Table of Contents

Making SSH available as a hidden service

This page describes how to setup a hidden service for SSH in Tor. For greater security, it is advised to follow these 2 documents first (in this particular order):

1. Making use of the BCM2708 hardware RNG
2. OpenSSH Hardening

While SSH is responsible for transport security and authentication, Tor will take care of the anonymization of your connection.

Install and configure Tor

On a Debian system, you would install Tor like this (if we're updating already, we might as well check for new firmware and so on):

```
# apt-get update
# apt-get upgrade
# rpi-update
# apt-get -y install tor
```

Thats about it.

Setting up the hidden service

Edit your `/etc/tor/torrc` to include these lines, adapting paths and file names where necessary:

```
SocksPolicy reject *
Log notice file /var/log/tor/notices.log
DataDirectory /var/lib/tor

# ssh hidden service
HiddenServiceDir /var/lib/tor/ssh/
# TorPort RealHost:RealPort
HiddenServicePort 22 127.0.0.1:22
```

Then restart Tor:

```
# /etc/init.d/tor restart
```

After restarting, you can find your .onion hostname the `/var/lib/tor/ssh/hostname` file. Make sure you never give away your private key (`/var/lib/tor/ssh/private_key`), otherwise other people can impersonate your .onion hostname.

Making SSH listen to incoming connections via Tor

IMPORTANT: In case you use the same server to accept connections over the clear net, make sure you have dedicated host keys for the clearnet ssh and the tor ssh! See here for details.

Edit your `/etc/ssh/sshd_config` and update it to include these settings:

```
Port 22
ListenAddress 127.0.0.1
```

The sshd has to listen on the same port on loopback as you configured in the torrc hidden service config.

Connect to your hidden service

Install `netcat` (sometimes named `nc`). Make sure you have Tor installed and running on the client end. Create a section for your hidden service in your `~/.ssh/config` file, adapting the HostName and ProxyCommand as necessary:

```
Host tor-ssh
  IdentitiesOnly yes
  IdentityFile ~/.ssh/id_ed25519
  HostName 1tl9dcp2xzvjhuso.onion
  ProxyCommand /usr/bin/nc -x127.0.0.1:9050 -X5 %h %p
```

Connect your hidden service:

```
# ssh root@tor-ssh
```

We're done. Of course the Tor network isn't the fastest when it comes to latency, but you can always opt-in to provide another exit node if you happen to have the resources to do so.

crypto, tor, openssh

From:
http://wiki.geiges.net/ - **DokuWiki**

Permanent link:
http://wiki.geiges.net/doku.php?id=ssh_tor

Last update: **2018/01/03 22:10**