CY702 Project –VLAN Setup Guidelines

Contents

This document includes Project Part I setup guidelines and mail client setup in the appendix (both are needed in part I), and Part 2 guidelines.

Project Part I

A virtual image has been created that mirrors as much as possible the target network. The image can be downloaded at the link given in the project description. This document provides the instructions to install the virtual image.

Installation and Configuration

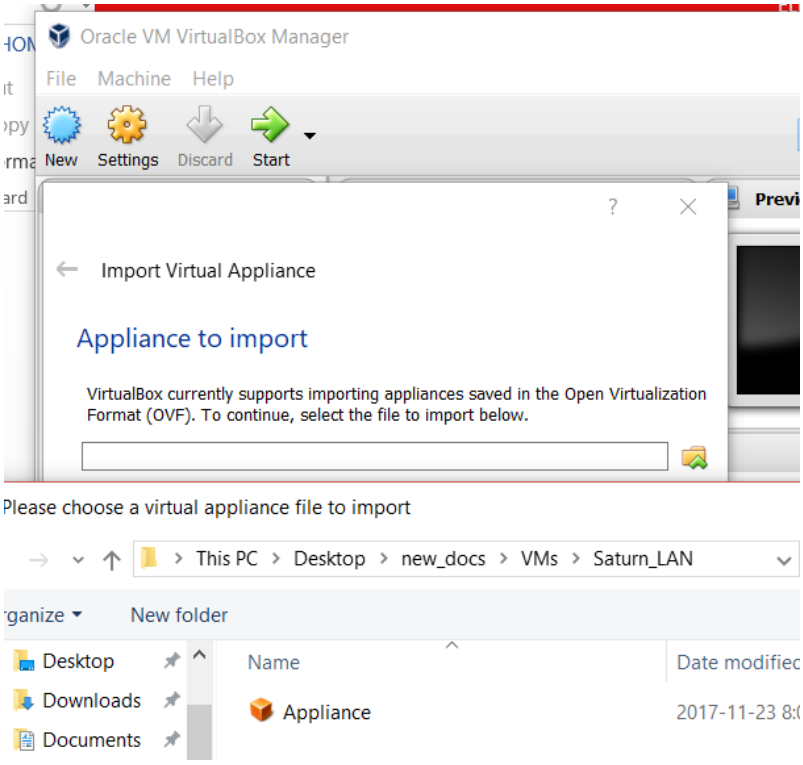
Target Network

The first step is to start up the virtual network and locate the LAN segment upon which it resides.

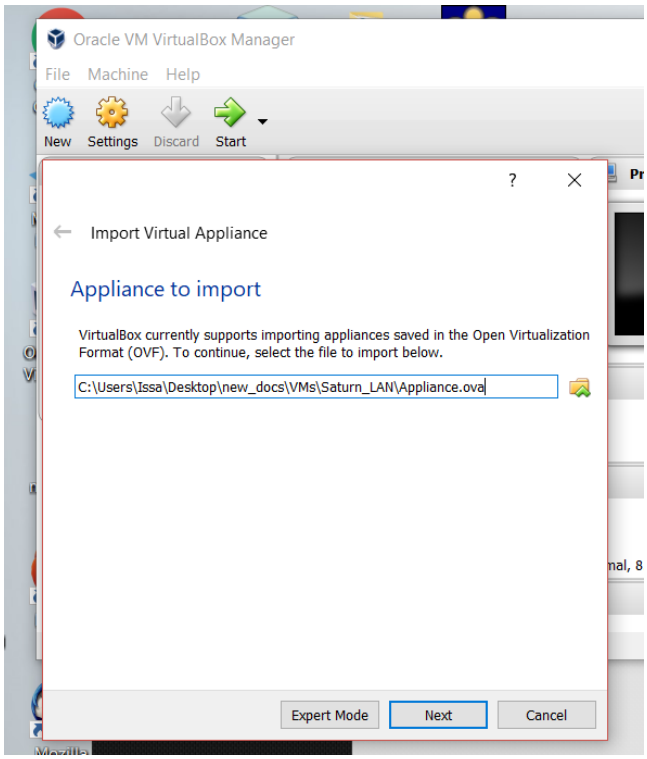
Download and uncompress the **Saturn_LAN.7z** file, which contains the virtual network. After uncompressing, you'll see 1 file named Appliance, which represents a virtual LAN (VLAN) containing 3 machines on the target network.

