**Overview of Prodaptive-NeT:**

Prodaptive-NeT is a system which helps in the proactive security response to host vulnerabilities.

This system is meant to be implemented in a network and prevents vulnerable devices from connecting the network. In order for a device to connect to the network, it has to undergo security scans conducted by Prodaptive-NeT, such as Nmap scans, etc. This helps to determine whether the device is vulnerable or not, and if it is discovered to be vulnerable, it will not be allowed to connect to the network. However, if the device successfully cleared the security scan, it will be deemed as a clean device and thus, be allowed to connect to the network.

In doing so, Prodaptive-NeT helps to reduce the risk of a network being potentially compromised by preventing vulnerable devices from connecting to the network so easily.

**Pre-requisites**

* VMware Workstation
* Mininet
* RYU Controller
* NMAP
* DNS Proxy (Captive Portal)
* MySQL Workbench
* Apache web server

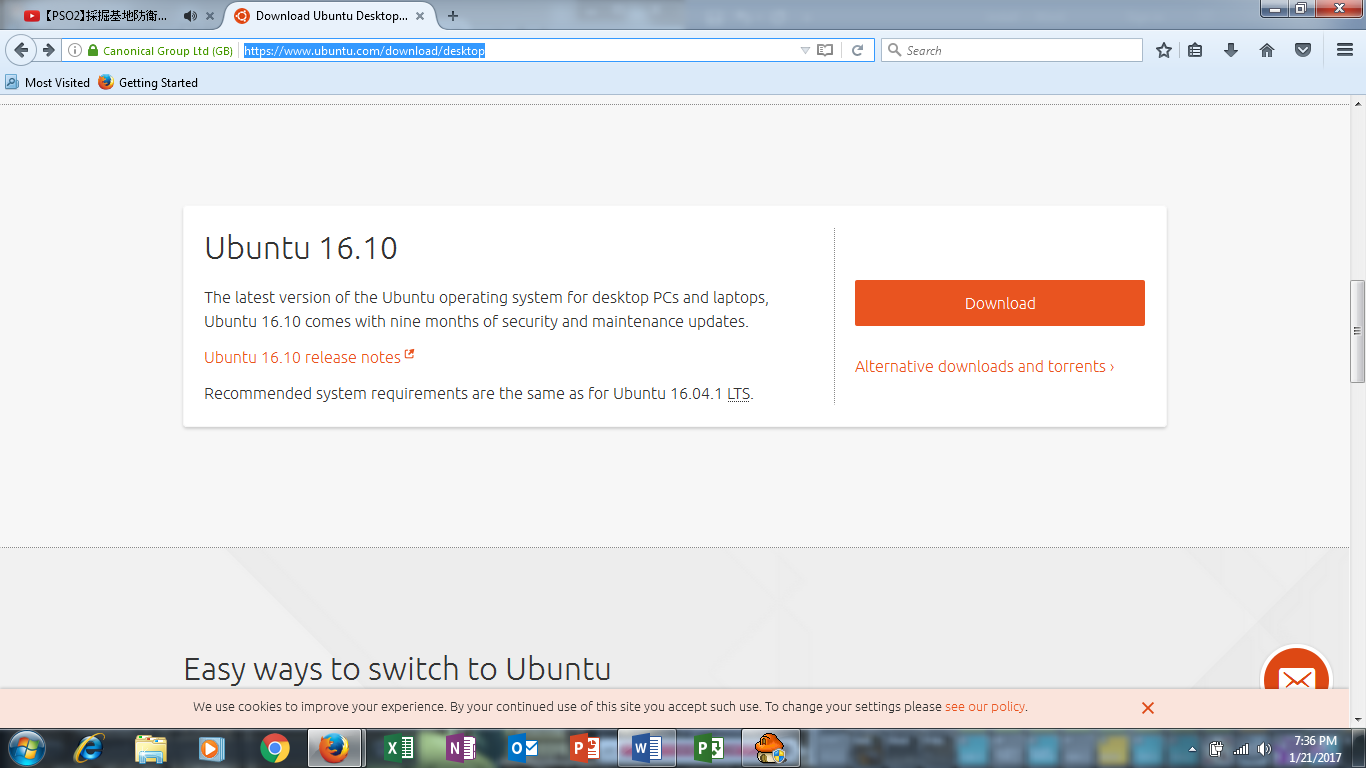
**Setting up VMware Workstation & Virtual Machine**

1. Download VMware Workstation Pro and install it.

(<http://www.vmware.com/ap/products/workstation/workstation-evaluation.html>)

1. Download Ubuntu ISO file (not the LTS version). This will be used as the VM base.

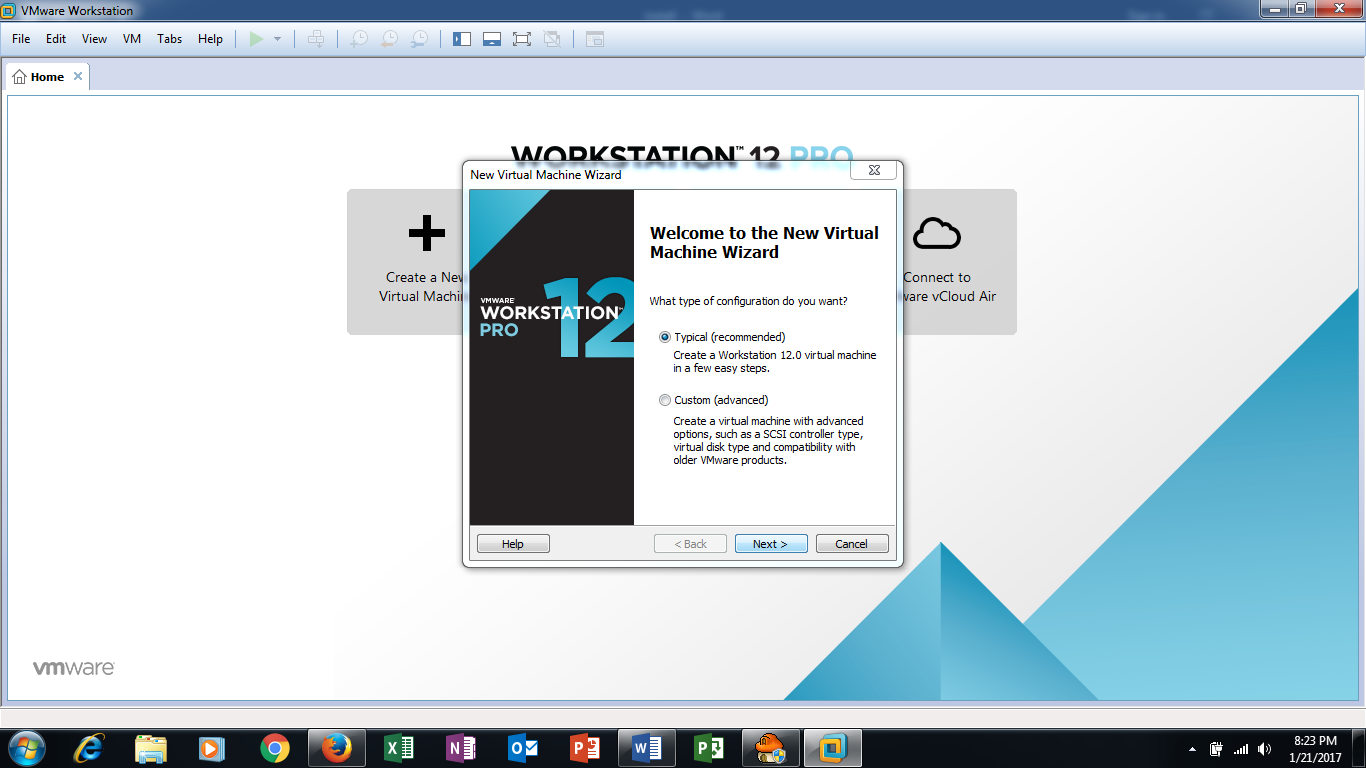
(<https://www.ubuntu.com/download/desktop>)



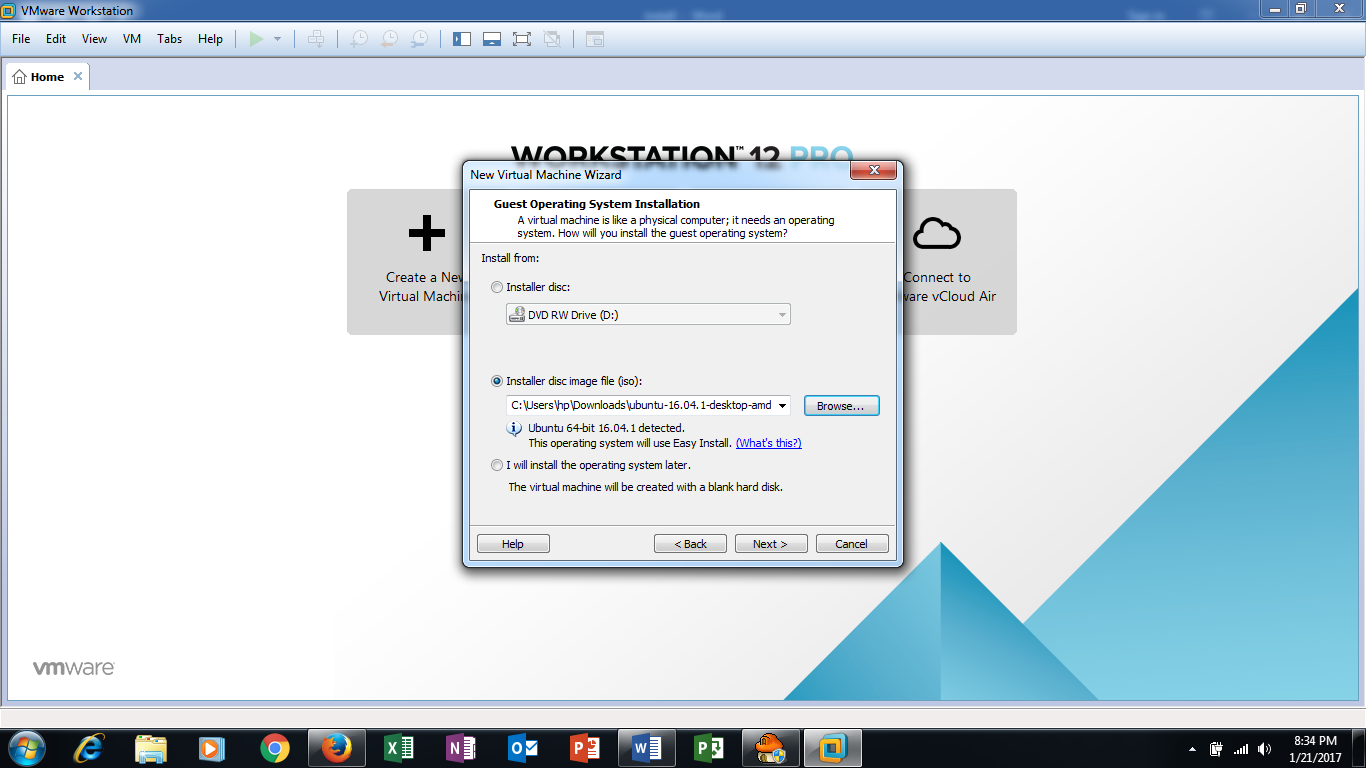
1. Launch VMware Workstation after downloading the ISO file.
2. Select “**Create a New Virtual Machine”**



