Shain Amzovski

MIS 5212 .001

Learnings from Metasploit

**Introduction:**

 The virtual machine I decided to run Metasploit against was Metasploitable 2. Metasploitable is a Linux virtual machine, that is intentionally set-up with vulnerabilities. The reason Metasploitable is an internationally vulnerable Linux machine is so that it can be used to conduct security training, test security tools, and practice common penetration testing methods. Essentially, it is a penetration testing lab in a box. For this particular assignment, Metasploit, a tool located in Kali-Linux 2016, was used to attack Metasploitable.

**Steps conducted for the experiment using Kali-Linux 2016:**

In order to attack the VMware virtual machine, Metasploitable 2, Nmap (Network Mapper) is run from Metasploit to discover hosts and services on a computer network. When the Metasploitable VM was called as the targeted host, it scanned the ports and provided a report of all of the open protocols. The main features of Nmap are host discovery, port scanning, version detection, OS detection, and scriptable interaction with the target.

After determining which ports were open on the Metasploitable Virtual Machine, finding exploits to attack the VM with were not difficult to come by. After completing some research on line, I was able to find many attacks that I was able to execute from Metasploit. One of the first vulnerabilities I was able to exploit was an IRC Server. First, I ran a command execution that exploits a malicious backdoor that was added to the Unreal IRCD 3.2.8.1 download archive. This command Checks if an IRC server is back doored by running a time-based command (ping) and checking how long it takes to respond. The command that was run from Metasploit to the RHOST was exploit/unix/irc/unreal\_ircd\_3281\_backdoor. After running this command execution, a hacker would have access to all of the directories on the remote host. It is possible to read and write to these directories.

Another exploit I was able to come across after looking at the open ports Nmap discovered on the Metasploitable VM was an FTP exploit on Port 21. A command I was able to execute was exploit/unix/ftp/vsftpd\_234\_backdoor. This command exploits a malicious backdoor that was added to the VSFTPD download archive. “This backdoor was introduced into the vsftpd-2.3.4.tar.gz archive between June 30th 2011 and July 1st 2011 according to the most recent information available. This backdoor was removed on July 3rd 2011.” Once this command is executed, the hacker gets root access to the vulnerable system.

The last vulnerability I discovered was a PHP exploit on Port 80 of Metasploitable. The command execution for this exploit is Command = exploit/multi/http/php\_cgi\_arg\_injection. When this command is run as a CGI, PHP up to version 5.3.12 and 5.4.2 is vulnerable to an argument injection vulnerability. This vulnerability leaks the source code of the application and allows remote code execution. This vulnerability also provides access to the root level of the system. All files and folders are accessible.

**Conclusion:**

Metasploitable VM can be a useful tool for penetration testers. It shows us how easy it is for a system to be compromised when certain ports are left open and vulnerabilities are left unpatched. Organizations must keep their machines up-to-date with patches and other security recommendations. It does not require a skilled hacker to gain access to a system. Vulnerabilities can be researched and a hacker can see if an organization is up-to-date on their patches.