Mengqi He
Advanced Penetration Testing
Wade Mackey
03/25/2017

Metasploit Analysis

For this task, I launched an attack on a Metasploitable virtual machine. I used Nmap, Nesussus and Metasploit on a Kali virtual machine to try to get in to the system and extract information from my target system.

First, I ran a ifconfig command on the metasploitable vm to get its ip address 192.168.69.142, and then ran a nmap scan on the Kali vm to see what I can get through the ip address. There were 977 ports closed and 23 ports open, and these open ports would be vulnerable to attacks. Secondly, I ran a Nessus scan, and found that there were 105 vulnerabilities, with 6 critical and 4 high in severity. I decided to focus on only critical vulnerabilities for this task. I found one vulnerability was rogue shell backdoor detection, and the ingreslock backdoor was listening on port 1524. I went back to nmap, and ran a telnet 192.168.69.142 1524 command to create a telnet session connecting with port 1524, and thus I could get access to the metasploitable.

After that, I turned to metasploit. I downloaded the Nessus scan report and imported it to metaspolit. I decided to try if there was any other backdoor. I searched the internet and found out a common module used to exploit backdoors, exploit/unix/irc/unreal_ircd_3281_ backdoor. I set the RHOST as 192.168.69.142, and ran an exploit command. I got one command shell session open and thus got access to the system and was able to do some change in the system through port 6667 that was running Unreal ircd. Another vulnerability I found was VNC server "password" password. I ran an auxiliary/scanner/vnc/vnc_login command, and set RHOST. It would scan metasploitable's ip address and attempt to login via VNC with either a provided password or a wordlist. Then I successfully got the VNC server password "password" which was a very weak password as Nessuss reported. At last, I made a brute force attack on SSH to gain administrative privileges. I firstly searched some common used SSH passwords and created a txt file called username to store them ensuring per password per line. Then, I used the module use auxiliary/scanner/ssh/ssh_login, set RHOSTS as 192.168.69.142, set USERNAME as root, set PASS_FILE as Desktop/username, and stated exploiting. However, all the passwords were wrong, and I failed to gain the password of root. At last, I unset the USERNAME, set USER_FILE as Desktop/username, and set USER_AS_PASS True. This time I would like to see whether I can get any access to the system even it would not be root account. I got one correct credential which username was user and password was user as well.