Brent L Easley

MIS 5212 – Advance Penetration Testing

Assignment 1

**Executive Summary**

Vulnerability assessment is an important part of penetration testing and is the process of identifying and assessing vulnerabilities on a target system. The purpose of this assignment was to successfully use Metasploit in Kali Linux 2.0 to exploit a system of my choosing, I decided to use Metasploitable, because it contains multiple vulnerabilities. During the first step of testing I used my Nessus scanner on my Metasploitable virtual machine. The scan results came back with multiple critical vulnerabilities to exploit using Metasploit. One of the vulnerabilities the results showed from my scan was the UnreallRcd Backdoor detection. The Nessus scanner explained that the remote IRC server is a version of UnreallRcd with a backdoor that allows an attacker to execute arbitrary code on the affected host. I then proceeded to use Metasploit to exploit vulnerabilities in Metasploitable, this test was performed in my virtual environment using VM Workstation 12.

* Performed Nessus scan on Metasploitable server to get critical updates to possibly exploit
* Ran ifconfig commands to IP addresses for both virtual machines. IP address for Metasploitable : 192.168.119.141, IP address for Metasploit : 192.168.119.128
* Performed nmap command scan on the IP address assigned in Metasploitable to check for open ports and versions of software
* Nmap command displayed open port: 6667/TCP, service : IRC, version : unreal ircd
* Unix/irc/unreal\_ircd\_3281\_backdoor was the command used to exploit the open port.

Running the exploit/unix/irc/unreal\_ircd\_3281\_backdoor command in Metasploit on the remote host IP address (192.168.119.141) for Metasploitable, I was able successfully gain access to the files on the Metasploitable server. According to the Nessus scan, the resolution to stop attacks like the one I performed using Metasploit, the client should re-download the software on the remote host and verify it using the published MD5 / SHA1 checksums, and re-install the software.