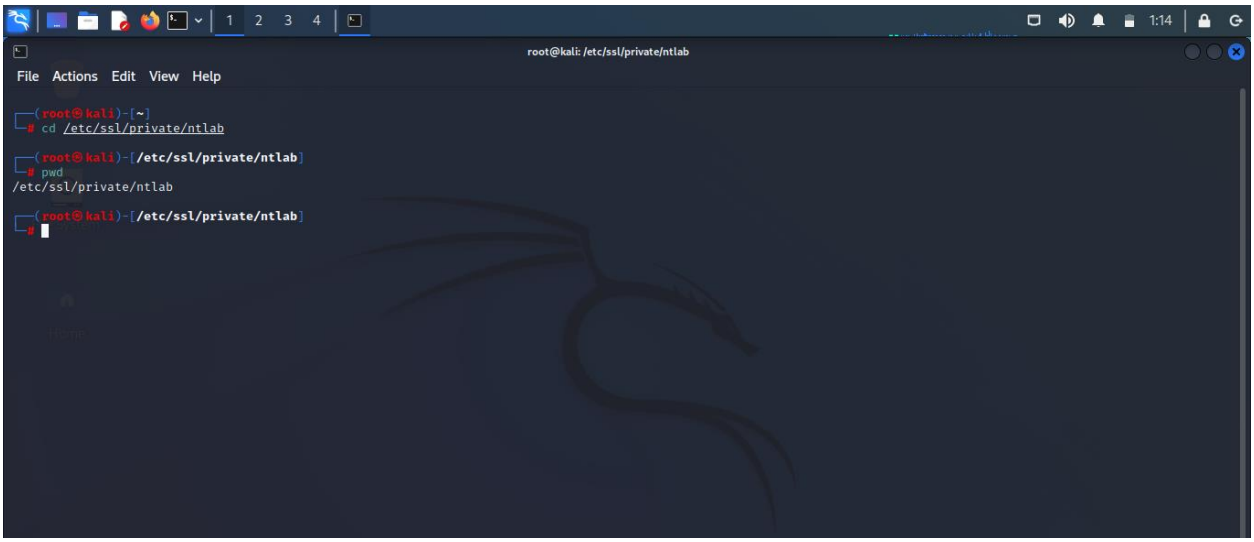
```
cd /etc/ssl/private/ntlab
```

Press **Enter**.



Step 12:

Notice that you have navigated to the directory successfully.



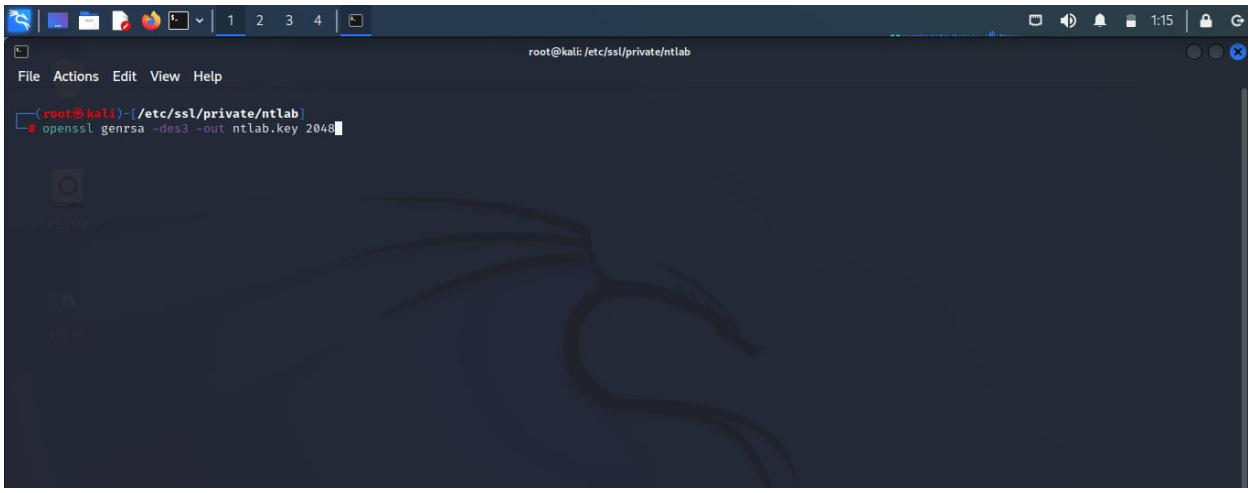
Step 13:

Clear the screen by entering the following command: ***clear***

You will now generate the key with the **openssl** command. Type the following command:

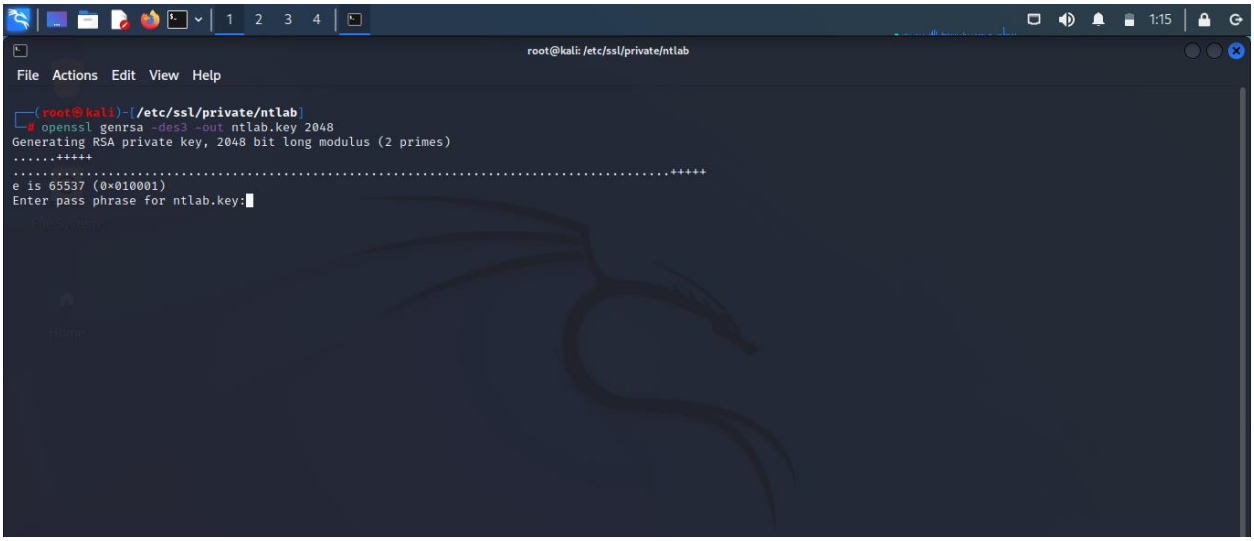
```
openssl genrsa -des3 -out ntlab.key 2048
```

Press **Enter**.



Step 14:

Notice that you are now prompted for a password.



Step 15:

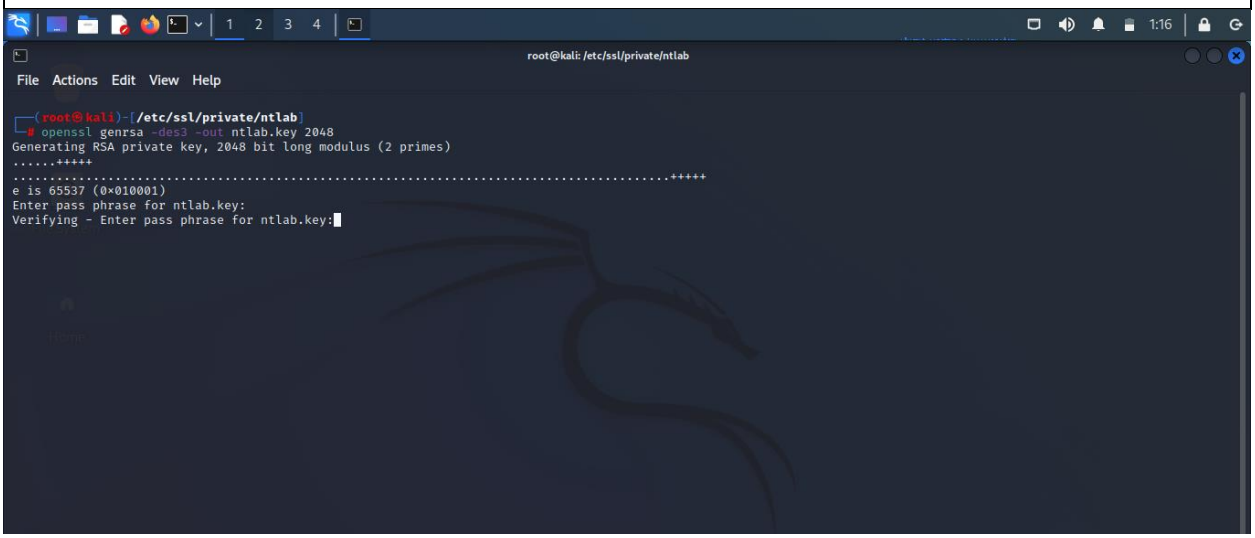
You need to now enter the passphrase. When prompted, type the following passphrase: ***toor***

Press **Enter**.