To install the image, start Virtualbox and select **File>Import Appliances**

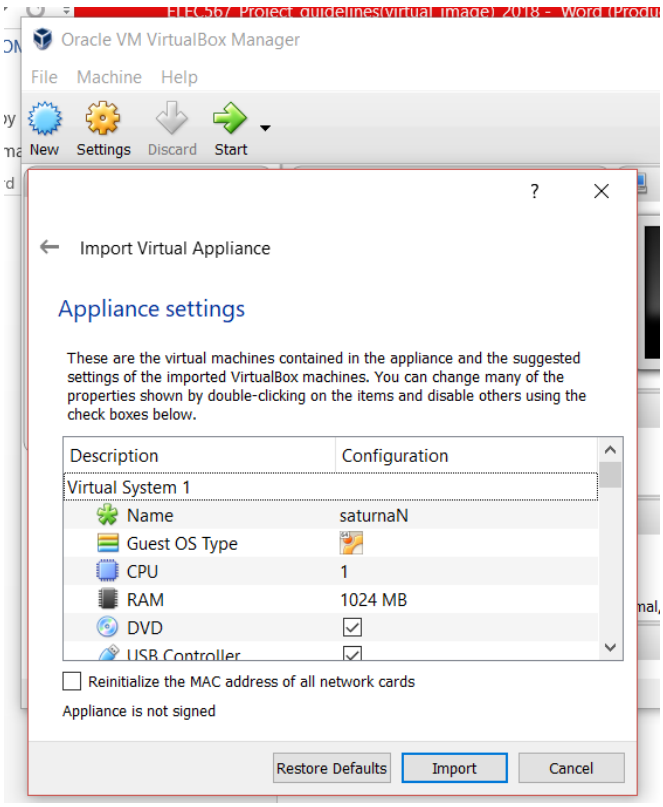
Browse to the uncrompressed directory, and select the file:



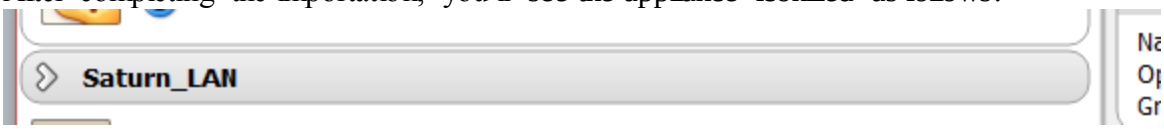
Click **Next**



Review and Keep the default. Click **Import** to finalize the importation.



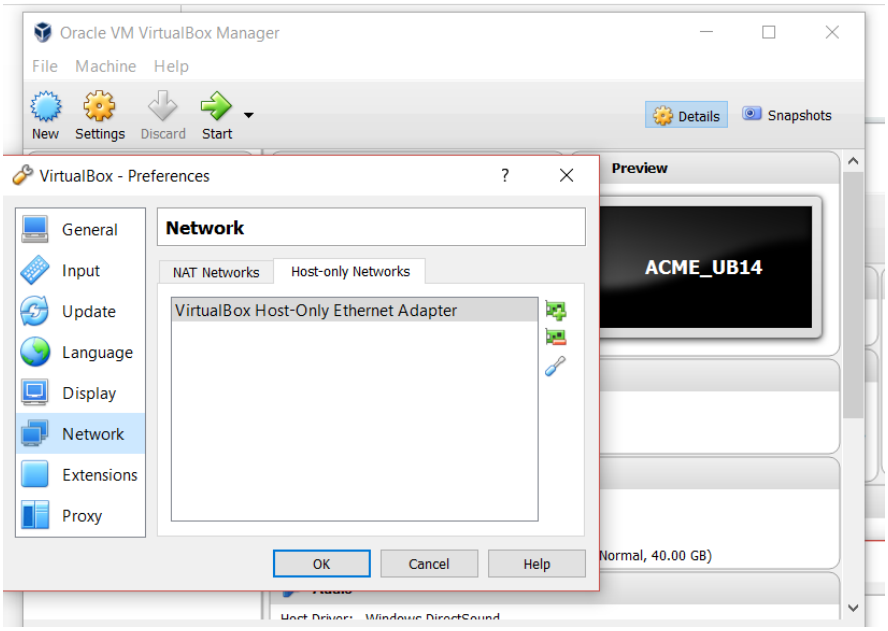
After completing the importation, you'll see the appliance iconized as follows:



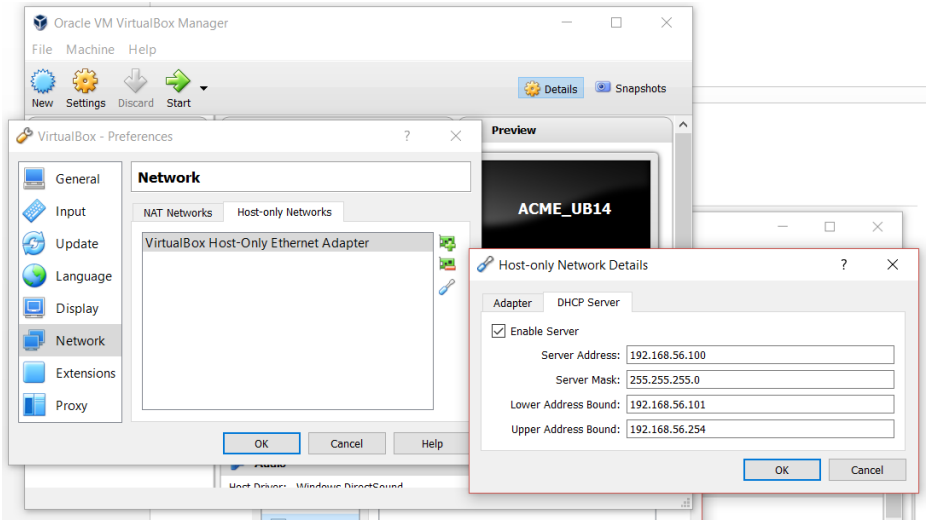
You can click on it to list the full network:

The next step is the network setup. Each of the machines are pre-configured to be attached on 2 network adapters: adapter 1 attached to **NAT** and adapter 2 attached to **Host-Only**. Host-only networking in VirtualBox allows the virtual machine to communicate with your hardware host, as well as any other virtual machines attached to the Host-only Adapter.

