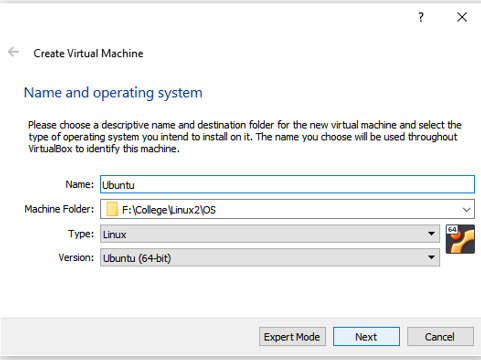
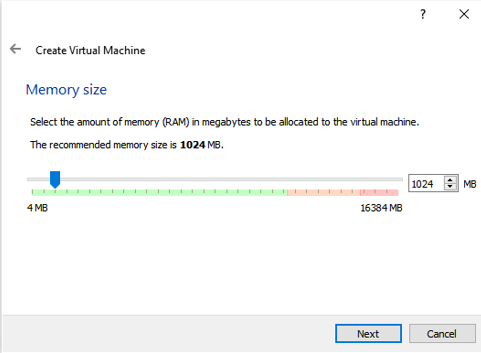
Practical 1

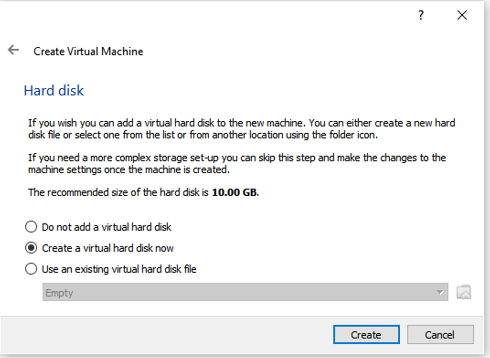
**Aim:** Install suitable Ubuntu/CentOS/Fedora OS

Procedure/Steps:

1. Install virtual box manager on your windows
2. In virtual box click on NEW, give name to your machine and the path where you want to store its data

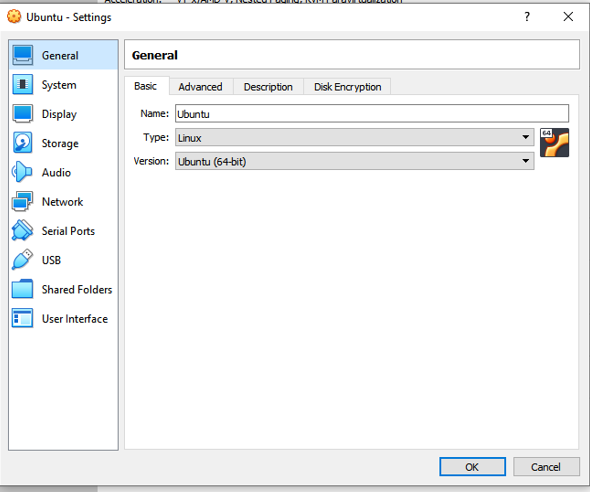




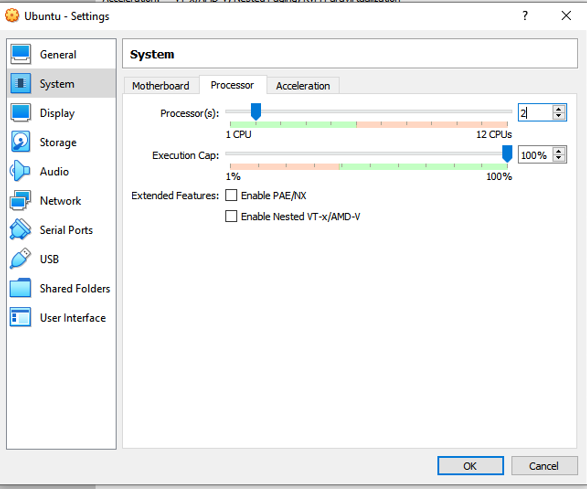


Click Create and again click Create without changing anything.

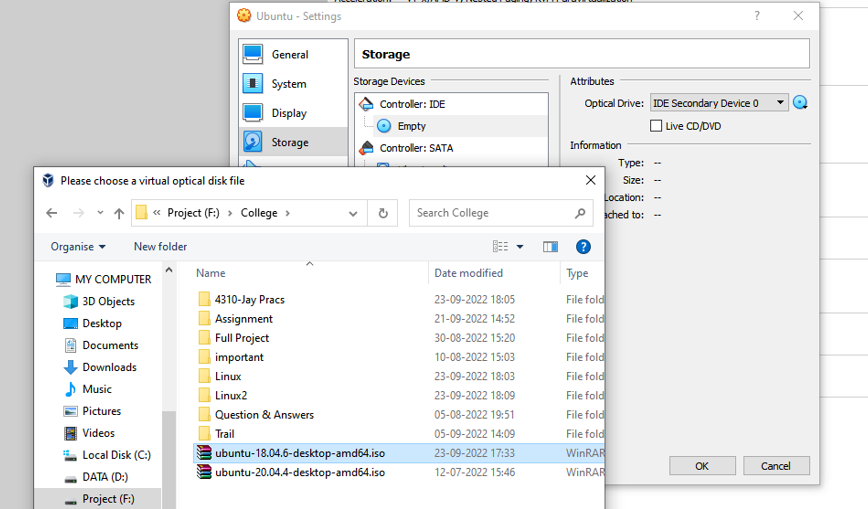
1. Now single click on the machine and then click on settings in virtual box



Here select System and change Memory Size as per your need and make sure to make processor count to be more than 1.



1. Now Select storage and in “Controller:IDE” there will be and empty disk select that and then in “Attributes” section click on the blue disk and add the iso file and start your ubuntu machine



1. Now start machine and click on install ubuntu and configure it according to your need.
2. Navigate to Virtual machine settings->storage->controller:IDE And remove the iso file added in step 4 And restart your machine

**UBUNTU IS INSTALLED.**

Practical 2

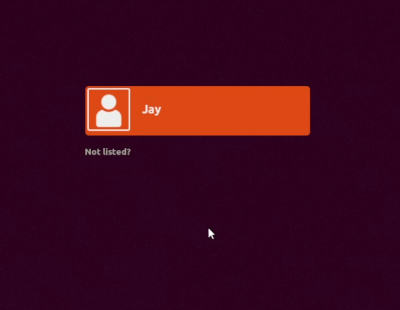
**Aim:** Basic Administration: User Management, Group Management, Network Management,Disable IPv6 if not needed, Configure Services, display the list of services which are running,Stop and turn OFF auto-start setting for a service if you don’t need it, sudo Settings

Procedure / Steps:

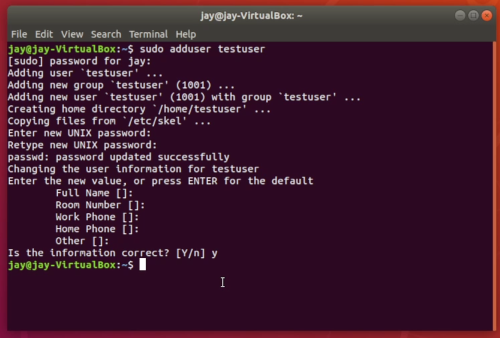
**A) USER MANAGEMENT**

1. Open ubuntu in Virtual Box

2. Start your machine and log in as root (i.e., Your first account created on the system)

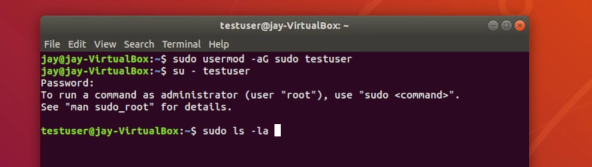


3. Adding the user In terminal and run the command “sudo adduser testuser”



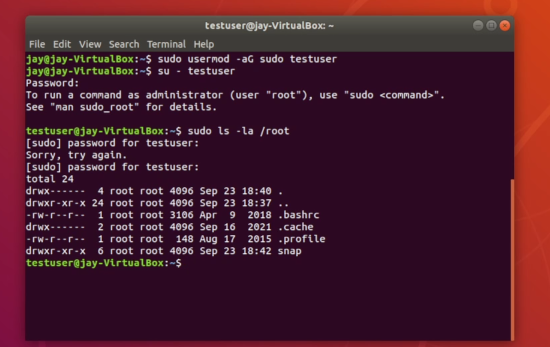
4. Adding the user to sudo group

5. Testing the sudo access In terminal and run the command “su - testuser”

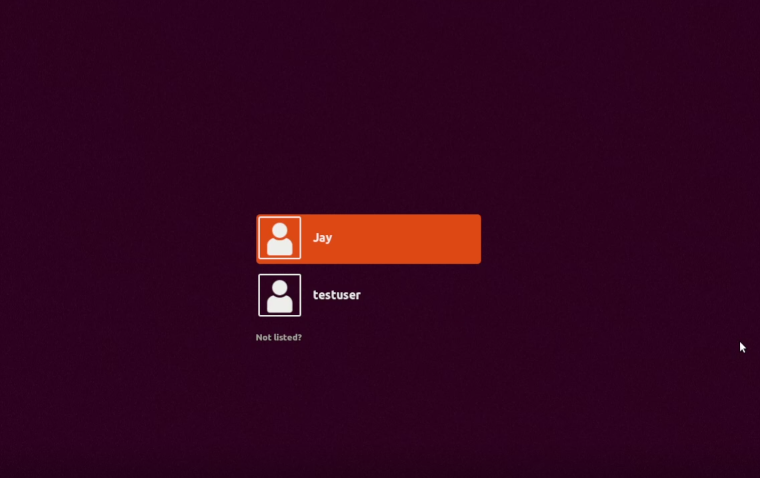


Now run any sudo command and test if this user has access to sudo or not

Such as (sudo ls -la /root)

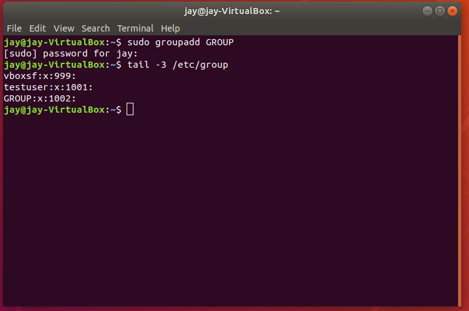


The image below shows that the user was added successfully with password authentication.



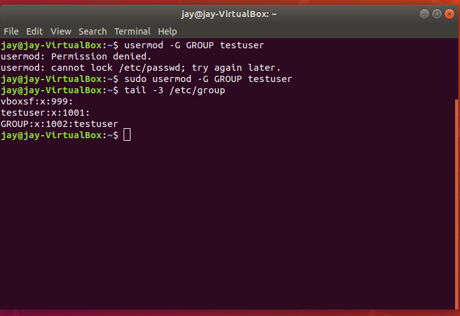
**Group management:**

1. Creating a Group Below command created a group with the name as provided. The group while creation gets a group ID and we can get to know everything about the group as its name, ID, and the users present in it in the file “/etc/group”.



Note: You can add password also to groups using gpasswd <group\_name>

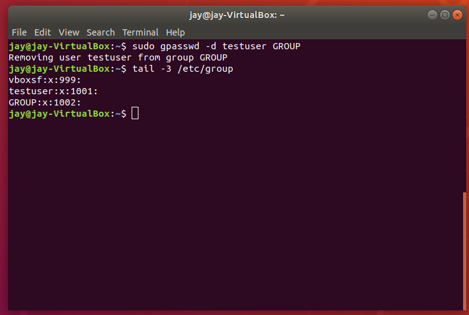
1. Command to add an existing user to an existing group 🡪usermod -G group\_name username



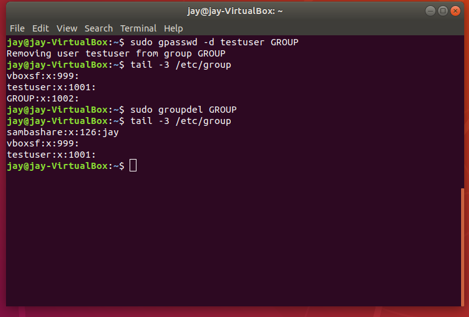
Note: If we add a user to a group then it automatically gets removed from the previous groups, we can prevent this by the command given below.

🡪 usermod -aG group\_name username

1. Command to Add multiple Users to a Group at once 🡪gpasswd -M user1, user2, user3 testuser
2. Command to delete a user from a group



1. Command to delete a group 🡪groupdel group\_name

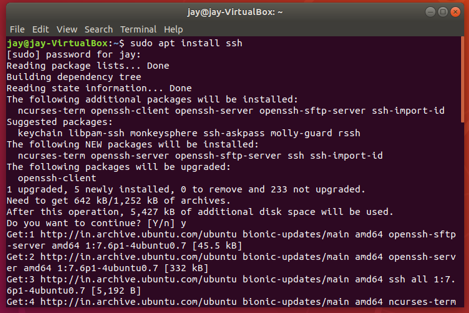


**Practical 3**

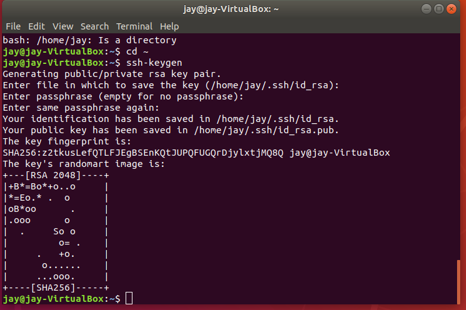
**Aim:** Remote connection using SSH: Configure SSH and server and manage a server from the remote computer, SSH client (Ubuntu & Windows)

ON UBUNTU:

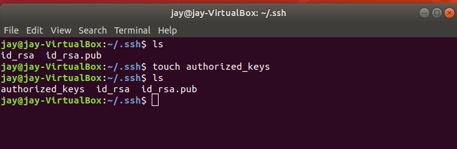
install ssh



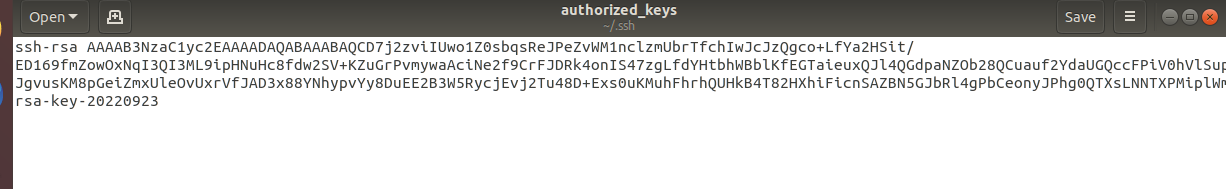
do ssh-keygen, which will create two keys in “.ssh” folder as a file namely “id\_rsa” and “id\_rsa.pub”



create authorized\_keys file in .ssh(it will be in your home directory)

