

Tunnel ssh et proxy sock

Pour renvoyer tout les données de mon port 1000 vers ip:port d'une machine vers laquelle je me connecte en ssh je fais comme sa

```
Ssh -p <port> user@ip -L 1000 @adrIp:port
```

Comme sa toute mes communication qui passe par mon port 1000 seront renvoyer vers l'ip port que j'ai spécifier

Pour rediriger une connexion via ssh de sorte que si je me connecte sur le port 1000 d'une machine sa me renvoie vers le port 22 il faut faire comme ceci

```
Ssh -p <port> user@ip -R 1000:localhost:22
```

Avec cette commande la quand je me connecte en ssh je fais une regle de PAT qui redirige tout les communications qui vont vers le port 1000 de la machine je les redirige vers le port 22 de cette dernière

Proxy socks :

```
Ssh -p <port> user@ip -D <unDeMesPorts> par exemple 5000
```

Et ici tout ce qui passera par mon port 5000 en http port 80 et 443 sera interfacé au nom de la machine local à laquelle je me connecte

Je vais sur mon navigateur je configure proxy socks je met mon ip ou localhost + port 5000 et sa fonctionne

Je vais effectuer différents test en me connectant à mon raspberry pi qui héberge un serveur web sur son port 80

Je vais transférer le port 80 de mon Raspberry vers mon port 8080

Pour cela j'ai lancé cette commande

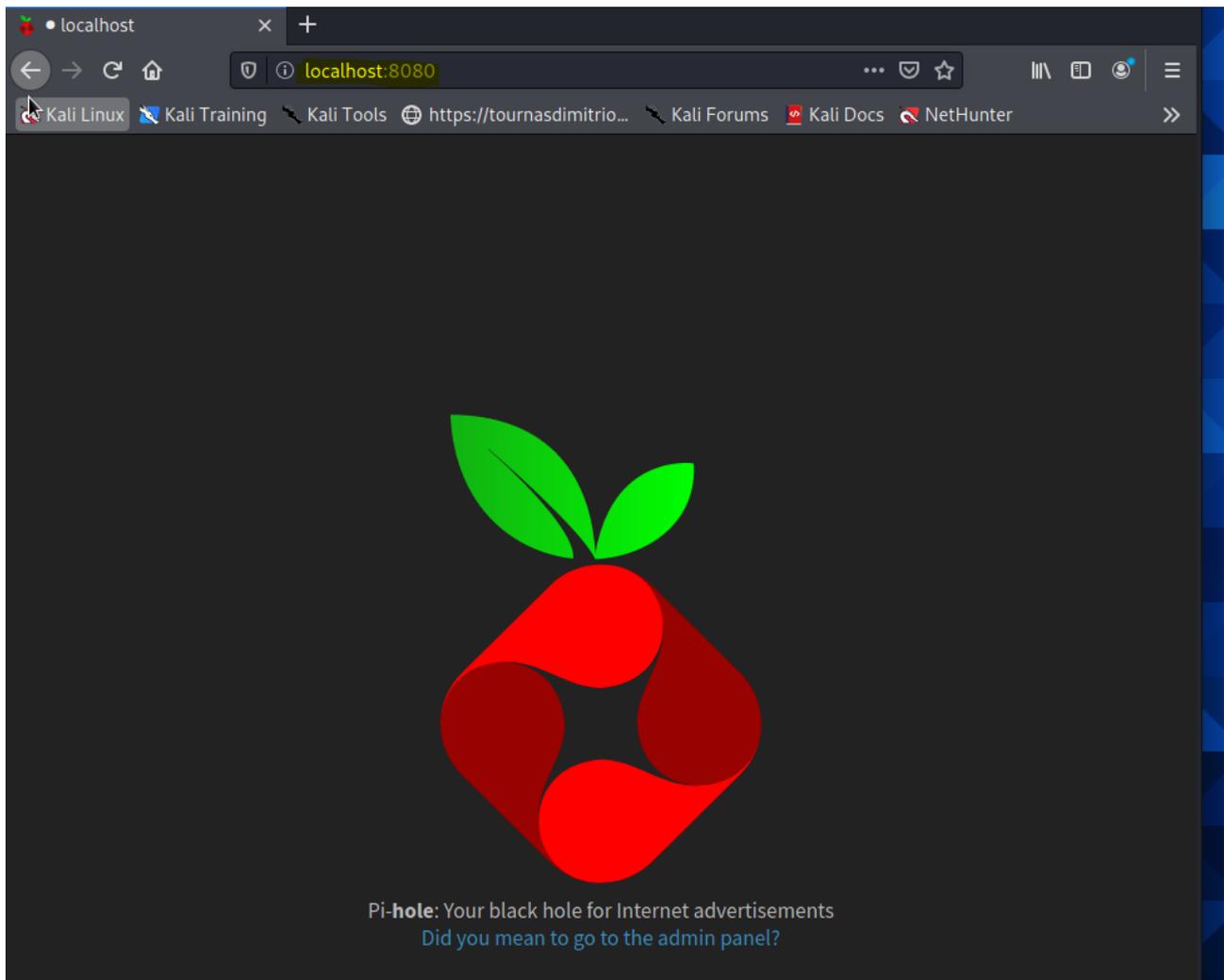
```
root@kali:~# ssh adel@192.168.1.4 -L 8080:192.168.1.4:80
The authenticity of host '192.168.1.4 (192.168.1.4)' can't be established.
ECDSA key fingerprint is SHA256:/xdU0PHyEUMQXthKhOU2FnE841W7YiFsLAFDDiyoYu0.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.4' (ECDSA) to the list of known hosts.
adel@192.168.1.4's password:
Linux raspberrypi 5.10.17+ #1421 Thu May 27 13:58:02 BST 2021 armv6l

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Thu Jun 24 22:26:53 2021 from 192.168.1.16
adel@raspberrypi:~ $
```

