Executive Summary

The purpose of this assignment was to break into a workstation using the Metasploit Frame work. I decided to use an old workstation and build a vista image with no patches installed and see if I could break in. Using a simplified attack method for identifying the system, identifying the vulnerabilities and exploiting the vulnerability

Using an NMAP to identify see what ports were open and to identify the OS. Once identified I used Nessus to look for vulnerabilities. Nessus found a high vulnerability in remote desktop (MS12-020) that could be used on Metasploit to exploit. Configured Metasploit to exploit the workstation with the MS21-020 vulnerability and ran the exploit, in most cases the workstation’s CPU went to 100% and did not come down for twenty minutes. In other cases, after the exploit was completed the CPU went to 100% and ultimately had to power off and power back on after the thirty minutes. There was one case when I ran the exploit the workstation blue screened.

The exploit exercise although I was not able to “break into” the workstation as I expected. I could disrupt a bare bones Vista Workstation from working by simply applying an exploit to the workstation. I get a little worried with tools such as Metasploit that are free and available for anyone and could be used to “test the environment” for good or harm. It was a good exercise to show how important it is to keep a workstation up to date with its system updates.