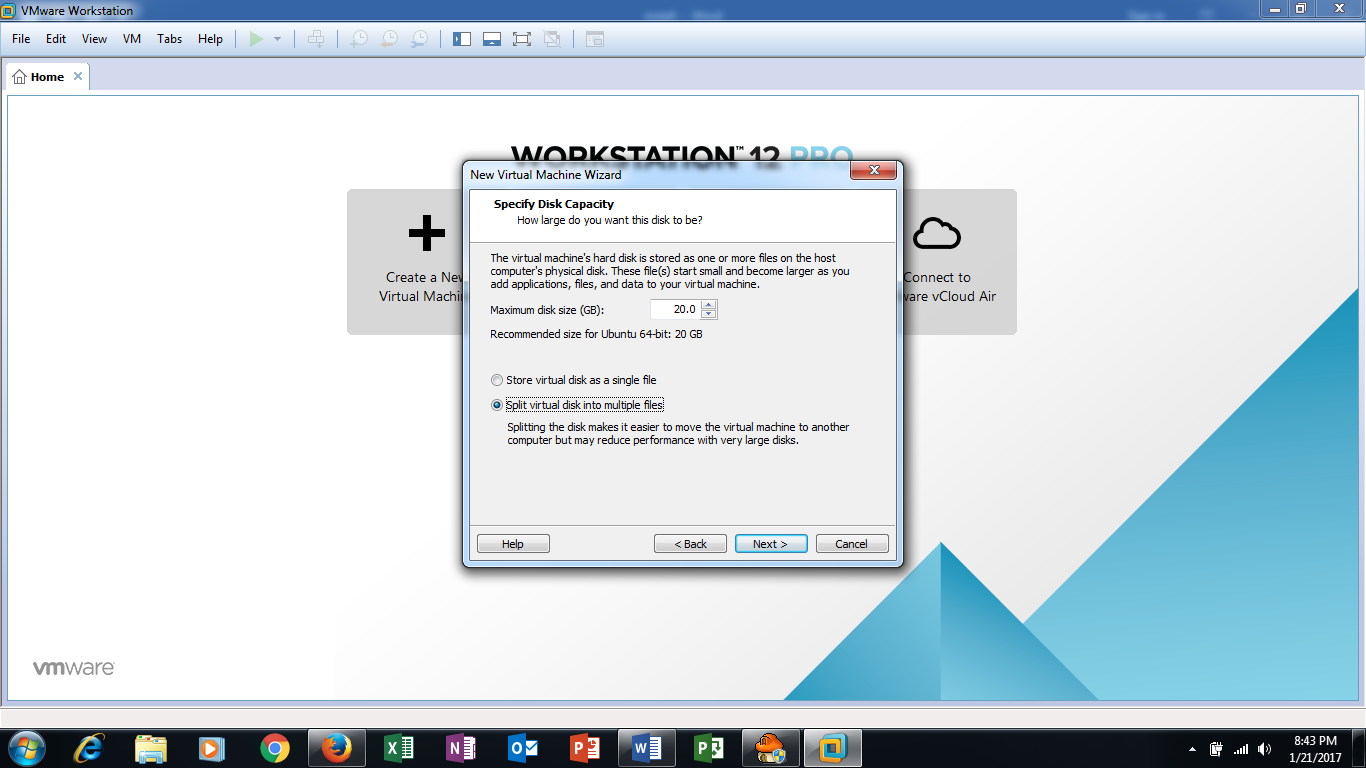
1. Select the “**Typical**” Option.



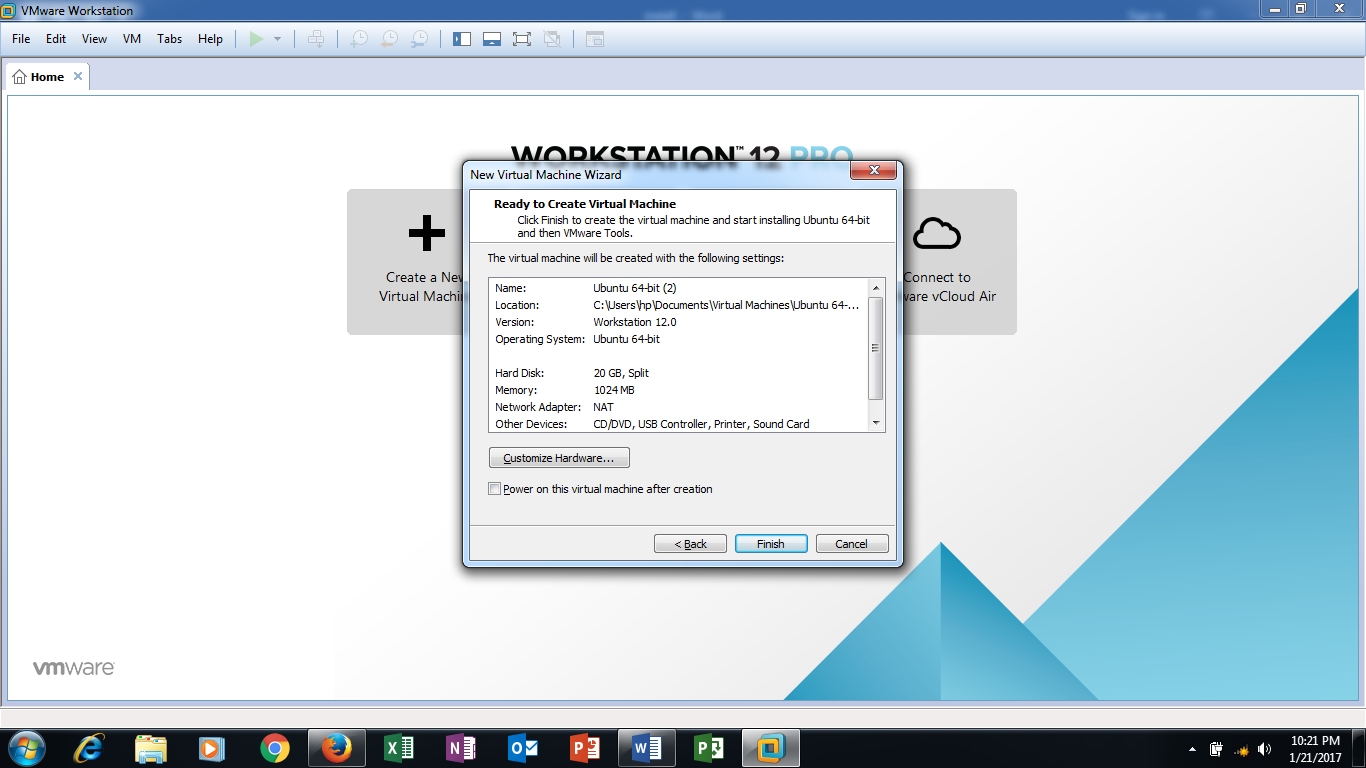
1. Select “**Installer disc image file (iso)**” and browse for the Ubuntu ISO file downloaded earlier.



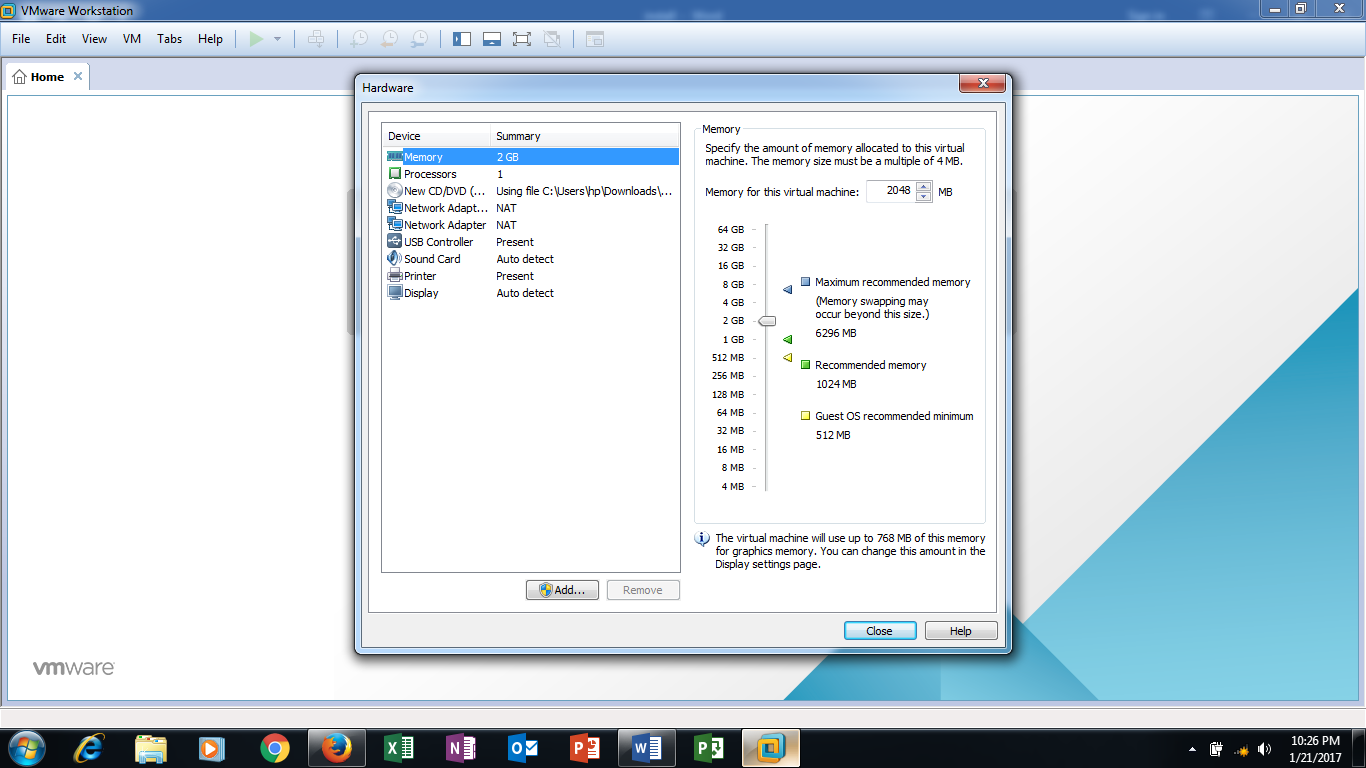
1. Give the VM a name, username and password. The username and password would be used for your account. Take note that username should only contain lowercase letters (a-z) and/or numbers (0-9).
2. Leave the Virtual machine name and location alone unless otherwise specified.
3. Leave the maximum disc size at **20.0 GB** and let it to **Split virtual disc into multiple files**.



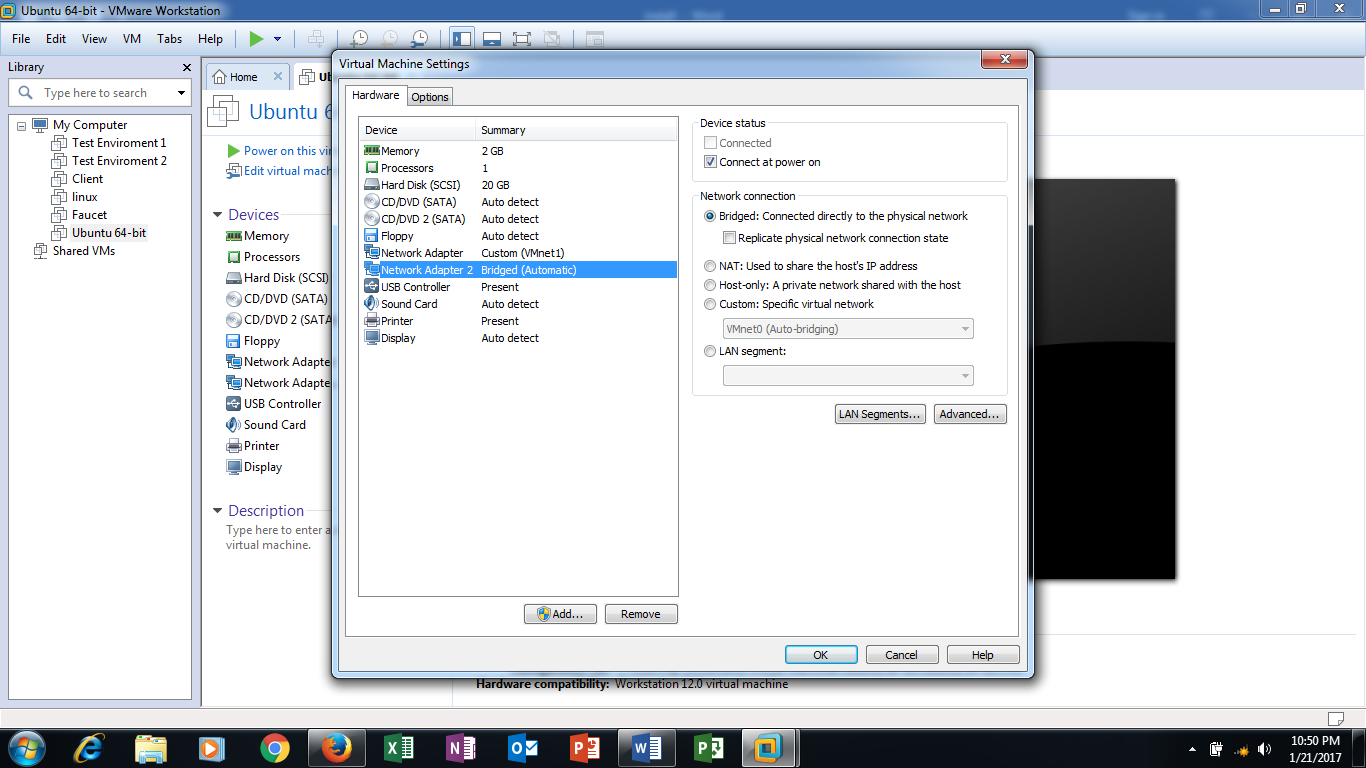
1. Uncheck “**Power on this virtual machine after creation**” and click **Customize Hardware**.