You will be prompted for the re-confirmation of the passphrase. Type the following: ***toor***

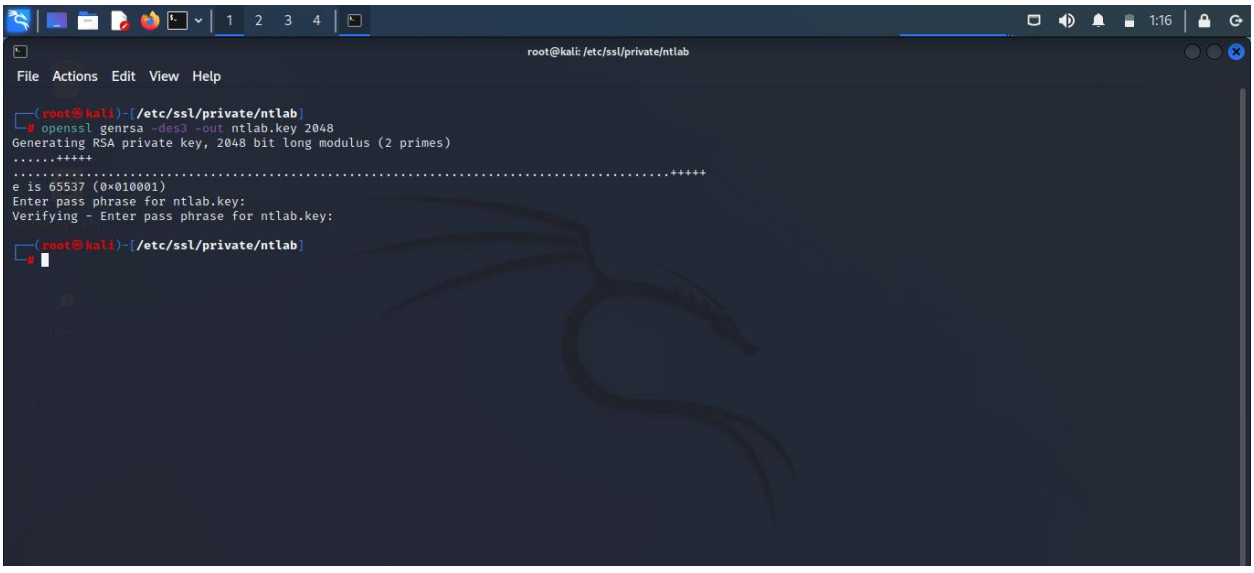
Press **Enter**.

Note: The cursor will not move when provoked to enter a pass express in the terminal and it'll not be shown whereas creating the key with the openssl command.



Step 16:

The password has now been set.



Step 17:

Clear the screen by entering the following command: ***clear***

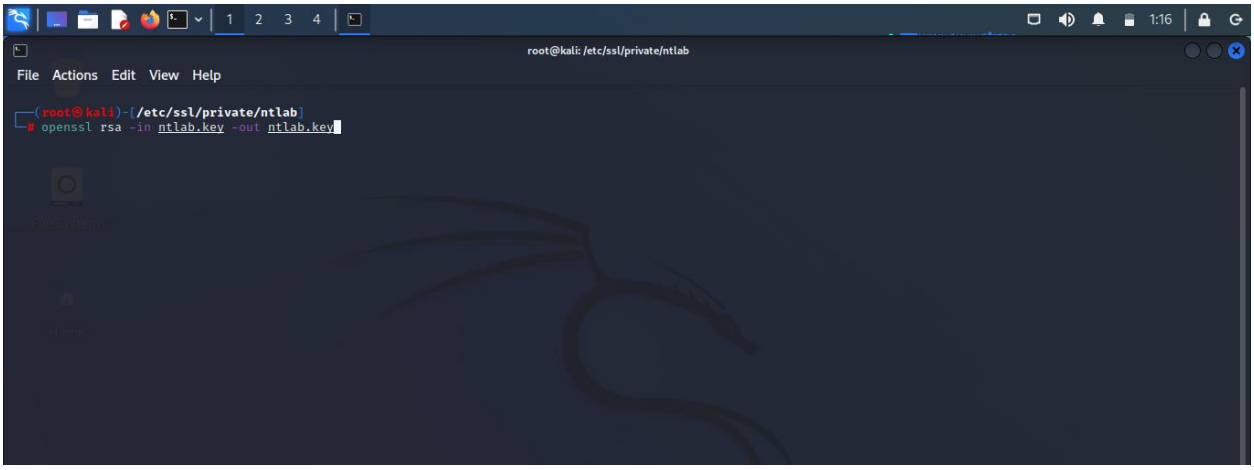
You should now remove the passphrase from the private key. Type the following command:

```
openssl rsa -in ntlab.key -out ntlab.key
```

Press **Enter**.

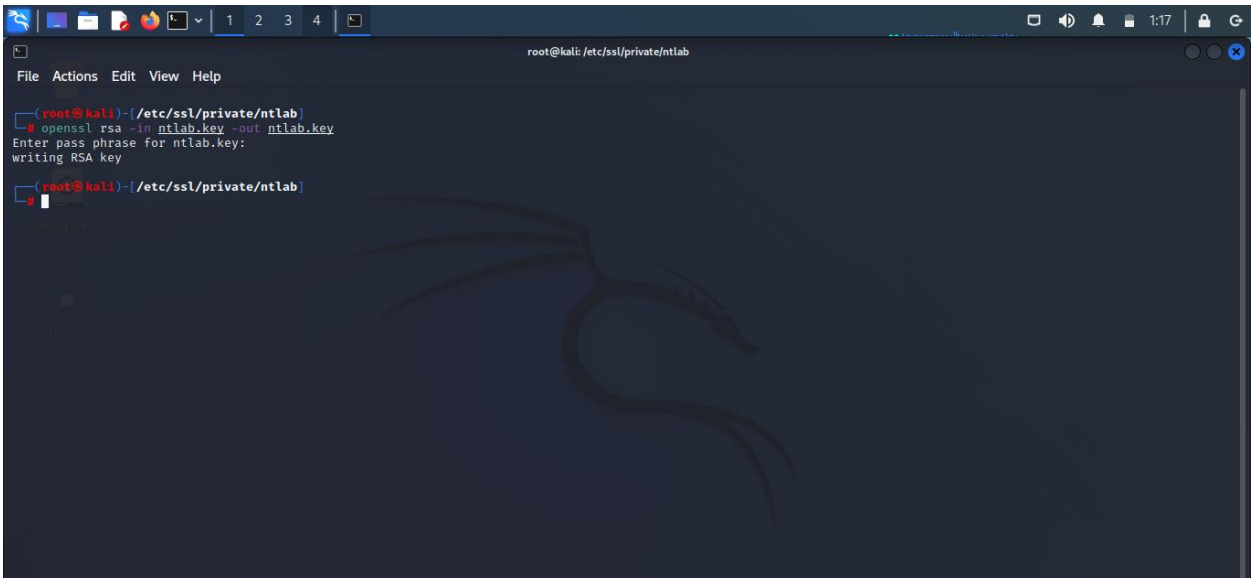
When prompted, type the following passphrase: ***toor***

Press **Enter**.



Step 18:

The passphrase is now removed from **ntlab.key**.



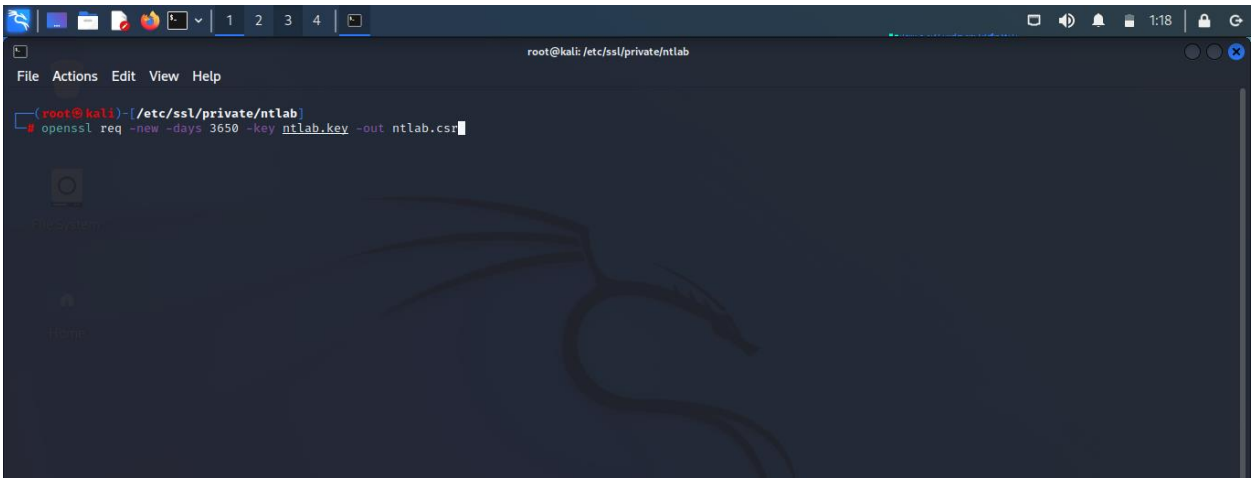
Step 19:

Clear the screen by entering the following command: ***clear***

As the next step, you need to generate the Certificate Signing Request (CSR). Type the following command:

```
openssl req -new -days 3650 -key ntlab.key -out ntlab.csr
```

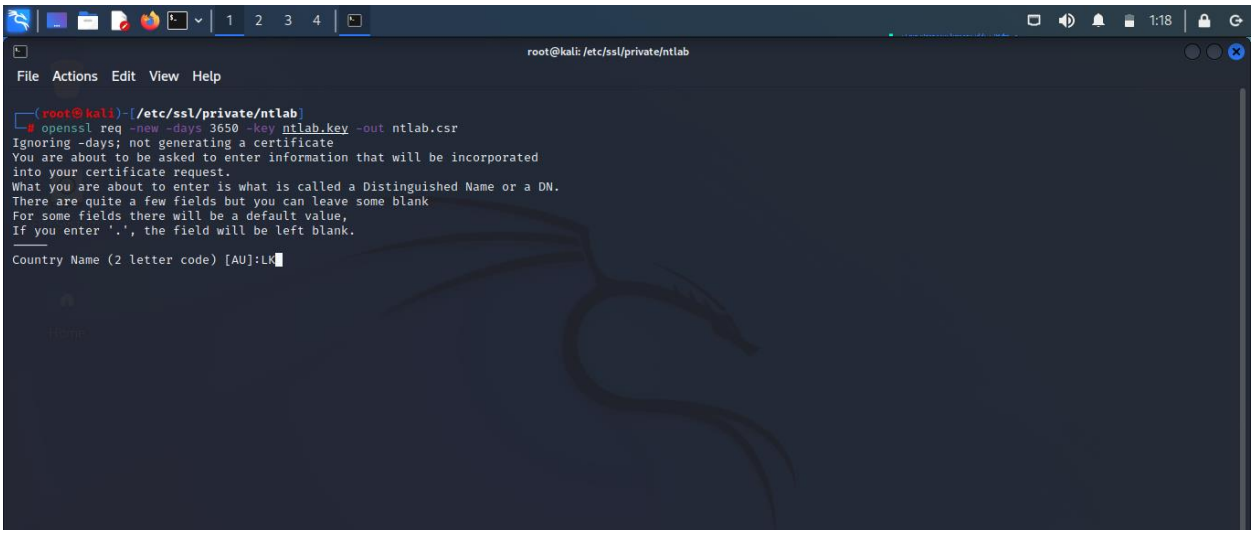
Press **Enter**.



