Pwndb avec Termux sur android / f-droid via Tor

Recherche d'informations d'identification divulguées à l'aide du service Onion

Après micro-contributions au projet de David Tavarez pwndb[1] avec visée d'usage de termux[2] sur android / f-droid, note de prise en main.

Installation

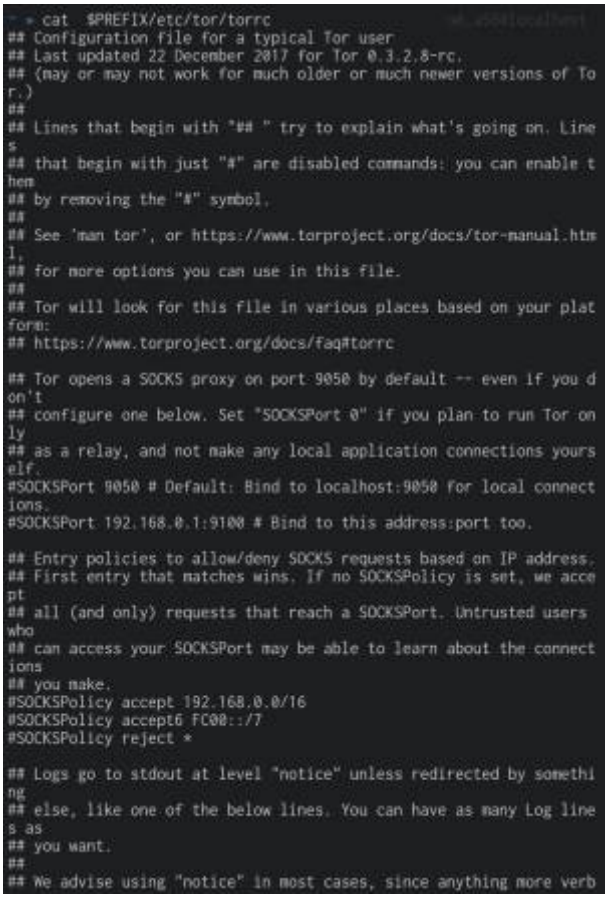
Pré-requis

1. Git : `$ pkg install git`
2. python
   - Comme archlinux, python de Termux est python3. `$ pkg install python` https://github.com/python/cpython
   - Après l'installation de python, le gestionnaire de paquets `pip` sera disponible. Pour installer les paquets python, vous pouvez utiliser `$ pip install [nom_du_paquet]`
     - Si nécessaire, car votre installation de python n'est pas récente, `$ pip intall –upgrade pip`
3. Virtualenvwrapper
   - `$ pip install virtualenv virtualenwrapper`
4. Tor : `$ pkg install tor` puis nous avons en option besoin de torsocks `$ pkg install torsocks`

Torsocks est une application permettant d'utiliser des applications réseau tels que SSH, IRSSI avec Tor. Torsocks permet d'utiliser la plupart des applications “socks-firendly” de façon plus sécurisée avec Tor.

