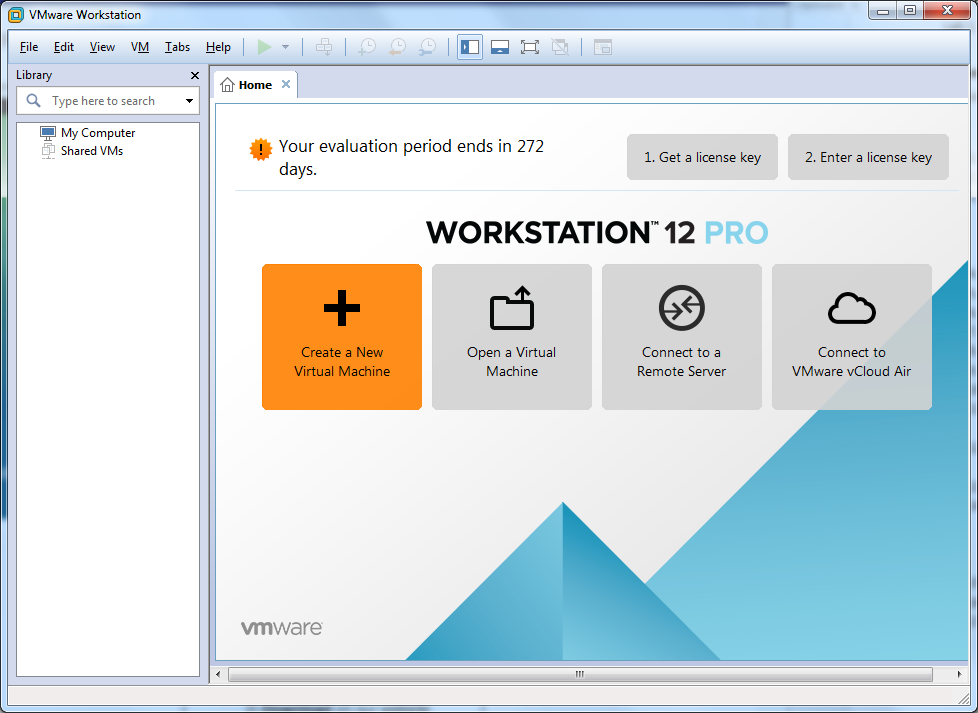
**Lab 1 – Kali and network scanning** Name \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

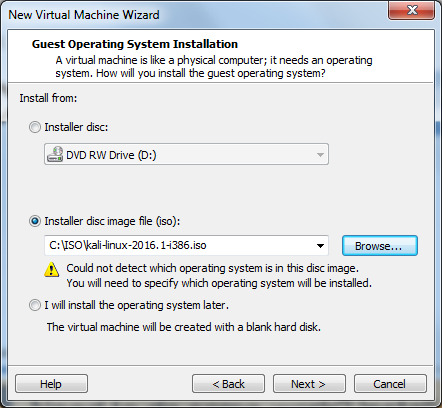
**Task 1 – Installing Kali**

In this task you will be installing a Kali virtual machine using VMWare workstation.

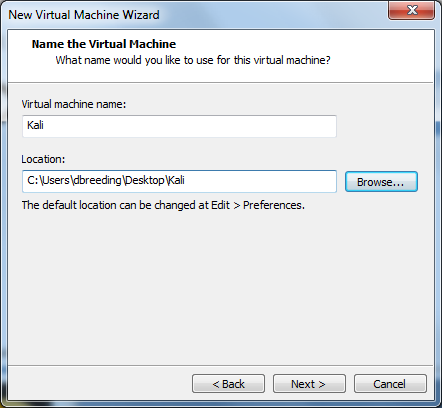
1. Start VMware Workstation



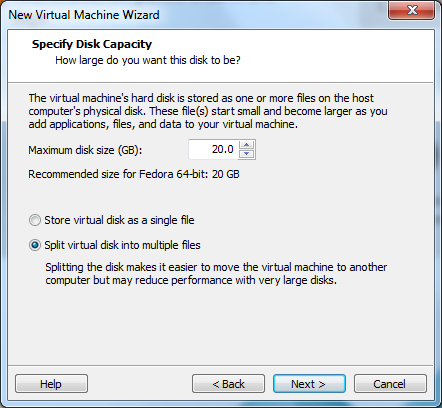
1. Click Create a New Virtual Machine. Choose Typical.
2. On the Guest Operating System Installation page, choose one of the following:
   1. Check Installer disc image file(iso): and click Browse to connect to Kali DVD ISO image.
3. Click Next.