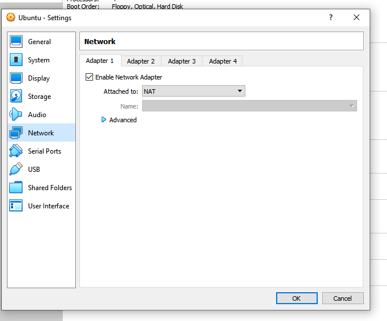


and copy public the key generated in windows (before copying perform the windows step so that you receive ssh public key that is to be copied)



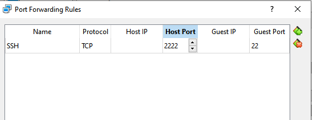
After performing above steps close your ubuntu machine

Now go to Network setttings for your ubuntu machine and change the network type of **Adapter1** to **NAT**.



Note: By default, ssh runs on port number 22.

And now click on **Advanced** and then on **Port Forwarding** and do a proper port-forwarding.



Give the name of the rule as: **SSH**

Give the name of the protocol as: **TCP**

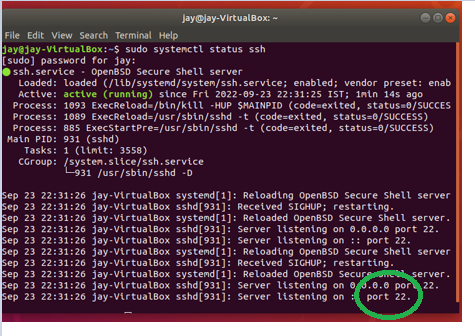
Specify your free post on the host(windows): **2222**

Specify the port on which ssh is running on in Guest port: **22**

Now click **OK.**

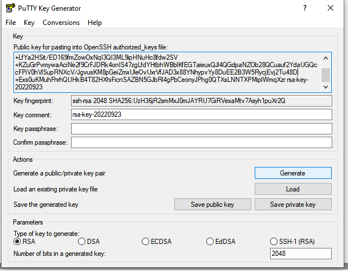
Now again start your ubuntu machine.

Now check if ssh is working and listening to port 22 or not

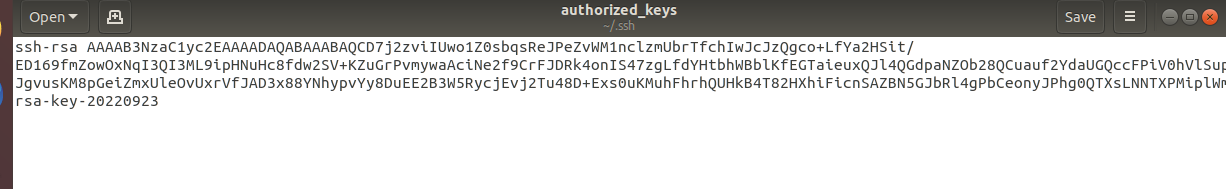


**ON WINDOWS:**

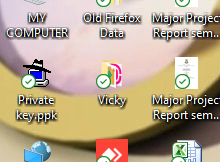
open puttygen and generate key



save the public key at path specified in UBUNTU (pub key to be stored in authorized\_keys)



save the private key on windows desktop



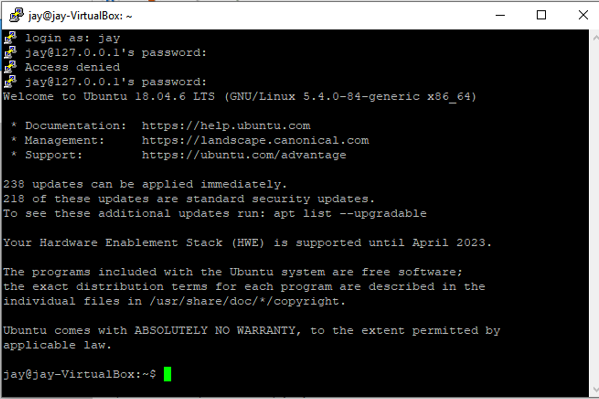
Below steps only to be performed if ssh is working in ubuntu.

Now time to connect to ubuntu through windows

Open putty and Click on **Session** in **category** window.

Enter the loop back ip address of ubuntu machine (i.e., 127.0.0.1) and the port number as 2222.

Enter username of your ubuntu machine and then the password.



**SSH IS WORKING.**

Practical 4

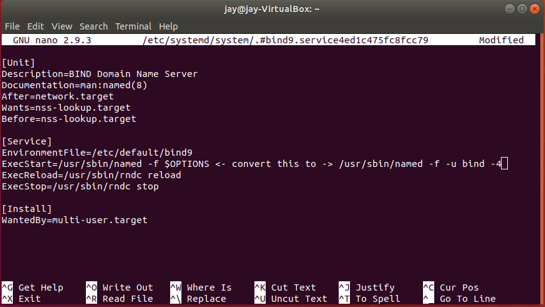
**Aim:** Install DNS Server BIND, Configure DNS server which resolves domain name or IP address, Install BIND 9, Configure BIND, Limit ranges you allow to access if needed.