Step 20:

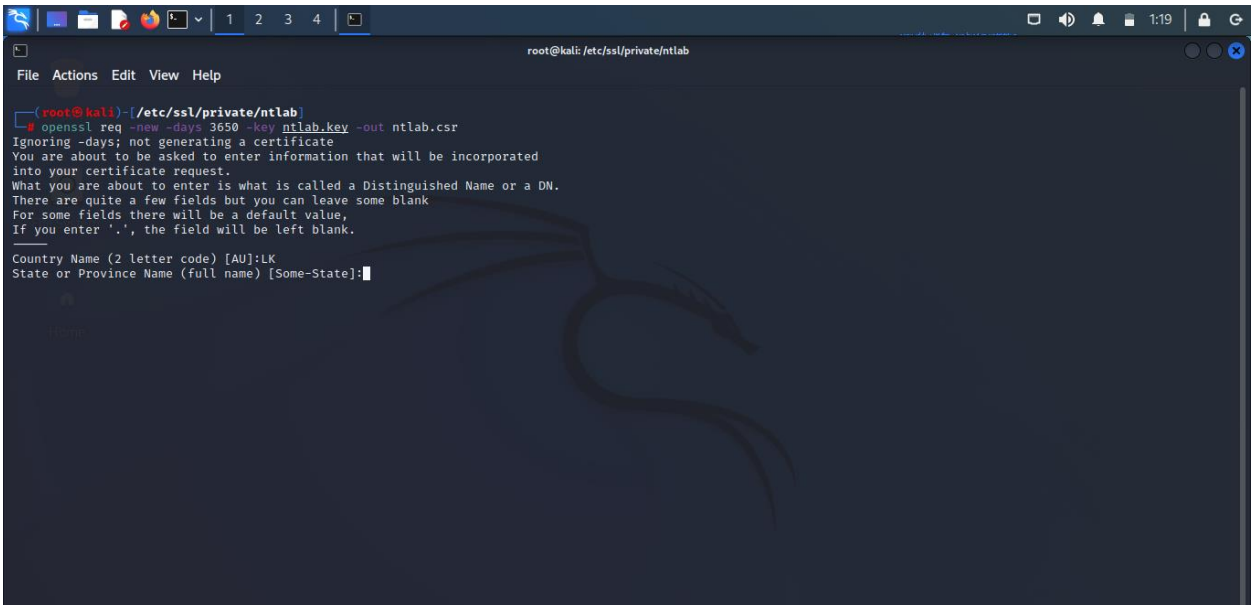
When prompted for the country name, type the following command: ***LK***

Press **Enter**.



Step 21:

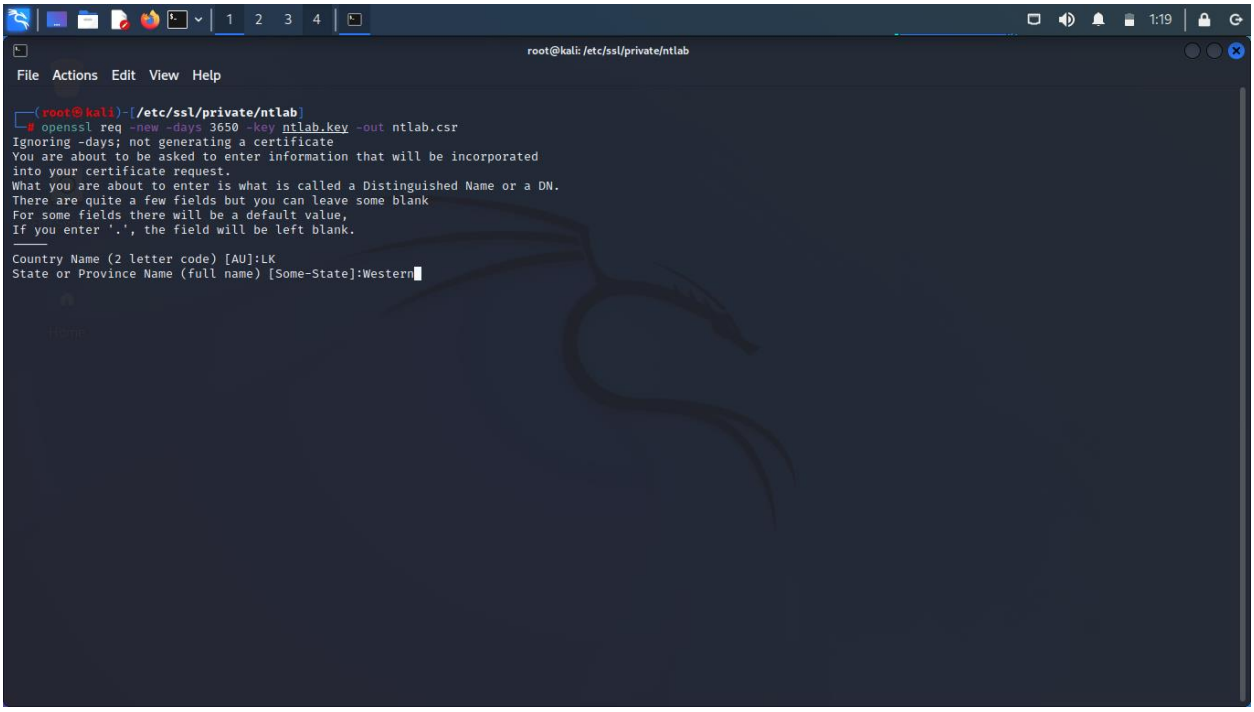
You are now prompted for state or province name.



Step 22:

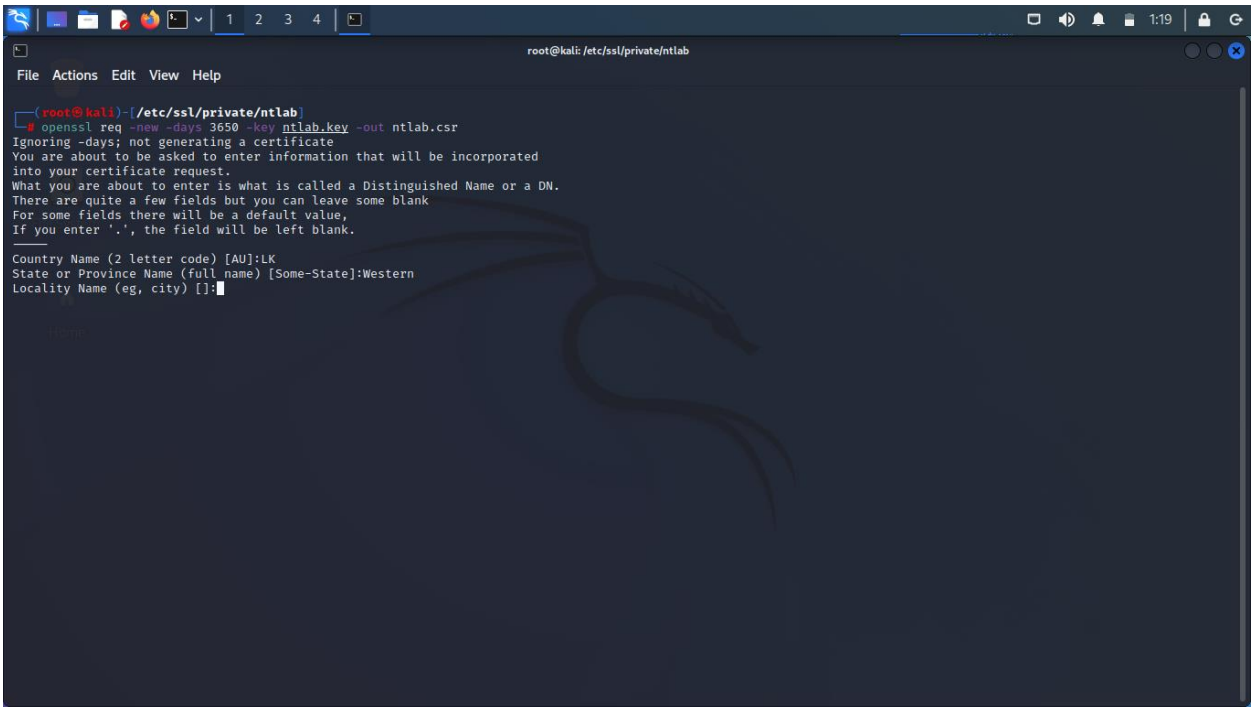
When prompted for the state or province name, type the following command: ***Western***

Press **Enter**.



