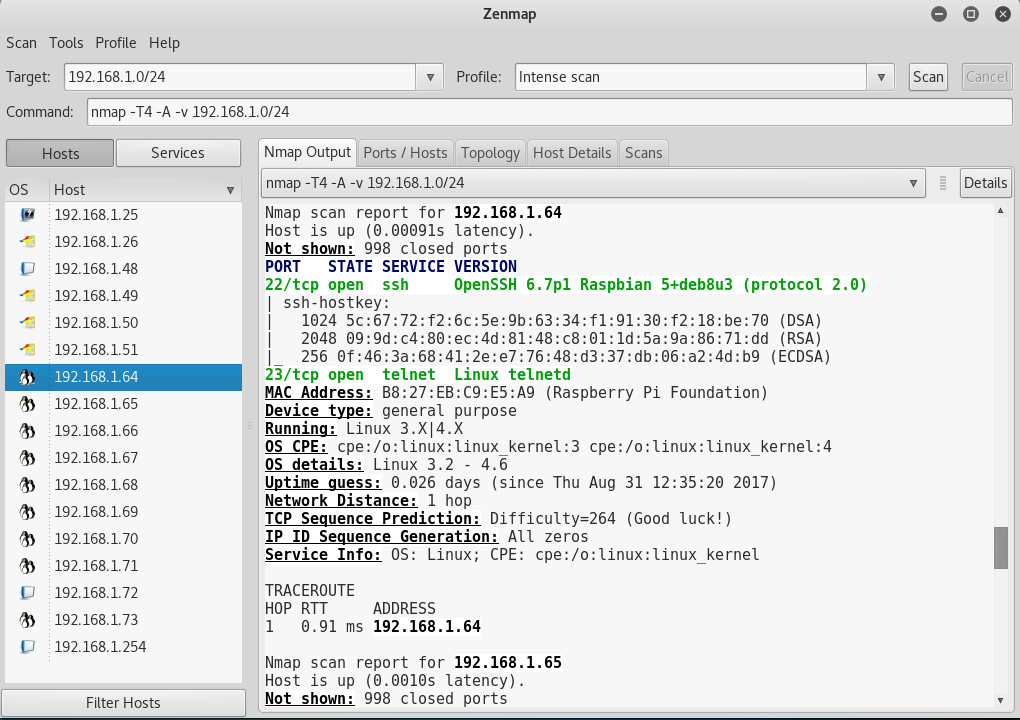
* From the host PC start VMware Workstation Pro
* Select the Kali2017.3 VM
  + The additional VMs we will use are stored in the D:\VMs folder
  + File – Open in VMware to find and open the VMX file to launch the VM
* Make sure the network settings for the VM are set to VMnet13 (the red cable)
* Take a snapshot of the VM (this is a good habit!)
* Power on the VM, then login with root and toor
* Connect the VM red cable to port 2/14 on your patch panel
  + Set kali IP address to 172.16.1.<POD+10>
  + Subnet 255.255.255.0
  + Default Gateway/Router 172.16.1.1
  + DNS 8.8.8.8

In Kali scan for open services on the victim

* 1. From the application menu – 01 – Information Gathering
  2. Choose zenmap
  3. Enter the IP address of 172.16.1.0/24 in the Target Box (this scans all possible in a range)
  4. Select Ping scan in the Profile, press scan.

The output will look something like this (IPs will change!): 

* Now move the red cable to one of the switches in your stack of CISCO kit (left side top half, right side bottom half)
* Unlock one of the other VMs (try win7-Vulnerable for example)
* Check its network settings are set to VMnet12 (the green cable)
  + For reference
  + **Red cable – vmnet13**
  + **Green cable – vmnet12**
  + **Blue cable – vmnet11**
* Plug the green cable into the same switch as your red cable
* Start up the VM and power on your cisco kit.
* Set the other VM to IP address such as 172.16.1.(POD+100)
* Check you can ping between the VMs, then try the zenmap scan again. Remember to change the target as required.