Download putty and puttygen on https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html

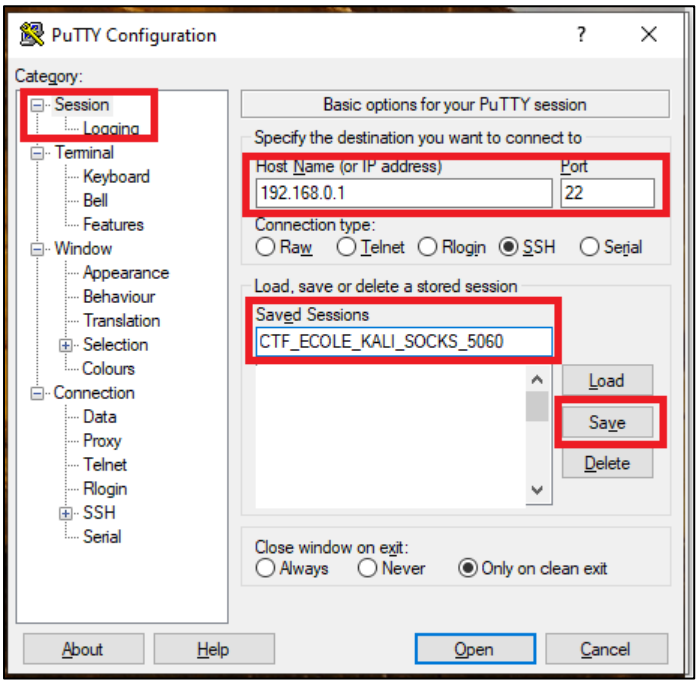
Table des matières

Create a proxy socks using PUTTY SSH on windows 2
Using a proxy socks with Firefox (proxy options) 6
Configure PUTTY to use a socks proxy 7
Convert a key file in PEM TO PPK 7
Create a proxy socks using SSH on Linux 10
Using a proxy socks on Linux and command line tools (Proxychains4) 10