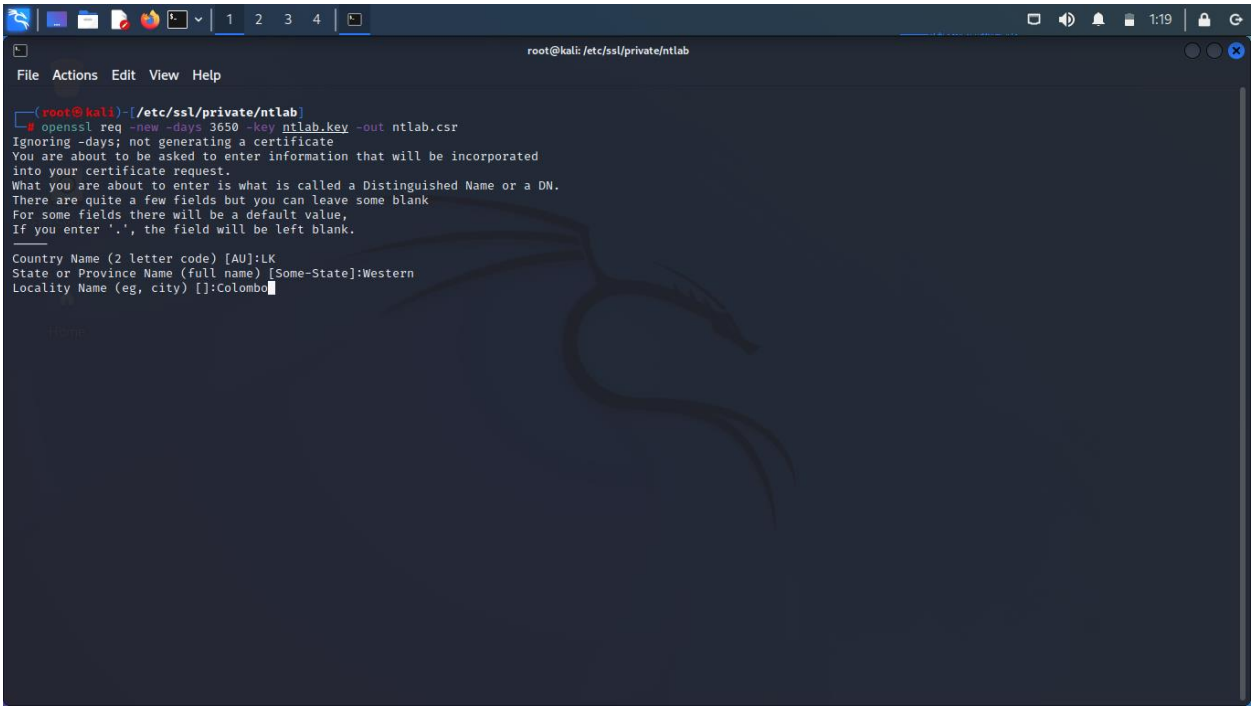
Step 23:

You are now prompted for a locality name.



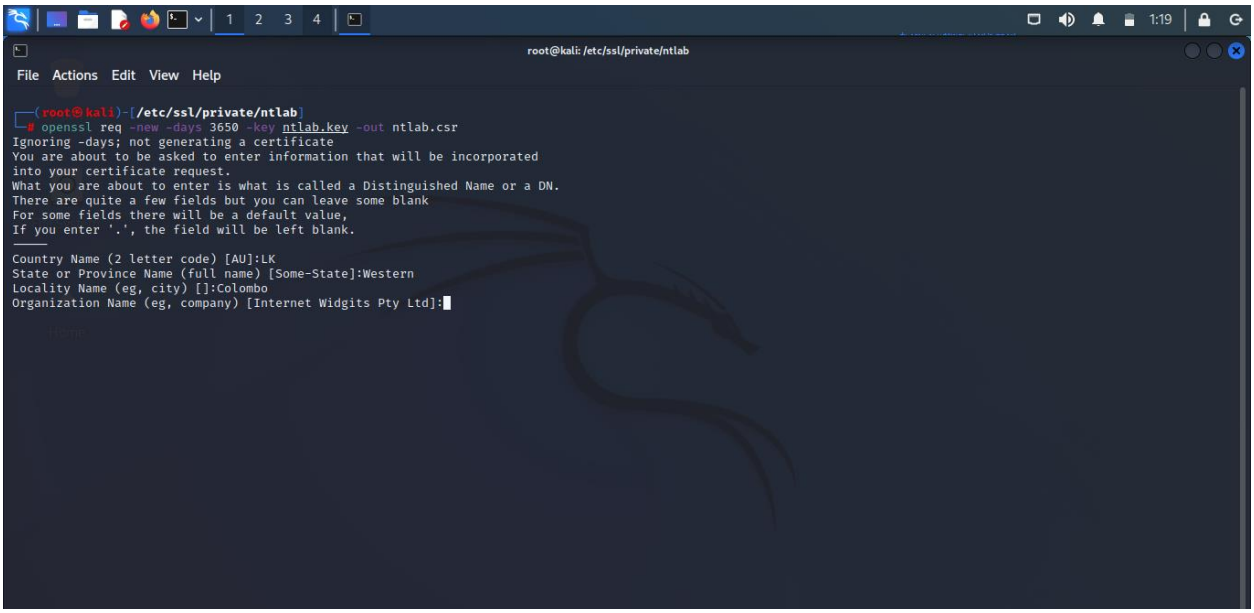
Step 24:

When prompted for the city name, type the following command: ***Colombo***



Step 25:

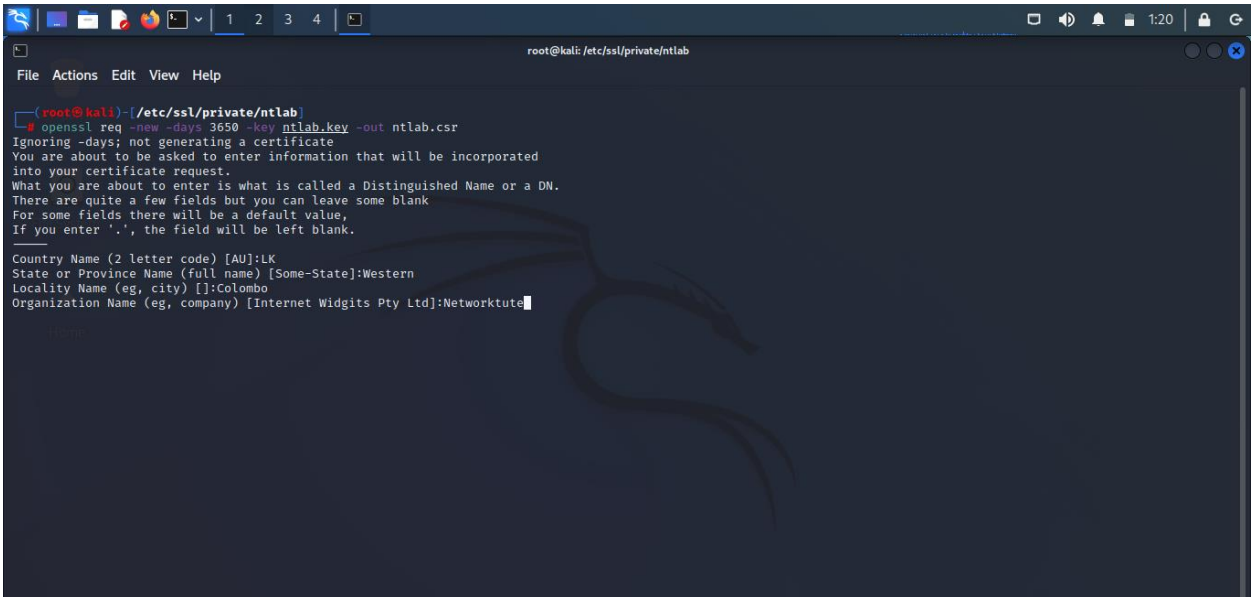
You are now prompted for the organization name.



Step 26:

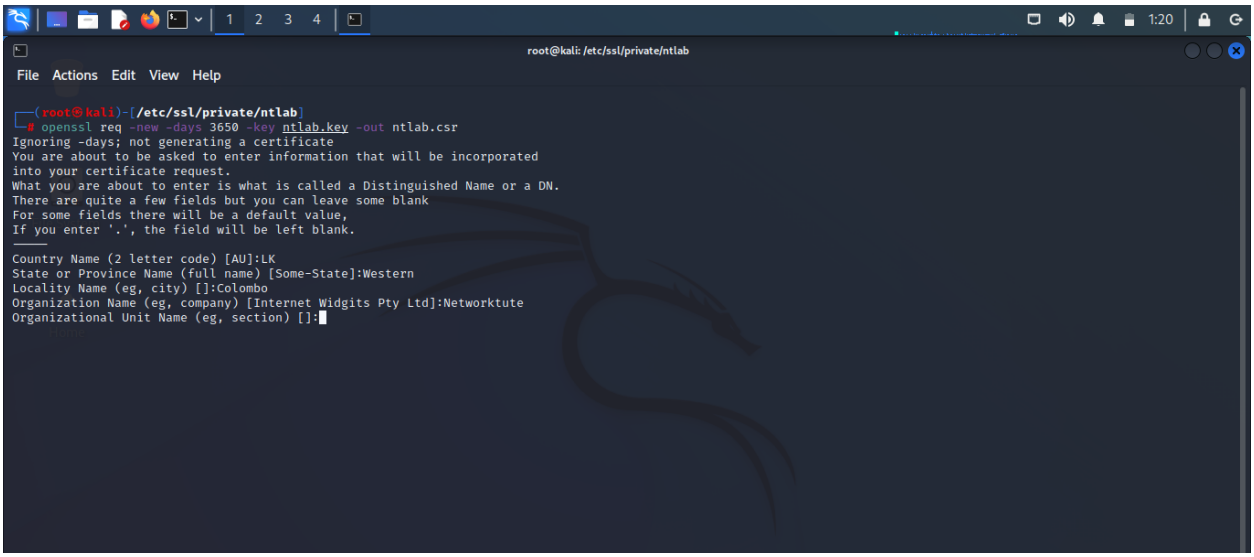
When prompted for the organization name, type the following command: ***Networktute***

Press **Enter**.