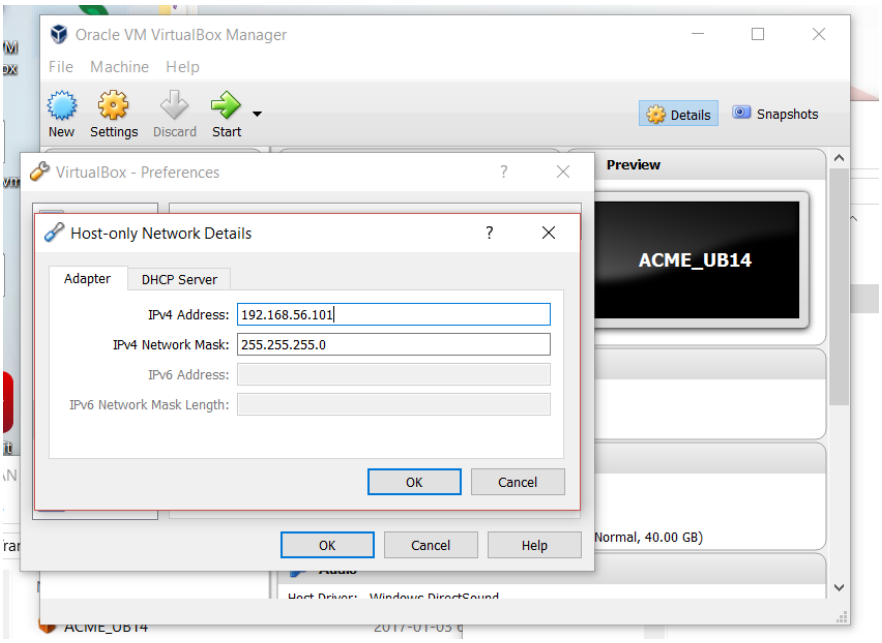
You can reuse an existing host adapter (if it is unused) or create a new one. To create a new host adapter, from the VirtualBox main screen, click on **File>Preferences**, then click on '**Network**' and then the '**Add**' icon (the green plus sign).



Next, you need to configure the adapter. Select the adapter, and click on the screwdriver icon on the right, this will display a configuration dialog. Update your configuration to match the one shown below:

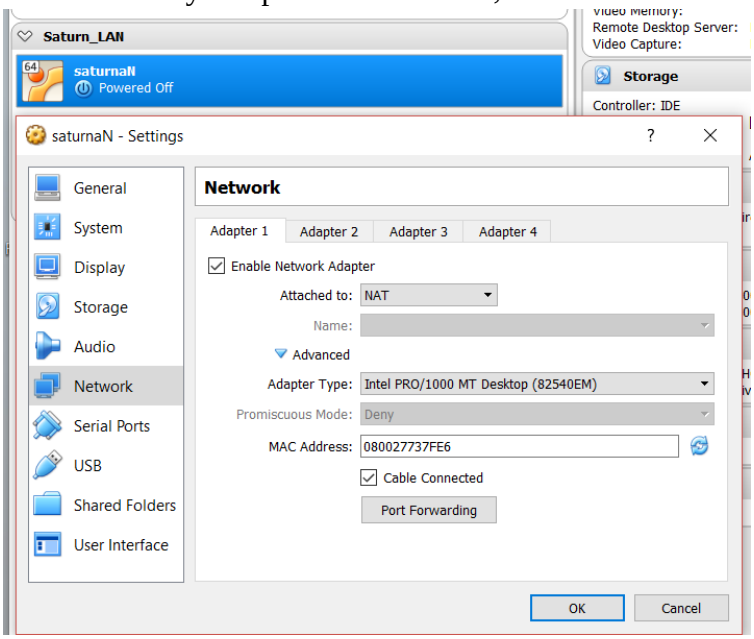


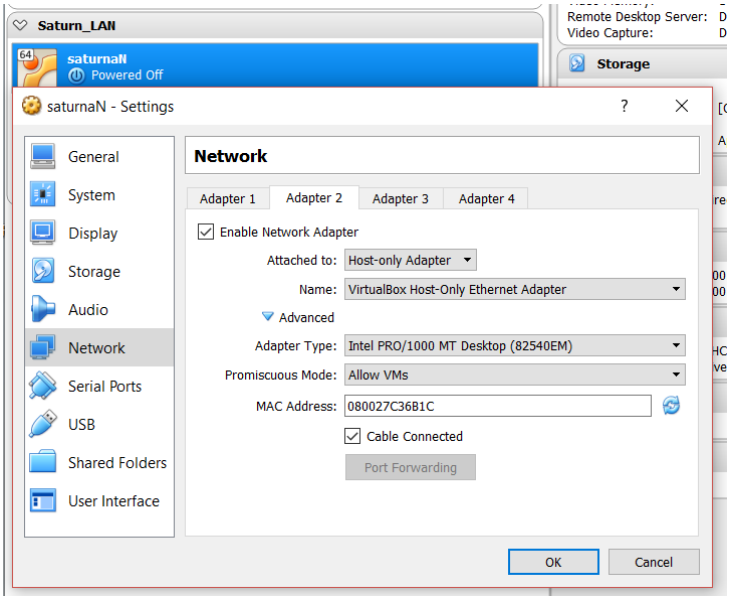
Check that the DHCP Server is enabled and configured as shown below.