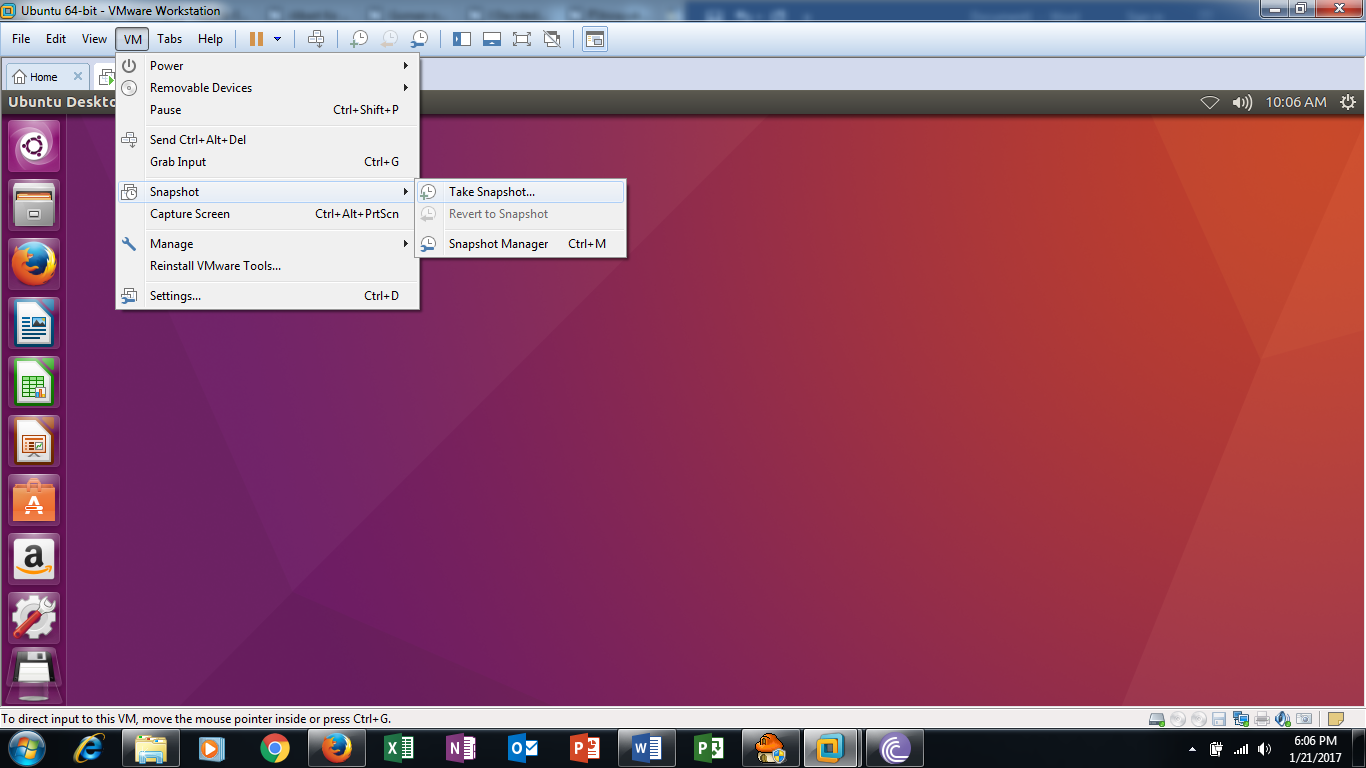
1. Add a new **Network Adaptor** and set the memory to **2 GB**. Finish the creating of the Virtual Machine.



1. Go to **Edit > Virtual Network Editor**. Add a custom network: **VMnet1**; **VMnet1** is a NAT.
2. Change the Hardware setting of the Virtual Machine. Set the first Network Adaptor to be **VMnet1** while the second Network Adaptor to be **Bridged**.



1. Power on the Virtual Machine and let it fully install.
2. Login as the user and take a snapshot. A snapshot is used to create a backup to fall back on if an irremovable error has occurred.



1. After the snapshot has finished backing up, restart the VM.

Installing the pre-requisites of Prodaptive-Net

1. Open a terminal.
2. Install any updates that Ubuntu may had missed out during the installation. Use the following commands one-by-one.
   1. Command: *sudo apt-get update*

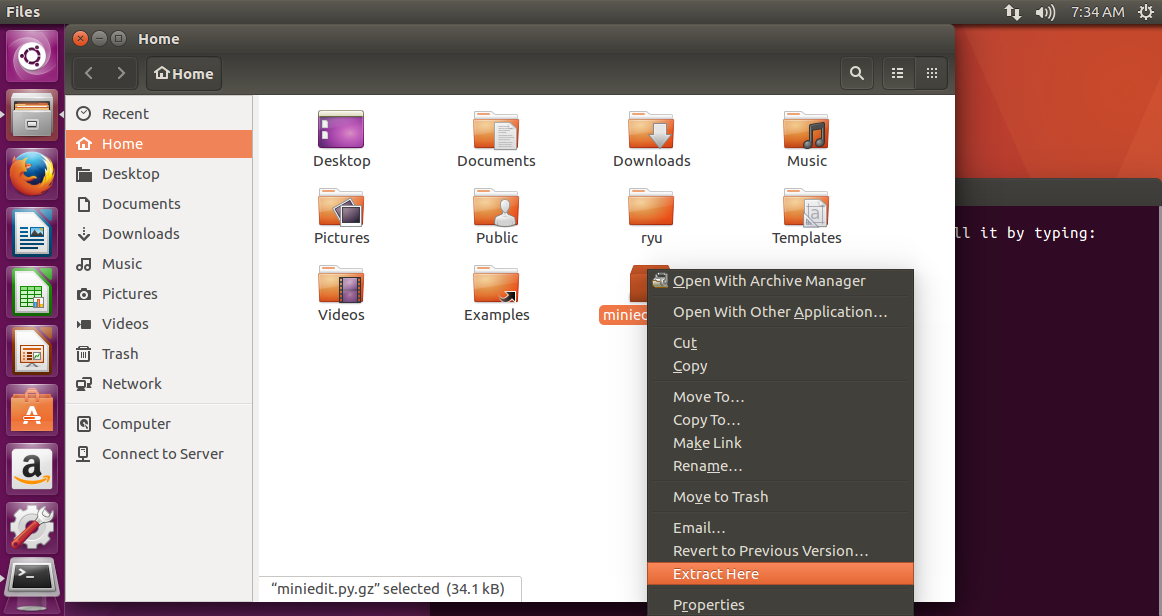
*sudo apt-get upgrade*

*sudo apt-get dist-upgrade*

1. Install pip and git. They are needed to install certain programs easier than apt-get.
   1. Command: *sudo apt-get install python-pip*

*sudo apt-get install git*

1. Install Mininet. This is used to craft a topology for bridging between the NAT and bridged network.
   1. Command: *sudo apt-get install mininet*
2. Move an archived file to the home. This archived file is used to easily craft the topology used for the Mininet.
   1. Command: *cp /usr/share/doc/mininet/examples/miniedit.py.gz./*
   2. Open file explorer and extract the archive in the home tab.



1. Install the Ryu library. The controller for switches runs on Ryu for the setup. Ensure you are in the home directory when running the commands.
   1. Command: *pip install ryu*

*pip install ryu-faucet*

*git clone https://github.com/osrg/ryu.git*

1. Install nmap. This is used to scan for vulnerable PC.
   1. Command: *pip install nmap*

*pip install python-nmap*

1. Install the following as they are prerequisite for running a program.
   1. Command: *sudo apt-get install python-tk*

*pip install datetime*

1. Install MySQL. This is used as the database system for Prodaptive-Net.
   1. Command: *sudo apt-get install mysql-workbench*

*sudo service mysql start*

*sudo service mysql enable*

1. Install the Apache web-server. This is used as a host to the webpages.
   1. Command: *sudo apt-get install apache2*
2. Install the DHCP server. This is used to provide an DHCP address for client PCs.
   1. Command: *sudo apt-get install isc-dhcp-server*
3. Get the interface name of the host-only network with *ifconfig*. For this guide, it is ***ens34***. Edit the ***isc-dhcp-server*** file in ***/etc/default***.
   1. Command: *sudo gedit /etc/default/isc-dhcp-server*

BEFORE



AFTER

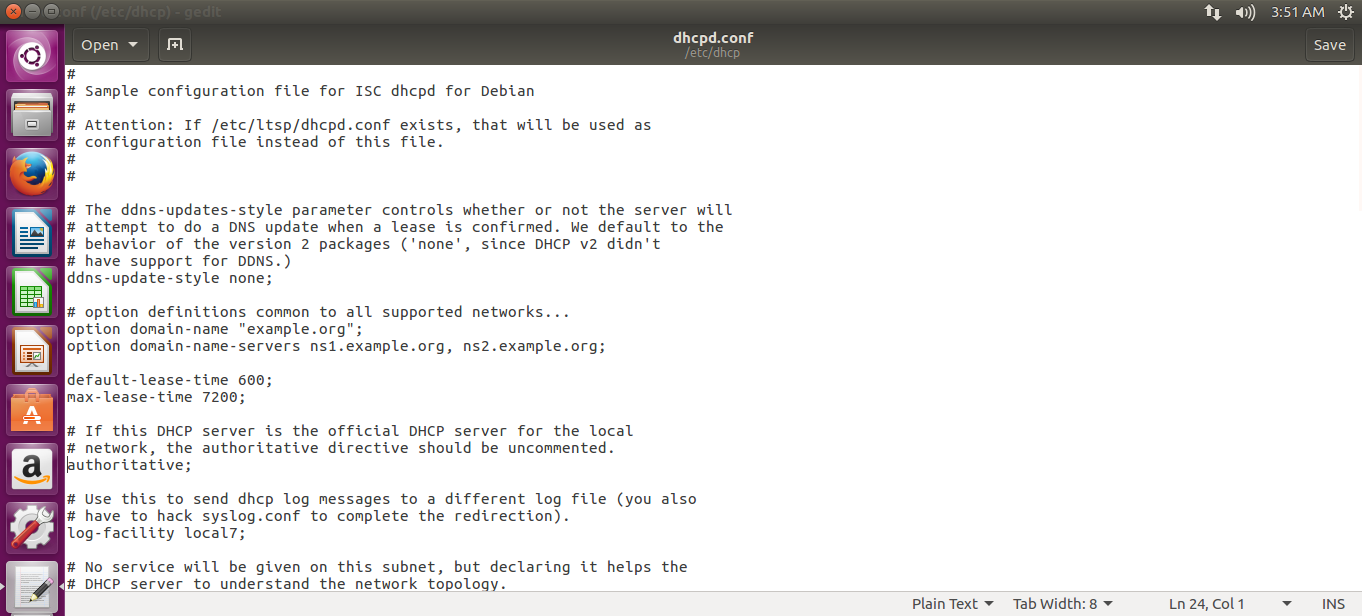


1. Edit the ***dhcpd.conf*** in ***/etc/dhcpd***. For this guide, assume that the bridged subnet is 192.168.237.0/24.
   1. Command: *sudo gedit /etc/dhcpd/dhcpd.conf*

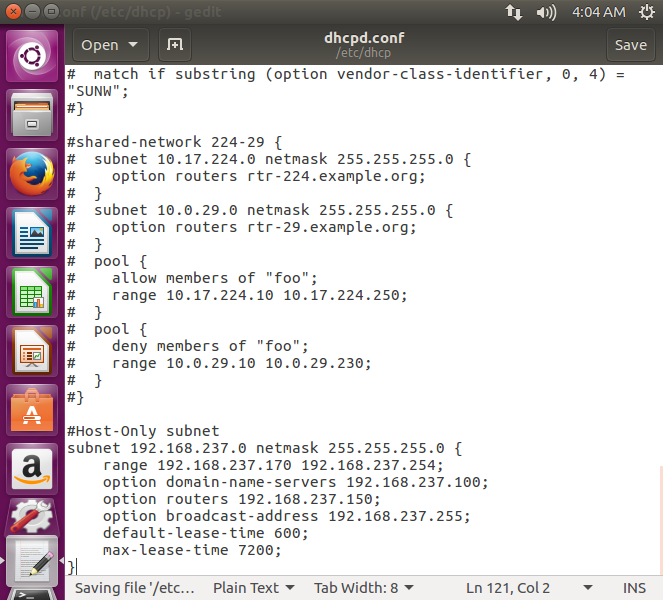
BEFORE



AFTER



Add the following lines at the end of the file.