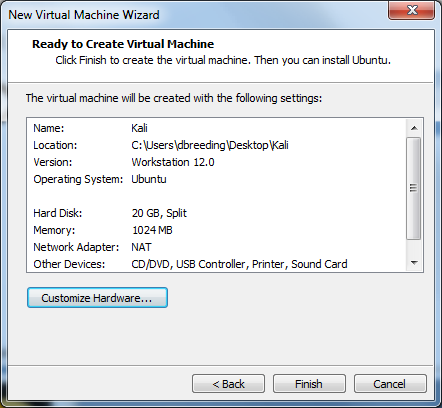
1. Name your Virtual Machine and place in your external drive or on the Desktop



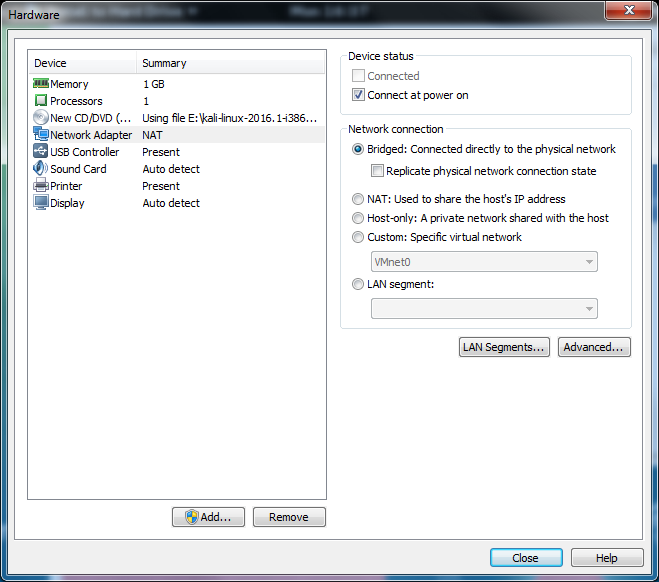
1. Specify your Disk Capacity at 20.0 GB



1. Click Customize hardware



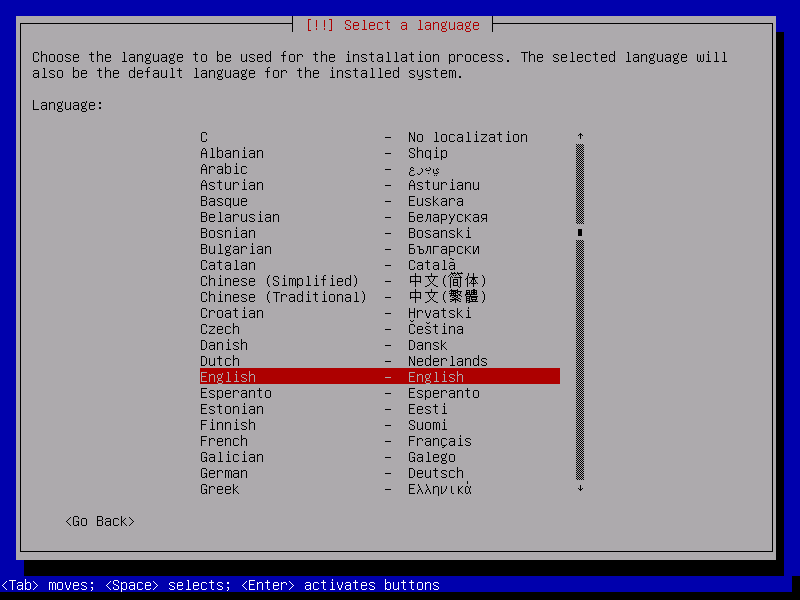
1. Click on Network adaptor and change it to Bridged



