ACIT 4630 – Lab 1 – Setup Kali Linux and Metasplotable 2

Notes:

You may optionally work with a partner for the labs in this course. Sign up for a Group for your set on the Learning Hub. Please choose wisely because: 1) you will work with the same partner for all labs and 2) both of you must be present in person for lab demos otherwise you will receiver zero on the lab.

Instructions:

Kali Linux is an advanced penetration testing Linux distribution that comes with lots of security tools preinstalled. Download a VM image for Kali Linux and set up a VM machine for it https://www.kali.org/get-kali/#kali-virtual-machines

- Make sure the VM's network is a NAT network
- Login to the VM. username: kali password: kali
- Explore different tools on Kali Linux.
- (Q1) How can you find this machine's IP?
- Find Metasploit (https://www.offensive-security.com/metasploit-unleashed/introduction/) and run it from the Applications menu. You should see msfconsole open. Almost all of your interaction with Metasploit will be through its many *modules,* which we explore more next week.

Metasploitable 2, is an intentionally vulnerable Ubuntu (64-bit) Linux virtual machine that is designed for testing common vulnerabilities. Download a VM image for metasploitable 2 and set up a VM machine for it https://sourceforge.net/projects/metasploitable/

- Make sure the VM's network is the same NAT network as Kali VM's
- Login to the VM. username: msfadmin, password: msfadmin
- (Q2) How can you find this machine's IP?
    - Note: If you're getting the same IP as the Kali Linux machine you need to change the network to a NAT network
- (Q3) Get yourself familiar with nmap command and its different options. How can you find this machine's **OS** as well as the **services** and their software **versions** running on open **ports** on this machine from your Kali VM?
    - nmap-cheatsheet.jpg nmap-cheatsheet - ACIT-4630-0 - Info Assurance and Security (x-list 202410) (bcit.ca)
    - An Nmap refresher Scan networks with Nmap (linkedin.com)
    - https://nmap.org/book/man.html
    - Security Testing: Nmap Security Scanning Running and interpreting a simple Nmap scan (linkedin.com)

    - Hint: If you cannot see any port open on this machine from the Kali machine double-check the NAT network
- (Q4) What's the use case when we need to use -Pn probing option with nmap?
    - Hint: try `nmap scan2.certmike.com`
        - The server is live on the internet, and ready for you to probe even though running above command might tell you differently.

Prep for Lab 2:

Please run following commands (with sudo) on your Kali VM before the Week 2 class

```
apt-get update

apt-get dist-upgrade

apt-get install openvas

gvm-setup (This command might be mentioned as openvas-setup in older resources. It needs to be run only the first time - and it will take a while. Take a note of the password for admin user when this is done)
```

Submission For Lab 1:

- Demonstrate your running VMs above to your instructor.
- Submit screenshots of your running VMs and answers to the questions in the lab to the Lab 1 dropbox on the Learning Hub.

This lab is due at the beginning of the Week 2 class and is worth a maximum of 10 marks.