Install BIND on DNS Servers

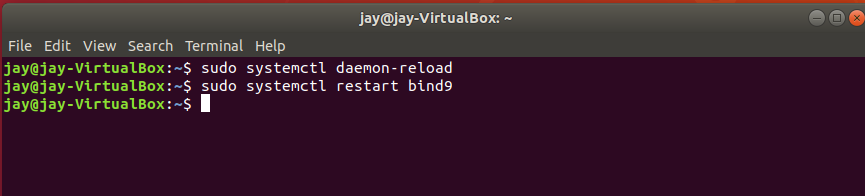
sudo apt install bind9

You can set BIND to IPv4 mode. Edit the bind9 systemd unit file by typing

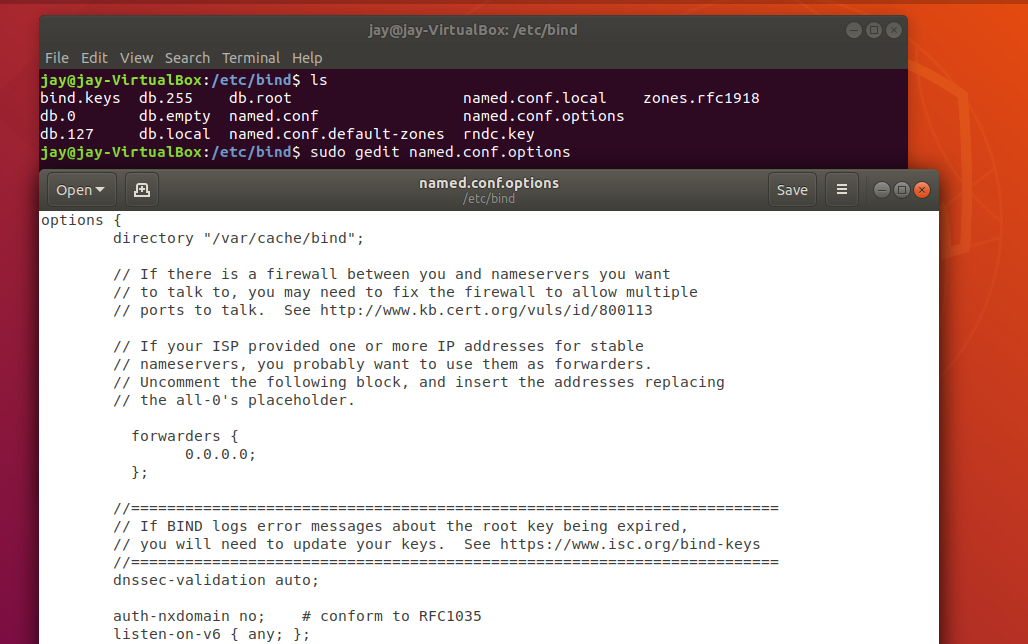
Sudo systemctl edit –full bind9



Reload the system daemon to read the new configuration into the running system and restart bind to implement the changes

****

Now open the named.conf.options file which is located at /etc/bind/named.conf.options and just uncomment the forwaders in the options.

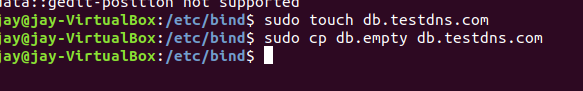


Now we will configure the named.conf.local to specify our forward zones:

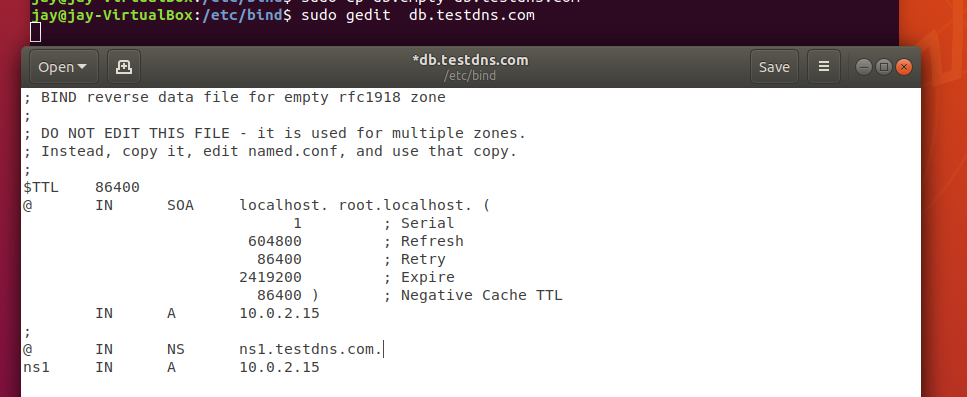


Now the file which we specified lets create it in the bind directory.

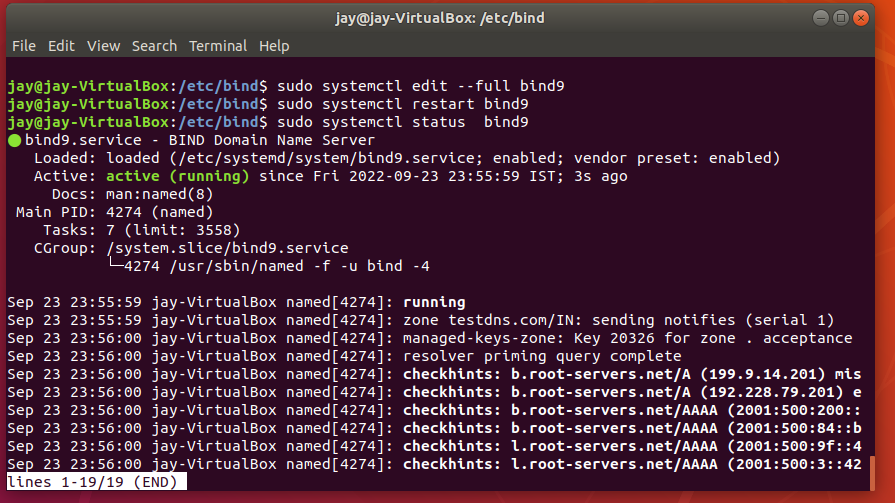
Now we will copy the default config to our created file.



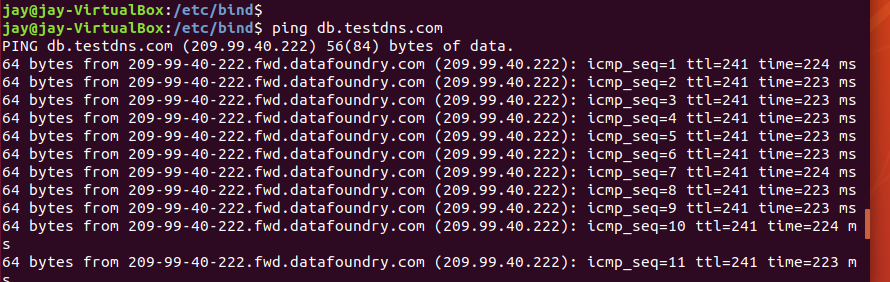
Now open this file(db.testdns.com) in editor of your choice and edit it like below or according to your situation and choice.

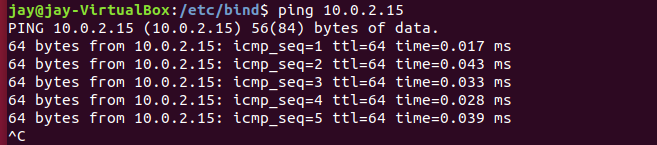


Now restart the bind9 and check its status

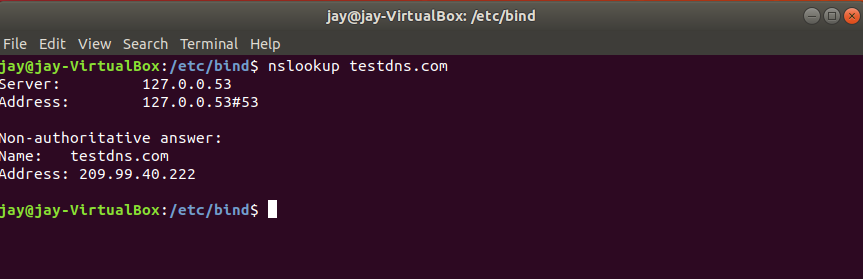


Now try to ping your domain name and your ip.