Step 27:

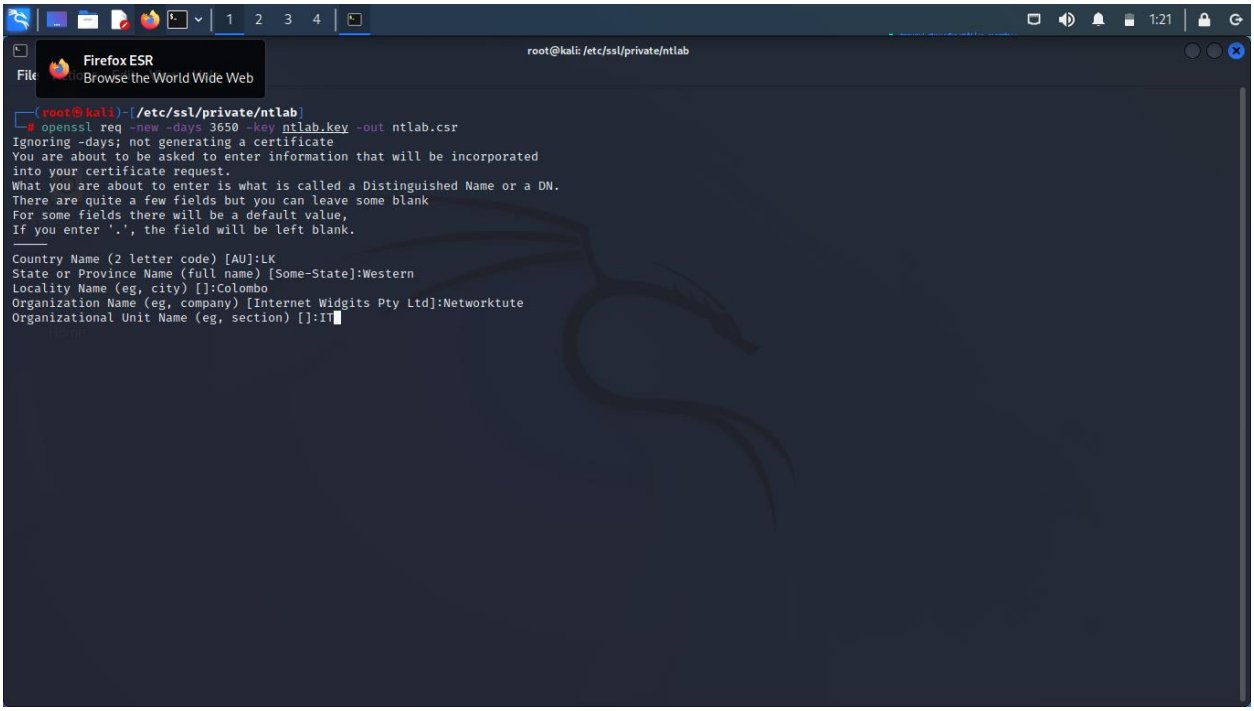
You are now prompted for the organizational unit.



Step 28:

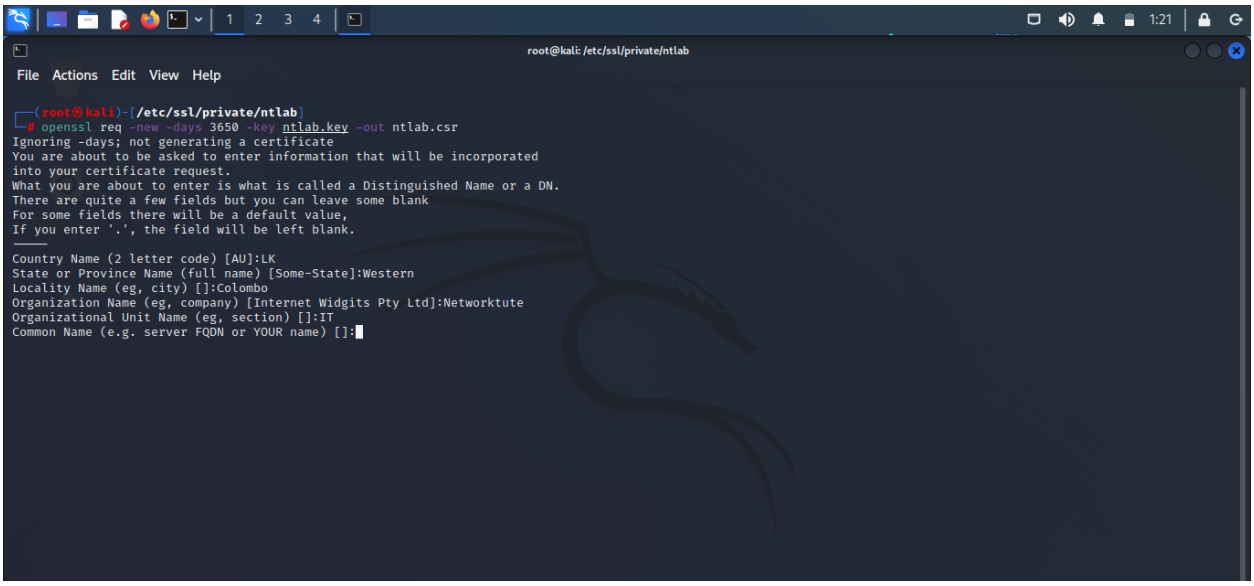
When prompted for the organizational unit name, type the following command: ***IT***

Press **Enter**.



Step 29:

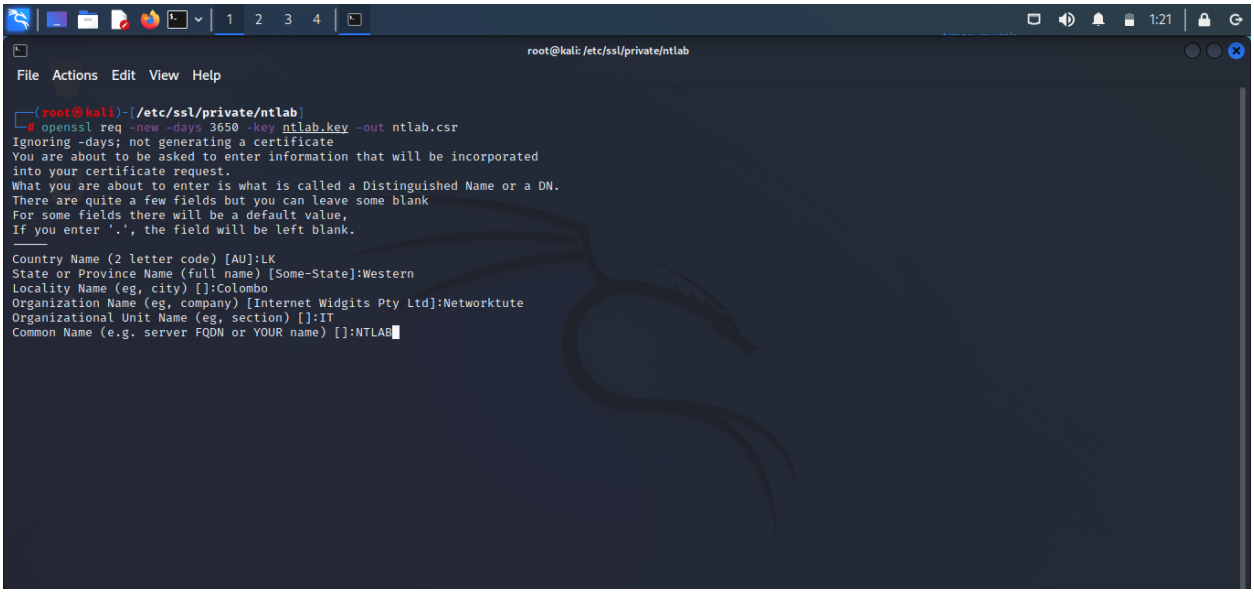
You are now prompted for the common name.



