|  |  |  |
| --- | --- | --- |
| Course # | James Riley Dorough | Custom Exploit Development/Deployment |
| CSIS 462 | **11FEB22** | **Semester Week 5, Lab 2** |

Title

* Enumerate blue team boxes to discover exploitable vulnerabilities
* Exploit a chosen vulnerability in effort to improve existing persistence

Introduction

This lab focuses on the processes of initial foot holding on target boxes. I use Metasploit’s windows meterpreter psexec reverse shell payload to gain access to a target machine. From here I attempt to better hide my activity. Once I have an active connection, I can begin uploading additional scripts and malware to the target system. All of this should be hidden behind a SSH tunnel.

Method

* Establish a SSH tunnel though the firing station to show all traffic as a NATed address
* Start Metasploit
* Set the module to exploit/windows/smb/psexec
* Set or ensure the payload is set to windows/meterpreter/reverse\_tcp
* Set the options to the target box and include valid credentials
* Run the exploit
* Check for running processes
* Migrate your meterpreter shell into a compatible process
* Use the upload command to send files to the target box
* An additional option is to run the impacket-psexec command with valid credentials to get a CMD shell on a target box

Results & Context

Text

Description automatically generated

My first step is to send returning traffic through a SSH tunnel on FirsingStation2.

A picture containing graphical user interface

Description automatically generated

I set up the attack with the smb psexec module. By default, Metasploit sets the payload to a reverse tcp meterpreter shell.

Text

Description automatically generated

These settings were used to test on the local network. To target the blue team, the settings will need to be adapted and the listening port should match the tunnel’s public port.

Text

Description automatically generated with medium confidence

Once connected, you should be logged in as SYSTEM.

Text

Description automatically generated

Running the ps command shows available processes to migrate into.

Text

Description automatically generated

I chose to migrate into a x64 SYSTEM owned process to better hide my session.

Graphical user interface

Description automatically generated with medium confidence

Using the upload command allows me to transfer files to the target machine. Running bg lets me access multiple sessions from the same terminal

Text

Description automatically generated

Here you can see the test file I transferred from my Kali box to the target. I intend to use a method like this to move my C2 implant onto blue team systems later on.

Text

Description automatically generated

Lastly, for a more direct approach, you may be able to directly access available writeable shares using the impacket-psexec command to pop a shell on the target box.

Conclusion

Firstly, a huge thanks to Ben Gordon for assisting me in understanding how to find exploits or how to vector my attack. I have learned a great deal of how to use Metasploit to attack systems. I used Chainsaw to review how my attack appeared on the target system. I’ve learned that the exploit and payload are distinct separate operations and using a proper combination can provide better access. Lastly, I’ve realized that hardly any exploits work unless you already have valid credentials for the system you are attacking.