Now to make sure DNS is working we will use **nslookup .**



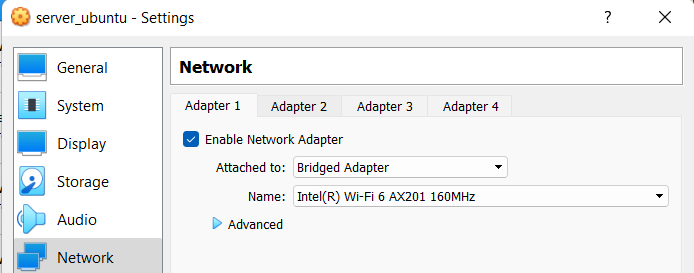
**Practical 5**

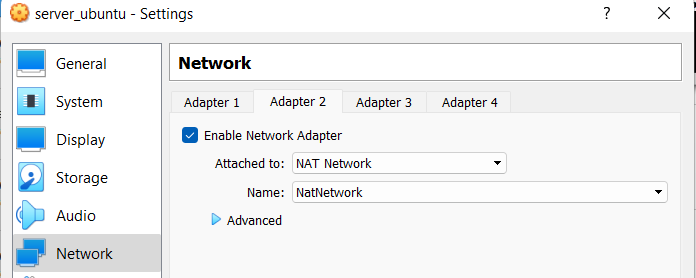
**Aim:** Configure DHCP Server, Configure DHCP (Dynamic Host Configuration Protocol) Server**.**

**#vbox config**

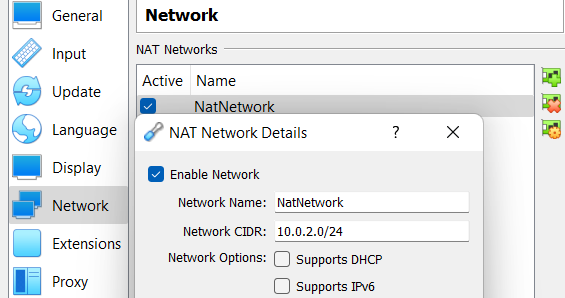
adapter 1 -> Bridged

adapter 2 -> NATnetwork





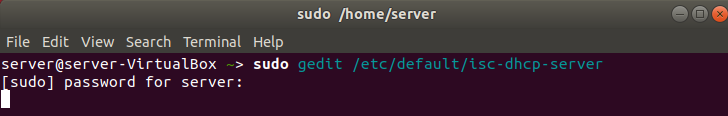
file->preferences->natnetwork->dhcp disabled

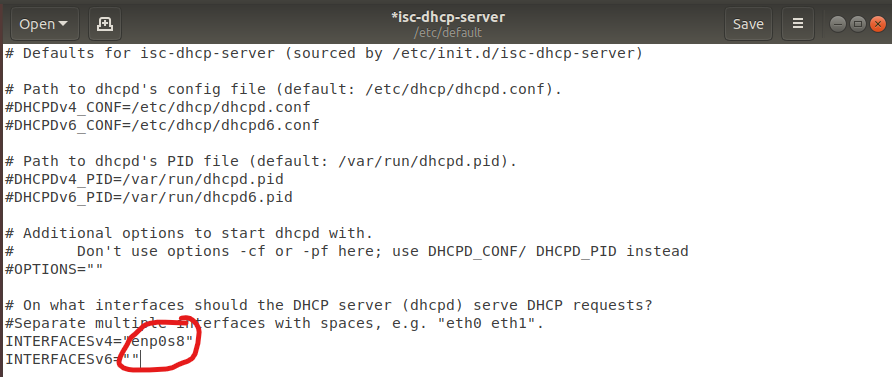




**Server side**

1) navigate to etc-> default-> isc-dhcp-server and just enter enp0s8 in interfacev4



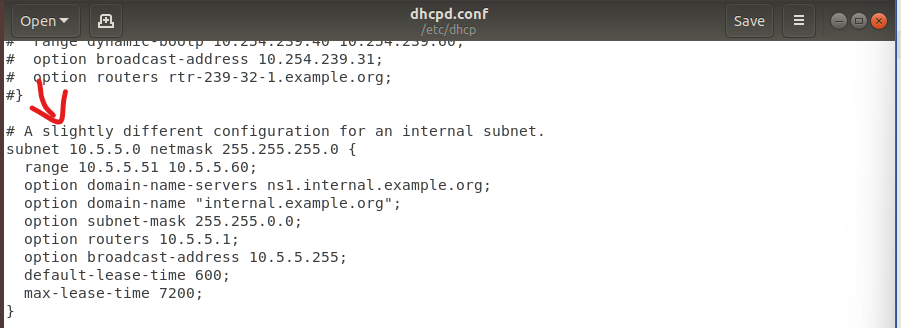


2) Now navigate to etc-> dhcp-> dhcpd.conf



Go to line mentioned below

**slightly different conf** and edit that line as mentioned below or according to your preference



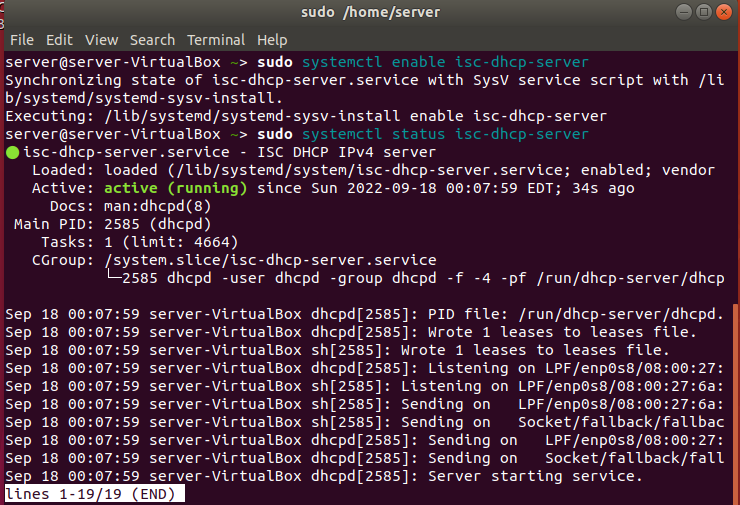
INTERFACES (cd /etc/network) FILE CONTENT

#interfaces and slightly configuration should be same so that dhcp starts



3) start dhcp

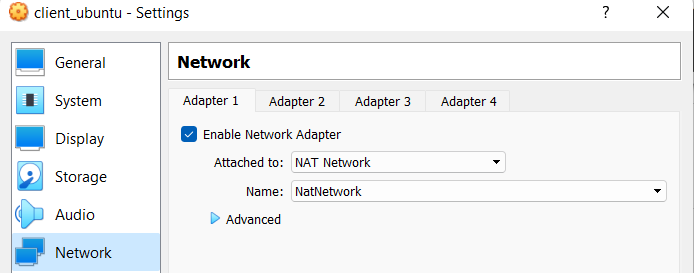
(if not started check the interfaces file etc->network->interfaces)



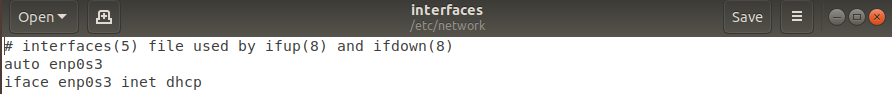
Client Side

**#virtual box config**

Adapter 1 -> NatNetwork



Now log into your client ubuntu machine and Navigate to /etc/network and interfaces and change content to



Notice that this machine gets the ip address from the range specified in dhcpd.conf file on the server side.