1. Finish and create your virtual machine
2. Boot your virtual machine
3. Kali Boot Option Menu – Select Install



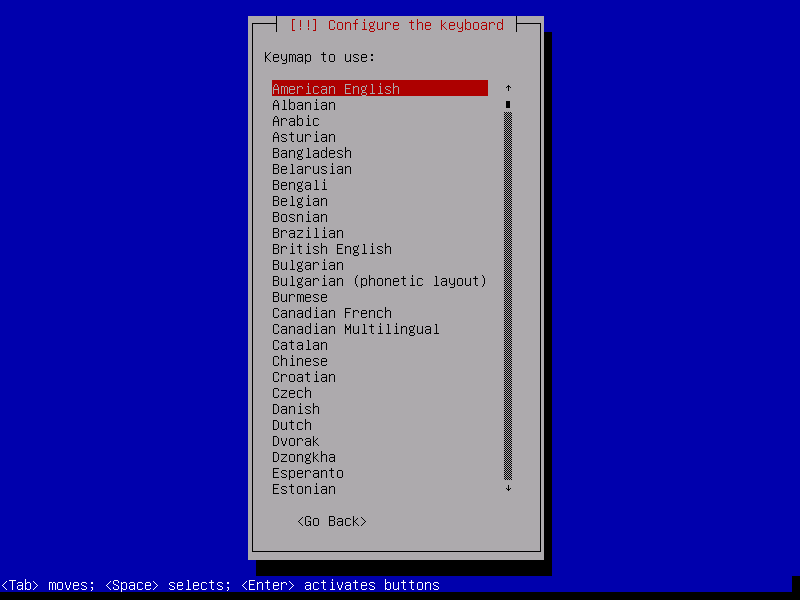
1. Select Language



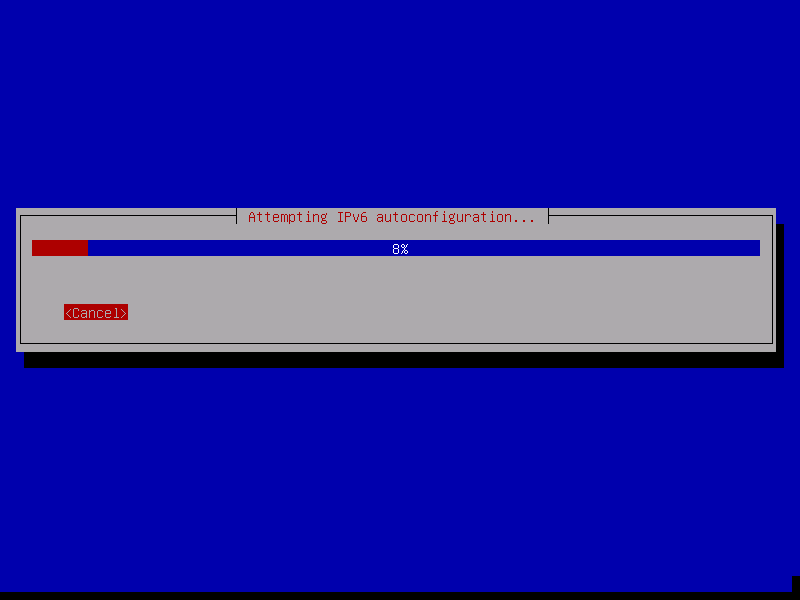
1. Select Location