Step 30:

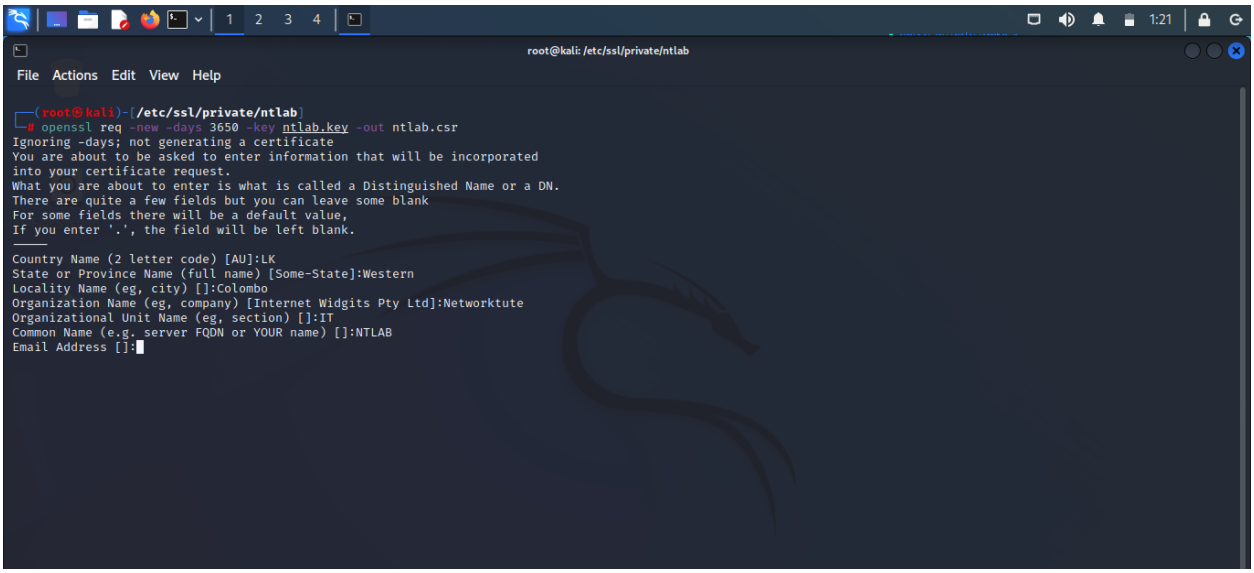
When prompted for the common name, type the following command: ***NTLAB***

Press **Enter**.



Step 31:

You are now prompted for the Email address.

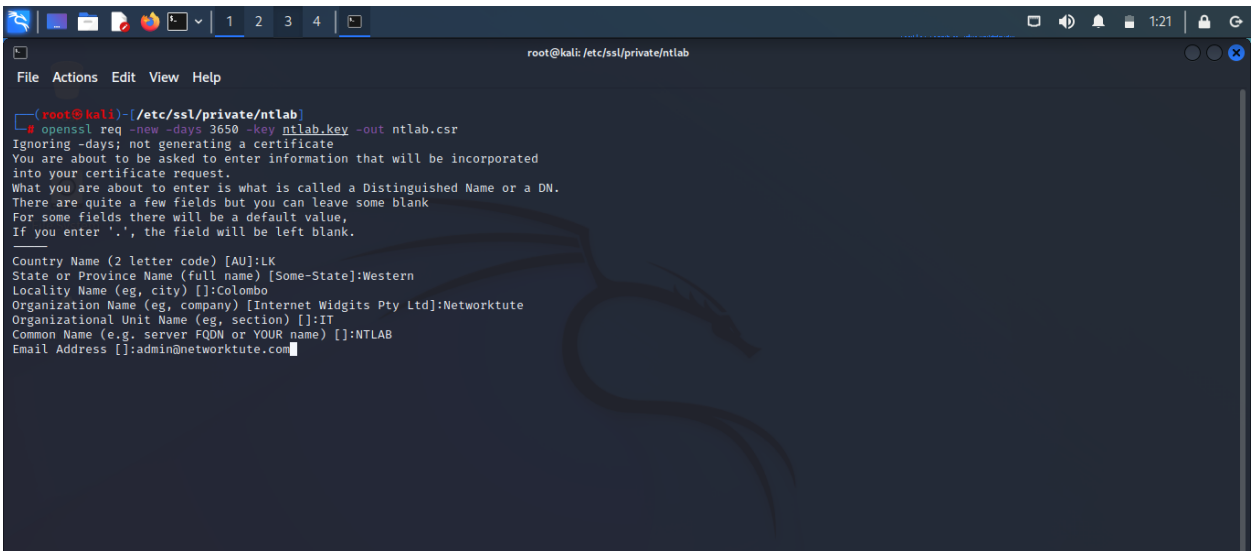


Step 32:

When prompted for the Email address, type the following command:

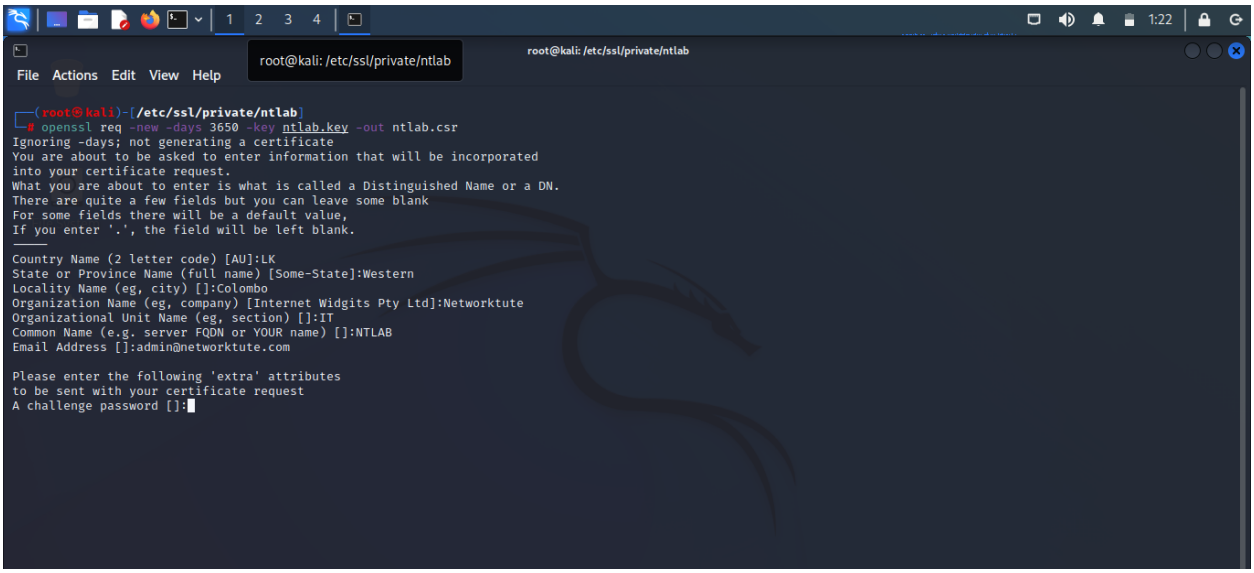
admin@networktute.com

Press **Enter**.



Step 33:

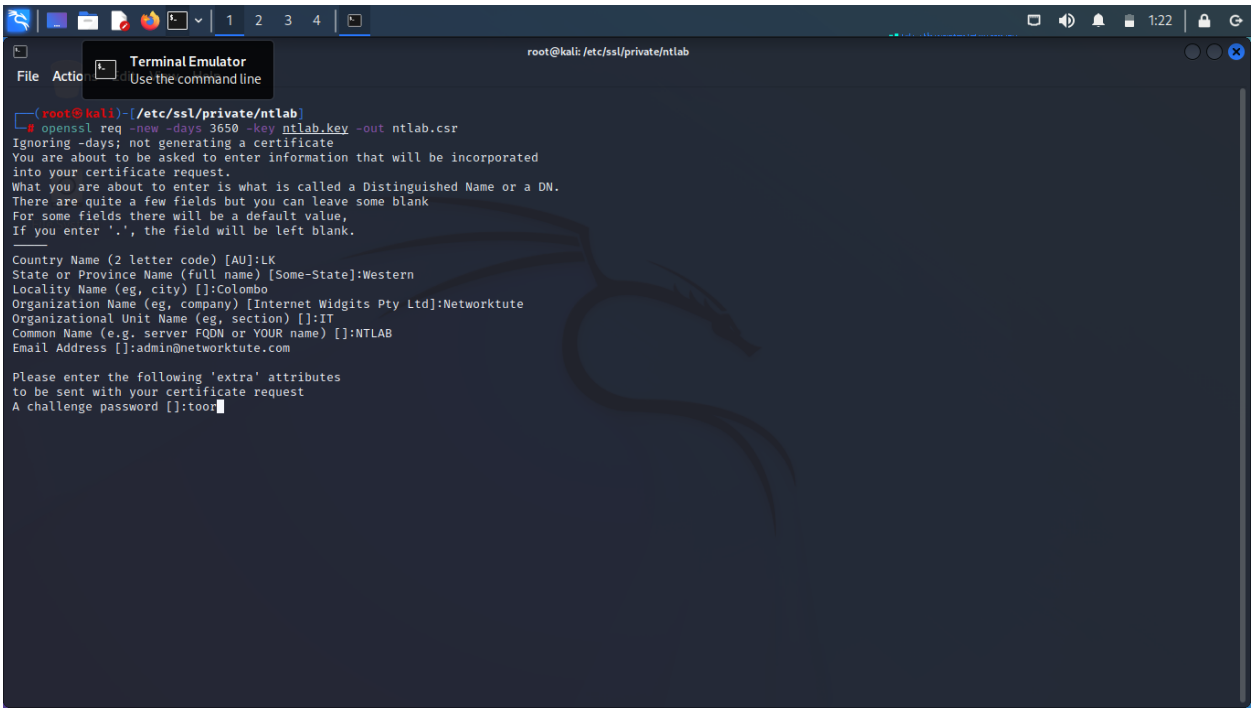
You are now prompted for a challenge password.