As we can see from the above figure the IP address for this adapter is 192.168.56.101. This tells us the address space that we need to scan later to find our target network (i.e. 192.168.56.101-254 in the above configuration).

Now, you must check that the network configuration of each of the target machines are as expected. Select each of the machines (one at a time), and check that adapter 1 is attached to NAT and adapter 2 to the host-only adapter created earlier, as shown below.





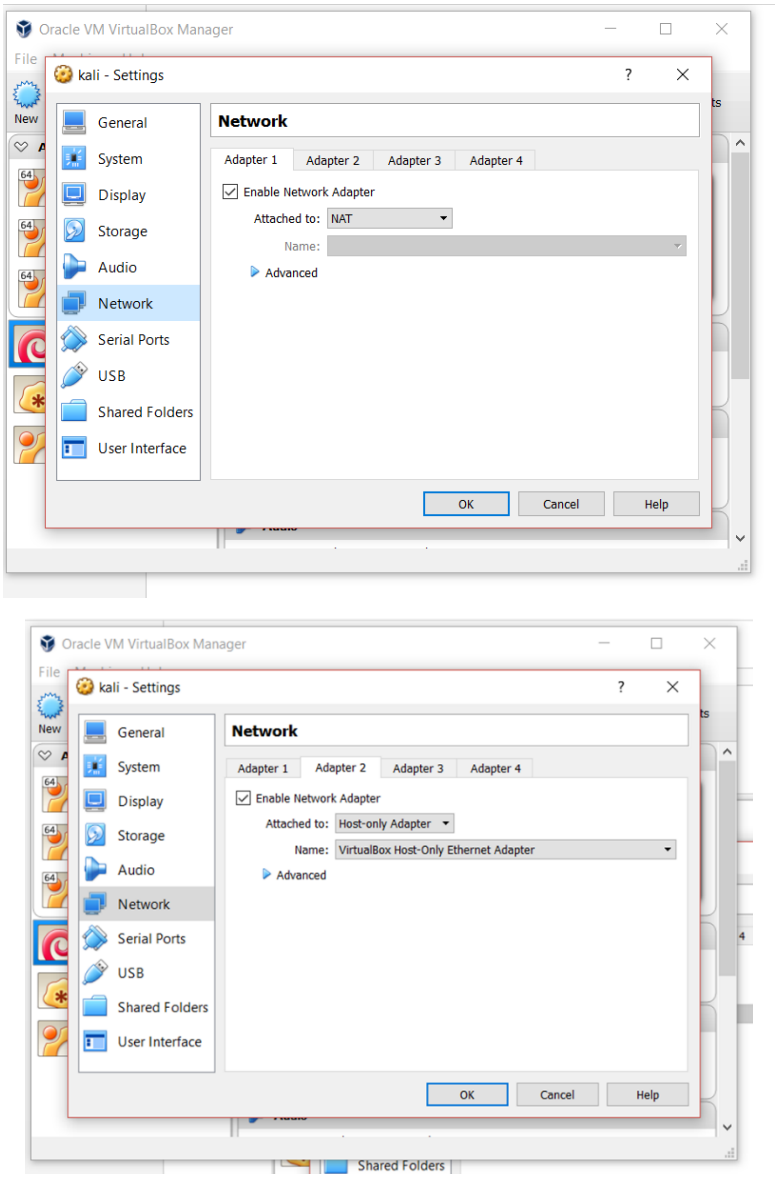
Make sure, by clicking on **Advanced**, that **Cable Connected** is selected. This must be done for both adapters. Make sure also that for machine SaturnaR, **Allow VMs** is selected under **Promiscuous mode** (at least for Adapter 2).

Make sure that you click on the **Ok** button to validate the settings. This must be done twice for each machine: once for adapter 1 (NAT) and another time for adapter 2 (Host-Only).

Attack Machine

The attack machine (i.e. your Kali VM) must be configured by assigning the same virtual networking settings as the target. This allows them to run on the same virtual LAN segment.

