Jason Lindsley
MIS 5212 – Advanced Penetration Testing
Analysis Report 1 – Metasploit Attack – Analysis Report

The purpose of this analysis exercise was to utilize the Metasploit framework to successfully run an exploit against a vulnerable host. I chose to use Metasploitable as my target for this exercise, which is a Linux distribution that is intentionally built as a vulnerable host for security training and penetration testing.

The first step I took was to perform information gathering on the target host. I used NMAP to identify the target host IP address, open ports, and perform footprinting to identify the OS version. The IP address was required to perform a vulnerability scan. Identifying the open ports are important to delivering the exploit and gaining command and control of the system. Identifying the OS version could later assist in using default user IDs and passwords to pivot within the environment and escalate privileges during an attack.

Next, I ran a vulnerability scan in Nessus using the target's IP address to identify vulnerabilities on the host. The vulnerability scan found eight Critical and one High risk vulnerabilities. I selected one Critical risk vulnerability – i.e. UnrealIRCd Backdoor Detection (CVE-2010-2075). This vulnerability record indicated that the system uses a vulnerable version of UnrealIRCd for the Internet Relay Chat (IRC) process. This version of UnrealIRCd has a backdoor that allows an attacker to execute arbitrary code on the affected host. The Nessus results also indicated that the vulnerability was exploitable with Metasploit's "UnrealIRCD 3.2.8.1 Backdoor Command Execution" exploit.

Metasploit is a powerful tool that is used by offensive security professionals to exploit known vulnerabilities. I used metasploit in my Kali Linux environment to search for the UnrealIRCD 3.2.8.1 Backdoor Command Execution exploit that was referenced in the Nessus scan. Once identified, I selected a Double Reverse TCP Unix command line shell as the payload and set the options for the exploit – including the target host, listening host, and ports. I confirmed that port 6667 was open by reviewing my initial NMAP scan.

Once the exploit was delivered, I had command line access to the target host. I ran a "whoami" command to identify that I was logged in as 'root'. I also queried the list of users on the host using the "cat /etc/passwd" command and concluded my exercise.

I've spent a lot of time in my career reviewing vulnerability scans and sharing them with IT Management for remediation. Although, I previously understood the risks associated with these vulnerabilities, I was very surprised by how simple it was to use a *free* version Metasploit to exploit them. This exercise reinforced the importance of implementing strong vulnerability and patch management practices to identify and eliminate vulnerabilities in an IT environment.