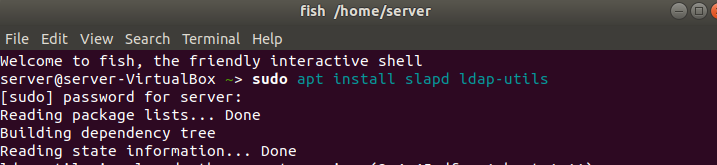


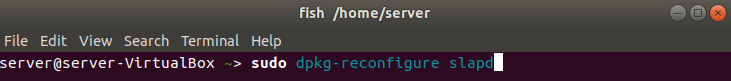
**DHCP IS WORKING.**

Practical 6

Aim: Configure LDAP Server, Configure LDAP Server in order to share users' accounts in your local networks, Add LDAP User Accounts in the OpenLDAP Server, Configure LDAP Client in order to share users' accounts in your local networks. Install phpLDAPadmin to operate LDAP server via Web browser.

Step 1 — Installing and Configuring the LDAP Server

****

****

****

There are quite a few new questions to answer in this process. We will be

accepting most of the defaults. Let’s go through the questions:

• Omit OpenLDAP server configuration? No

• DNS domain name?

• This option will determine the base structure of your directory

path. Read the message to understand exactly how this will be

implemented. You can actually select whatever value you’d

like, even if you don’t own the actual domain. However, this

tutorial assumes you have a proper domain name for the

server, so you should use that. We’ll

use example.com throughout the tutorial.

• Organization name?

• For this guide, we will be using example as the name of our

organization. You may choose anything you feel is appropriate.

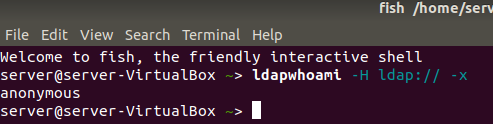
• Administrator password? enter a secure password twice

• Database backend? MDB

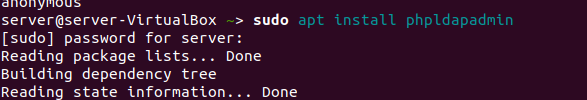
• Remove the database when slapd is purged? No

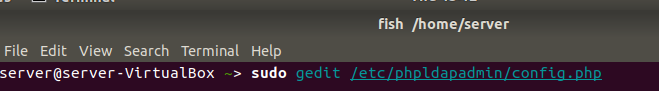
• Move old database? Yes

• Allow LDAPv2 protocol? No



**Step 2 — Installing and Configuring the phpLDAPadmin Web Interface**

****

****

In that search for the following lines:

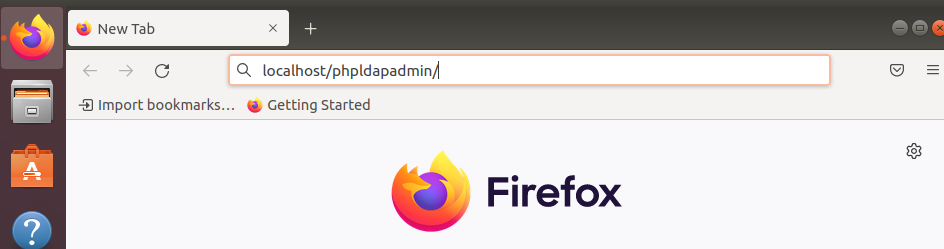
1) $servers->setValue('server','name','Example LDAP');

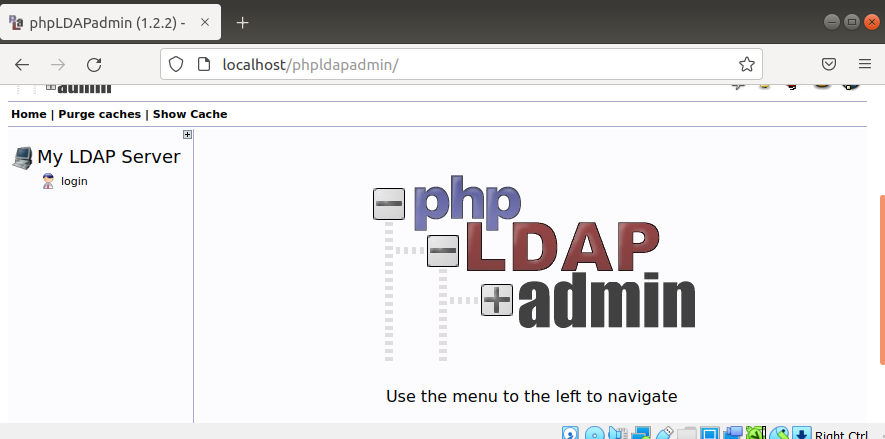
2) $servers->setValue('server','base', array('dc=example,dc=com'));

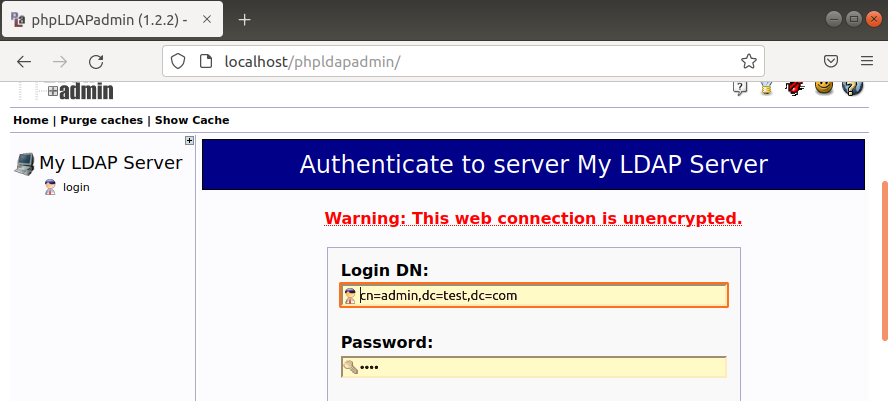
3) #$servers->setValue('login','bind\_id','cn=admin,dc=example,dc=com');

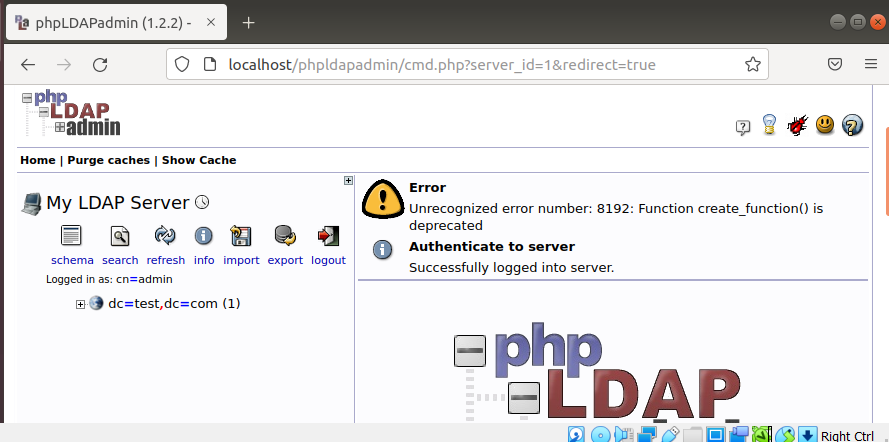
4) $config->custom->appearance['hide\_template\_warning'] = true;

