Executive Summary

The need to secure networks and systems have never been so high, every day we hear more and more about businesses falling victim to cyber-attacks. For this assignment the Kali Linux 2.0 Metasploit framework was used to exploit vulnerabilities with a metasploitable VM. I ran a reconnaissance on the metasploitable VM with Nessus Vulnerability Scanner to show all known vulnerabilities and the NMap command to show all open ports. The Nessus scanner determined that there are 107 vulnerabilities and NMap revealed there are 22 open ports. For the purpose of this assignment I targeted 2 vulnerabilities found at open port 21 and open port 6667. I then used the Metasploit framework tool built into Kali Linux to exploit those two vulnerabilities. Both ports were acceptable to backdoor command executions.

Port 21 is open for File transfer protocol(FTP) version VSFTPD. VSFTPD has a known compromise exposing systems to a backdoor attack allowing attackers access to the root of the file system.

Port 6667 is open for Internet Relay Chat(IRC) version Unreal IRCd. Unreal IRCd is another known compromise exposing systems to backdoor attacks allowing access to the root of the file system.

Other vulnerabilities found which are exploitable with Metasploit:

* + Rlogin Service (rlogin Authentication Scanner)
  + rsh Service Detection (rlogin Authentication Scanner)
  + NFS Exported Share Information Disclosure (NFS Mount Scanner)

Both Unreal IRCd and VSFTP vulnerabilities have been addressed by developers. The end users just need to re-download software, verify it using the published MD5 / SHA1 checksums and re-install.