**Nmap**

In this tutorial we will be looking at a tool called Nmap, Nmap is a port scanning tool that comes installed on kali.

We will be scanning the network for a specific computer/server hosting a website on port 80(Http port).

A quick run though of some of the different types of packets sent by Nmap and ports.

SYN packets are sent to a port to see if it open.

ACK packet is sent back to say that the port is open and you can connect to what is behind it.

RST packet resets the connection for example SYN packet is sent, an ACK packet is sent back then the computer that sent the SYN packet will send a RST packet to reset the connection. This also happens if the port is not open no ACK packet is returned just a RST.

Sometimes no packet is returned this could be caused by a firewall that has been set up to ignore all packets on that port. This makes it hard to find certain servers as they don’t reply on the common ports such as 80 and 20(ftp)

Several years ago someone discovered a bug in the TCP protocol (SYN> <ACK > RST three way handshake) they found if you didn’t send the RST packet the server would keep the connection open and never close it. This allowed the person to fill all the connections of the server. This was a very basic DOS attack that was patched quickly as it could be done quite easily.

Lets open Nmap

Click applications, information gathering and then Nmap

Once in Nmap you can type nmap then a IP address to scan ports 1-1024 on that host. But we are going to use it to find a IP address that is hosting a website on port 80.

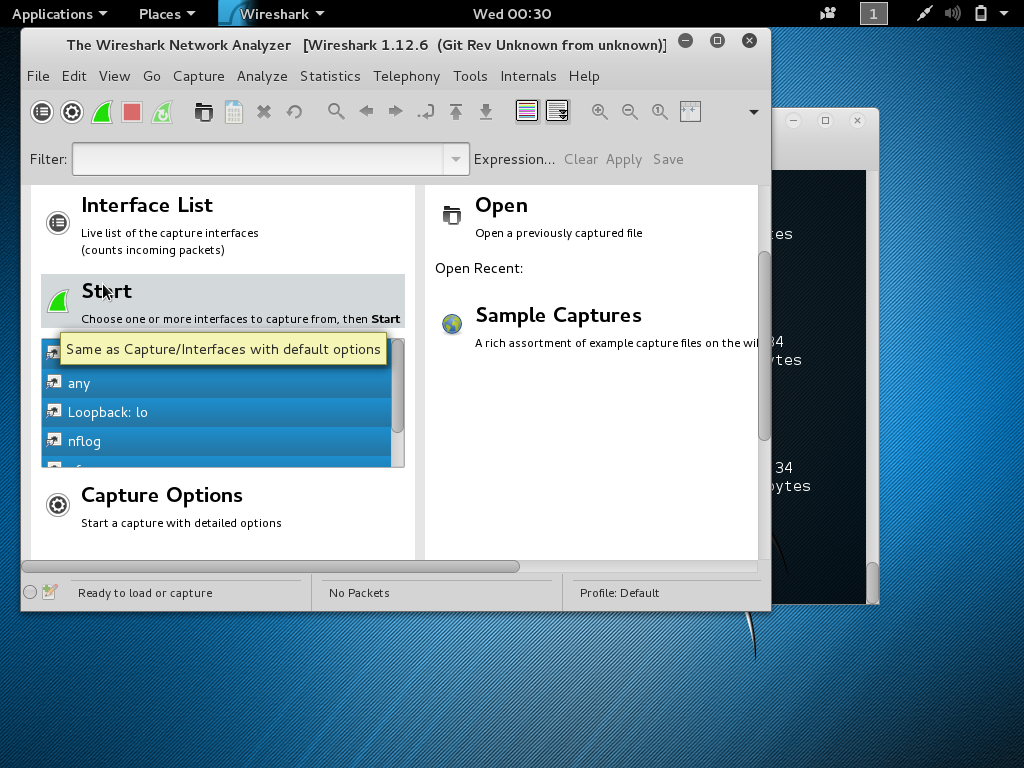
If you enter nmap –sP 10.0.2.1/24

This will scan all the hosts on the network there may be a lot in the lab so this may take some time. Once it has completed start at the top and enter each ip one by one starting with nmap then an ip address this will show you what ports are open on that host. Once you find one that has port 80, open your web browser (iceweasel) and enter the IP address into the address bar.

You should see a massive smiley face. If not you have entered the wrong IP or the server has been DDOSed we will look at that later.

If you go back to applications and go to sniffing & spoofing and select wireshark. Wireshark will let use see what nmap is doing and how powerful one command can be. Wireshark may give a few errors when its loading but it should be fine.

Under start it will show all of the network interfaces hold shift and select them all and press start as shown below.



If you go back to the terminal and ping the webserver IP you found earlier you should see in Wireshark ICMP packets and where they are going. If you go back to the web browser you should see TCP packets or http packets in Wireshark.

This is just a basic over view of how to scan a network and use Wireshark. If you would like to see the server with the smiley face be DDOSed just ask me. I would put the command in here but if a few people did it at once the network would probably crash and I’m guessing the university wouldn’t be too happy.

If the usb Wi-Fi dongles are free you should try and do the other tutorial on cracking a wireless password I only have five dongles so it may take a while to get to you =( (or amazon haven’t delivered them ….)