Arkadiy Kantor

MIS 5212 - Metasploit assignment

For this assignment, I had attempted to find vulnerabilities in several virtual machines and various hosts on my network using the Nessus Vulnerability Scanner. I had hoped to find a vulnerability in an older Windows 7 VM that has not been patched in a while but unfortunately it didn’t find anything of interest. I ended up using the Metasploitable Linux distro which had plenty of vulnerabilities to exploit. I had All my tools running in a windows 10 VM on a windows 10 Host. The network was configured in a bridged mode so that each client had a unique IP.

After running a Nessus scan I had exported my results and imported them into Metasploit. I had explored the various vulnerabilities and executed several. One that I found interesting was the **“vsftpd Smiley Face Backdoor”** this vulnerability exploits an FTP server which was compromised in a particular release in July 2011. The issue occurs when a user inputs a “☺” into the username, the user is granted access to the command shell on port 6200.

The Metasploit framework had the exploit available and I was able to successfully execute it. I could access the shell and execute several commands successfully with root access.

For mitigation strategies, I would suggest that the application and system admins stay up to date on patching the software they use, and disable ports that are not commonly used. System monitoring would also be helpful to note that the FTP server may be used or active on a machine that may not typically require it.