**Step 3 — Logging into the phpLDAPadmin Web Interface**

****

****

****

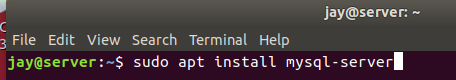
****

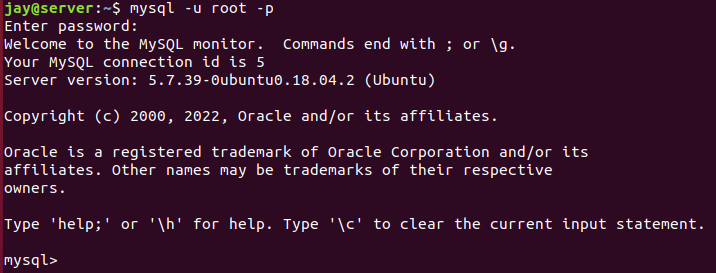
**LDAP IS WORKING PERFECTLY.**

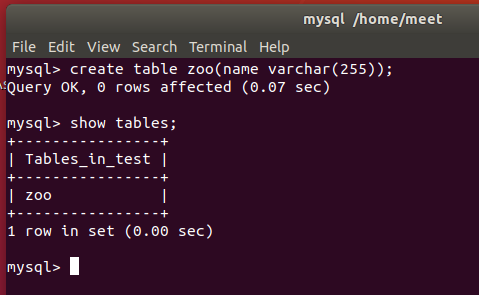
**Practical-8**

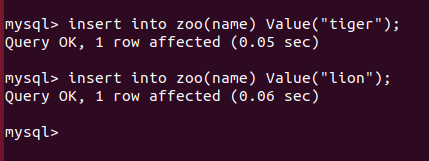
**Install MySQL/MariaDB to configure database server, install phpMyAdmin to operate MySQL on web browser from ClientMYSQL**