Step 34:

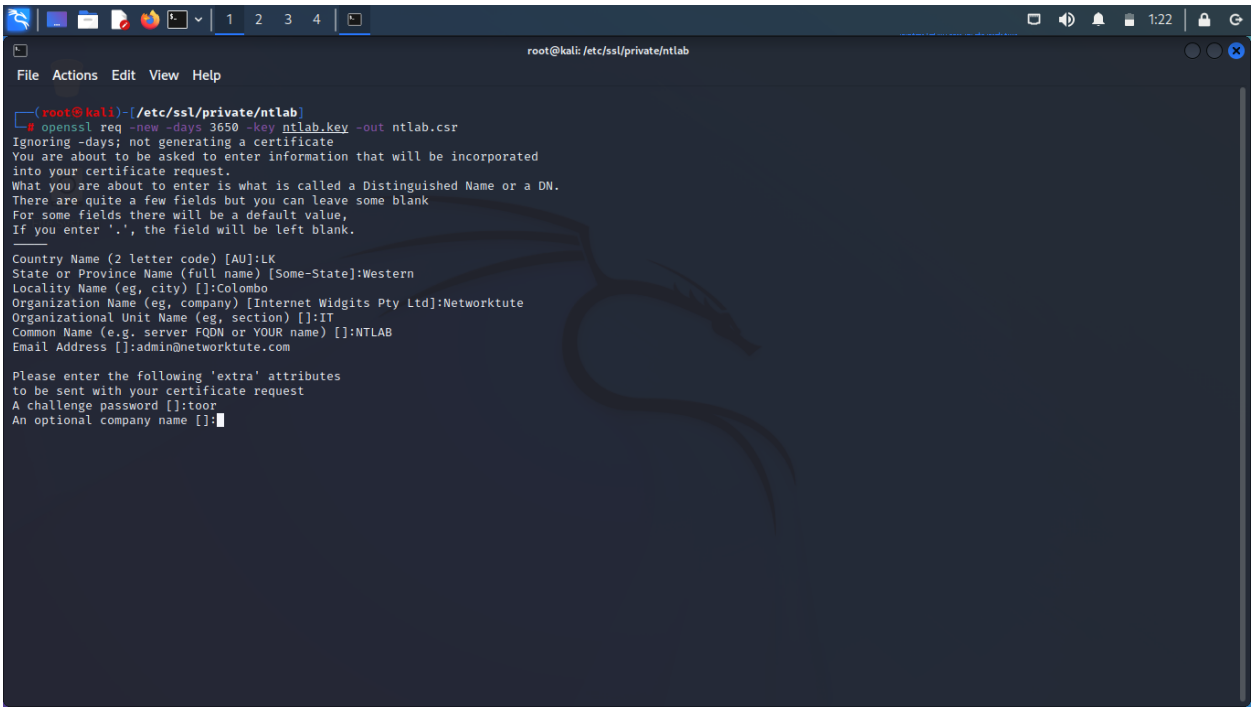
When prompted for the challenge password, type the following command: ***toor***

Press **Enter**.



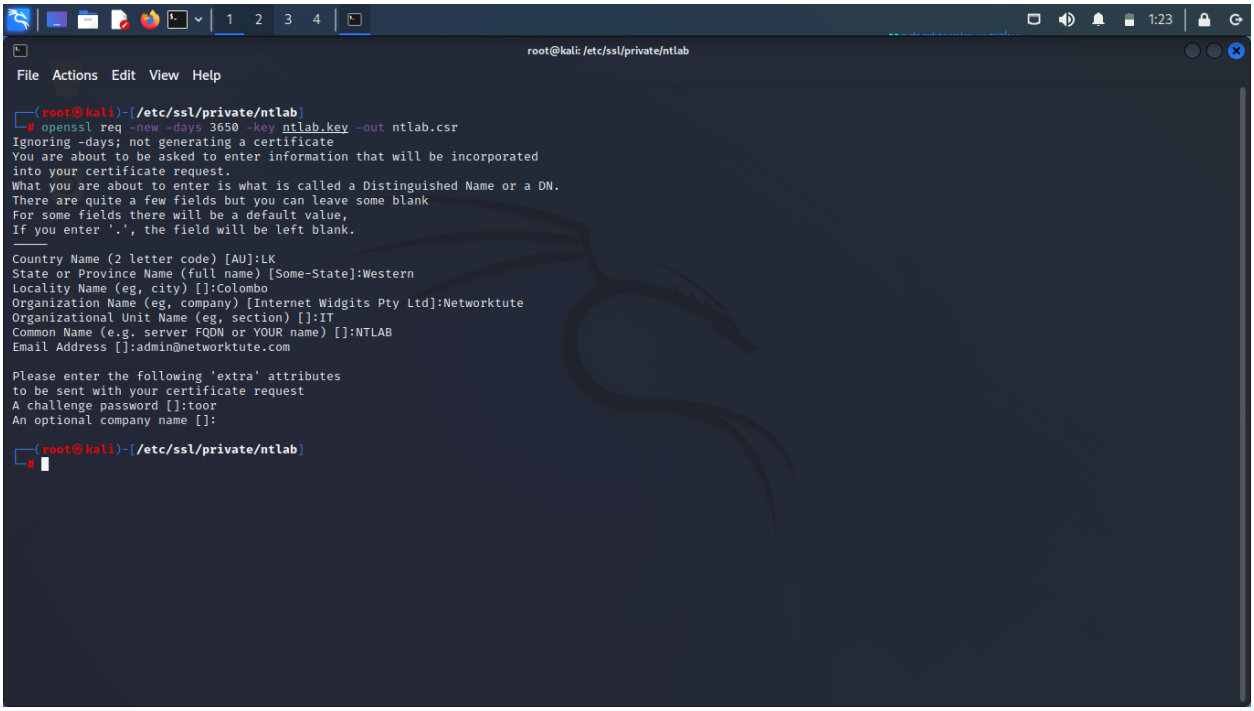
Step 35:

You are now prompted for an optional company name.



Step 36:

When prompted for an optional company name, press **Enter**. The CSR file is now generated



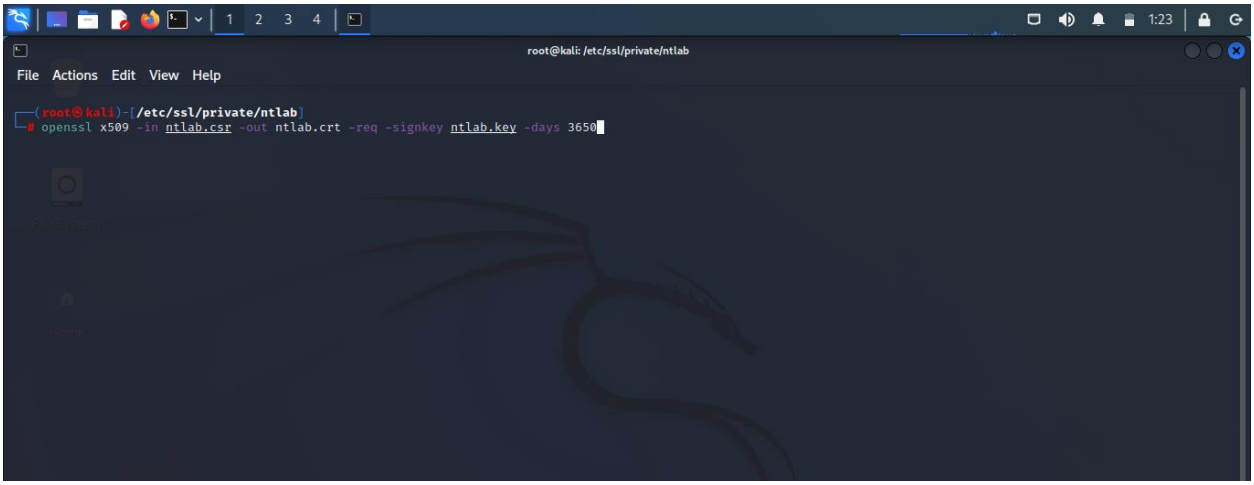
Step 37:

Clear the screen by entering the following command: ***clear***

You will now generate the certificate file from the CSR and the private key files. Type the following command:

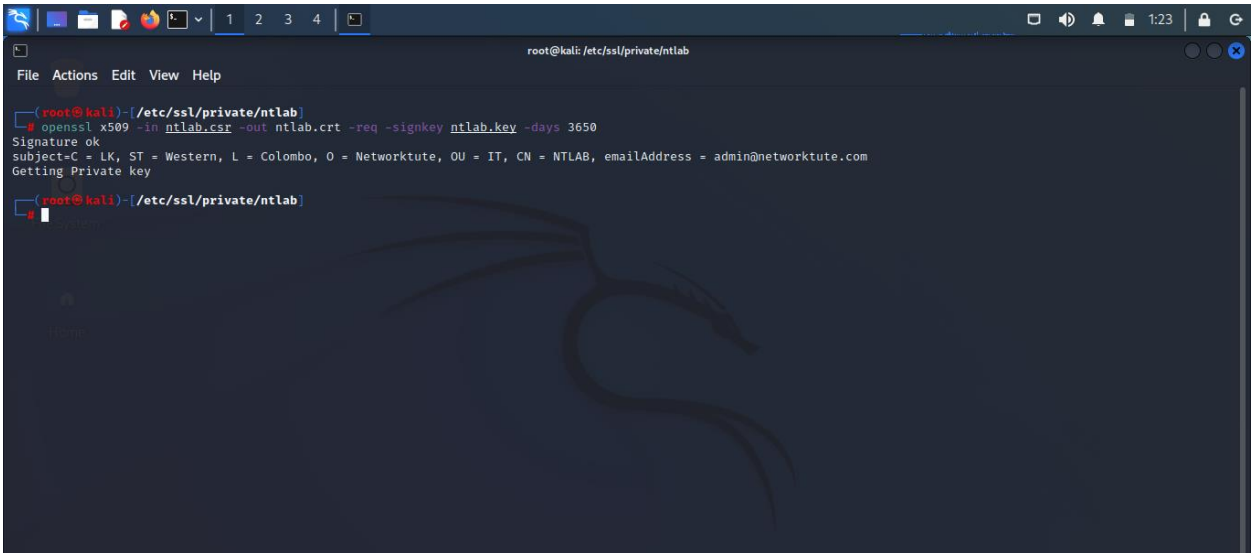
```
openssl x509 -in ntlab.csr -out ntlab.crt -req -signkey ntlab.key -days 3650
```

Press **Enter**.