Create a proxy socks using PUTTY SSH on windows

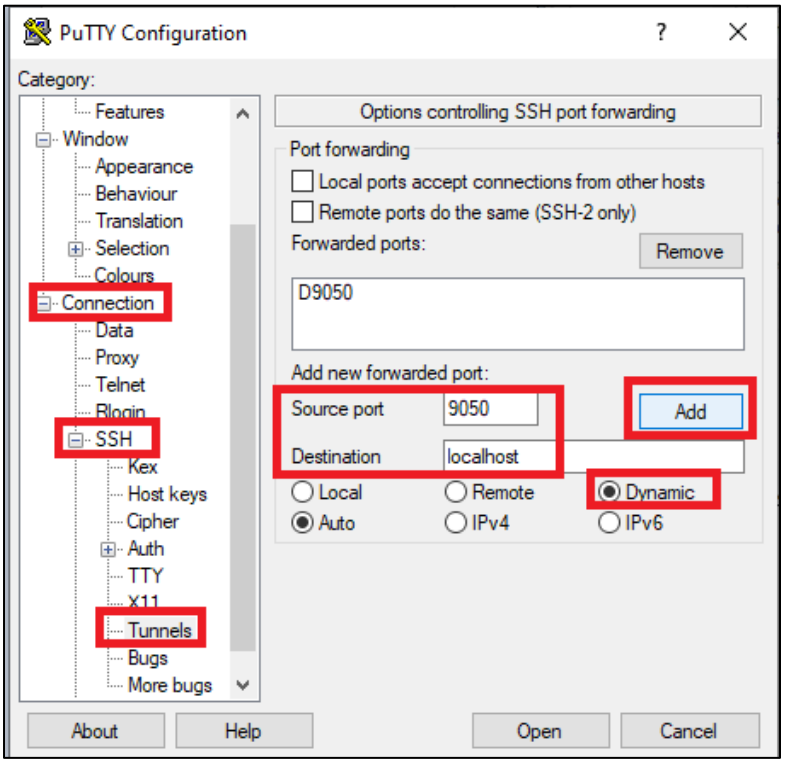
Open Putty

In the hostname enter the KALI IP given by the CTF team



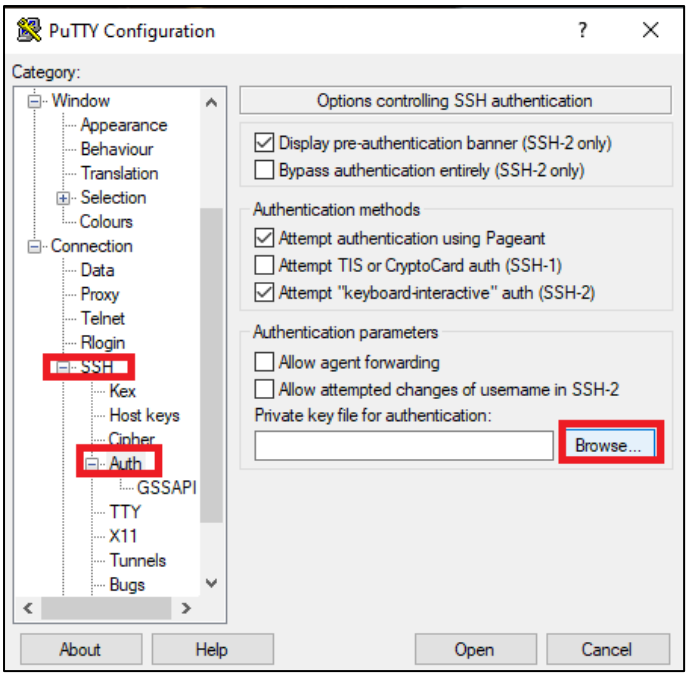
Give a name in the Saved_sessions fields and click on Save button

