Anthony Fecondo

Wade Mackey

Advanced Penetration Testing

February 21, 2017

Metasploitable Assignment

I was tasked with leveraging Metasploit Framework to launch an attack on a machine that I owned. In order to do so, I elected to install Metasploitable, an intentionally vulnerable operating system, onto a virtual machine. Once that was created, I ran a Kali Linux virtual machine to launch the attack. The beginning of the assignment consisted of reconnaissance. Using ifconfig on the Metasploitable machine, I identified the IP address as 192.168.171.140. If I didn’t own the target machine, I could have identified it by performing an nmap scan, such as nmap –sP 192.168.171.0/24 because I knew the machine was on the same network as my machine. After I had the target IP address, I ran nmap –sS –A 192.168.171.140 to gather more information about the OS, the open ports, etc.

From here, being new to Metasploit, I searched online for more resources so I could identify an appropriate exploit. The Metasploitable 2 Exploitability Guide on rapid7.com walked through a variety of exploits from which I chose two to try on my own. The exploits I ran were the unreal ircd 3281 backdoor and a PHP injection. Both were ran the same way; First, I called the exploit with the command use \*exploit name,\* then I used the show options command to determine what inputs were required from me to launch the exploit. Both only required the IP address of the target machine. Using the Set RHOST command I entered the IP address of Metasploitable that I previously discovered. Then I ran the exploit using the exploit command. After the exploits finished, a message printed saying that a shell terminal was opened in the target machine. Now that I was in, I experimented a little to see what I could see and do. In both cases I was able to move around the root directory, create folders, change permissions, etc. After a little experimentation I used ctrl+C to terminate the exploit.

During this assignment, I was exposed to a plethora of exploits built into Metasploit. I realized that Metasploit is a hugely powerful tool as it only requires users to know 1) a vulnerability on a machine and 2) a corresponding exploit for that vulnerability. As soon as that info is known, Metasploit can efficiently automate the task of running the exploit. As Metasploit has a huge library of exploits, this makes the life of penetration testers a lot simpler if there is a need to demonstrate a system’s vulnerability. Using Metasploit, a penetration tester can communicate to a client that they are vulnerable by showing them how easy it is to exploit the system.