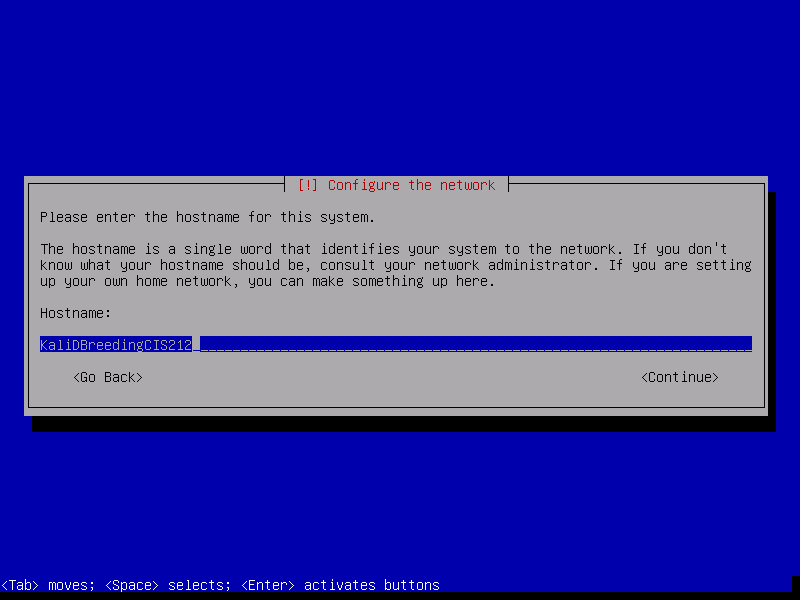
1. Configure Keyboard



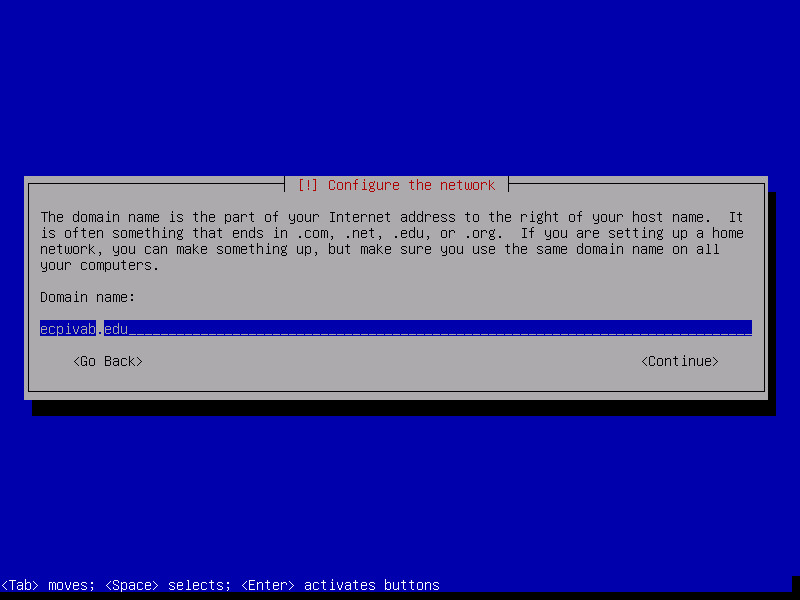
1. Kali does autoconfiguration



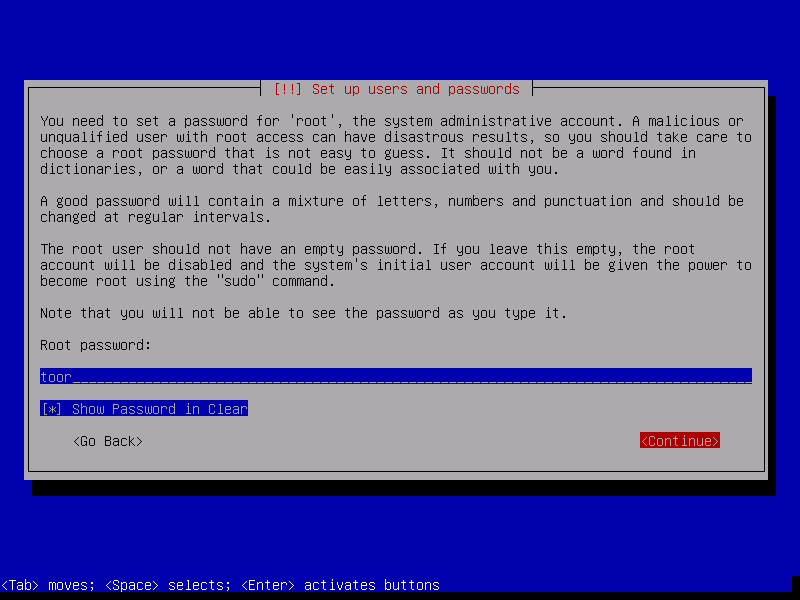
1. Select hostname – Kali<yourname>CIS212