In the Connection-SSH-Tunnels settings enter the followings and click on ADD button

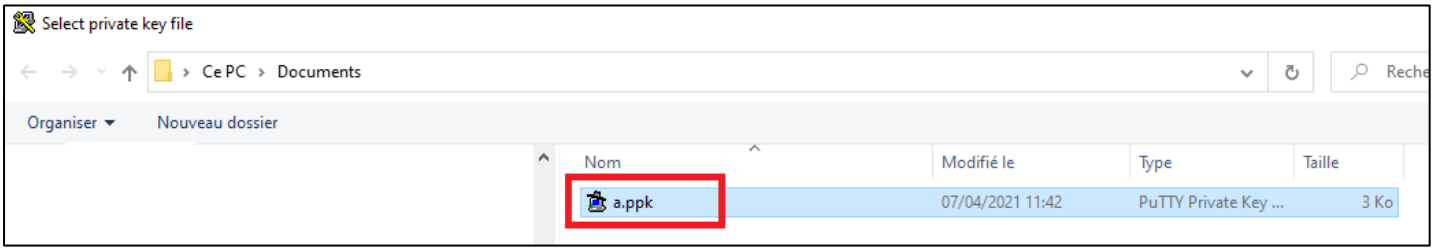


Optional: Configure SSH KEY authentication

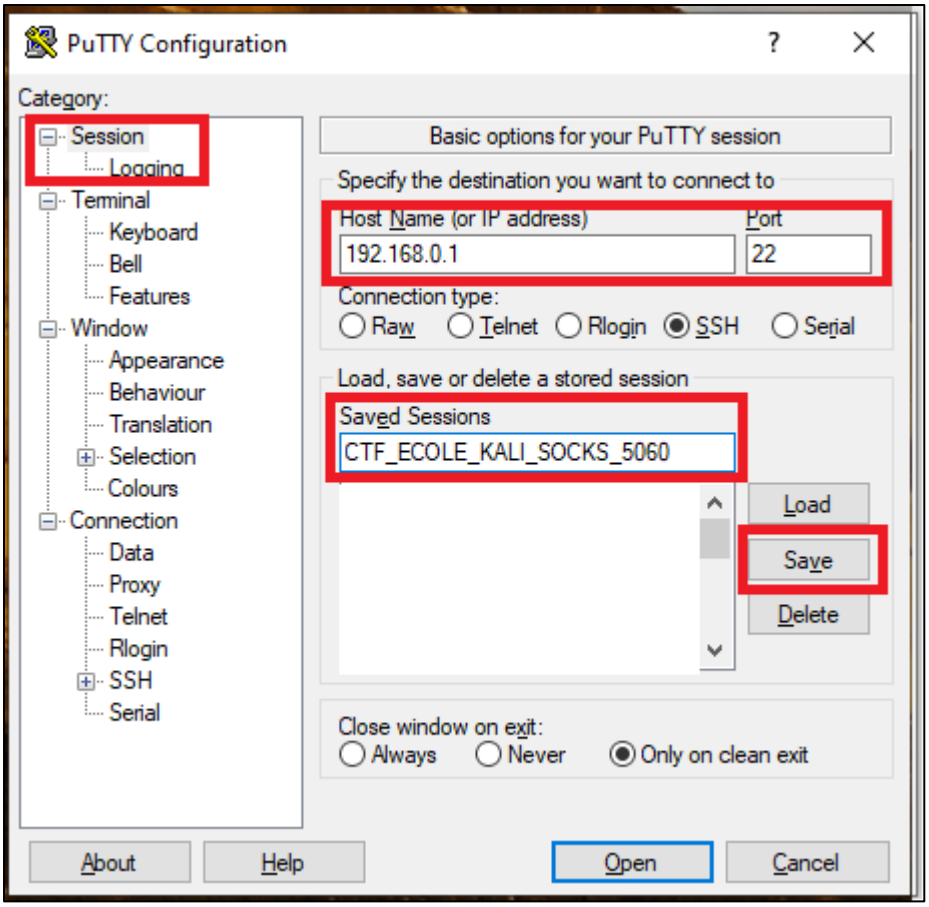
Click on SSH-Auth settings and click on the browser button