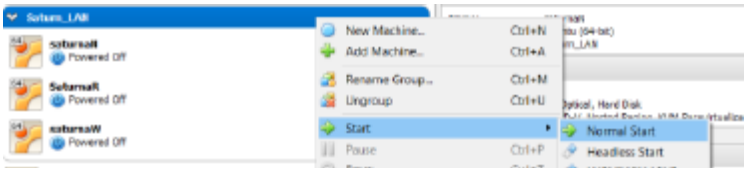
To do that, right click on the Kali VM machine from the VBOX manager and select settings. Go to the Network section and configure your network by attaching the machine to NAT (if it is not yet) and the same "Host-only Adapter" you created in the previous steps. Press the OK button. See the following figure:

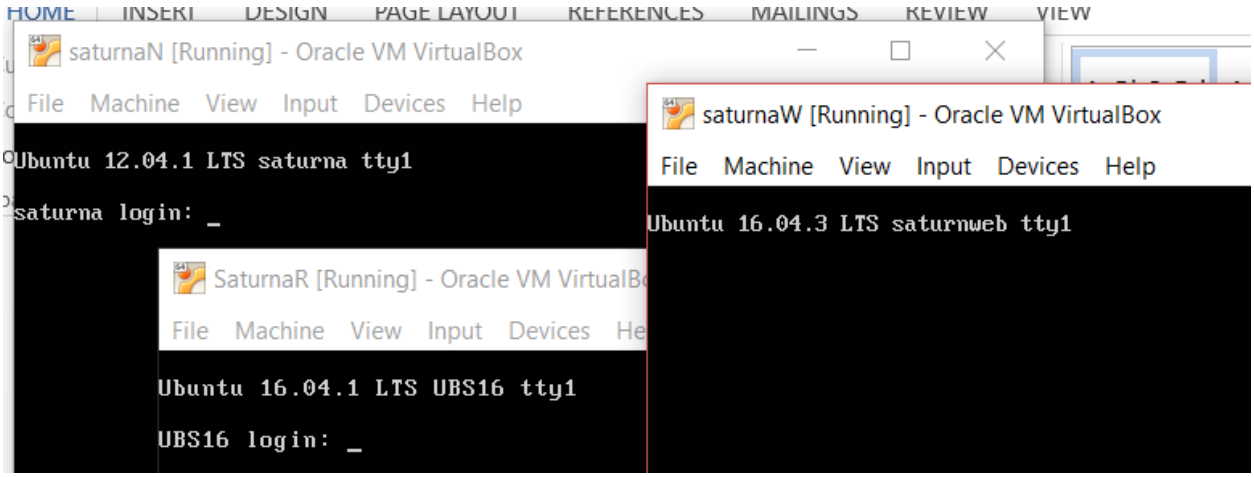


Like above, make sure that the **Cable Connected** option is selected for both adapters.

Starting Up

To perform the project, start the target machines and the attack machine in Kali. All machines should be up and running. You can start each machine individually, or as a group, by right-clicking on Saturn_LAN and **Start>Normal Start**.



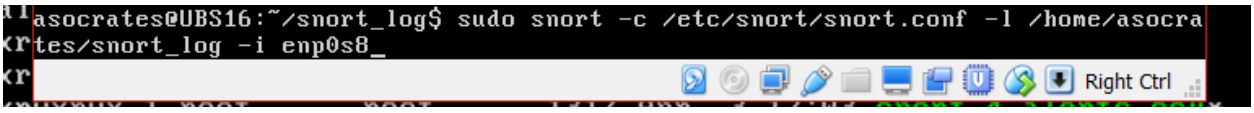


Important note/warning: it is assumed that the attacker does not have physical access to the target network. So all access should be performed (remotely) through the attack machine. Results obtained by analyzing directly the target machine are invalid, and will be assigned **zero**.

Project Part II

Snort is installed and configured on Machine SaturnaR. The credentials to access this machine will be provided after the deadline for Part 1.

In Part II (only) you can login directly in SaturnaR, and start snort as follows:



To get the alerts, go to the specified directory (you can create and specify above any directory to store the alerts). You can transfer the log file to Kali, and read it with a CSV reader such as libreoffice. To do that change the permissions for the log file as shown below:

```
asocrates@UBS16:~/snort_log$ ll
total 16
drwxrwxr-x 2 asocrates asocrates 4096 Apr  3 17:02 ./
drwxr-xr-x 6 asocrates asocrates 4096 Apr  3 15:49 ../
-rw-r--r-- 1 root      root      1312 Apr  3 17:03 snort_d_alerts.csv
-rw------- 1 root      root       936 Apr  3 17:03 snort.log.1491264172
asocrates@UBS16:~/snort_log$ sudo chmod 777 snort_d_alerts.csv
asocrates@UBS16:~/snort_log$ ll
total 16
drwxrwxr-x 2 asocrates asocrates 4096 Apr  3 17:02 ./
drwxr-xr-x 6 asocrates asocrates 4096 Apr  3 15:49 ../
-rwxrwxrwx 1 root      root      1312 Apr  3 17:03 snort_d_alerts.csv*
-rw------- 1 root      root       936 Apr  3 17:03 snort.log.1491264172
asocrates@UBS16:~/snort_log$ _
```

On Kali log in SaturnaR using SFTP, as follows (make sure you remember the directory from where you are logging in, as the file will be transferred to it; below, I'm doing it from the Desktop):

