Marcus Wilson

MIS5212

Assignment 1

**Exploiting Metasploitable**

**The Exploit Background**

* To perform the penetration test I used a Kali Linux VM as my host machine. I attempted to exploit an VM running Metasploitable 2. I used the NMAP feature to return a list of open ports and versions of common applications that may be susceptible to an attack.
* Through this reconnaissance I was able to find that port 3306 was open running MySQL 5.0.51and port 21 was open using an FTP application vsftpd 2.3.4

**The FTP Exploit**

* I began the FTP attack by searching metasploit for an attack that could compromise the open FTP port. I found that there was a specific backdoor attack for the exact FTP client that the target server was running.
* After executing the exploit, I was able to gain root access to a shell on the target system. I verified my access using a “whoami” command which returned root and a “pwd” command confirmed that I was indeed in the root directory.
* I was able to change the root password of the system successfully. I then was able to SSH to the target machine using the new updated credentials that were compromised.

**The MySQL Exploit**

* I began the MySQL attack by searching for a MySQL exploit using the same search method as I used for the FTP exploit above. I found there was a MySQL login exploit that tries to login using no password or can be supplied a dictionary to use a brute force attack.
* After executing the exploit, I gained access to a root MySQL user. I was then able to change the root password and create an additional user with root privileges.

**Summary**

Both of these exploits are concerning. The FTP exploit allowed me to take full control of a system fairly easy and the MySQL exploit gave me the opportunity to compromise an entire database. The good thing is there are basic exploits that can be solved by using software patching and using complex passwords.