Select the private Key file in the PPK format and click on open

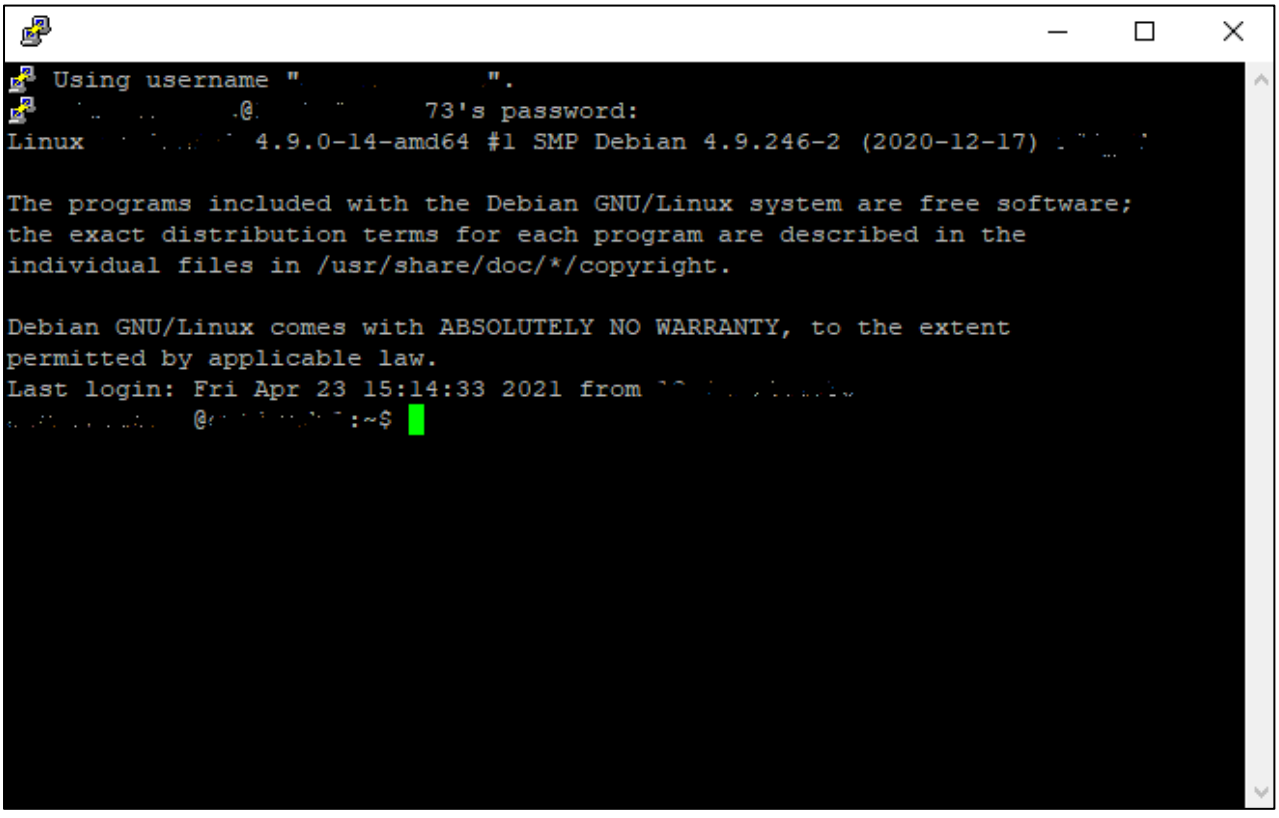


Go back in the Sessions Settings and click again on the Save Button

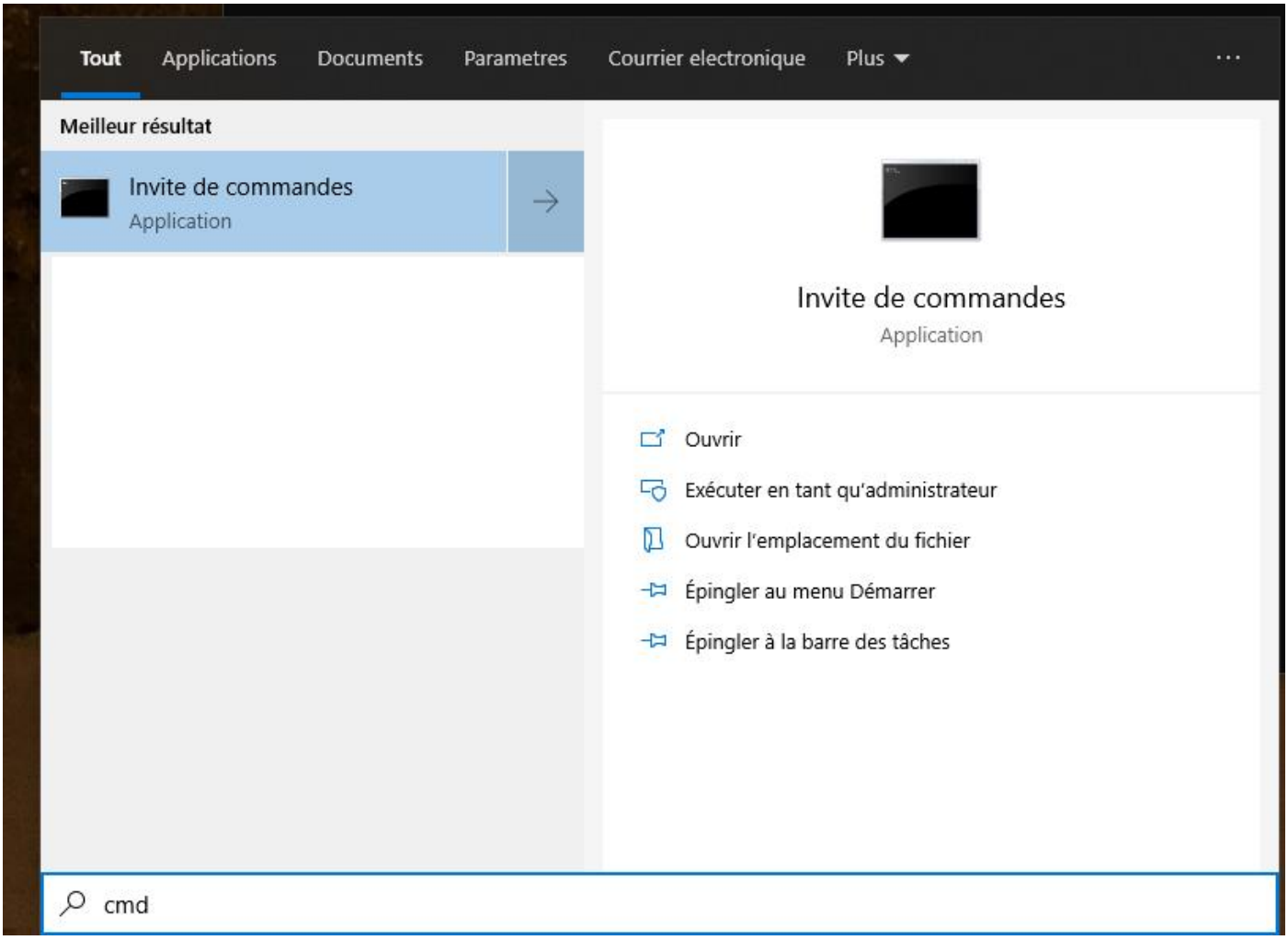


Now click on Open to launch the SSH connexion.

Log in using your login/password given by the CTF team then prompted.