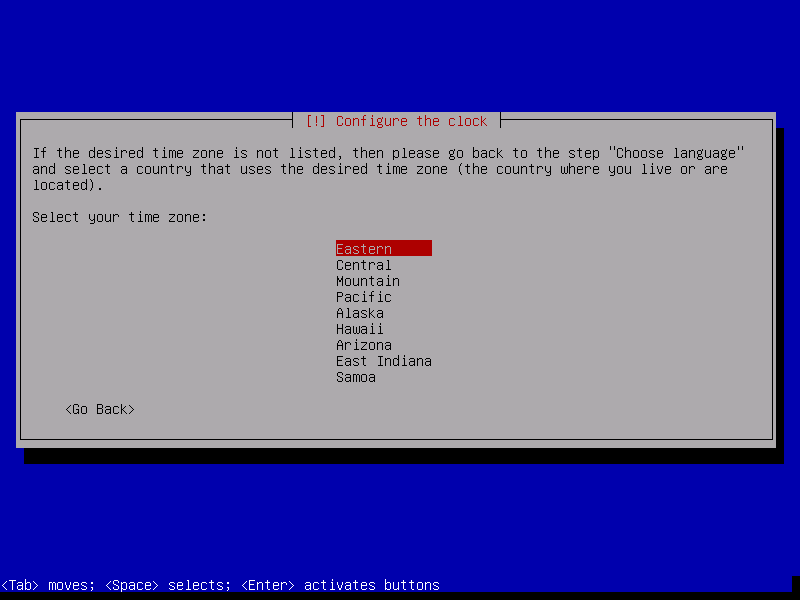
1. Select your domain name ecpivab.edu



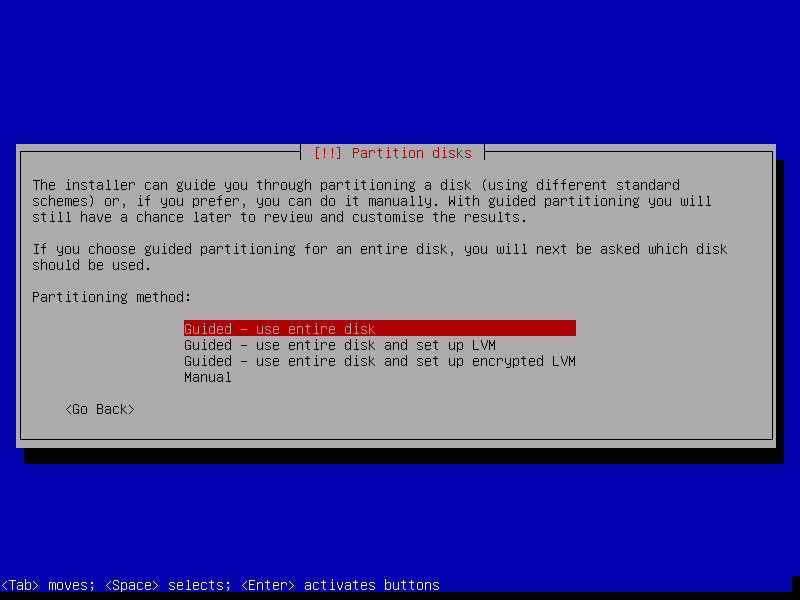
1. Set up your root password as *toor*



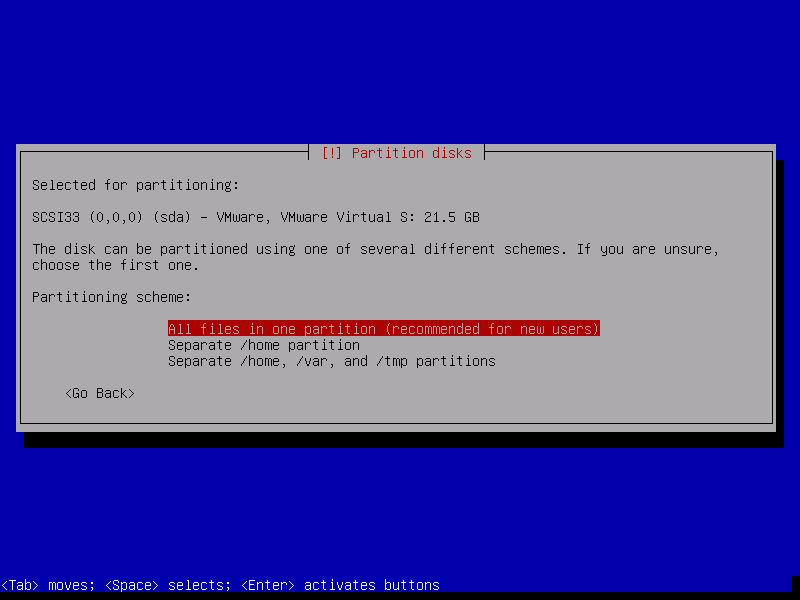
1. Configure the clock - Eastern



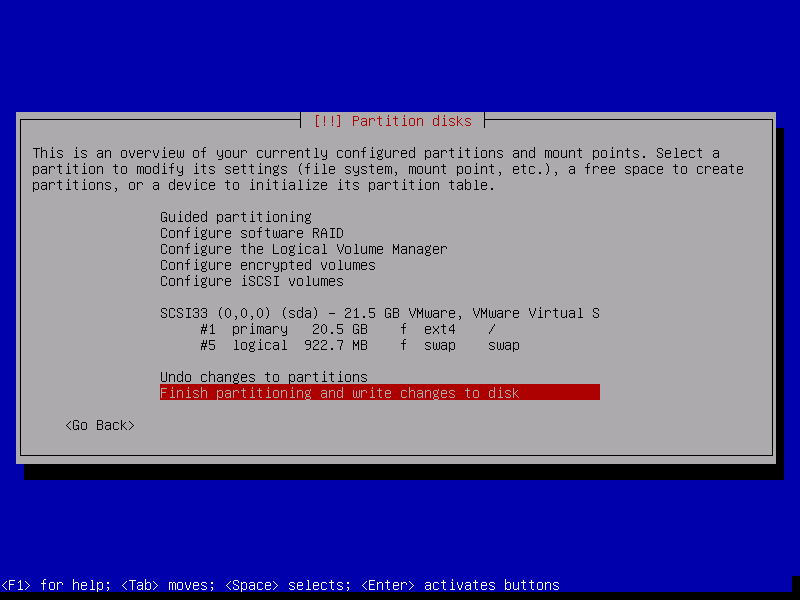
1. Partition disks – Use entire disk



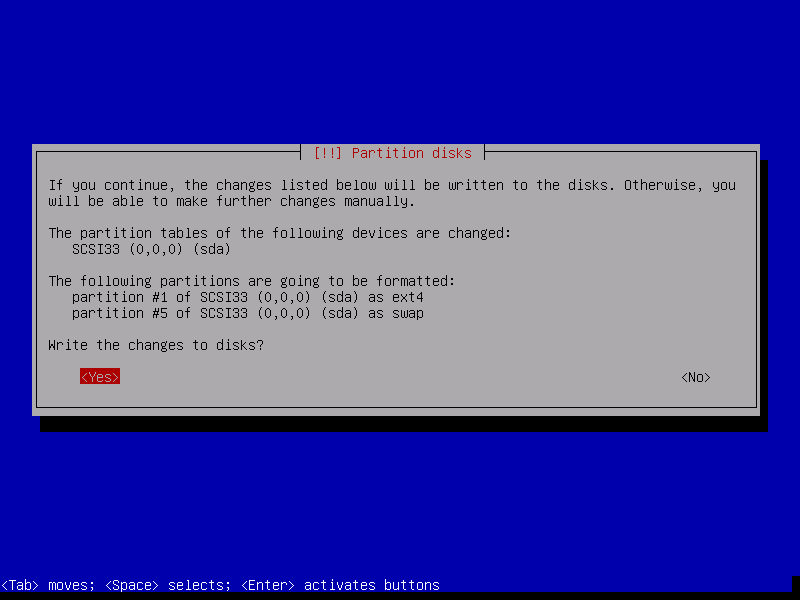
1. Partition disks – All files in one partition



