# Cyber Defense Organization

Metasploit Workshop - Ben Olm - 06/13/2020

**Setting up VM's**

What is required?

a. Kali Linux Virtual Machine (Link Here)
    i. Default credentials are root/toor
b. Metasploitable 2 Download (Link Here)
    i. When creating a new VM in virtualbox (https://www.virtualbox.org/) choose "Use an existing virtual hard disk file" and select the Virtual Machine Disk file in Metasploitable download to set up this box. Password and username is listed above the login terminal.
c. Creating a Network. (In Virtualbox) File>Preferences>Network>Add New Network (Right Click to rename).
d. Right click on each VM and click Settings>Network>Attached to: NAT Network> Name: "Network/Whatever you named it".

**Start / Recon**

1. Start both VM's at the same time (Make sure you allocate enough resources to them).
2. Login into kali using root/toor. Login to the Metasploitable box using msfadmin/msfadmin.
3. Type '*ifconfig'* into both terminals, make sure to note their seperate ip addresses as you will use them soon. **THIS WILL BE THE ONLY COMMAND YOU RUN ON YOUR METASPLOITABLE BOX. The rest of the commands will be done on your Kali box.**
4. The first thing we will do is initiate a nmap ping sweep.
    a. Nmap -sn 10.0.2.0/24 (Use the ip of the metasploit box that you have created but still use the .0/24 ending).
5. Here you can see the ip address of your Metasploit VM.
6. Next will be another NMAP scan showing all the ports that are left open (intentionally) on the metasploit Virtual Machine.
7. Nmap -sS 10.0.2.0/24 -vvv -p-  (Use IP of the metasploiable machine's box)

**Running an Exploit.**

1. After the last NMAP scan you can find all the open ports that are open on the other machine. Metasploit has exploits for each different thing listed but for this exercise we'll be using a VSFTP exploit.
2. To see what is running on this port we are going to do another NMap scan.
    a. Nmap -p 21 -sC -sV 10.0.2.15 (Ip of your Metasploitable box)
        i. -p is to designate that your scanning a port
        ii. -sC is for default scripts
        iii. -sV will enumerate for version

3. Anonymous FTP is running on this port and you can see the version listed in the results of the scan.
4. After figuring out the version running its as simple as copy and pasting the version into google, followed by ‘exploit’ to find an exploit module.
5. You can then start the metasploit framework by typing ‘*msfconsole’* into the terminal. May take a while to initiate since its your first time starting the framework on this Virtualbox.
6. Once you are into the framework type *‘use vsftp’* to find what metasploit modules can be used on this port.
7. You will see at least one module listed. Select and copy the whole path of the module name (exploit/unix/ftp/vsftpd_234_backdoor) and enter this into the terminal.
8. We will then set our remote host to our target IP Address by typing *‘set rhosts 10.0.2.15(Use your metasploitable IP)’* and press enter.
9. The last thing you have to do is run the command! Type in ‘exploit’ or ‘run’ in the command line and let it do its thing!
10. You should now be inside of your Metasploitable Virtual Machine! You can now type any command you would regularly type on the Target machine in the terminal of your Kali machine and it will take effect on the Metasploitable VM.