Open a CMD shell



and enter the following command: ***netstat –na***

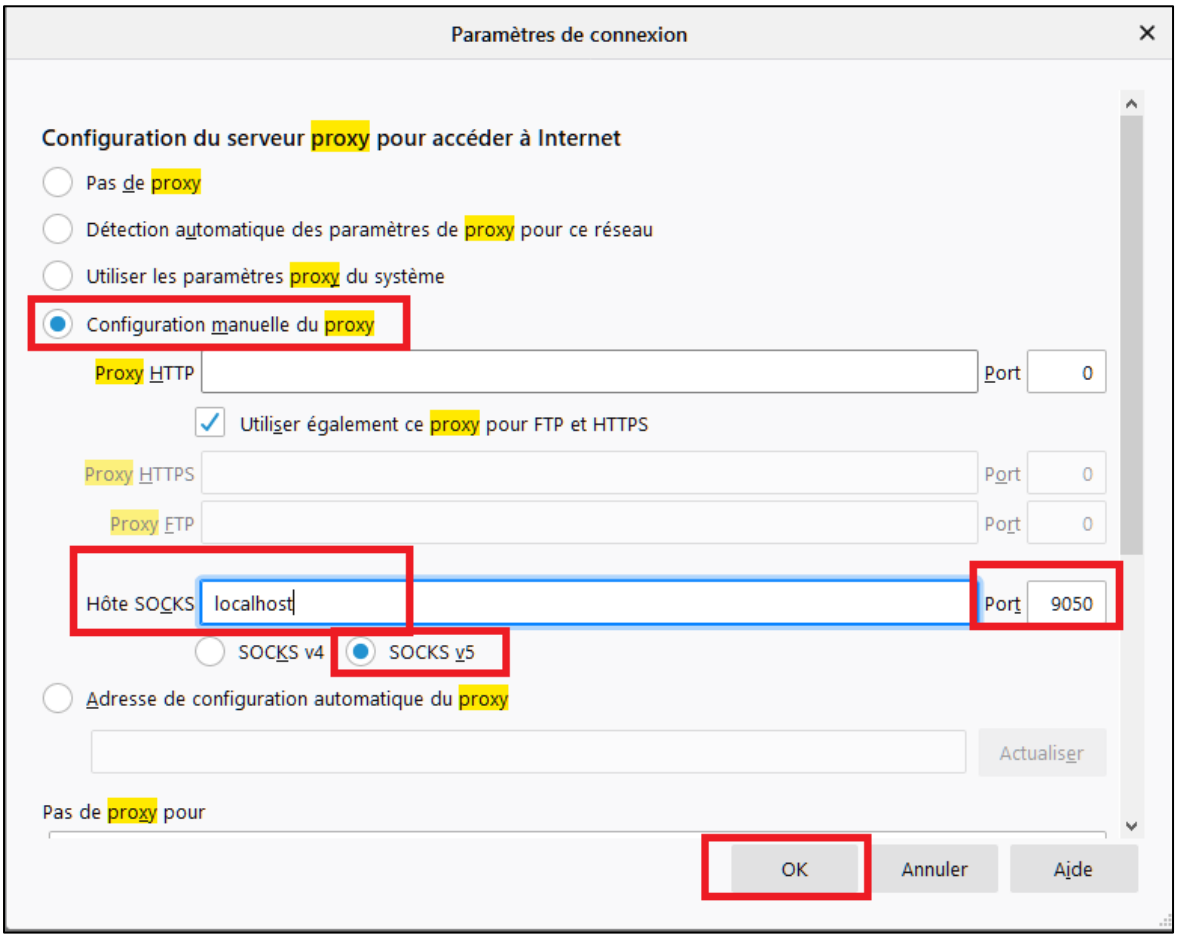
Double check that you have the following line : 127.0.0.1:9050 in LISTENING MODE

```
U:\>netstat -na

Connexions actives

  Proto  Adresse locale         Adresse distante       État
  TCP    127.0.0.1:8080         0.0.0.0:0              LISTENING
  TCP    127.0.0.1:8443         0.0.0.0:0              LISTENING
  TCP    127.0.0.1:8447         0.0.0.0:0              LISTENING
  TCP    127.0.0.1:8448         0.0.0.0:0              LISTENING
  TCP    127.0.0.1:8449         0.0.0.0:0              LISTENING
  TCP    127.0.0.1:8921         0.0.0.0:0              LISTENING
  TCP    127.0.0.1:9050         0.0.0.0:0              LISTENING
```