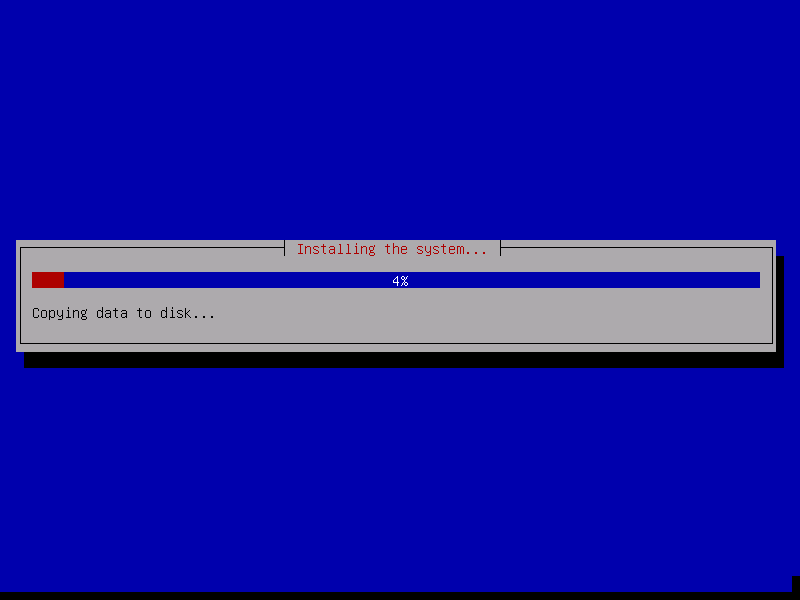
1. Finish partitioning disk



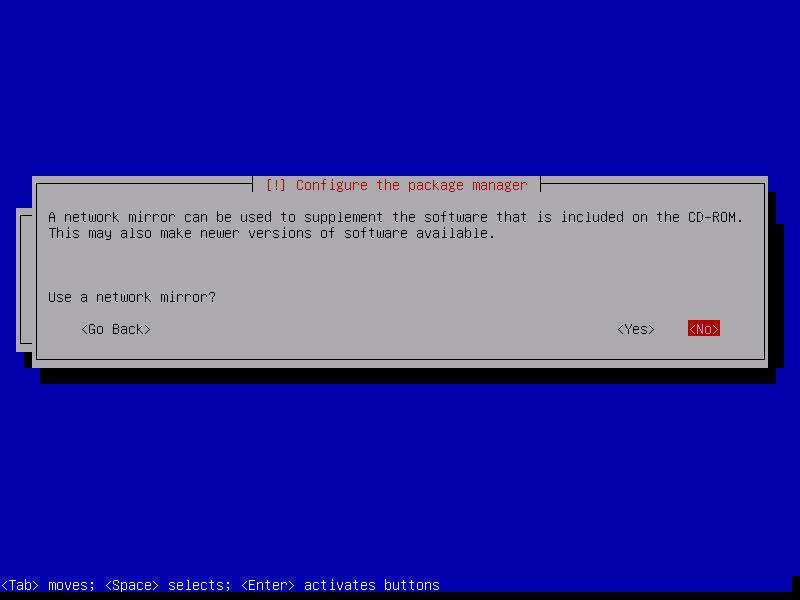
1. Write changes to disk



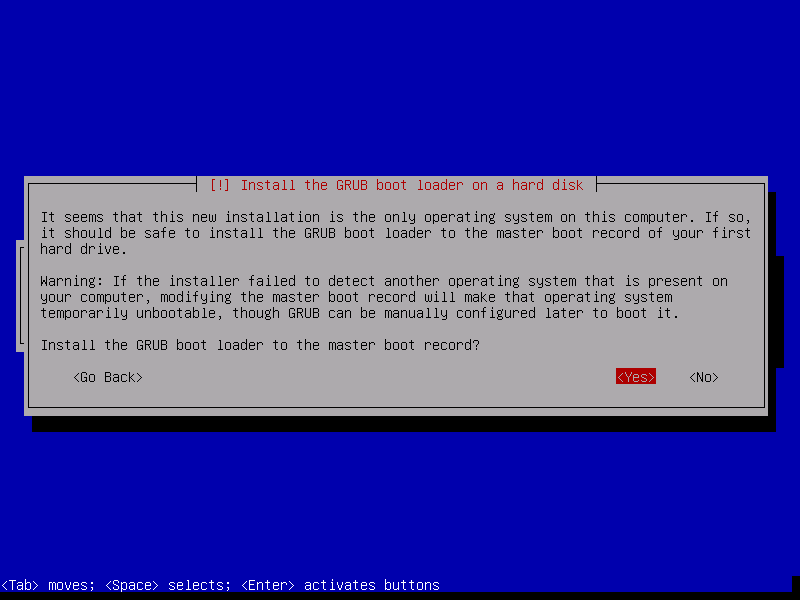
1. Installing the system



1. Configure Package manager – No



1. Install GRUB boot loader



1. Install boot loaded on a hard disk – /dev/sda



1. After your reboot go into VM and manage. Pull up a terminal and type *ifconfig*. What is your network address? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
2. Go back to your PC and pull up a command window. Type *ipconfig.* What is the network address for your PC? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
3. Attempt to ping from your PC to your virtual machine by typing *ping 10.XX.XX.X*
4. Attempt to ping your neighbor’s virtual machine. Did it work? Why or Why not.

Task 1 Deliverables:

Screenshot of your virtual machine

Screenshot of your ifconfig from your virtual machine

Screenshot of your ping from PC to virtual machine

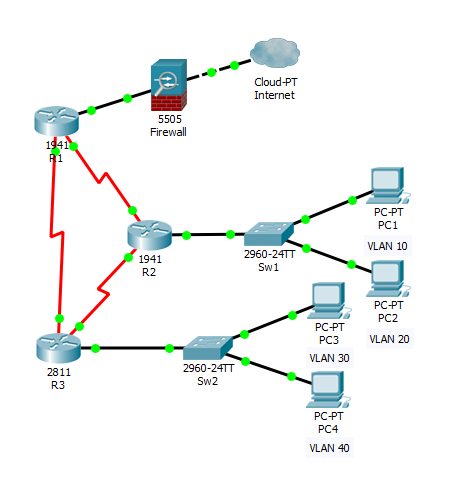
Screenshot of a ping from your virtual machine to your neighbor’s VM

Answer the questions 28, 29 and 31 about your virtual machine

**Task 2 – Network Reconnaissance**

One of the most important parts of Pen testing is information gathering. There are several ways to collect information about an unknown network and we will be setting up and collecting information in a few different ways.

