SPRING 17

UNIDAD 2

EJERCICIO 2

WINDOWS

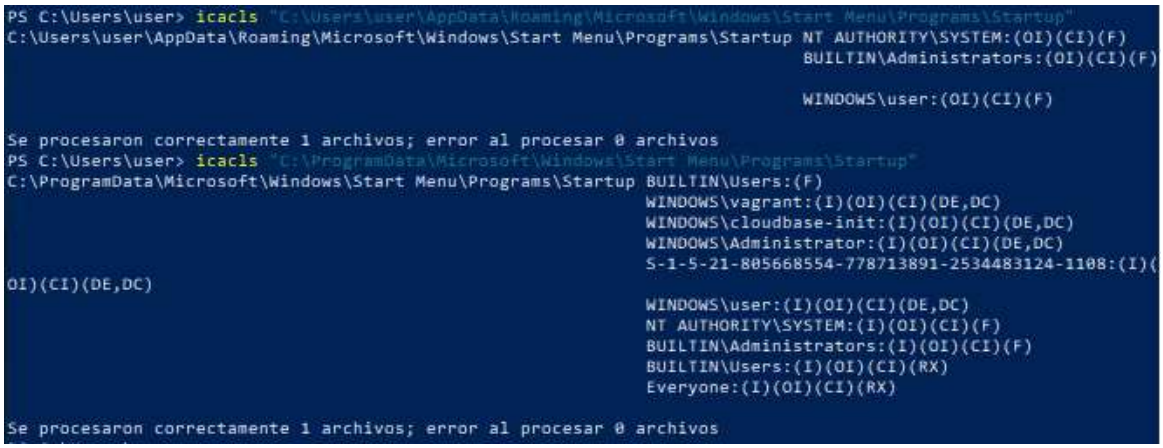
METODO “STARTUP OTHERS”

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 maquina 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\

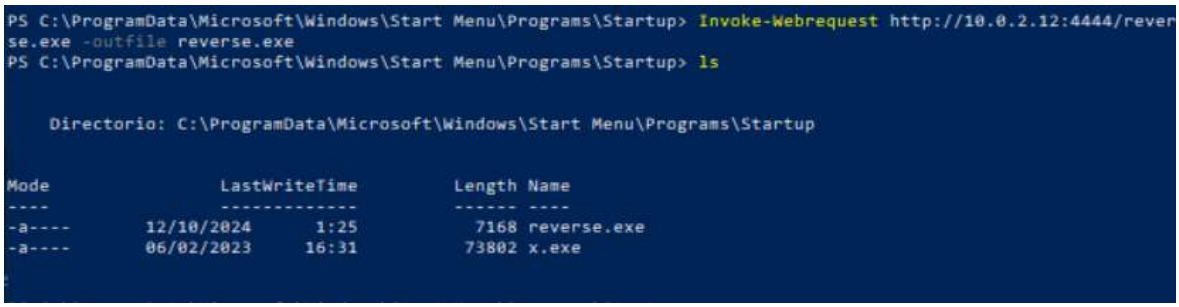
    Se comprueban ambas rutas, correspondiendo la primera a los servicios y aplicaciones que se ejecutan cuando el usuario "users" inicia sesión, y en segundo lugar, corresponde todos los servicios y aplicaciones que los usuarios en general ejecutan como inicio de sesión, teniendo acceso su propio usuario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



*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.

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



3.- Se ejecuta el comando Invoque-Webrequest para la trasferencia del archivo al sistema Windows

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