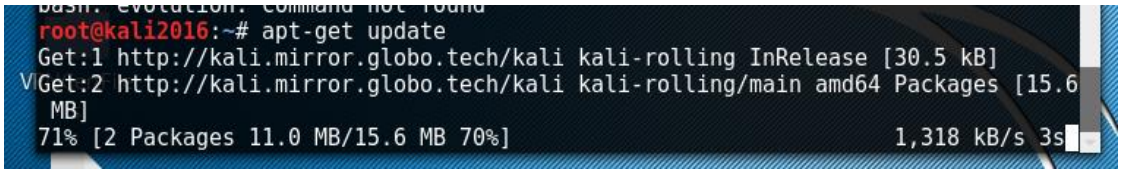
```
root@kali:~# cd Desktop
root@kali:~/Desktop# ls
mount-shared-folders.sh  myDict  project
root@kali:~/Desktop# sftp asocrates@192.168.56.101
asocrates@192.168.56.101's password:
Connected to 192.168.56.101.
sftp> ls
snort_log  snort_src
sftp> cd snort_log
sftp> ls
snort.log.1491264438  snort_d_alerts.csv
sftp> get snort_d_alerts.csv
Fetching /home/asocrates/snort_log/snort_d_alerts.csv to snort_d_alerts.csv
/home/asocrates/snort_log/snort_d_alerts.csv                  100%  982     1.1MB/s   00:00
sftp> bye
root@kali:~/Desktop# ls
mount-shared-folders.sh  myDict  project  snort_d_alerts.csv
```

As you can see, the file is on the Desktop; you can open it now.

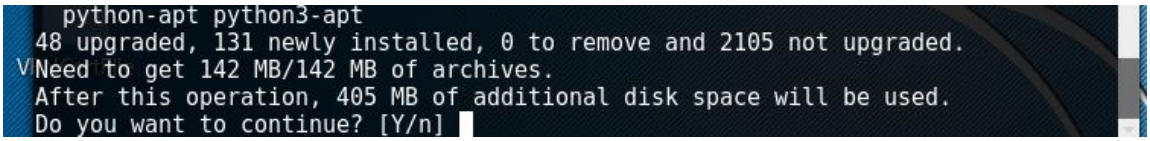
Appendix: Evolution Mail Client Setup

In Part I, you will need access to email messages. As suggested, you may use the Evolution Mail Client or any other mail client to read from valid accounts on the target network.

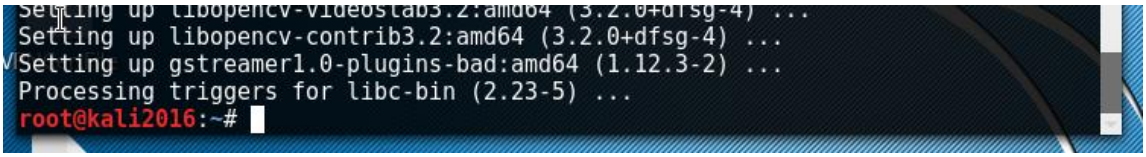
To install Evolution on Kali, open a command window, type apt-get update:



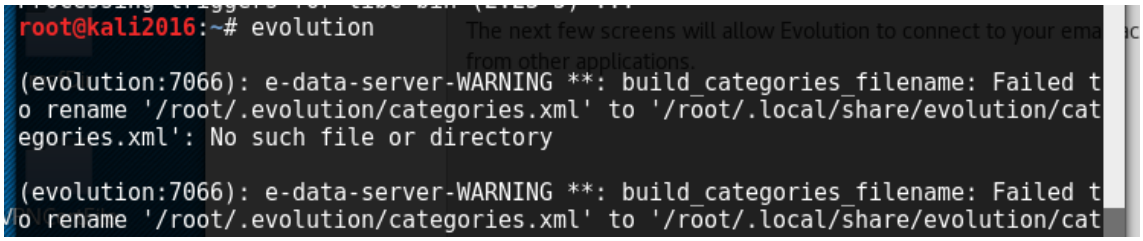
And type apt-get install evolution as follows:



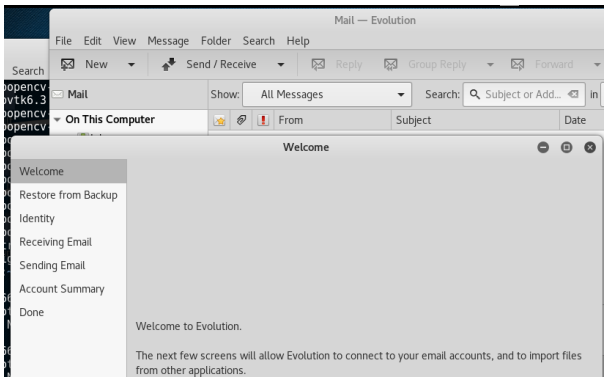
Type Y:



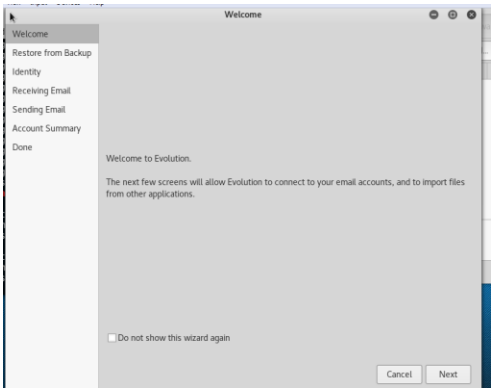
To start Evolution, type evolution as follows:



Evolution setup appears.