Step 38:

The certificate file is now generated.



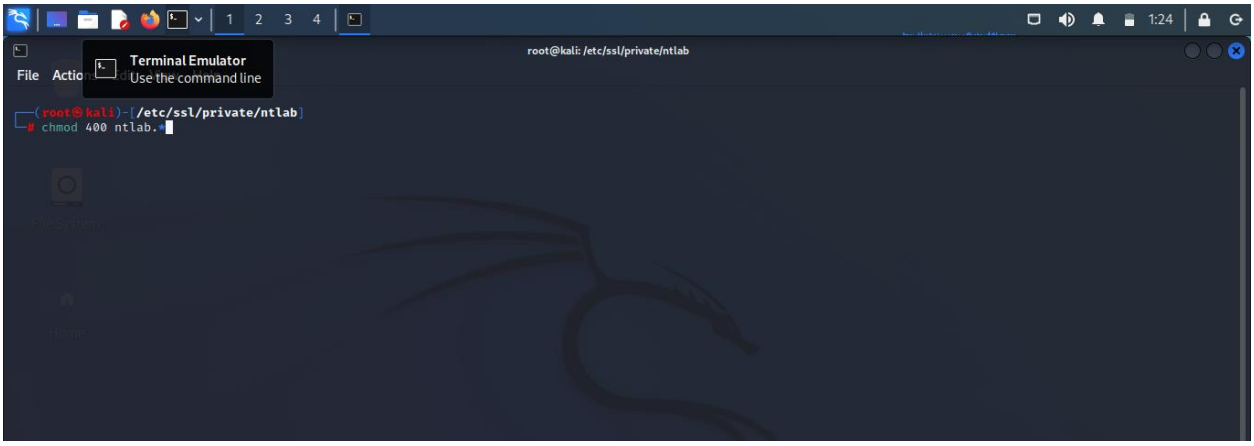
Step 39:

Clear the screen by entering the following command: ***clear***

You will use the chmod command to ensure that these files are not accessible to other users. You will set the read permission for the root user. Type the following command:

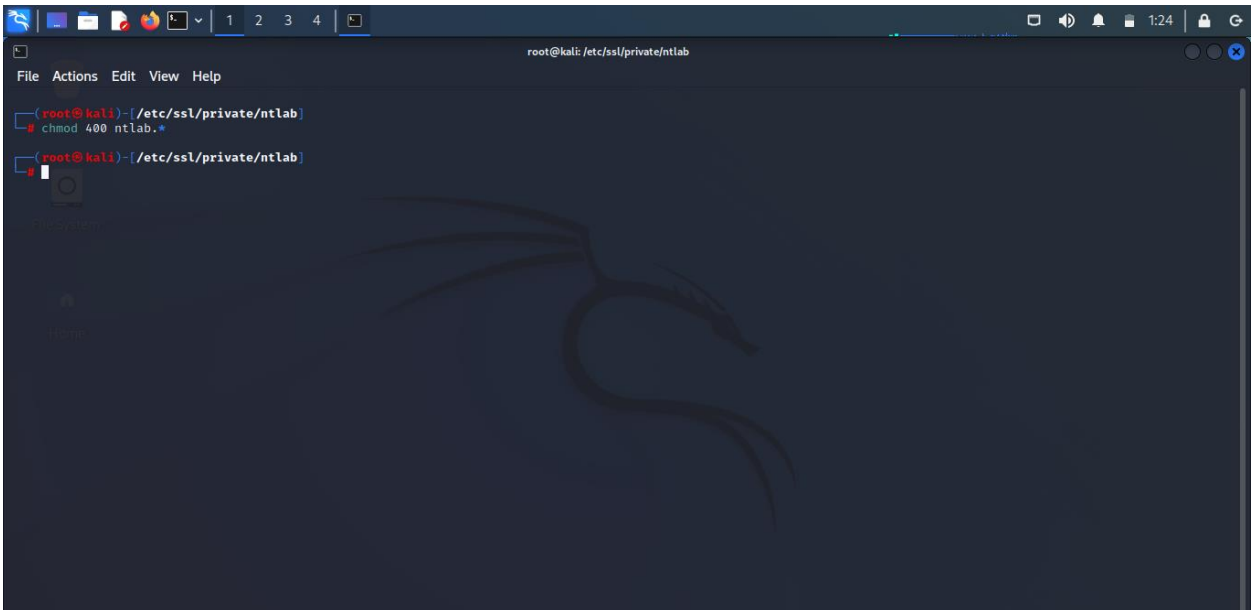
```
chmod 400 ntlab.*
```

Press **Enter**.



Step 40:

Notice that you have changed the permissions for multiple files at once.

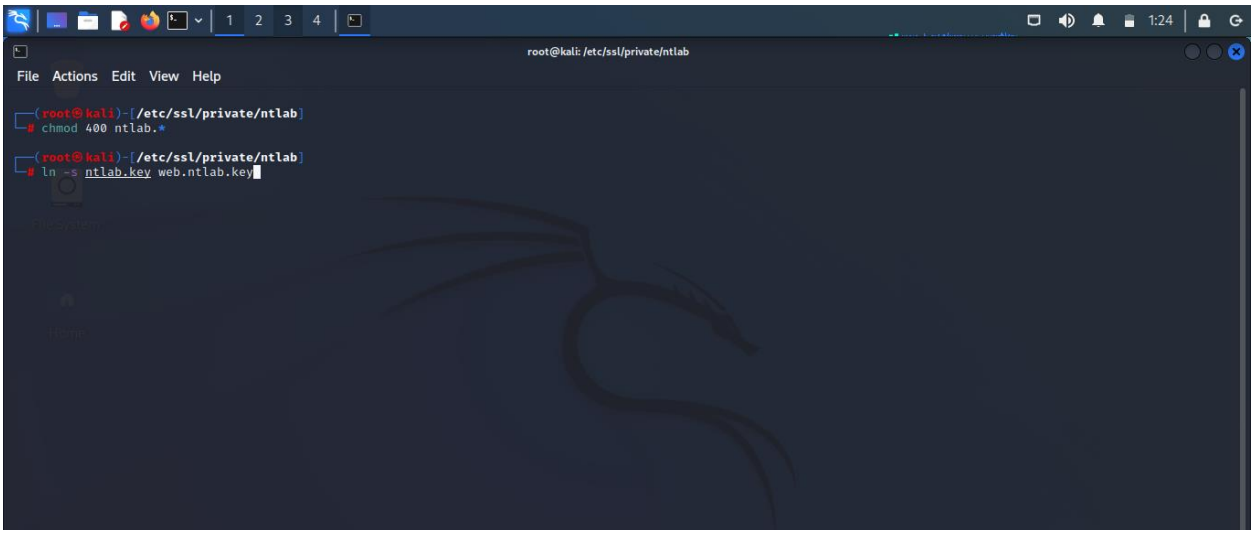


Step 41:

You will now create the symbolic links for the .csr and .crt files. Type the following command to create the symbolic link for the **ntlab.key**:

```
ln -s ntlab.key web.ntlab.key
```

Press **Enter**.

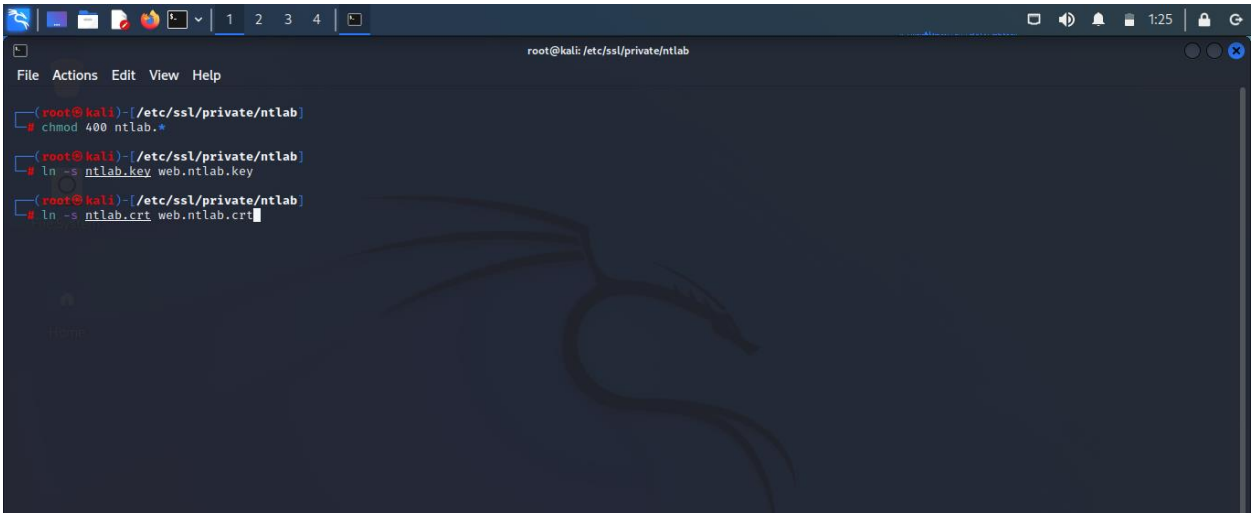


Step 42:

To create the symbolic link for the **ntlab.crt** file, type the following command:

```
ln -s ntlab.crt web.ntlab.crt
```

Press **Enter**.



Step 43:

Clear the screen by entering the following command: ***clear***

You can list the files in the **/ntlab** directory. Type the following command: ***ls -l***

Press **Enter**.

Note: After creating the certificate, you can integrate it into the Web server, such as an Apache Web Server.