The subnet of each IP in the file should be changed accordingly, however everything else must be the same.

1. After configuration is done, start up the DHCP service.
   1. Command: *sudo service isc-dhcp-server start*

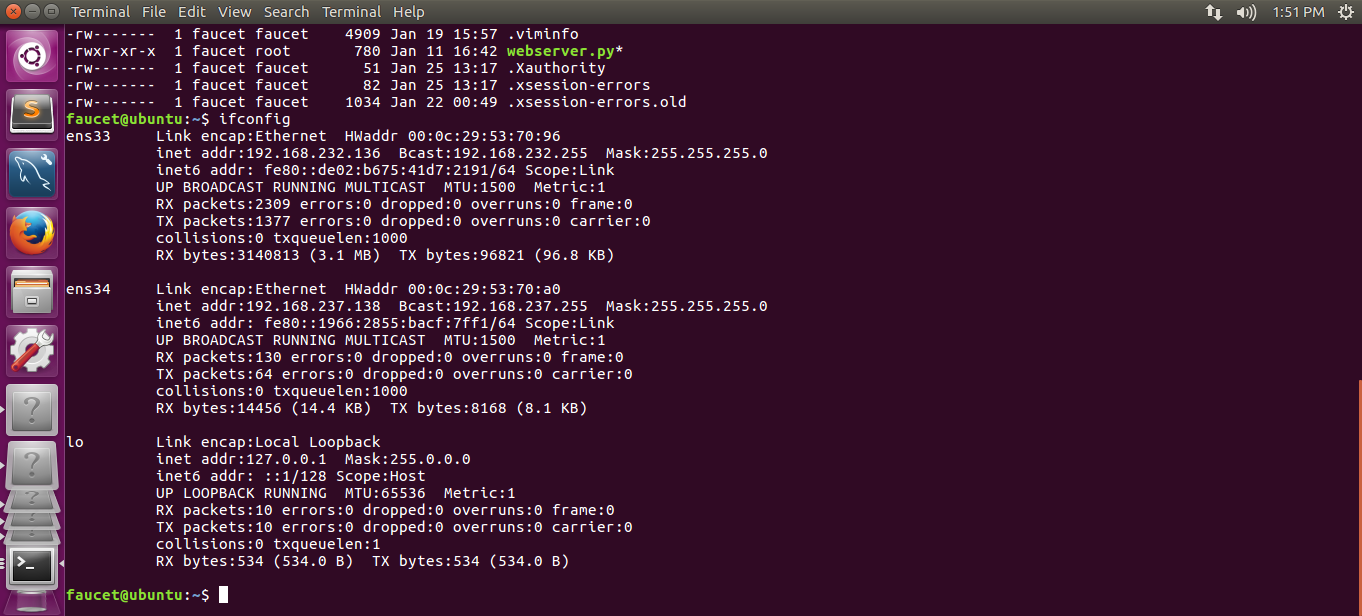
*sudo service isc-dhcp-server enable*

**Mininet guide**

Overview:

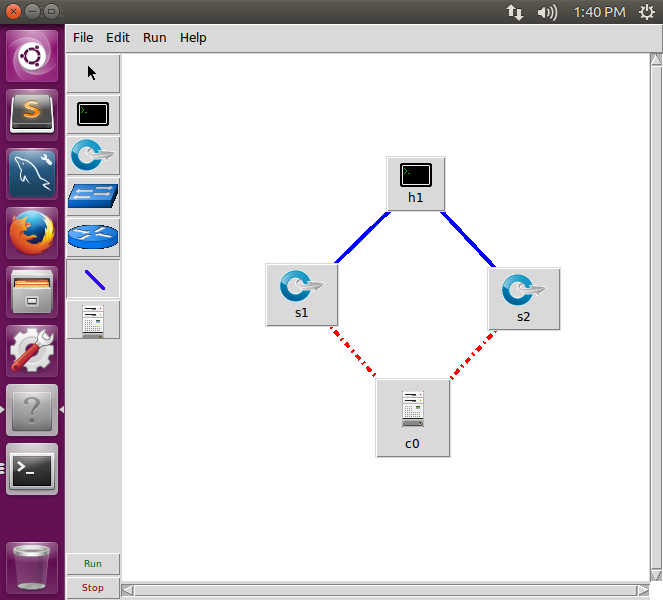
The purpose of this guide is to guide the user to set up Mininet and configuring Mininet. Refer to General Installation Guide for the installation of Mininet. This guide would assume that Section B of the General Installation Guide has been completed.

1. Create the Mininet topology with Miniedit
2. The Mininet file that is in a deployable state is attached to this guide and is called ***PnetMininet.py***. This file still needs to be configured to your IP addresses. Store the file in the home directory.
3. Change the permission of **miniedit.py** so that it could be executed.
   1. Command: *sudo chmod +x miniedit.py*
4. Find out the network interfaces present. If General Guide is followed, there should be 2 network interfaces (excluding lo).
   1. Command: *ifconfig*
   2. The following should be shown. Take down the IP address and subnets of the interfaces and figure out which interface is NAT and Bridged.



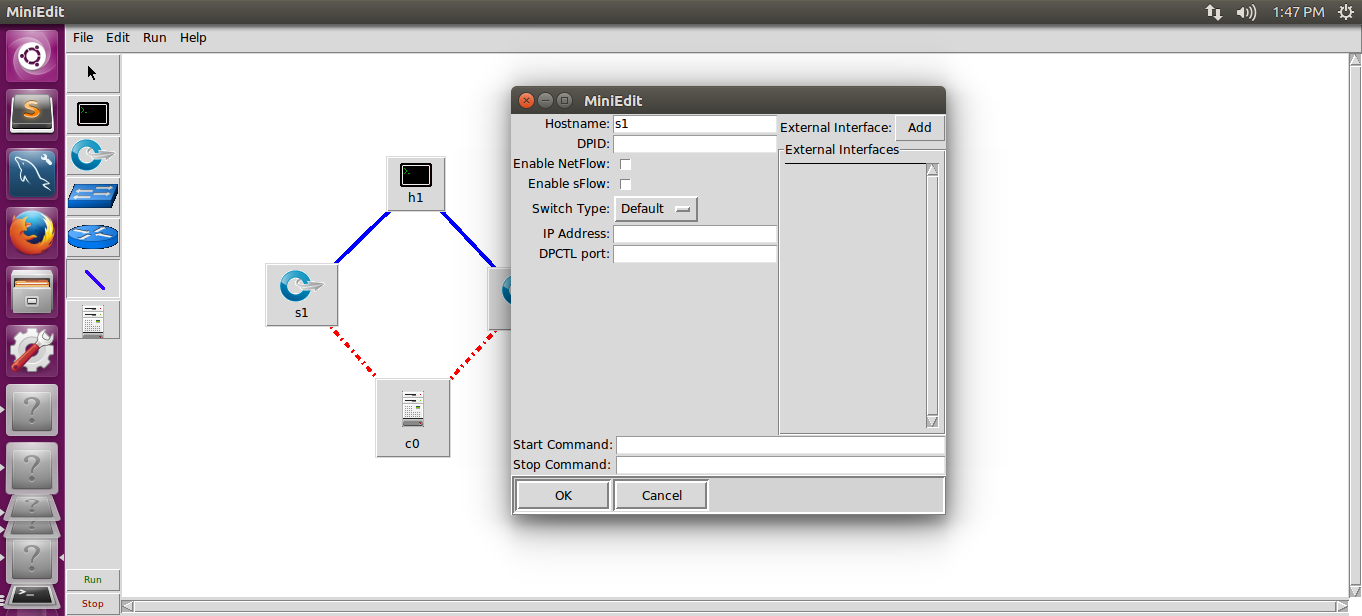
In this case: ens33 is NAT while ens34 is Bridged.

1. Start miniedit.py and it will open a GUI to create the Mininet topology.
   1. Command: *./miniedit.py*
2. Use the Miniedit GUI and make the following topology.



This will be the default topology used and will be configured with for Prodaptive-Net use.

1. Right Click and hold on **s1** and open **Properties.** The following diagram should be shown.



Under **DPID**, type in 00000002 and press **Add**. Under the new blank, type in **ens33**. This will bind **s1** to the network interface **ens33**, for reasons explained later.

1. Repeat step 5 for **s2**. However, this time, set the **DPID** as 0000000A and the network interface as **ens34**.
2. Go to **File > Export Level 2 Script**. This will create the basic Mininet topology to configure. Save it under any name you want. For the guide, this file would be referred as **PnetMininet.py**.
3. Editing the Mininet Topology file for Prodaptive-Net use
4. Change the permission of **PnetMininet.py** to be able to be executed.
   1. Command: *chmod +x PnetMininet.py*
5. Use an editor to configure the **PnetMininet.py** file.
   1. Command: *gedit PnetMininet.py*
6. Multiple changes need to be made for the topology to work.