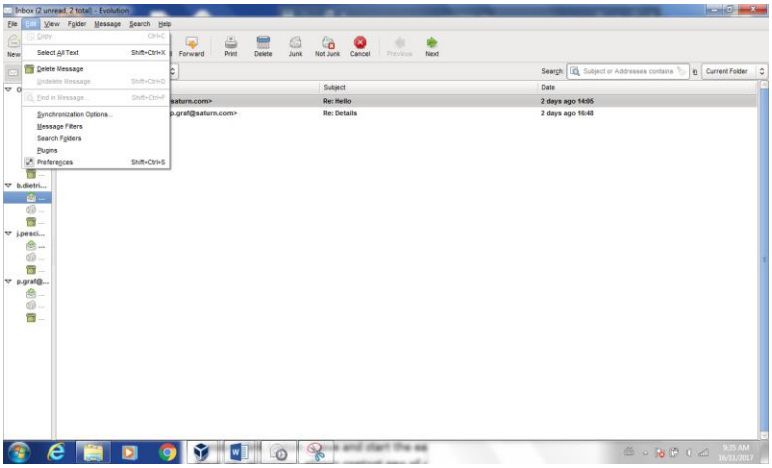
Click **Cancel** to close the welcome window.



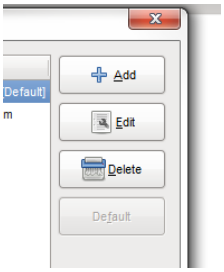
The guidelines to configure Evolution for the project are explained in the following.

The assumption at this stage is that you've successfully cracked the credentials of specific users on the target network, and would like now to read their emails. So you know the user email address and email account password, and will setup the mail client from the attack machine. (You can create as many email accounts as needed).

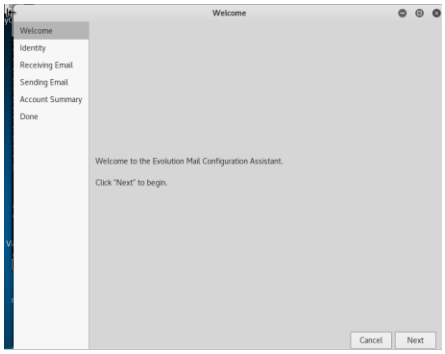
Use the main panel to create the individual email accounts. Click on menu **Edit>Preferences**



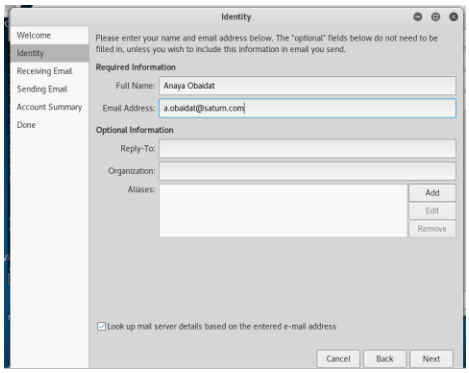
Click on **Add** button:



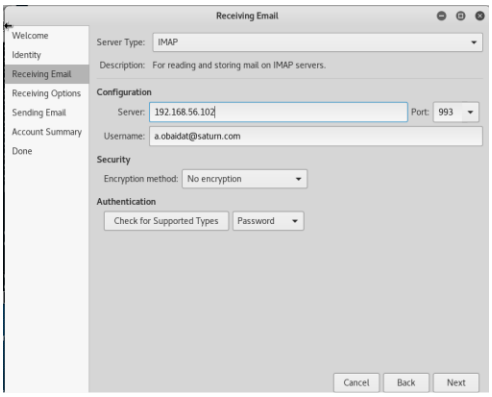
Click on **Next** button:



Enter e-mail account information as shown below (email address and name), and click **Next**:

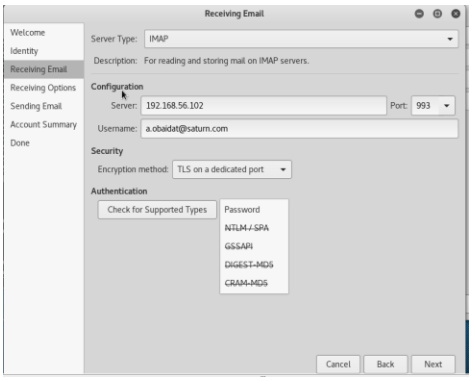


Enter email address, (target) mail server IP/Port (and keep everything else as shown):

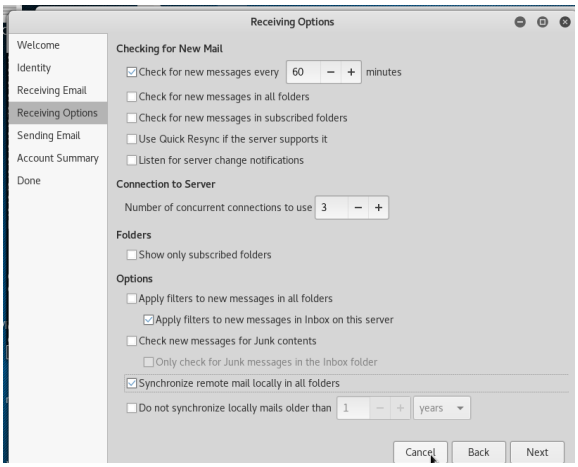


Select (under **Encryption method**) **TLS on a dedicated port** and then click **Check for Supported Types**:

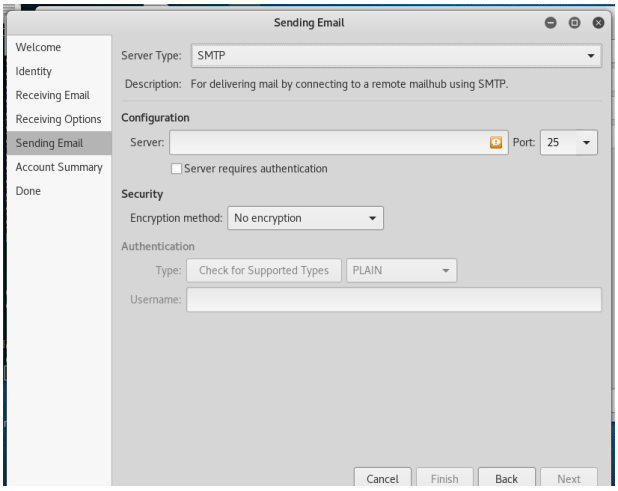
Click **Accept Permanently** (for the certificate). You should get something like the following for the **Authentication Type** (as listed in the drop-down):



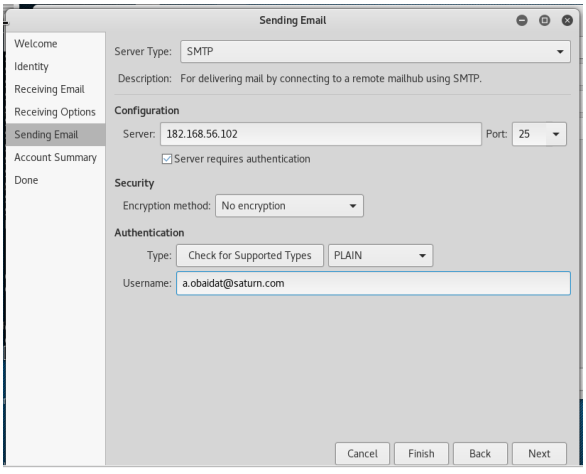
Click **Next**, select the options as follows:



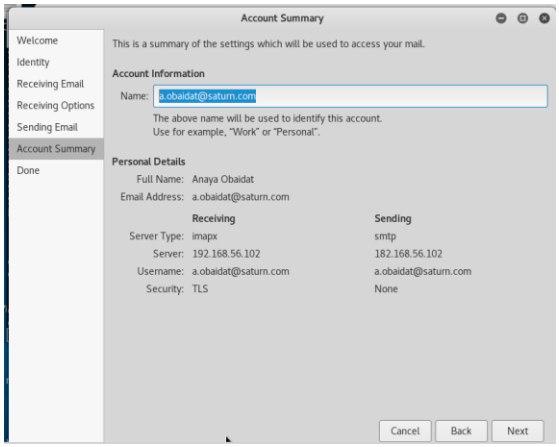
And Click **Next**. This will display the following window:



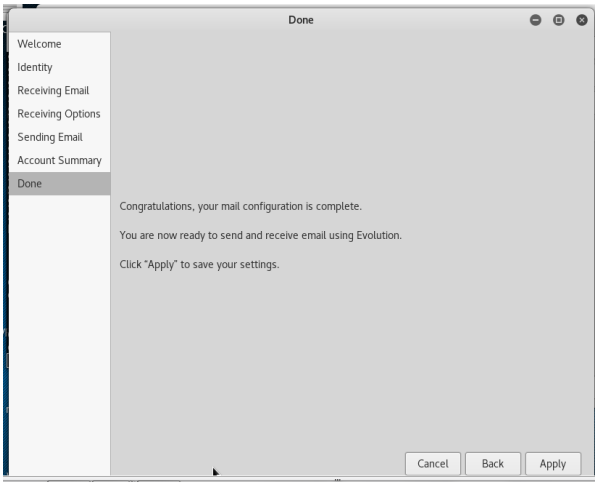
Enter the mail server address; check **Server requires authentication**; enter the email address as follows:



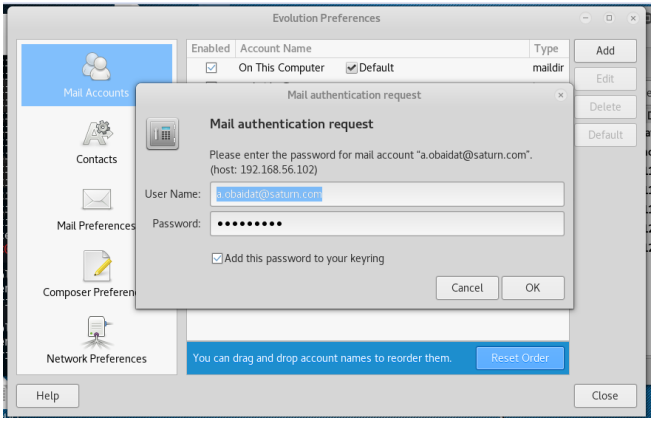
Click Next:



Click Next:



Click Apply:



Enter email account password and select **Add this password to your keyring** as shown above. Click **Ok**. Click **Close**. You can now test by sending emails between valid accounts on the target network.