20 March 2017

I) Notes:

1) Events:

   a) ACM and Cyber Security Club Game Night: This Friday, 24 March 2017 from 6:00pm until 6:00am

2) Useful Links:

   a) For Downloading Virtual Box:
      - https://www.virtualbox.org/wiki/Downloads

   b) For Downloading Kali Linux (What You Would Use to Attack Metasploitable):
      - https://www.kali.org/

   c) For Downloading Metasploitable VM (The Vulnerable Virtual Machnine):
      - https://information.rapid7.com/metasploitable-download.html

   d) For Running Tutorial with Metasploit:
      - https://www.offensive-security.com/metasploit-unleashed/

   e) Other Useful Links:
      - http://mountrouidoux.people.cofc.edu/CSIS490/links.html

   f) Nessus (Vulnerability Scanner):
      - https://uwnthesis.wordpress.com/2013/07/31/kali-how-to-install-nessus-on-kali/

3) Connecting Two Virtual Machines:

   a) Metasploitable Virtual Machine – A framework virtual machine for testing exploits and vulnerabilities; Made to be vulnerable

   b) You should try to set up two virtual machine (One Kali Linux, One Metasploitable)

   c) In order to connect two virtual machines, open up their settings, select the “Network” tab, and switch the “Attach To:” field “Internal Network”

   d) Now, after restarting both of them, they should both be on the same network
      - This will make it so that they cannot connect to the Internet again
      - If you want them to reconnect to the Internet, you will have to change the same “Attach To:” field back to “Bridged Adapter” and restart them

   e) After they have been restarted, you should open the terminal and type ifconfig in order to see the current IP Addresses of the machines

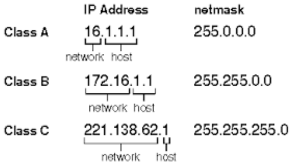
   f) Chances are, on the first line under eth0, you will see something that looks like ether XX: XX: XX: XX: XX: XX – this is not what you want

   g) In order to change this, you should type in the terminal sudo ifconfig eth0 10.10.0.1

   h) This will assign eth0 the IP Address 10.10.0.1

   i) However, you still need to assign a netmask

   j) To do this, type sudo ifconfig eth0 netmask 255.255.0.0:
      - This means that machines in this “network” will all begin with the same three numbers – in this case 10.10.0. but they can end with anything between 0 and 255
      - You want something to look like Class B below:



k) On the second machine, you will do the exact same thing, but will use a different number at the end – maybe have an IP like 10.10.0.2

l) However, make sure to keep the same netmask (255.255.0.0)

m) To ensure that the two are on the same network as each other, you can ping from one machine to the other.

- ping 10.10.0.2 is what you would run on your 10.10.0.1 machine to make sure it can talk to your 10.10.0.2 machine
- ping 10.10.0.1 is what you would run on your 10.10.0.2 machine to make sure it can talk with your 10.10.0.1 machine
- This sends an ARP request that essentially says, “Who has IP 10.10.0.$X$?”
- 10.10.0.$X$ responds by saying, “That’s me.”

n) On your Kali machine, you can run nmap to find out information about the Metasploitable machine

- The command nmap gives information about other machines on the network

o) MAC Address – Hardware address burned into the device you are using; Unique; Address by which things communicate; RARELY Changes

p) IP Addresses – Virtual and can be manually assigned; Can change often

q) How Packets Travel:

- Imagine you want to fly from Charleston to Seattle
- Airports would be like “Routers”
- Airplanes are like “Ethernet Frames”
- Your luggage is like “Packets”
- So, the luggage (packets) get from Charleston to Seattle, but by coming in contact with DIFFERENT routers and by being carried by DIFFERENT ethernet frames

4) Using Nessus:

a) First, use the link at the beginning to install Nessus

b) Type in http://127.0.0.1:8834

c) Login, go to “Scan Templates” and then “+ New Scan”

d) There, type in the eth0 IP of the Metasploitable machine and click “Run Scan”

5) Random:

a) The command netsat -tulpn tells you what ports are opend and what they are being used for

b) The command ps -ef shows you all of the system’s current processes