***BEFORE***

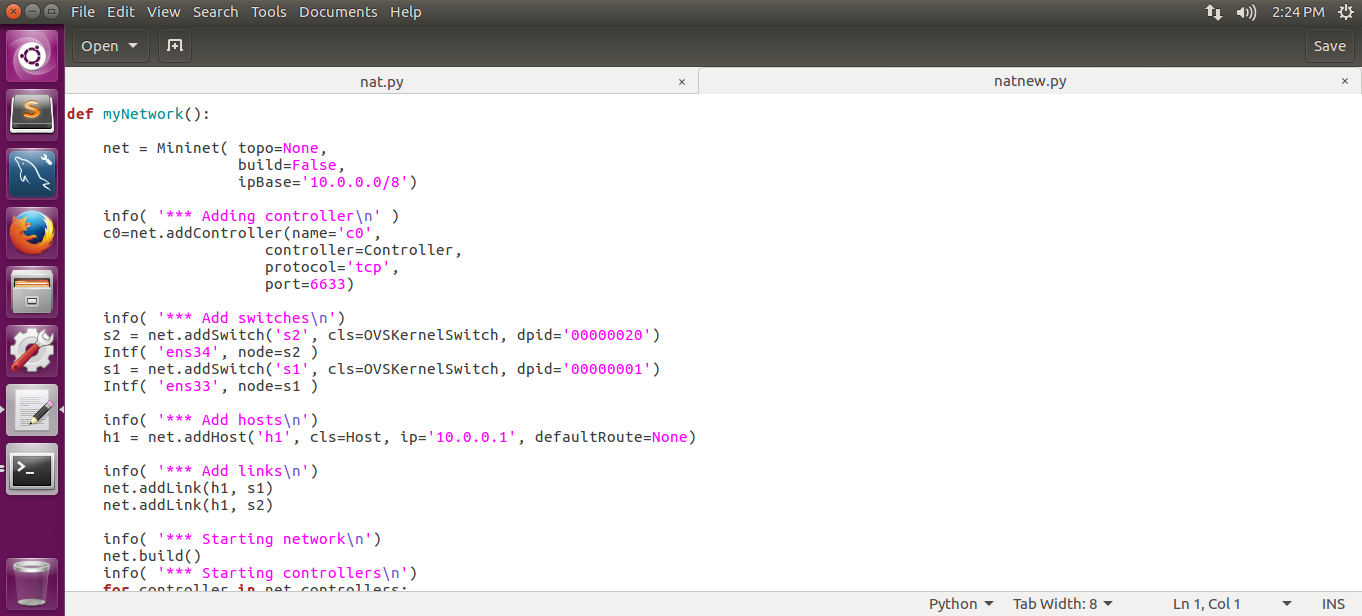


***AFTER***

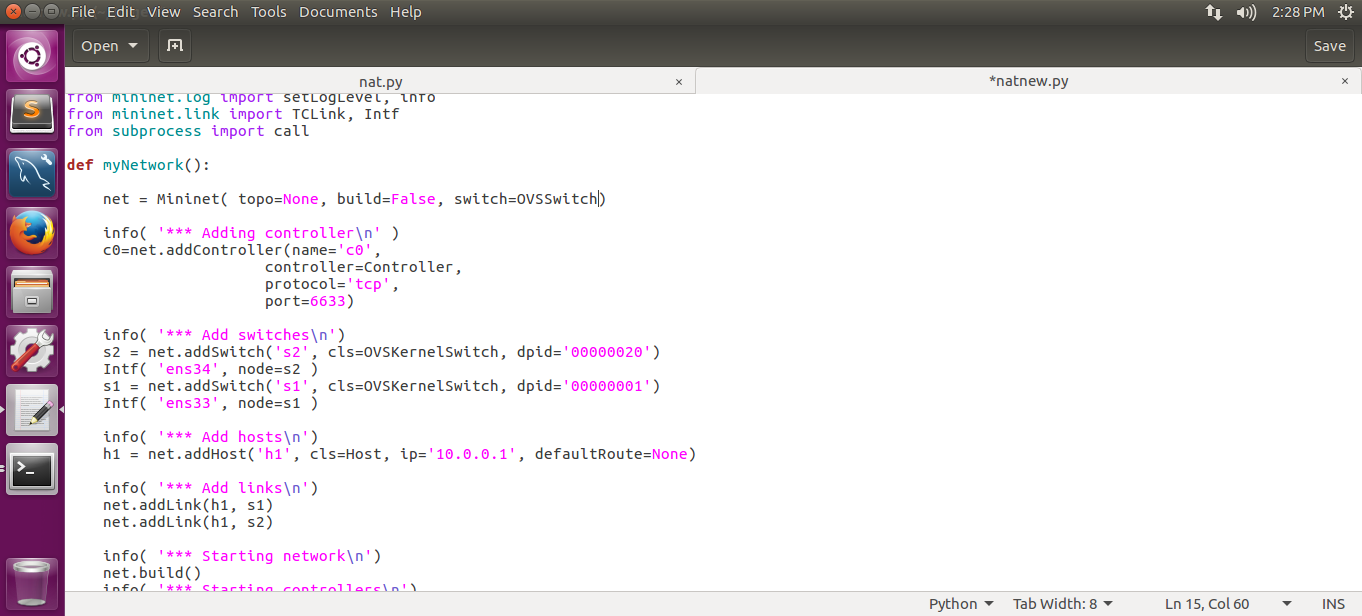


Import OVSSwitch from mininet.node

1. ***BEFORE***

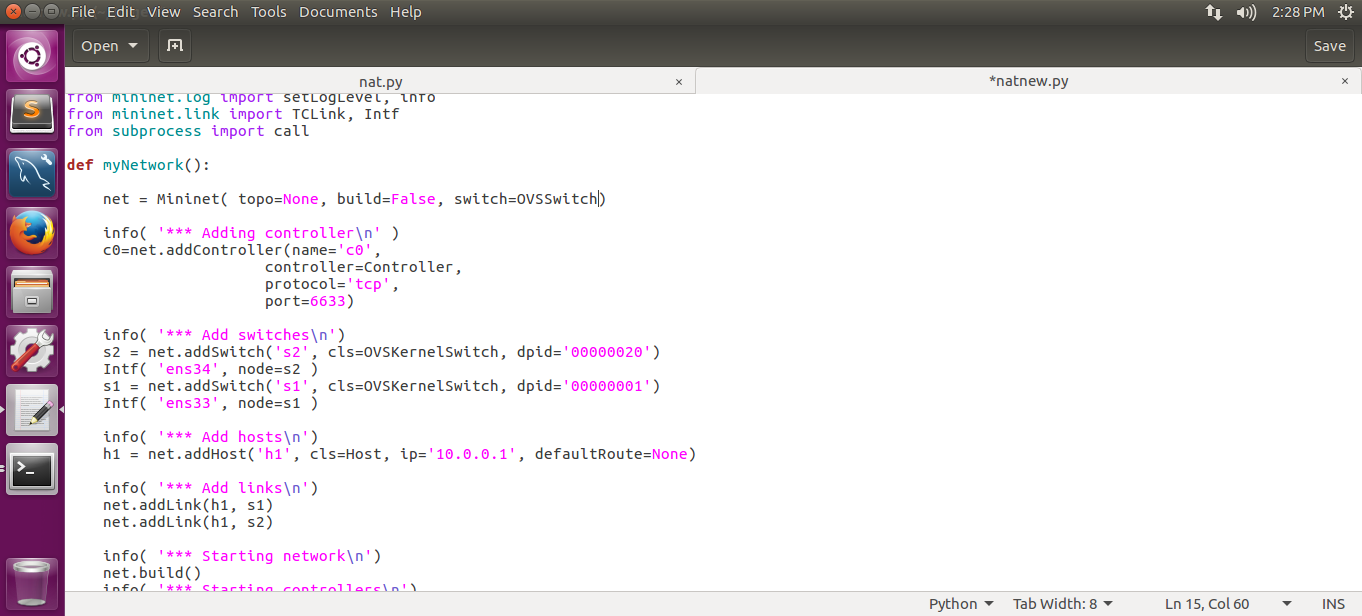


***AFTER***



By defining the switch, Mininet will know that all switches in this topology is an OpenvSwitch (OVS). The ipBase is removed as there is 2 different subnets in the topology which could not be used as a base.

1. ***BEFORE***



***AFTER***



Instead of using the controller provided by Mininet, the controller would be an external controller from Ryu. For more information, refer to the **Ryu Controller Guide**.

1. ***BEFORE***



***AFTER***

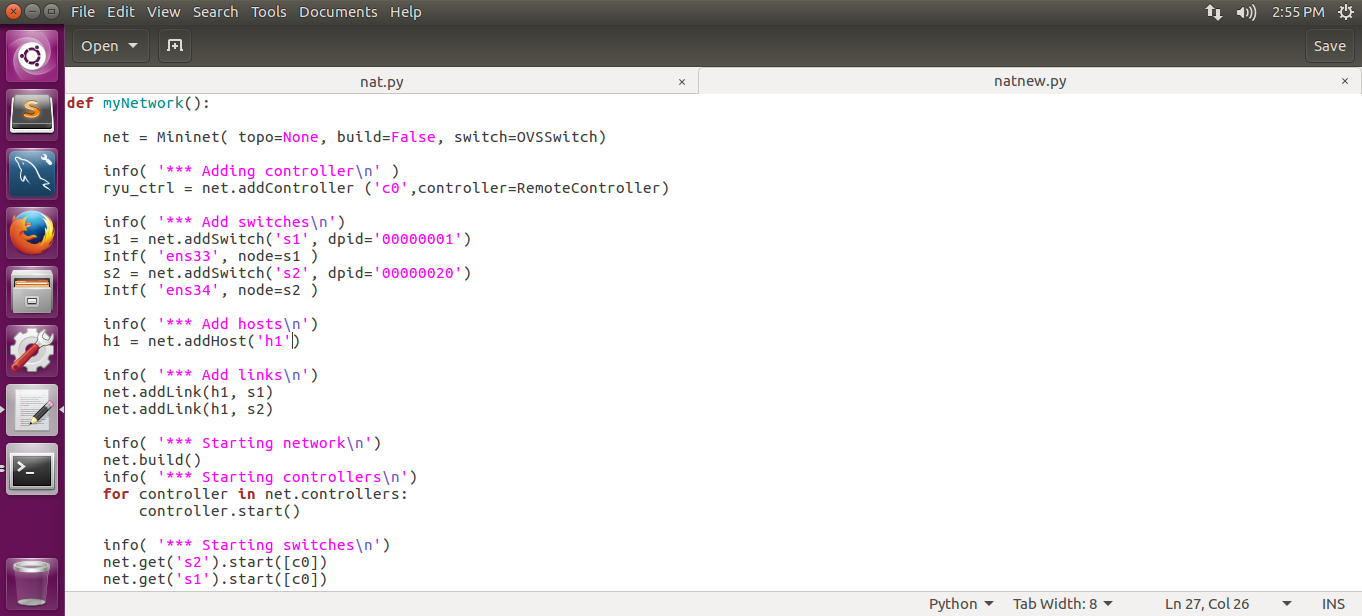


Swap around **s1** and **s2** lines to avoid confusion and since the switch is already defined as an OpenvSwitch, the cls is redundant.

1. ***BEFORE***

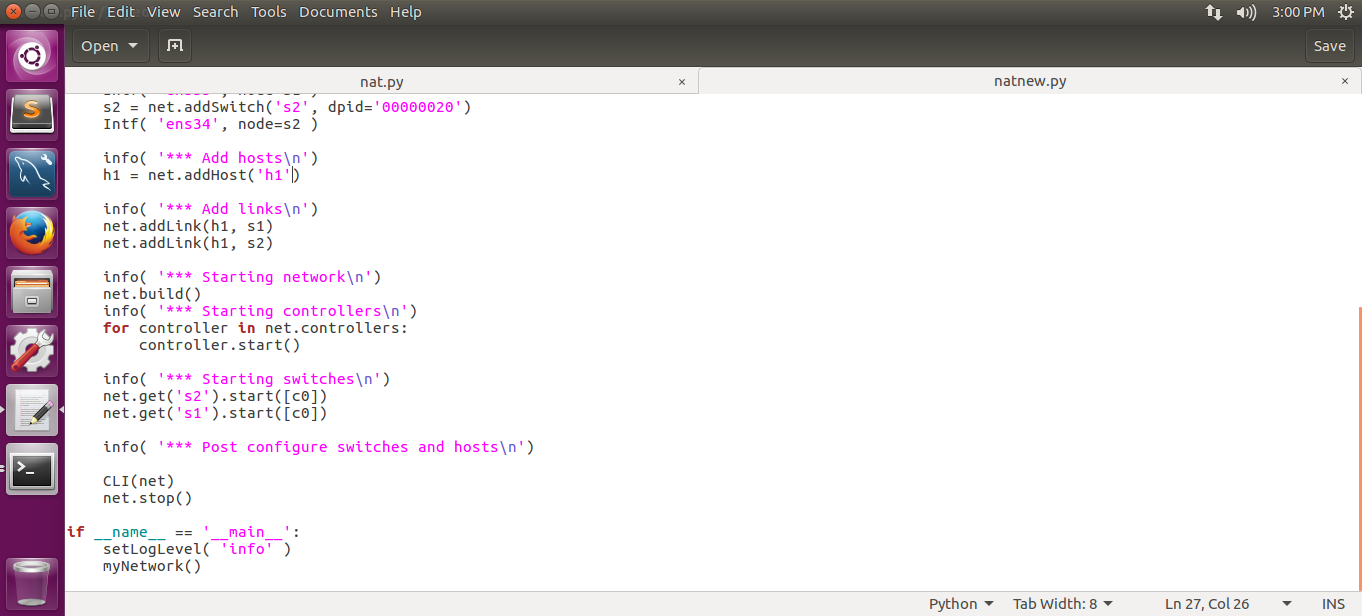


***AFTER***

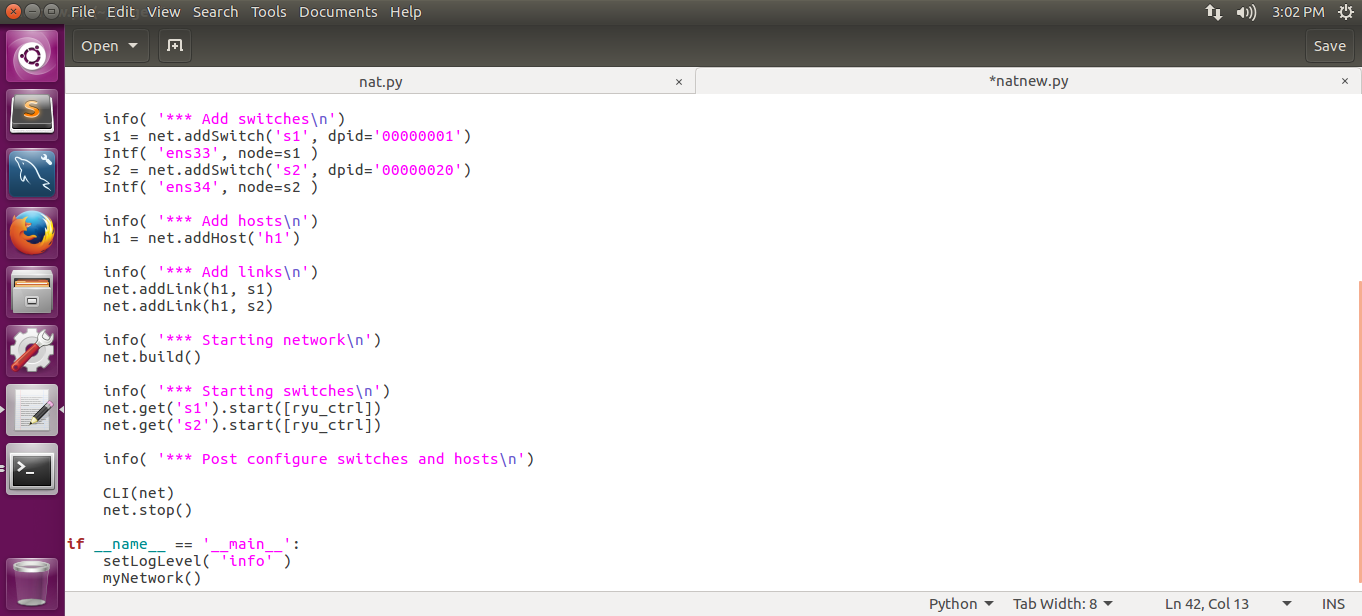


The characteristics of h1 will be defined in the later part of the program.

