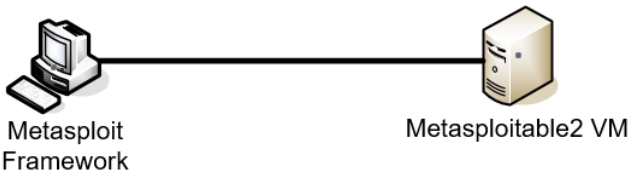
Metasploit Lab Assignment (v1.2)



1. (1 pt) Install and run Metasploit framework (http://www.metasploit.com) on your computer (or **run Metasploit Framework icon from within Kali Linux installed in** VMware or **VirtualBox**). Submit a screenshot showing the IP address (not loopback IP) of computer running Metasploit Framework.

2. (1 pt) Download, install, and **run metasploitable2** (a VM that was designed to contain numerous vulnerabilities) on VMware or **VirtualBox**. Submit a screenshot showing the IP address of computer running metasploitable2 VM.

3. (1 pt) Submit a screenshot showing that the two computers can ping each other.

4. (1 pt) From the computer running Metasploit framework, run Nessus vulnerability scanner (or **run nmap with -sV option**) to find which ports are open on metasploitable2 VM and are vulnerable to an attack. Submit a screenshot(s) of identified vulnerable applications and their port numbers.

5. (1 pt) Find an exploit (**different from vsftpd_234_backdoor**) within Metasploit framework that can be used successfully against the metasploitable2 VM by using Metasploit's **search, info, show, use, set, check, locate, and exploit/run** commands.

a. For which specific vulnerability (service, version, & port number) in step 4 are you exploiting?

b. Submit a screenshot of output of Metasploit's **search** command that shows the name of the exploit and payload that you are using.

6. (1 pts) After you have finished configuring Metasploit Framework to use a specific exploit via **use** command and have configured all required variables and payload via **set** command, show the final configuration providing screenshot of output of "**show options**" command.

7. (4 pts) Run the exploit via **exploit** or **run** command.

a. Submit screenshot of output displayed by running the exploit

b. Submit screenshot of "netstat -nt" on Kali Linux and circle the IP addresses and port numbers of the endpoints of the TCP connection used or created by the exploit.

c. Run Wireshark on Kali and submit packet captures and decodes of the exploit traffic that was sent between Metasploit Framework and the metasploitable2 VM.

d. Explain how the exploit was accomplished and correlate your explanation with the packet captures and decodes.