Mise en place du service Onion

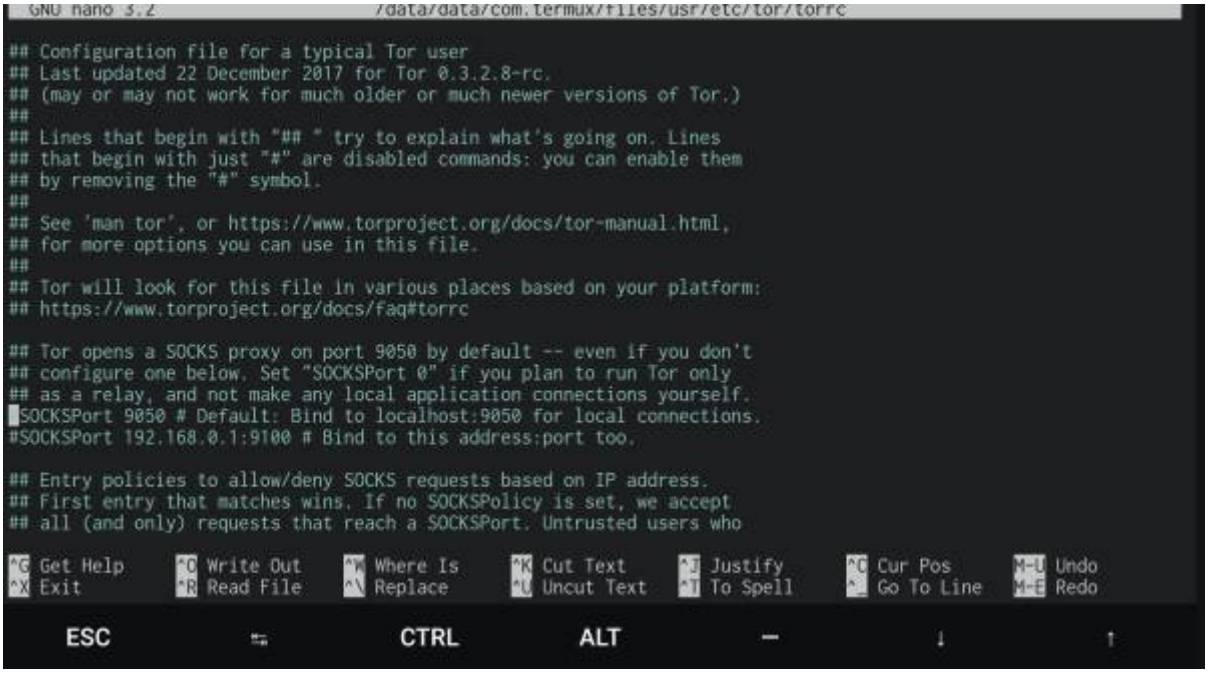
Vous devez modifier le fichier de configuration par défaut de tor `$PREFIX/etc/tor/tor/torrc`. Voici un exemple de l'état après installation



Pour pnwdb nous avons besoin d'un service tor opérationnel pour se connecter sur le port 9050. Vous pourvez aussi en profiter pour configurer un accès SSH comme ici

Le port 9050 est en place par défaut, mais vous pouvez personnaliser votre configuration

```
$ nano $PREFIX/etc/tor/tor/torrc
```



Install Pwndb

```
$ git clone https://github.com/davidtavarez/pwndb
Cloning into 'pwndb'...
remote: Enumerating objects: 10, done.
remote: Counting objects: 100% (10/10), done.
remote: Compressing objects: 100% (9/9), done.
remote: Total 10 (delta 2), reused 4 (delta 0), pack-reused 0
Unpacking objects: 100% (10/10), done.
```

```
$ cd pwndb

~/pwndb(master) » virtualenv venv
Using base prefix '/data/data/com.termux/files/usr'
New python executable in /Users/davidtavarez/pwndb/venv/bin/python
Installing setuptools, pip, wheel...done.
```

```
~/pwndb(master) » source venv/bin/activate
```

```
(venv)
~/pwndb(master) » pip install -r requirements.txt
Collecting PySocks==1.6.8 (from -r requirements.txt (line 1))
...
```

