ITEC-2010 (Introduction to Cyber Security)
Lab 4: Scanning and Reconnaissance

Introduction
The key to successfully exploit or intrude a remote system is about the information you have. The first step for penetration is the scanning and reconnaissance. In this lab, you will learn how to use tools to scan and retrieve information from a targeting system. You will be using the nmap tool. We will use two Linux virtual machines: One is a Kali Linux with nmap installed; and the other one is intentionally vulnerable Linux. We will use the nmap to scan the vulnerable Linux for open ports.

Software Requirements
- The VMWare Software
- The Kali Linux, Penetration Testing Distribution
- Metasploitable2: Vulnerable Linux Platform
- nmap: the Network Mapper - Free Security Scanner

Starting the Lab 3 Virtual Machines
- We need to use two VMs for this lab: the Kali Linux and the Metasploitable2-Linux. First, select the Kali Linux and press Start up. Login into the Kali Linux with username root, and password.
- Select Metasploitable2-Linux, and press Start up. This is an intentionally vulnerable Linux VM that you will attack against.
- Log into the virtual machine with username and password.
- Create a new Nat Network on Vbox using File->Preferences->Network
- Assign each VM machine on a separate network adapter, so each machine will have its own IP address
- Switch to a different network adapter if kali Linux is not connected to the public net
- Using the following command to setup the GUI on Metasploitable 2:
  
  msfadmin@metasploitable:~$:sudo rm /tmp/.X0-lock
  msfadmin@metasploitable:~$:startx

Task 2: Finding the IP address of the target
For the purpose of this lab, it uses Metasploitable2-Linux as the attacking target.
- We need to find the host IP address of the target to launch a scanning.
- You can use the command “ifconfig” (ipconfig is the windows equivalent). This command allows you to find all the connected interfaces and network cards. Go to the Metasploitable2-Linux VM, and execute the following command $ ifconfig

Note: This is not a public IP but we can access it within the subset.
Task 1: Scanning the target using nmap

**nmap** ("Network Mapper") is an open source tool for network exploration and security auditing. Though it was designed to rapidly scan large networks, we use it for scanning the target host in this lab.

- Go to the Kali Linux, and open up a terminal by clicking the icon. Since nmap has been installed on the Kali Linux,
- Launch the scanning in the terminal by typing the following command: `$ nmap -T4 X.X.X.X`

**nmap** is the execution command; option `-T4` means faster execution; and `X.X.X.X` is the IP address of the target. We can see that there are many open ports and services on the target system including FTP, SSH, HTTP, and MySQL. These services may contain vulnerabilities that you can exploit.

**Deliverables:**
- Use nmap to scan the target and find the software version of the OS and the running services (list at least all of them).
- Write a report about your observation.

Happy Scanning!