Given the network below you will be doing a passive reconnaissance on the network.



Reconnaissance can be divided into two categories, active and passive. Active reconnaissance requires that you interact with the target computer system to gain information about it. Although this can be very useful and accurate, it risks detection. If you're detected doing reconnaissance on a system, the system admin may choose to block your IP address and you'll leave a trail to your subsequent activity.

If possible, we would prefer to gather the essential information without ever interacting with the system, thus leaving no trail to trace back to us. That's what passive reconnaissance is.

During passive reconnaissance you will be collecting data about a network without logging in or touching the system. What can you tell simply by observing the network above and how the network is wired together?

Give the results of your passive reconnaissance below.

Active Reconnaissance

You will now switch to active reconnaissance on the network using NMAP which is part of Kali Linux. To do this you will need to make sure you are connected with a good IP address prior to the instructor isolating the network. After the network is isolated you can continue your active reconnaissance.

## Step 1 - Open Nmap

Let's go to our Kali Linux, and open up nmap. To find it, go the Kali button at the bottom left of the screen to open up the initial menu options. Then, select **Kali** -> **Information Gathering**, and click on **nmap**.



## Step 1 – Finding the network

## The first thing you must do is find the network you are connected to. Open a terminal window and type *ifconfig* to find the IP address for the network.

## 

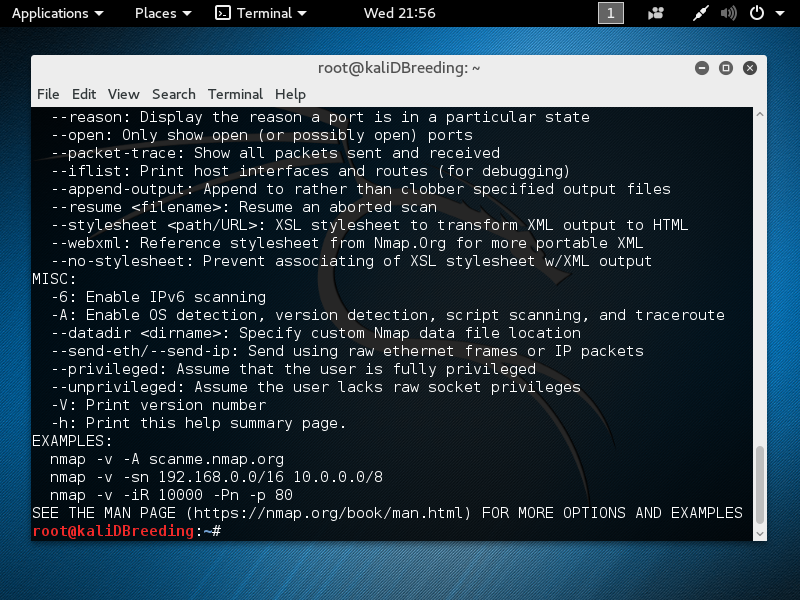
## Step 2 – Scanning the network

## Go to Applications -> Information Gathering -> netdiscover and open the program. You will now type netdiscover –r 10.XX.XX.0/24 (or whatever your network is). The system will then scan the network for other systems.

## 

## Step 2 - Using Nmap

When you select nmap, you'll open a screen that looks like the screenshot below.



Note that it opens a Linux terminal with the help screen for nmap. Whenever you want to see the help screen, you can simply type at the command prompt:

* **# nmap -h**

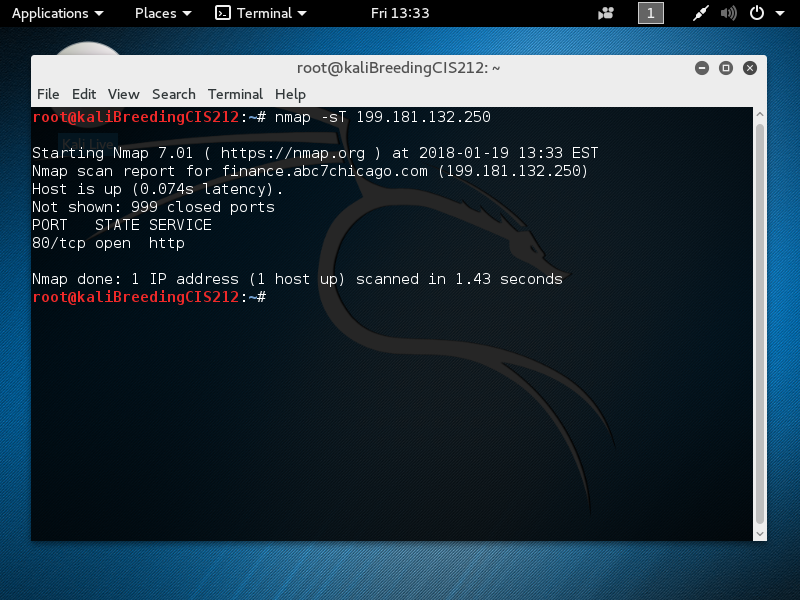
You can also get the manual for nmap by typing:

* **# man nmap**

Nmap is a delightful tool for gathering information on a network or site. For instance, if we want to gather information on espndeportes, we can type:

* **# nmap -sT 199.181.132.250**

We can see some of the output below.