If not, please check you putty tunnel options

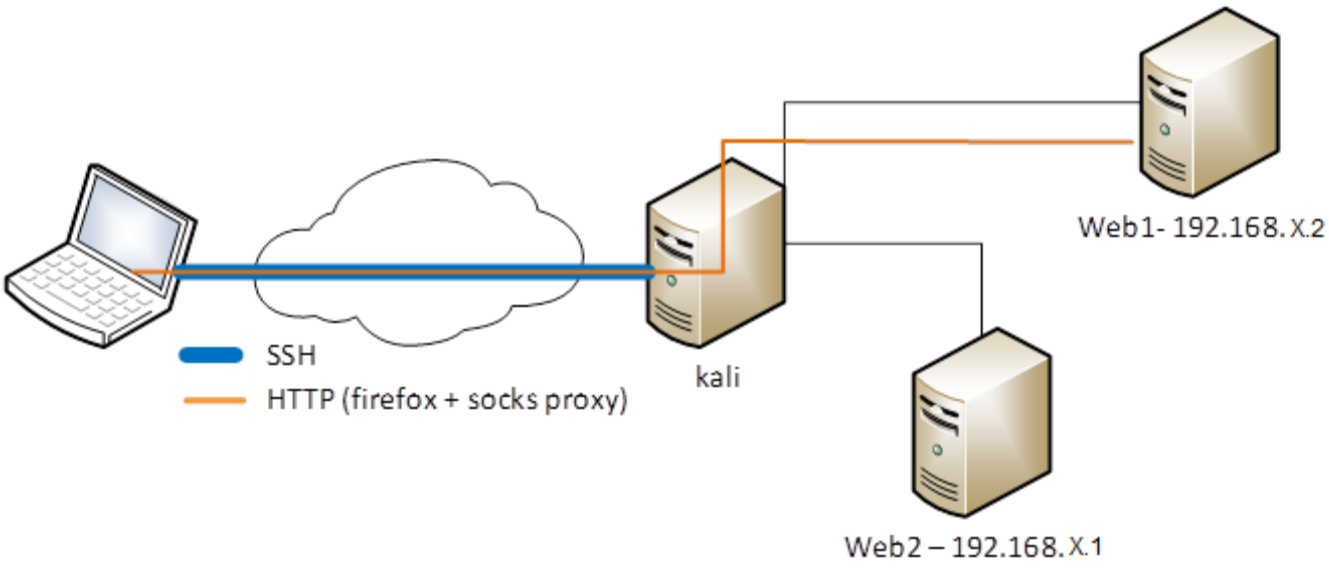
Using a proxy socks with Firefox (proxy options)

Open Firefox, then options, then network options and set the options as following:



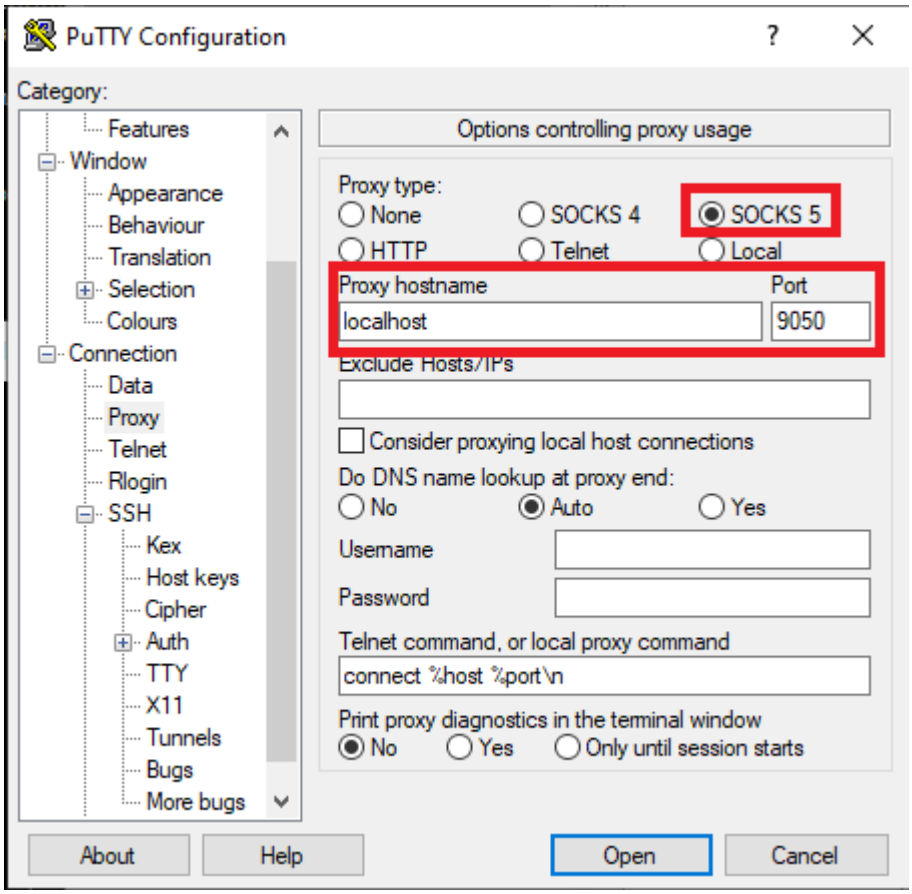
You can now access to the servers located BEHIND the KALI machine.

