

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 Tavares [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 install --upgrade pip`
3. [Virtualenvwrapper](#)
 - `$ pip install virtualenv virtualenvwrapper`
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-friendly" de façon plus sécurisée avec Tor.

Mise en place du service Onion

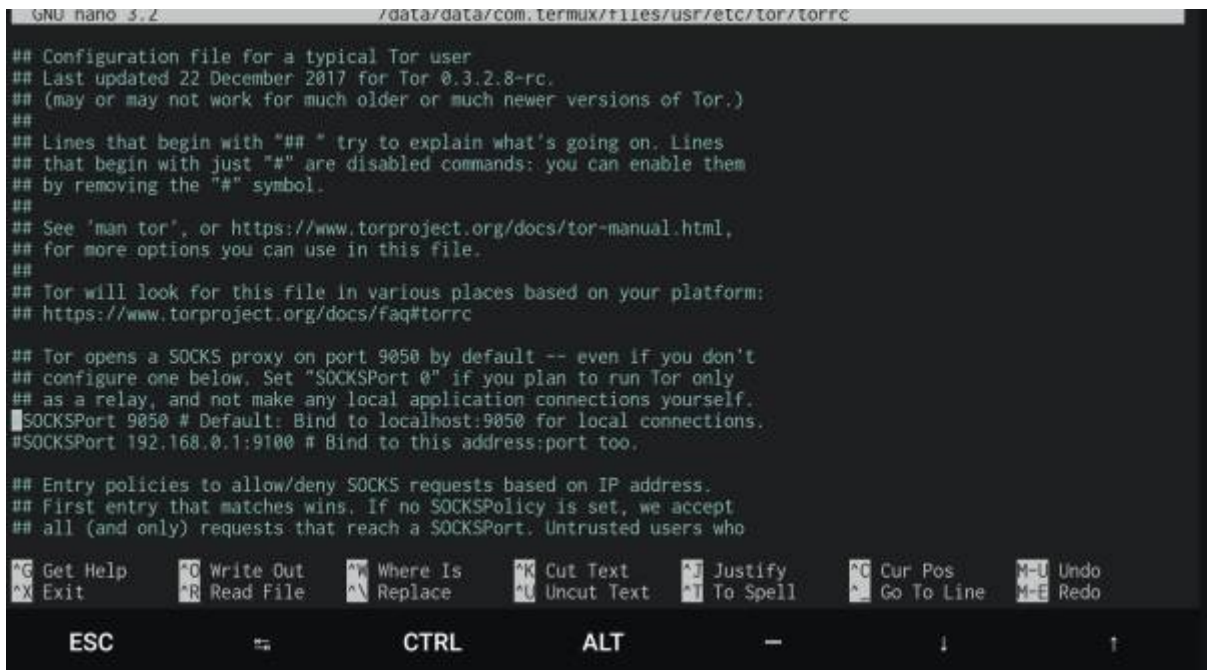
Vous devez modifier le fichier de configuration par défaut de tor `$PREFIX/etc/tor/tor/torrc`. Voici un exemple de l'état après installation

```
~ = cat $PREFIX/etc/tor/torrc
## Configuration file for a typical Tor user
## Last updated 22 December 2017 for Tor 0.3.2.8-rc.
## (may or may not work for much older or much newer versions of Tor.)
##
## Lines that begin with "## " try to explain what's going on. Lines
## that begin with just "#" are disabled commands: you can enable them
## by removing the "#" symbol.
##
## See 'man tor', or https://www.torproject.org/docs/tor-manual.html,
## for more options you can use in this file.
##
## Tor will look for this file in various places based on your platform:
## https://www.torproject.org/docs/faq#torrc
##
## Tor opens a SOCKS proxy on port 9050 by default -- even if you don't
## configure one below. Set "SOCKSPort 0" if you plan to run Tor only
## as a relay, and not make any local application connections yourself.
##SOCKSPort 9050 # Default: Bind to localhost:9050 for local connections.
##SOCKSPort 192.168.0.1:9100 # Bind to this address:port too.
##
## Entry policies to allow/deny SOCKS requests based on IP address.
## First entry that matches wins. If no SOCKSPolicy is set, we accept
## all (and only) requests that reach a SOCKSPort. Untrusted users who
## can access your SOCKSPort may be able to learn about the connections
## you make.
##SOCKSPolicy accept 192.168.0.0/16
##SOCKSPolicy accept6 FC00::/7
##SOCKSPolicy reject *
##
## Logs go to stdout at level "notice" unless redirected by something
## else, like one of the below lines. You can have as many Log lines
## as you want.
##
## We advise using "notice" in most cases, since anything more verb
```

Pour pwndb nous avons besoin d'un service tor opérationnel pour se connecter sur le port 9050. Vous pouvez 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 Tavaréz, 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`

```

Feb 08 15:12:31.727 [err] Reading config failed--see warnings above.
~ » tor
Feb 08 15:13:01.165 [notice] Tor 0.3.5.7 running on Linux with Libevent 2.1.8-beta, OpenSSL 1.1.1a, Zlib 1.2.8,
Liblzma 5.2.4, and Libzstd N/A.
Feb 08 15:13:01.166 [notice] Tor can't help you if you use it wrong! Learn how to be safe at https://www.torproj
ect.org/download/download#warning
Feb 08 15:13:01.166 [notice] Read configuration file "/data/data/com.termux/files/usr/etc/tor/torrc".
Feb 08 15:13:01.172 [notice] Opening Socks listener on 127.0.0.1:9050
Feb 08 15:13:01.173 [notice] Opened Socks listener on 127.0.0.1:9050
Feb 08 15:13:01.000 [notice] Parsing GEOIP IPv4 file /data/data/com.termux/files/usr/share/tor/geoip.
Feb 08 15:13:01.000 [notice] Parsing GEOIP IPv6 file /data/data/com.termux/files/usr/share/tor/geoip6.
Feb 08 15:13:01.000 [notice] Bootstrapped 0%: Starting
Feb 08 15:13:01.000 [notice] Starting with guard context "default"
Feb 08 15:13:02.000 [notice] Bootstrapped 5%: Connecting to directory server
Feb 08 15:13:02.000 [notice] Bootstrapped 10%: Finishing handshake with directory server
Feb 08 15:13:04.000 [notice] Bootstrapped 15%: Establishing an encrypted directory connection
Feb 08 15:13:04.000 [notice] Bootstrapped 20%: Asking for networkstatus consensus
Feb 08 15:13:04.000 [notice] Bootstrapped 25%: Loading networkstatus consensus
Feb 08 15:13:05.000 [notice] I learned some more directory information, but not enough to build a circuit: We ha
ve no usable consensus.
Feb 08 15:13:05.000 [notice] Bootstrapped 40%: Loading authority key certs
Feb 08 15:13:06.000 [notice] The current consensus has no exit nodes. Tor can only build internal paths, such as
paths to onion services.
Feb 08 15:13:06.000 [notice] Bootstrapped 45%: Asking for relay descriptors for internal paths
Feb 08 15:13:06.000 [notice] I learned some more directory information, but not enough to build a circuit: We ne
ed more microdescriptors: we have 0/6649, and can only build 0% of likely paths. (We have 0% of guards bw, 0% of
midpoint bw, and 0% of end bw (no exits in consensus, using mid) = 0% of path bw.)

```

Puis dans une seconde session, par exemple pour vérifier si des mots de passe d'accès à une adresse 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]

From: <https://notecc.frama.wiki/> - **Note CC**

Permanent link: https://notecc.frama.wiki/norae:si:infosec_note-recherche-1

Last update: **2019/02/08 18:30**