Je vais maintenant voir en localhost sur mon port 8080 si je vois l'interface d'administration de mon serveur pi-hole

Sa fonctionne parfaitement



Je vais passer à l'option du proxy socks maintenant

Je me déconnecte et me reconnecte en définissant mon proxy socks sur le port 5000

Pour cela j'effectue cette commande

```
connection to 192.168.1.4 refused.
root@kali:~# ssh adel@192.168.1.4 -D 5000
adel@192.168.1.4's password:
Linux raspberrypi 5.10.17+ #1421 Thu May 27 13:58:02 BST 2021 armv6l

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sun Jun 27 19:53:37 2021 from 192.168.1.71
adel@raspberrypi:~$
```

Je vais maintenant dans les parametre de mon navigateur firefox et je définis le proxy socks

Manual proxy configuration

HTTP Proxy Port

Also use this proxy for FTP and HTTPS

HTTPS Proxy Port

FTP Proxy Port

SOCKS Host Port

SOCKS v4 SOCKS v5

Je vais maintenant me connecter à mon propre serveur apache et voir si sa me connecte depuis l'ip de mon raspberry ou non

Après m'être connecter je suis partis regarder dans les log et la connexion au site sur mon serveur apache ce fait bien depuis le Raspberry

```
192.168.1.4 - - [27/Jun/2021:20:59:55 +0200] "GET / HTTP/1.1" 200 500 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
192.168.1.4 - - [27/Jun/2021:20:59:55 +0200] "GET /favicon.ico HTTP/1.1" 404 490 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
root@kali:~#
```

Si cette erreur apparaît ce n'est pas grave sa fonctionne quand même

```
adel@raspberrypi:~$ channel 8: open failed: connect failed: Connection refused
channel 8: open failed: connect failed: Connection refused
channel 8: open failed: connect failed: Connection refused
channel 12: open failed: connect failed: Connection refused
channel 12: open failed: connect failed: Connection refused
channel 12: open failed: connect failed: Connection refused
channel 14: open failed: connect failed: Connection refused
channel 16: open failed: connect failed: No route to host
channel 20: open failed: connect failed: No route to host
channel 16: open failed: connect failed: No route to host
channel 20: open failed: connect failed: No route to host
channel 11: open failed: connect failed: Connection refused
```