Example:



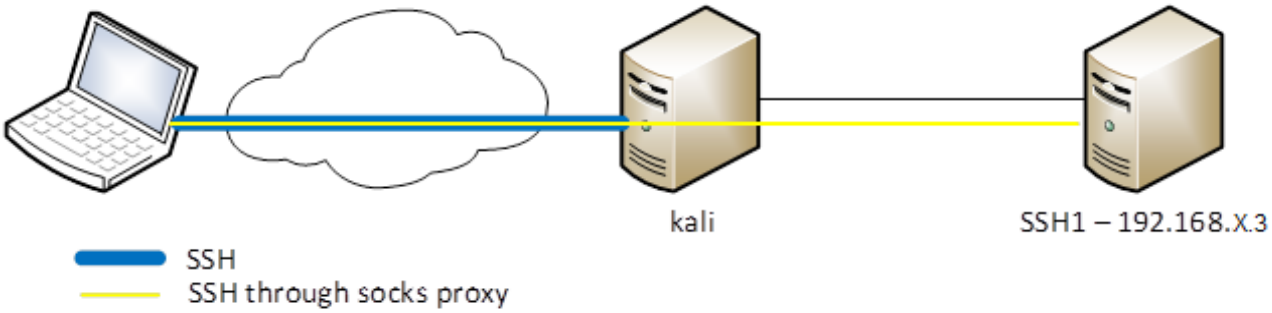
Configure PUTTY to use a socks proxy

Create a new connexion then open the Connection->Proxy settings:



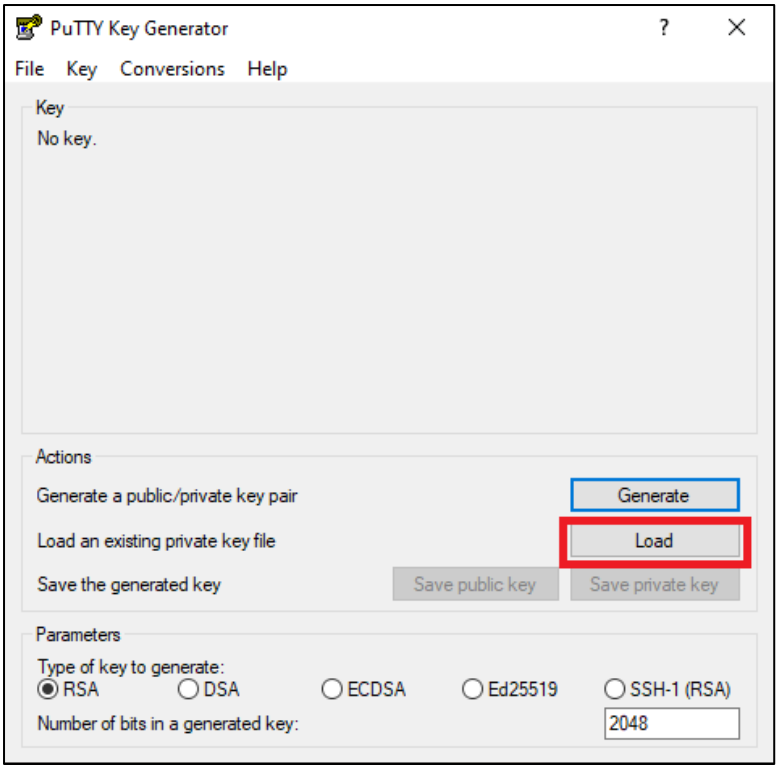
Then go back to the sessions options and click on the save button.

Example:

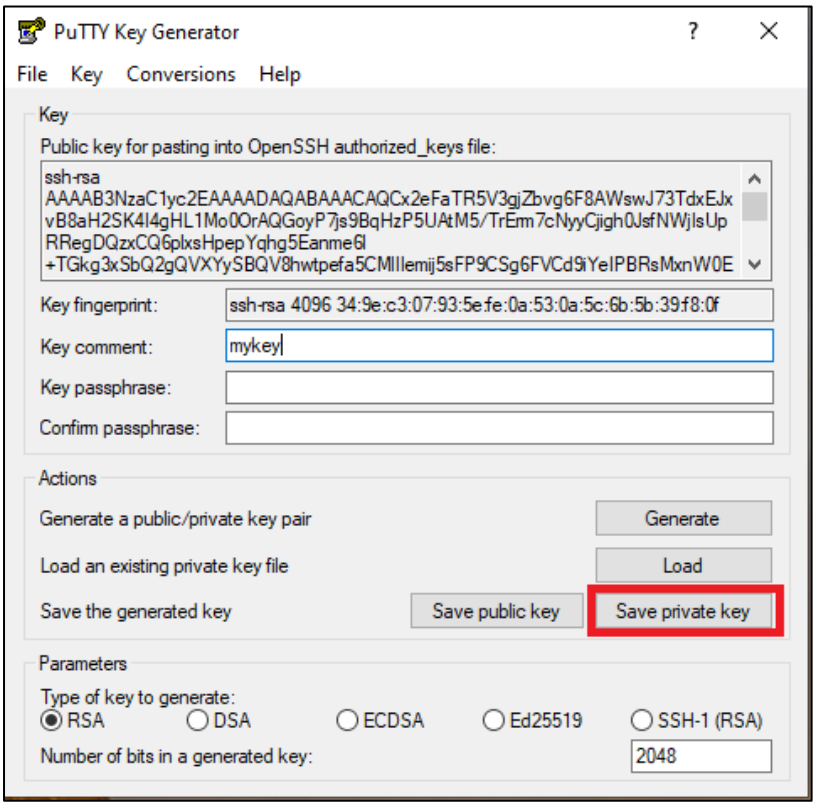


Convert a key file in PEM TO PPK

Open puttgen

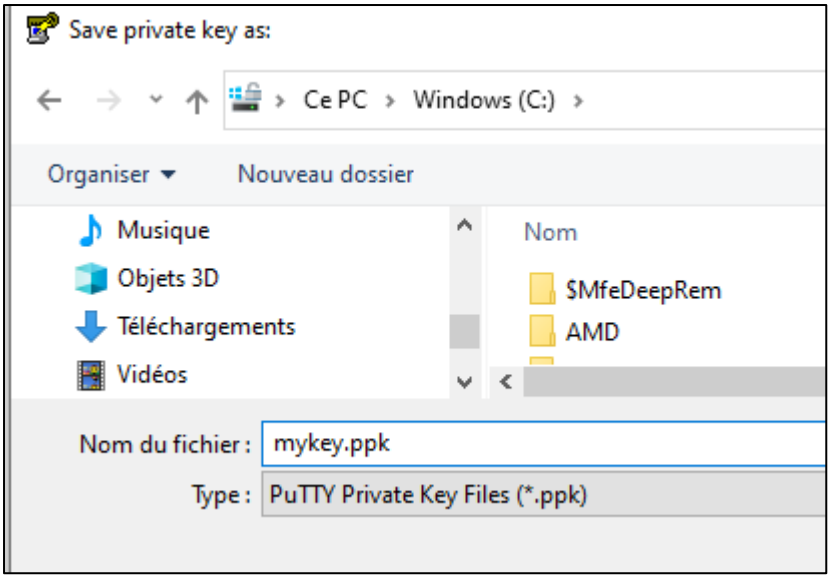


Then click on load and select the private key in the PEM format



(optional, you can set a password on privateKeyFile)

Click on Save Private key to save the key in PPK format


Save private key as:
Ce PC
Windows (C:)
Organiser
Nouveau dossier
Musique
Objets 3D
Téléchargements
Vidéos
Nom
$MfeDeepRem
AMD
Nom du fichier :
mykey.ppk
Type :
PuTTY Private Key Files (*.ppk)

Create a proxy socks using SSH on Linux

Open an shell and run th following command:

```
ssh -D 9050 login@ip
```

Example

```
user@machine:~$ ssh kali@192.168.30.5 -D 9050
kali@192.168.30.5's password:
Linux optixtcs6 4.19.0-9-amd64 #1 SMP Debian 4.19.118-2+deb10u1 (2020-06-07)
x86_64

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: Tue Apr 27 16:48:23 2021 from 192.168.30.1
kali@192.168.30.5:~$
```

Open other terminal and **check the following command output:**

```
user@machine:~$ netstat -tenpaul | grep 9050

tcp        0      0 127.0.0.1:9050          0.0.0.0:*               LISTEN
1002       122975593  3865/ssh
```

Using a proxy socks on Linux and command line tools (Proxychains4)

Create a file named proxyoptions.conf as follow:

```
strict_chain
remote_dns_subnet 224
tcp_read_time_out 15000
tcp_connect_time_out 8000
[ProxyList]
socks4  127.0.0.1 9050
```

Now you can use proxychains4 tools:

```
proxychains4 nmap -sT 192.168.100.0/24
proxychains4 firefox
proxychains4 ssh root@192.168.100.5
```

Congrats you have read the doc : {flag:aWNoZWNrZWR0aGVkb2M=}