1. ***BEFORE***



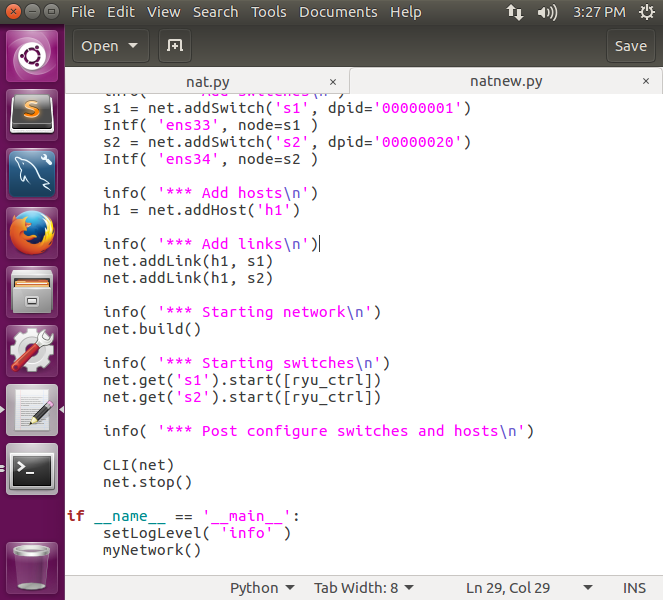
***AFTER***



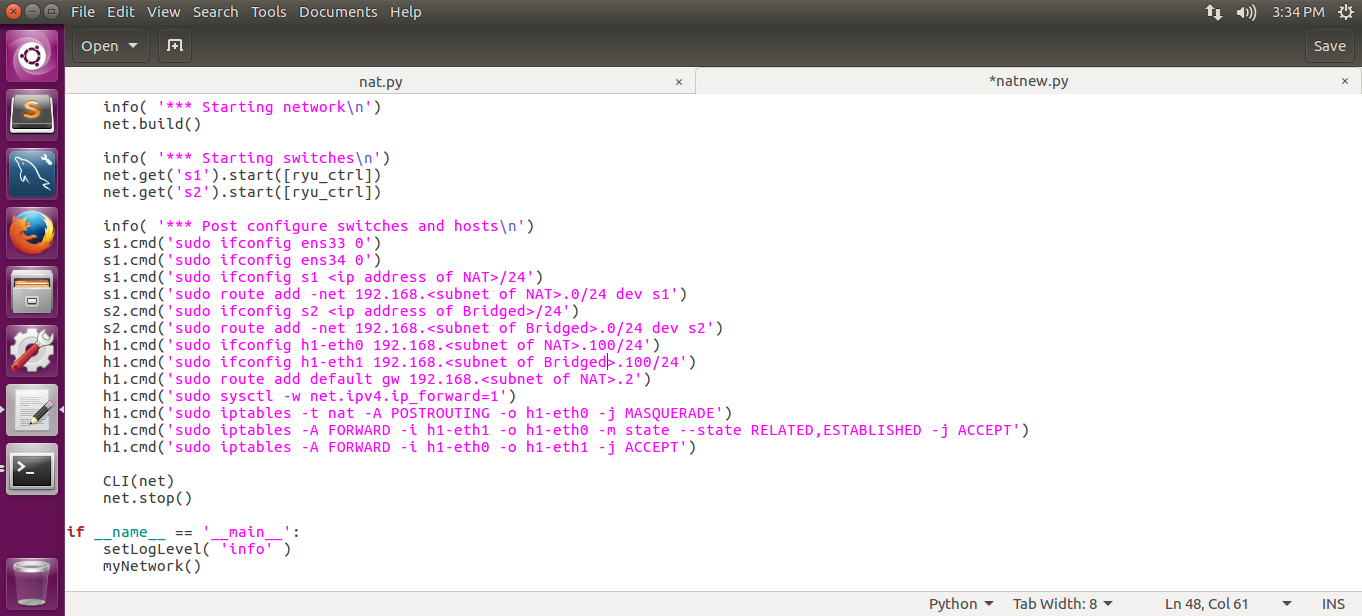
Since the controller used is an external controller, starting the controller is unnecessary. Since the controller is named **ryu\_ctrl** and not **c0**, adjust accordingly.

1. Take note of the IP address of the two network interfaces of the VM.

***BEFORE***

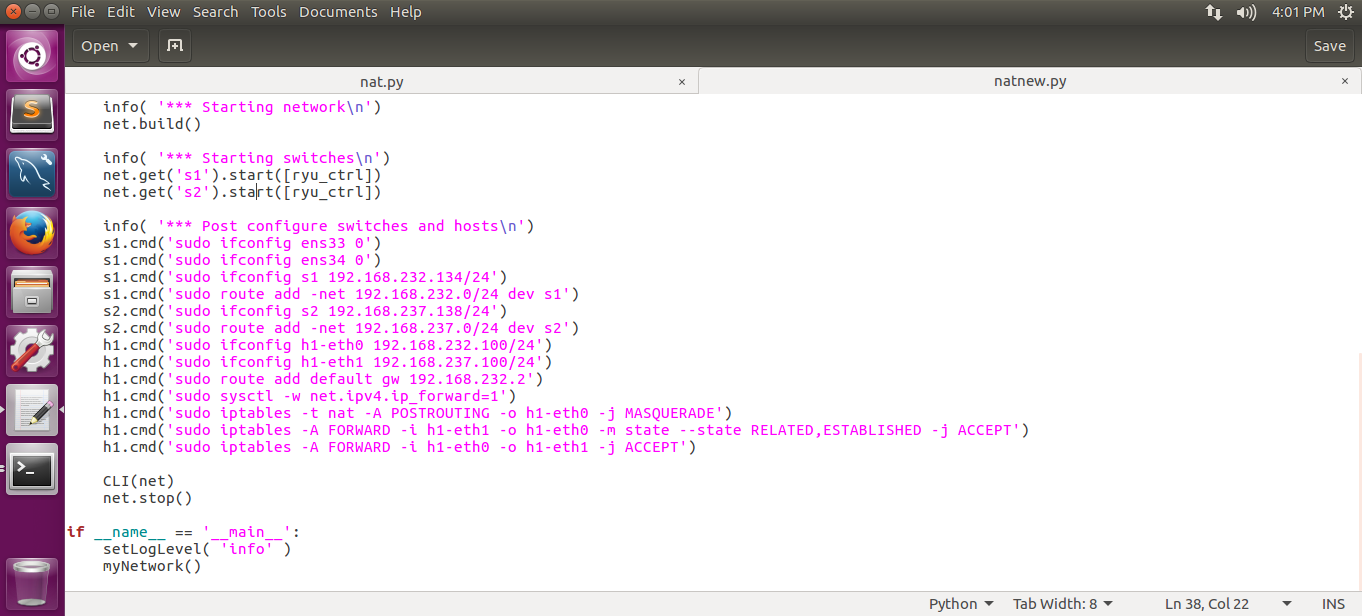


***AFTER***



* Remove the IP of both the Network Interfaces and give it to the two switches so that all the traffic that comes from the internet or the bridged side goes through the switches instead of the Network Interfaces.
* Set the default route of subnets so that Mininet knows which switch to send packets to if it belongs to a certain subnet.
* Set the network interfaces of **h1**.
* The default route for all packets that do not belong to either of the subnet is sent to the DHCP of the VM.
* The last 4 lines is needed for the packets to flow between the two subnets. This allows any computer from Bridged subnet to access the Internet if it has the permission to do so.
* PLEASE REPLACE THE PART IN THE <> WITH YOUR OWN IP/SUBNETS!

1. ***BEFORE***



***AFTER***



This modification will give the IP back to the network interfaces once the Mininet is closed.

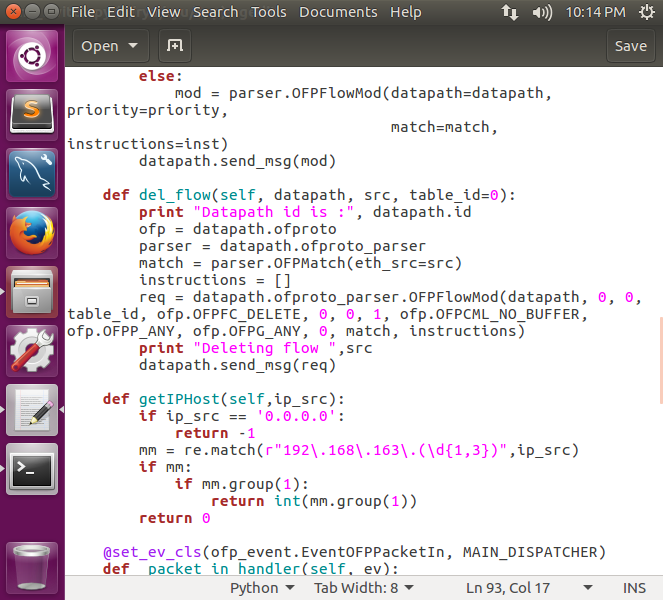
1. Save the file with CTRL + S and close the editor.
2. The Mininet Topology is now in a deployable state for Prodaptive-Net. To execute the file that was set up, simply type in the following command.
   1. Command: *./PnetMininet.py*

**RYU Controller guide**

Overview:

The purpose of this guide is to guide the user to set up Ryu Controller. Refer to General Installation Guide for the installation of the Ryu Controller. This guide would assume that Section B of the General Installation Guide and the Mininet Guide has been followed.

1. Preparing for configuring of the Ryu Controller
2. From the home directory, change directory into **ryu/ryu/app**.
   1. Command: *cd ryu/ryu/app*
3. Download two scripts attached to this guide. The names are ***my\_switch.py*** and ***my\_rest.py*** and they should be store under ***ryu/ryu/app***.
4. Change permission of ***my\_rest.py***. This would be the file executed for the Ryu Controller.
   1. Command: *chmod +x my\_rest.py*
5. Download two scripts attached to this guide. The names are ***my\_db.py*** and ***my\_ovs\_db.py*** and they should be store under ***ryu/ryu/app***.
6. Configuring ***my\_switch.py***
7. The deployable version can be found attached to the guide with the name ***my\_switch.py***. However, configuration of IP address is still needed due to the subnet.
8. Use an editor to edit ***my\_switch.py***.
   1. Command: *gedit my\_switch.py*
9. Edit the function called ***getIPHost***.

