|  |  |  |
| --- | --- | --- |
| Course # | James Riley Dorough | Custom Covert C2 Platform Development/Deployment |
| CSIS 462 | **17FEB22** | **Semester Week 6, Lab 3** |

Title

* Generate a custom C2 implant to be used against blue team systems
* Embed the custom implant onto the blue team systems
* Ensure that the implant provides benefited persistence

Introduction

This lab is to demonstrate how C2 server callback implants can provide advanced persistence in a system while remaining covert. The methods discussed in this lab can be vastly improved to hide activity. An example being embed the service executable binary into a benign system binary or tool such that the running implant is hardly distinguishable from normal activity. After an implant is installed, it should provide the attacker excellent access to operate within the target system.

Method

* A C2 server must exist prior to the generation of implants
* Access the C2 server services to create a new payload
* Set the payload for the operating system you intend to exploit
* Alter the domain that the payload calls back to
* Change the port to 443
* Name the payload (this should be covert and easily hidden with other applications on the target system)
* Download your payload
* Hide your payload on the target system using any access or exploit available

Optional:

* Use a service manager to set your implant as a service
* Set the service to activate on boot

Results

On some of the boxes I used the accessible hidden shares to easily transfer the necessary files to the target machine.

Graphical user interface, application

Description automatically generated

Here I transferred the NSSM service manager binary and the implant I have created to a target Windows 10 machine.

Graphical user interface, text

Description automatically generated

To install the executable implant as a service I used the backdoor on the machine through the Remote Desktop Protocol to set up the service. You could also use tools such as “impacket-psexec”. However, this requires you to run nssm in the command line and the tool has next to no usable documentation that matches the syntax required to execute the commands.

Graphical user interface, application

Description automatically generated

I set the path of the service to the C2 implant.

Graphical user interface, text, application, email

Description automatically generated

I set the service name to blend into the VMware services slightly better. Although when running the process shows under NSSM.

Graphical user interface, text, application, email

Description automatically generated

I set the service to run as the system authority

Graphical user interface, application

Description automatically generated

I set the process priority to high to ensure it has a better chance of responding though various levels of target system performance.

Text

Description automatically generated

Lastly I started the service on the target machine.

Graphical user interface, application, table

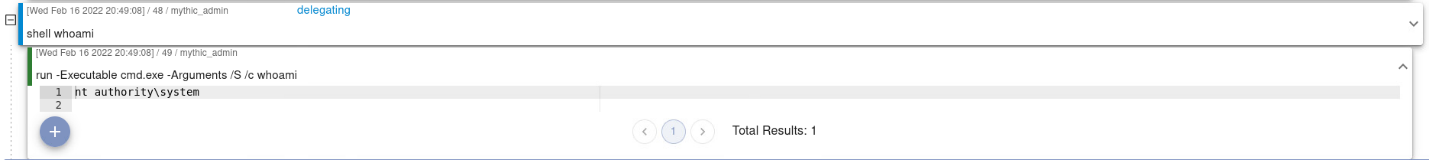
Description automatically generated

Returning to the C2 service, you can see the new implant on a Windows 10 box in the BFSSW domain responding.

Graphical user interface, text, application

Description automatically generated

To ensure that this was the correct box I just worked on, I run the shell command and pass it the argument of ipconfig to make sure the returned IP address matches the OS. I also ran “shell tracert <C2 NATed IP address> to ensure that the IP subnet matched the team’s domain.



Here I confirm that I have system authority on the target windows box.



Lastly, I document and reconfigure the description to label the implant callback. From here I move on to repeating the process with various exploits to install the same C2 implant setup on various boxes.

Conclusion

I have learned how C2 servers operate and how they hide their activity from unsuspecting users. I became better familiar with the blue team services installed and where I should hide my implant. I also learned a little more about how to use windows shares. Last of all I hope that my added persistence can help me provide better, future learning experiences for myself and the blue team.