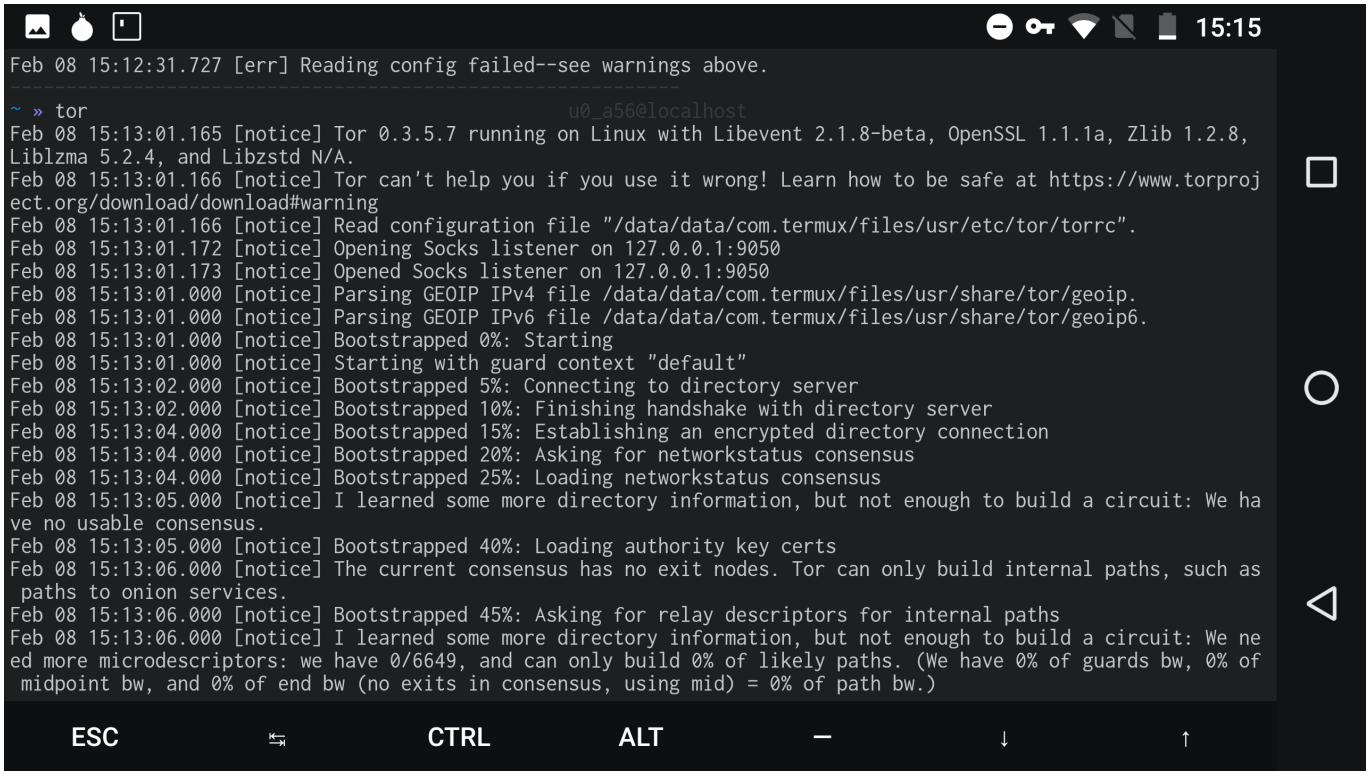
```
(venv)
~/pwndb(master) » python pwndb.py -h

usage: pwndb.py [-h] [--target TARGET] [--list LIST] [--output OUTPUT]

optional arguments:
  -h, --help       show this help message and exit
  --target TARGET  Target email/domain to search for leaks.
  --list LIST      A list of emails in a file to search for leaks.
  --output OUTPUT  Return results as json/txt
```

Usage

pwndb.py, par David Tavarez, est un outil en ligne de commande pour rechercher les informations d'identification divulguées en utilisant le service Onion, pwndb[…].onion

Avertissement légal : Utiliser pwndb.py pour attaquer des cibles sans avoir le consentement mutuel préalable est illégal. Il est de la responsabilité de l'utilisateur final d'obéir à toutes les lois locales, d'état et fédérales applicables. Les développeurs n'assument aucune responsabilité et ne sont pas responsables de toute mauvaise utilisation ou dommage causé.

Dans une première session termux lancer Tor ~» `tor`



Puis dans une seconde session, par exemple pour vérifier si des mots de passe d'accès à une addresse mail *ont fuité* :

```
(venv)
~/pwndb(master) » python pwndb.py --target testing@email.com
...
```

1)
dabord sur le code https://github.com/davidtavarez/pwndb/pull/8 puis sur la licence https://github.com/davidtavarez/pwndb/issues/9
2)
résolution de DNS sur le domaine termux.com SOA retourne darl.ns.cloudflare.com. dns.cloudflare.com. 2030032971 10000 2400 604800 3600 □ [Authenticated by DNSSEC]