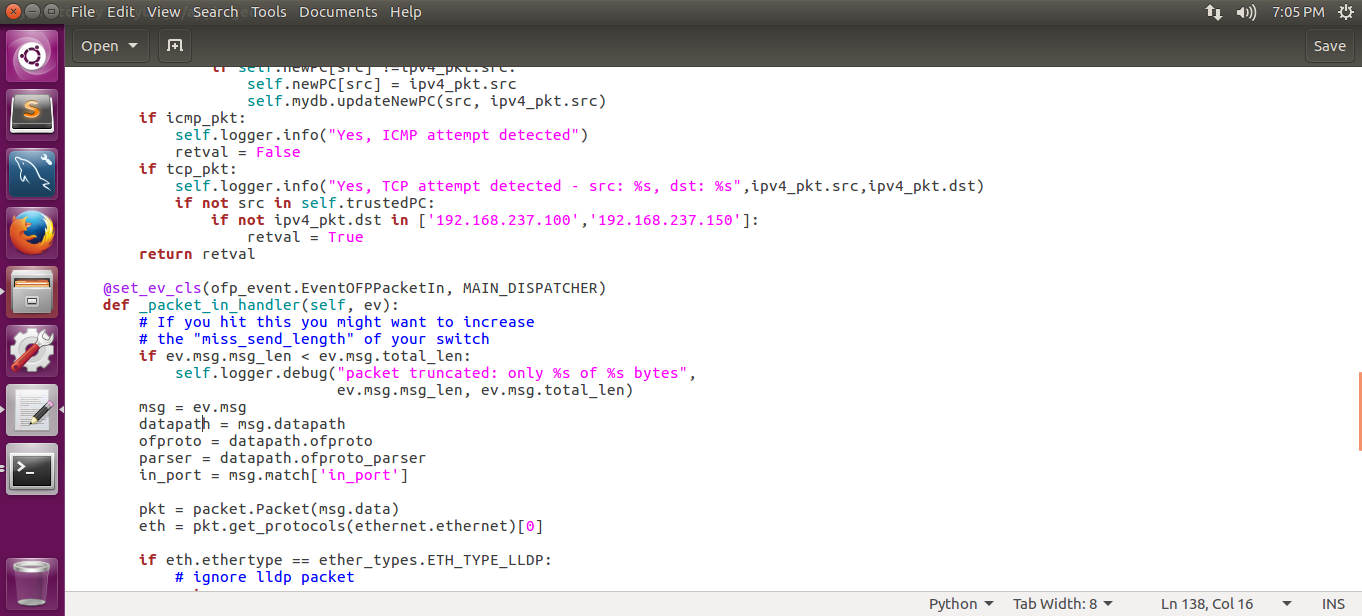


Change the following line to your bridged subnet.

E.g. My bridged subnet 192.168.100.0/24. Line would be changed to:

***mm = re.match(r”192\.168\.100\.(\d{1,3})”,ip\_src)***

1. Edit the function called ***handleNewPC***.



Change the following line to your bridged subnet.

E.g. My bridged subnet 192.168.100.0/24. Line would be changed to:

***if not ipv4\_pkt.dst in [‘192.168.100.100’,’192.168.100.150’]***

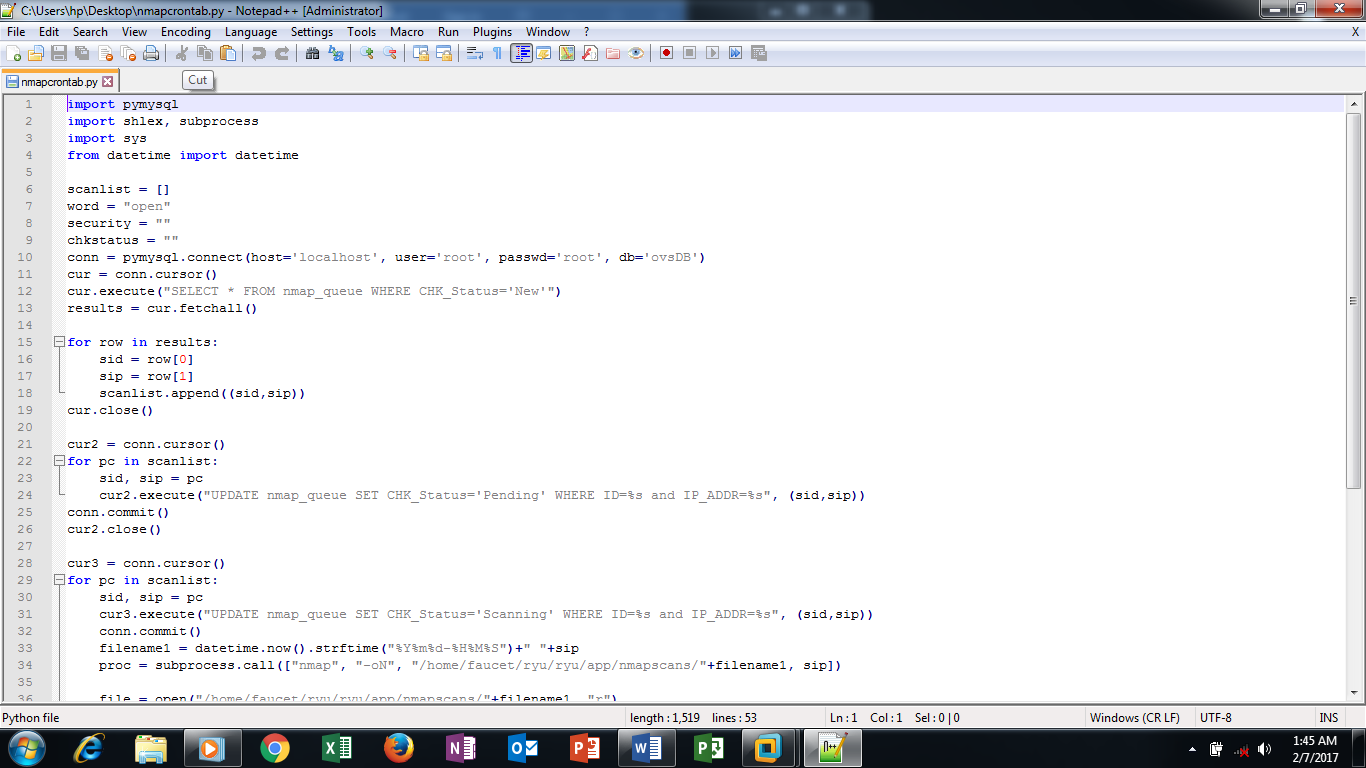
**NMAP guide**

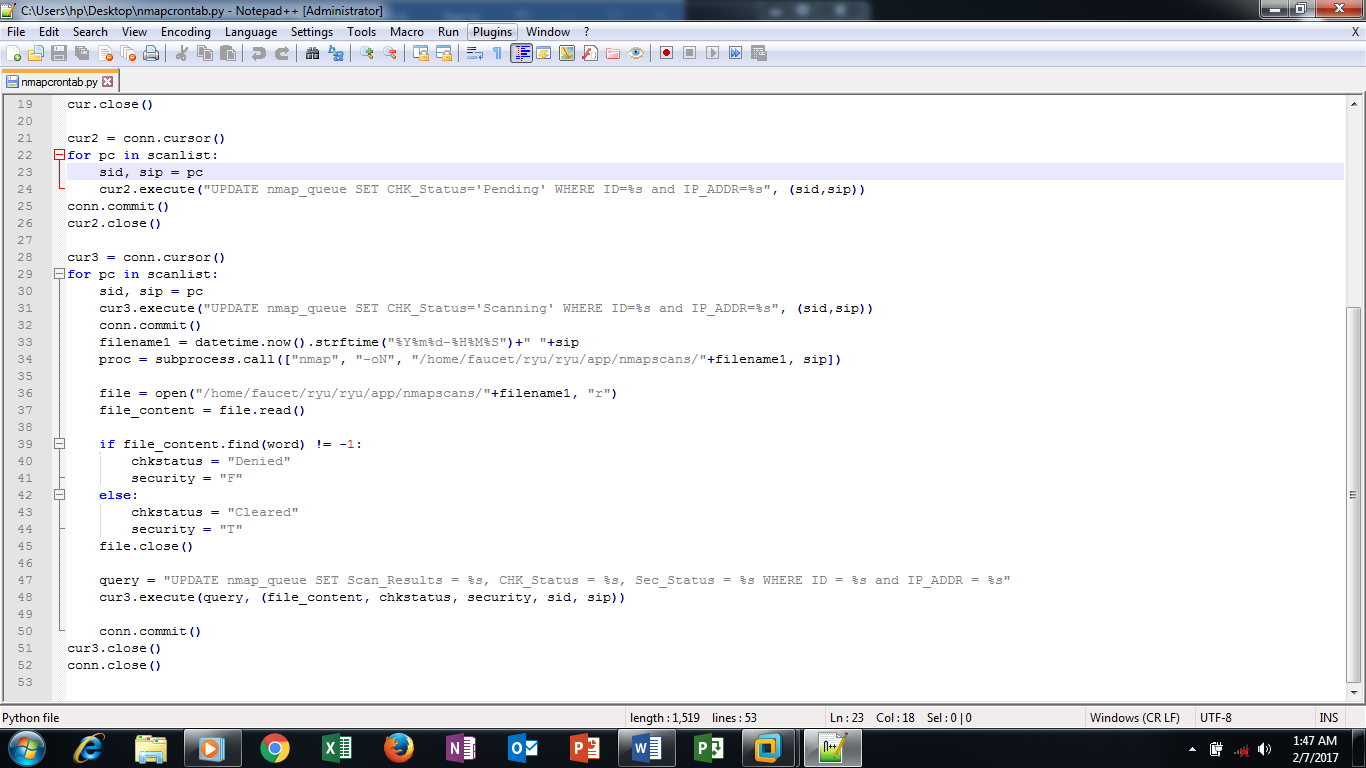
Overview:

The purpose of this guide is for the setting up of Nmap. Nmap is used to scan for vulnerabilities in a PC before letting it into the network.

For this guide, Nmap would be set at the lowest level and would not allow any PC with ports open to enter the network.

1. Creating the Nmap scanning file
2. The deployable version of the file can be found attached to the guide with the name ***nmapcrontab.py***. Some configuration of the file path is needed for the script to work. For this guide the home directory will be called ***/home/faucet***.
3. Create a directory in your ***~/ryu/ryu/app*** folder named ***nmapscans***.
   1. Command: *mkdir ryu/ryu/app/nmapscans*
4. Create a file called ***nmapcrontab.py***. Place this file in your home directory.
   1. Command: *touch nmapcrontab.py*
5. Use an editor to edit ***nmapcrontab.py***.
   1. Command: *gedit nmapcrontab.py*
6. Editing ***nmapcrontab.py***
7. The entire script is below:



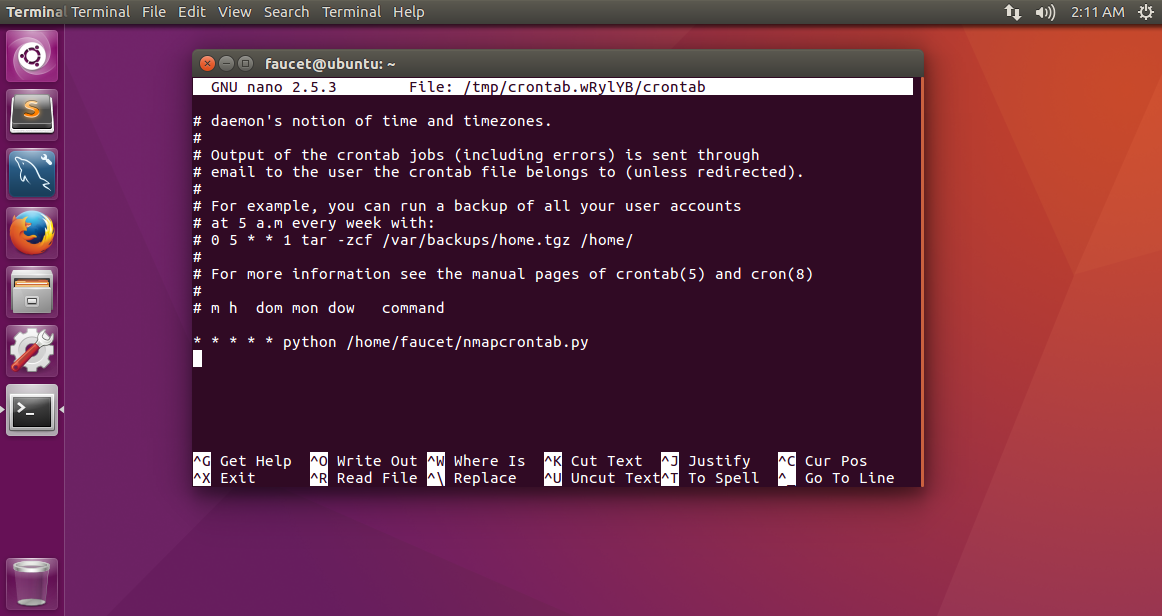


1. For Line 34 and 36, edit the file path accordingly to the ***nmapscans*** folder created in Section A Step 2.
   1. E.g. My home directory name is bob.

File directory: */home/bob/ryu/ryu/app/nmapscans/*

Deploying ***nmapcrontab***

1. After editing the file, edit the crontab file.
   1. Command: *sudo crontab -e*
2. Scroll all the way down through the crontab file and type in the following.