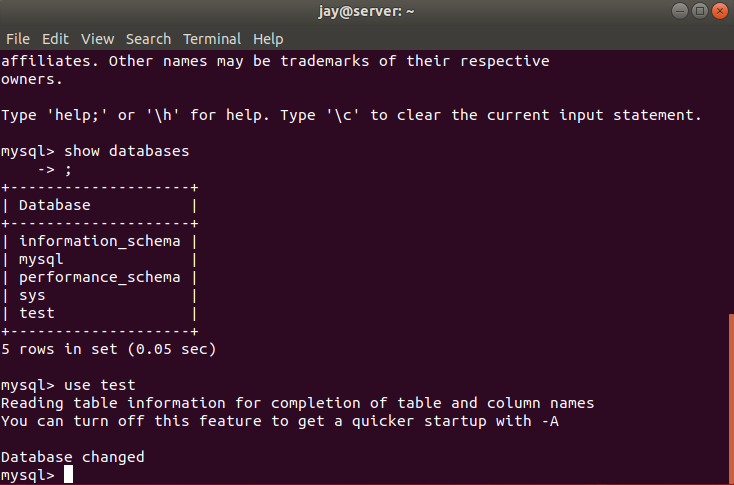
Installation

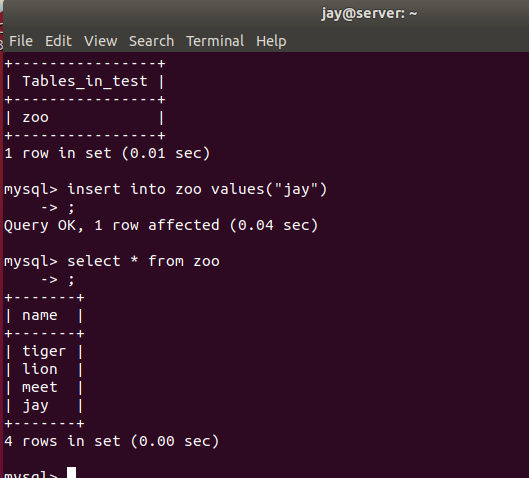


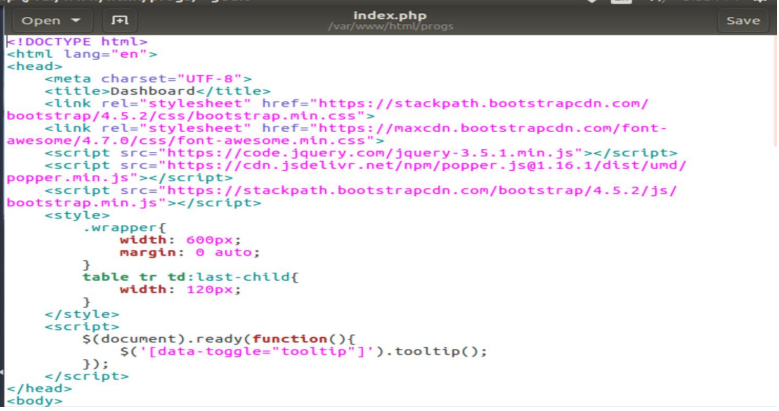


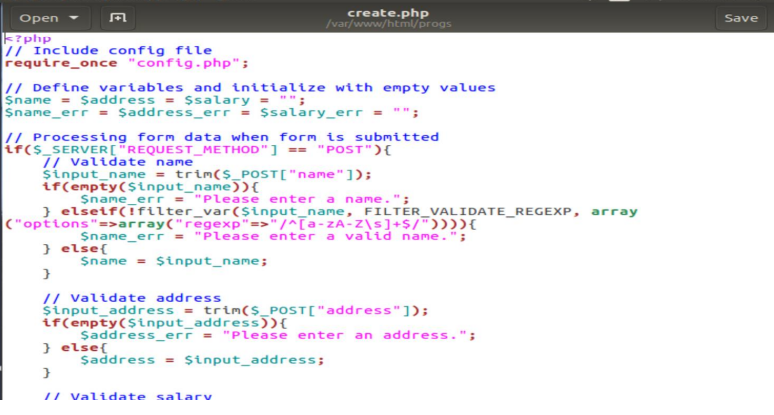




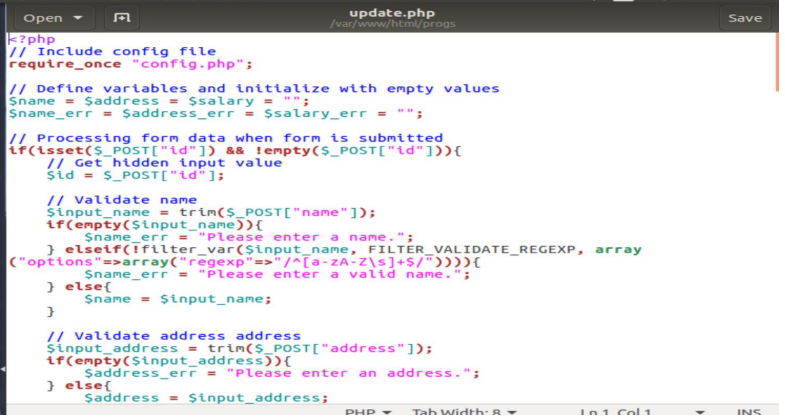


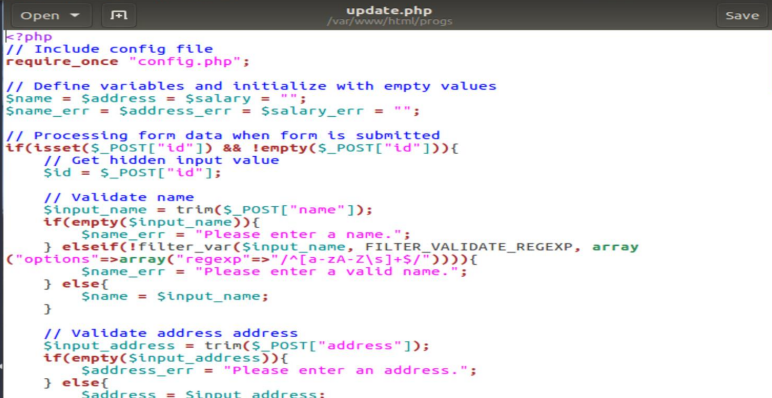


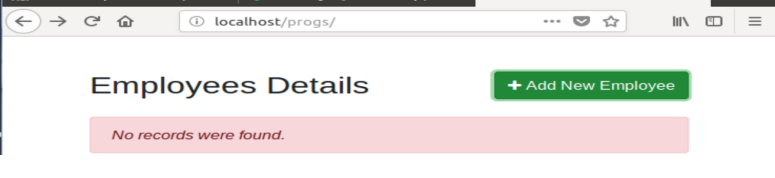








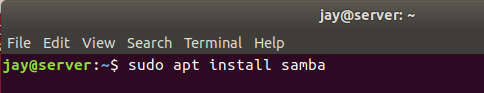




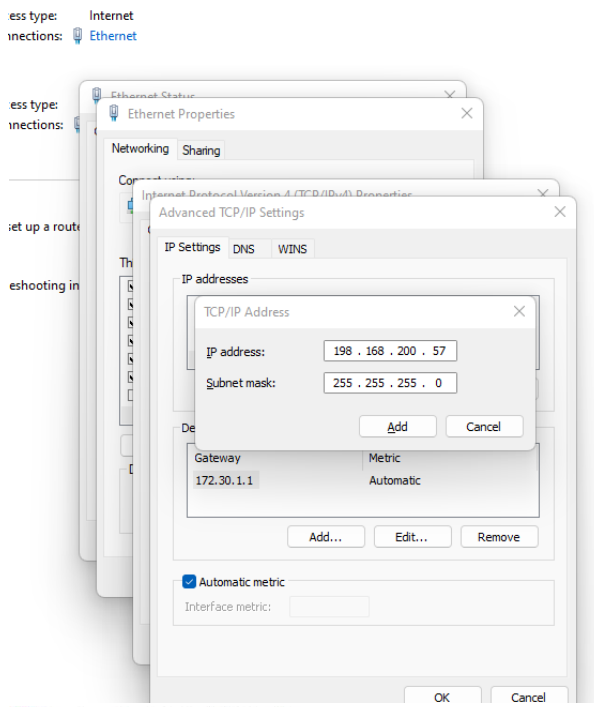
**Practical-9**

**Install Samba to share folders or files between Windows and Linux.**

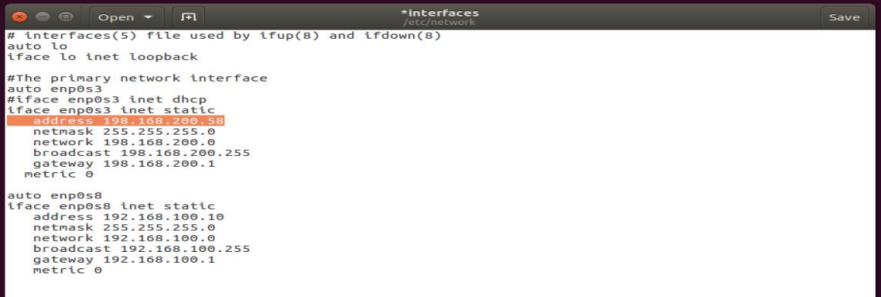
Install



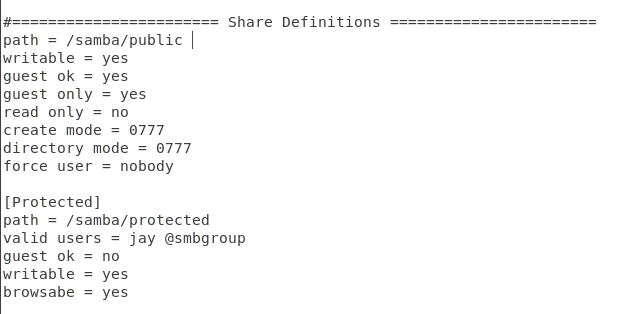
Add ip of your ubuntu machine to windows



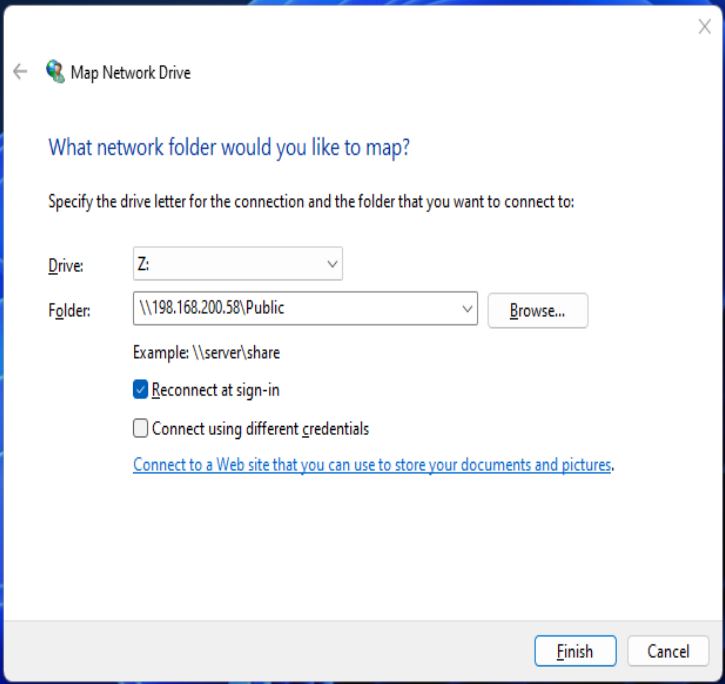
Configure the interfaces file



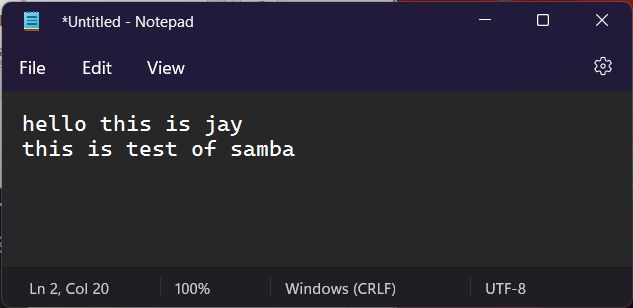
Ping the ip address of your ubuntu in your ubuntu terminal and open smb.conf



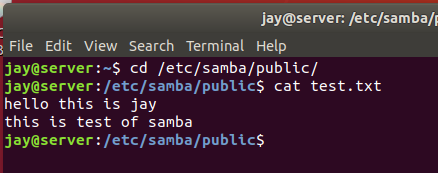
Map the drive to your network



Touch notepad in your network drive editing anything you want



Confirm it



Samba is working