This command shows the open ports on this system that are available to exploit by an attacker. Go through each of the other systems on the network and see which is most vulnerable to attack.

## Step 3 - Operating System Detection

Nmap is also capable of detecting and making a guess as to what the operating system is. Type:

* **# nmap -O 10.XX.XX.118**



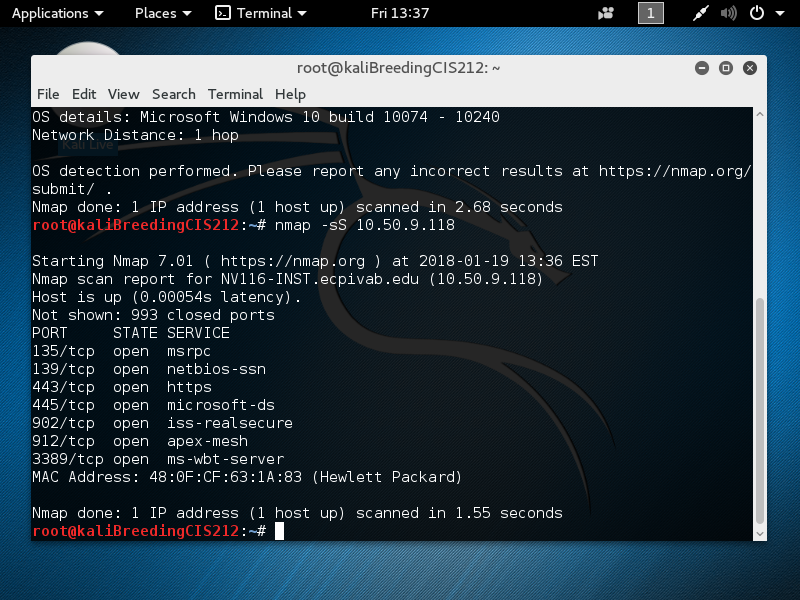
We can see from the screenshot above that NMAP discovered that this host was running Windows 10.

## Step 4 - Stealth Scan

The above scan by nmap is highly reliable, but its drawback is that it's also easily detectable. Nearly every system admin will know that you're scanning their network as it creates a full TCP connection, and this is logged with your IP address in the log files.

A more stealthy scan can be conducted using the -sS switch in nmap. This scan uses SYN flagged packets that do NOT create a connection on the target machine and therefore are not logged. This type of scan is slightly less reliable, but is much more stealthy. Type:

* **# nmap -sS 10.XX.XX.118**



As we can see in the screenshot above, it gave us the less results but without our activity being logged by the target system.

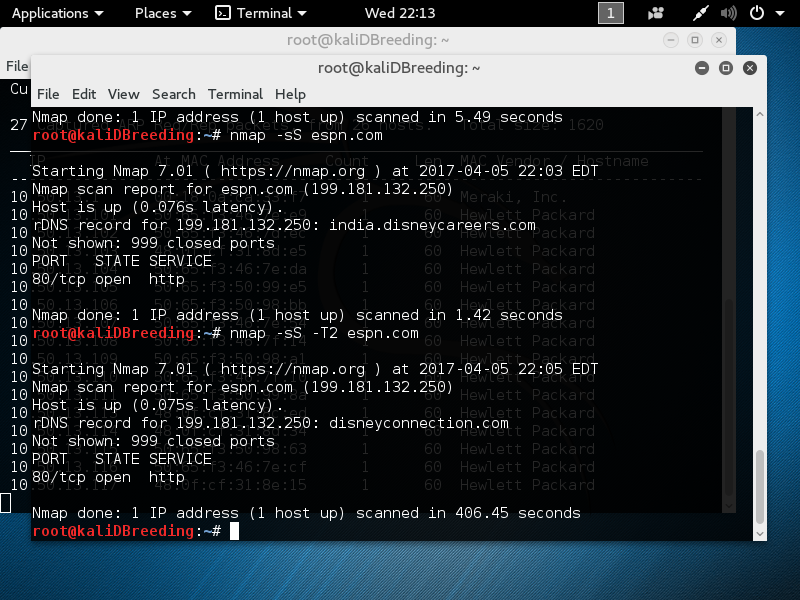
## Step 5 - Evading Intrusion Detection Systems

Most commercial servers and websites have intrusion detection systems (IDS) protecting them. These systems look for telltale signs of malicious activity, then alert the security administrator. Scans such as ours are easily detected by these systems and can set off an alert.

However, there are numerous ways to evade these IDSs, and we'll look at one here.

IDSs usually have a threshold setting. This means that if it sees numerous packets that appear to be scans, then it will alert the admin. To avoid detection, we can simply slow down our scan below this threshold. Nmap has numerous speed settings. Here we'll use the "sneaky" speed setting. Let's type:

* **# nmap -sS –T3 10.XX.XX.118**



The –T3 setting tells nmap to use the sneaky speed. This scan will take longer, but it is much more likely to go undetected by the IDS.

When you have collected all of the information for the network switch to a 2nd network and run the same results for that network.

Deliverables for Task 2

Screenshot of netdiscover

Screenshot of nmap help screen

Screenshot of information from ESPN.com

Screenshot of -sT for each PC on the network

Screenshot of -O for each PC on the network