The ***/home/faucet*** in this line should be replaced with your own home directory.

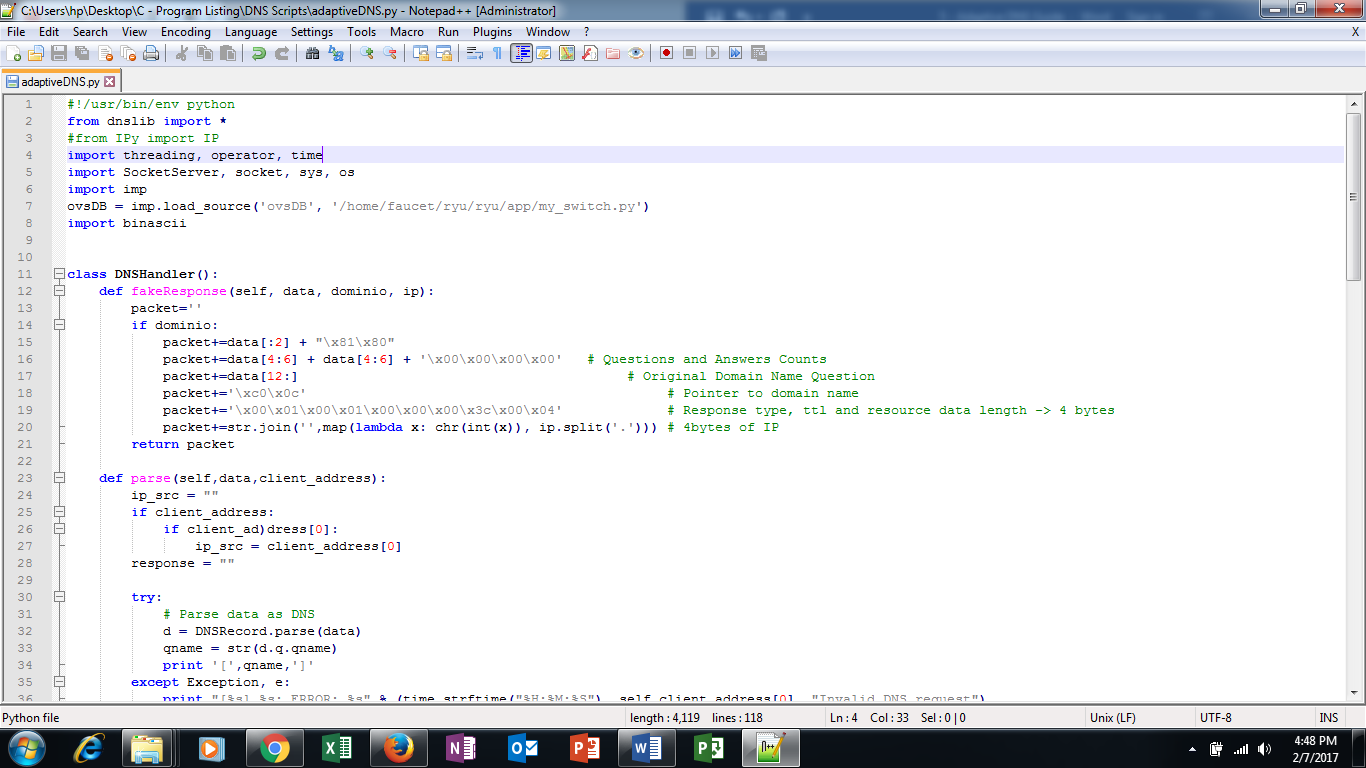
1. Save and exit the crontab file. The file will now conduct a search through the database every minute to search for new targets to scan. Once scanned, it will modify the database, allowing or denying new IPs from accessing the network.

**Adaptive DNS guide**

Overview:

The purpose of this guide is to setup an adaptive DNS. This DNS is used to provide answers to connections depending on the state of a PC in the database. This guide would assume that Section B of the General Installation Guide has been followed.

1. Creating and Configuring the DNS file
2. The deployable version of the file is attached to the guide with the name ***adaptiveDNS.py***. Some configurations to the file path is needed for the script to work. For this guide, the home directory is ***/home/faucet/***.
3. Download the script and put it into ***ryu/ryu/app***.
4. Change the permissions of the file.
   1. Command: *sudo* *chmod 777 adaptiveDNS.py*
5. Edit the file.
   1. Command: *gedit adaptiveDNS.py*
6. Edit the following line.



Change the file path ***/home/faucet/ryu/ryu/app/my\_switch.py*** to your own home directory.

E.g. My home directory is bob. This file path change to ***/home/bob/ryu/ryu/app/my\_switch.py***

Save and exit the file. The file is now in a deployable state.

**MySQL Workbench Installation guide**

Overview:

The purpose of this guide is to setup MySQL for the Prodaptive-NeT system to store the device information.

We will be installing MySQL as our database system to store all the details.

First, launch a terminal, type the following command shown in Fig. X to install MySQL

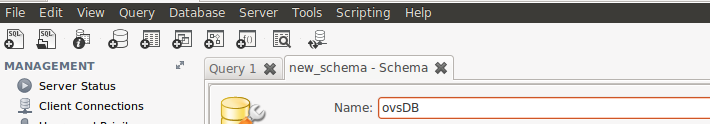


Once the installation is done, start/enable the service by entering the following commands,

sudo service mysql start

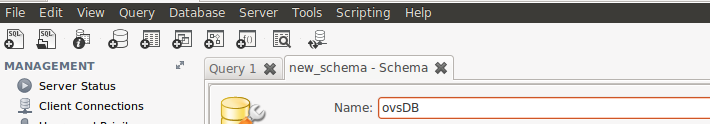
sudo service mysql enable

Launch MySQL Workbench, click on the cylinder icon to create a Schema and click on the table logo to create a table as shown in Fig. X

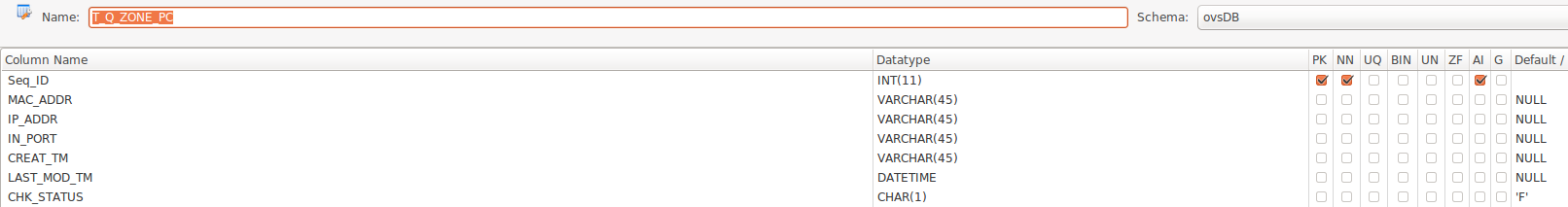


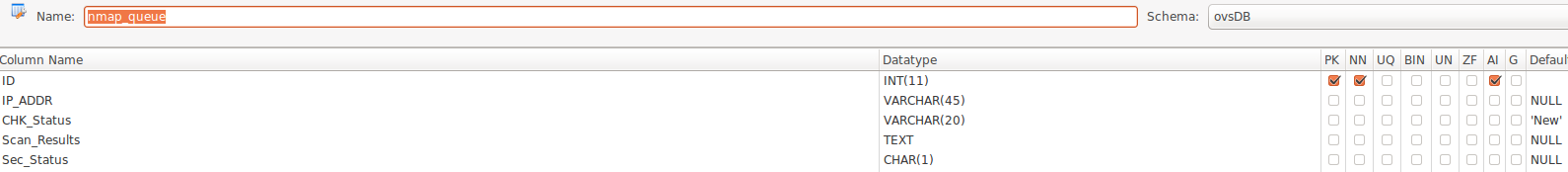
In this project, we have one schema and three tables, now we will create them

We will create a schema named “ovsDB”.

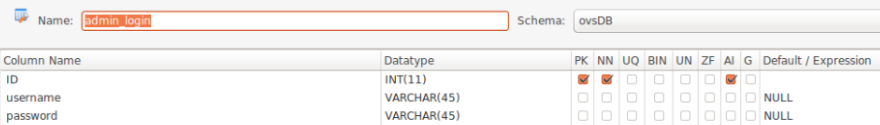


After that, create three tables and name them “T\_Q\_ZONE\_PC” and nmap\_queue. T\_Q\_ZONE\_PC table will store information of the trusted and untrusted PC as well as their MAC address and IP address. For nmap\_queue, it will contain information of PCs which are either pending to be scanned by Nmap or cleared by Nmap scans. Lastly, we will name the third table “admin\_login” which will be used to store login credentials of the administrator to login to the dashboard.





\*Remember to select VARCHAR as the datatype for IP\_ADDR as each octet are separated by a “.”



**Installation/configuration of Web Server**

Overview:

The purpose of the guide is to install and setup the web server so that the users can successfully access the captive portal.

We will set up a web server in our environment to host our webpage where the devices will be directed to before successfully joining the company’s network. There are many available web server applications but we will be installing Apache web server.

First, open a terminal and execute the command shown in Fig. X



This command will install Apache web server

Once installation is done, open the main configuration file with a text editor as shown below

sudo nano /etc/apache2/apache2.conf

At the bottom of the file, add a ServerName directive pointing to your domain name.

ServerName 192.168.163.130 <- Replace with your server’s IP or domain name

**\*If you do not have a domain name, you can use your server’s IP address**

Now restart/enable the web server by entering the following commands

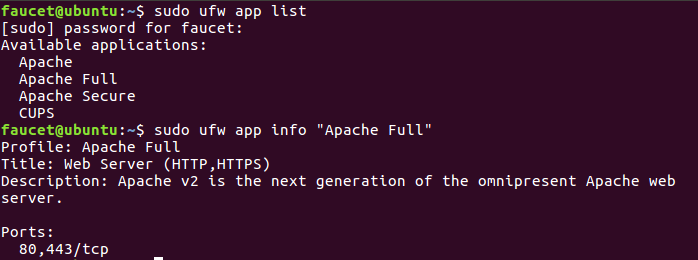
sudo systemctl restart apache2

sudo systemctl enable apache2

Next we will adjust the firewall to allow web traffic. To do this, make sure that your firewall allows HTTP and HTTPS traffic. You can make sure that UFW has an application profile for Apache by entering:

sudo ufw app list

This will list the available applications

****

The following command will display the ports that are enabled

sudo ufw app info "Apache Full"

Now we will allow incoming traffic for Apache

sudo ufw allow in "Apache Full"

As PHP is 1 of the component, we will install PHP with the following command

sudo apt-get install php libapache2-mod-php php-mcrypt php-mysql

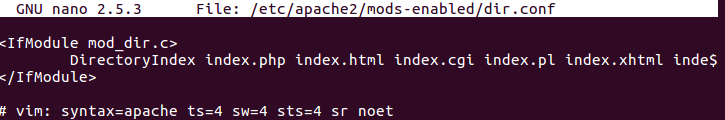
After installation is completed, we need to Apache to look for PHP file instead of HTML.

Open a text editor to edit the dir.conf file

sudo nano /etc/apache2/mods-enabled/dir.conf



Move “index.php” to the front as shown in the fig below



Once you are done, save the file and restart the server by entering the command

sudo systemctl restart apache2

Now the web server is ready to be used.

**Deployment guide**

Overview:

The purpose of this guide is start up the system for use.

1. Create a shell script
2. There are two script attached to the guide called ***exec\_switch.sh*** and ***exec\_DNS.sh***. Download the scripts and place it in the ***ryu*** folder.
3. There is a script attached called ***startPnet.py***. Download the script and place it in your home directory.
4. Configure ***startPnet.py*** and change the file directories ***/home/faucet/ryu*** into your own home directory.

E.g. My home directory is bob. Thus, change the file directory to ***/home/bob/ryu***.

To start the program, type the following commands to start Ryu Controller

cd ryu

sudo ./exec\_switch.sh

Open another terminal to start the DNS and Mininet by typing the following commands

Sudo ./startPnet.py

Now you should have three terminals being displayed on your screen, namely Ryu Controller, Mininet and DNS proxy server (Captive Portal)

For the convenience of the administrator, we’ve built a Dashboard for the administrator to analyze the records of main table and Nmap table where he can delete the records using the user interface.

**For testing purpose, the login ID and password is “admin”**

****