SSH FOR HACKING

Cristian Cezar Moisés

February 18, 2024

Dedicate to all my teachers, friends and family.

Contents

Abstract: In this research we do analysis for using techniques to ssh usage with high level of security and obfuscation.

1 [Introduction]

One of the most secure tools to connect two devices over the internet are openssh. Created in december 1999 by OpenBSD developers. [1, OpenSSH is a derivative of the original free ssh 1.2.12 release from Tatu Ylönen. That version was the last one free enough for reuse. Parts of OpenSSH still bear Tatu's license, which was contained in that release. That version, and earlier ones, used mathematical functions from the libgmp library, which was directly included at the time. It is now made available under the Lesser GNU Public License, but versions of that era were under the regular GNU Public License.] The project page on Github. We join the disposable root servers avaiable from the THC. Many services are avaiable for automate the work with OpenSSH servers.One of this projects are Segfault created by THC(**The Hackers Choice**). We start joining the service with Tor for obfuscation and anonymity.

2 [Research]

Disposable servers are good for automate the work with openssh; and we use tor for increase the level of security and anonimity over the internet. See the following command :

```
$ torify ssh root@adm.segfault.net
```

Now type the password: **segfault**
The server return you a result like this:

```
################################################################
Thereafter use these commands:
--> ssh  aroundwisdom
--> sftp aroundwisdom
--> scp  aroundwisdom:stuff.tar.gz ~/
--> sshfs -o reconnect aroundwisdom:/sec ~/sec
----------------------------------------------------------------
Token              : No See https://thc.org/segfault/token
Your workstation   : 200.101.113.232    (Sao Paulo/Brazil)
Reverse Port       : Type curl sf/port for reverse port.
Exit CryptoStorm   : 185.117.118.23  (Finland)
Exit Mullvad       : 146.70.197.254  (Copenhagen/Denmark)
Exit NordVPN       : 94.101.114.253  (Zurich/Switzerland)
TOR Proxy          : 172.20.0.111:9050
Shared storage     : /everyone/AroundWisdom
(encrypted)
Your storage       : /sec
(encrypted)
Your Onion WWW     : /onion
(encrypted)
Your Web Page
http://2xyr7jug4.onion/aroundwisdom/
SSH                : ssh -o "SetEnv␣SECRET=twbr" \
root@adm.segfault.net
SSH (TOR)          : torsocks ssh -o "SetEnv
SECRET=twbr" \
root@twbr.onion
SSH (gsocket)      : gsocket -s NG ssh -o "SetEnv
SECRET=twbr" \
root@adm.segfault.gsocket
```

**All data listed above are fake and used for representation only.*

3 [Anonymity]

Segfault has two domains for access: **lsd.segfault.net** *(Used for terminal)* and **adm.segfault.net** *(Used on the website ShellSegfault.)*

Tor has many layers for protect user privacy online and Segfault has two domains but domain *lsd.segfault* cant joint another session in *lsd.segfault.net.* With many tests we achieved a sucessfull connection using *adm.segfault.net* to *lsd.segfault.net*; and the same using *lsd.segfault.net* to *adm.segfault.net.*

We used:

```
$ torify ssh root@adm.segfault.net
```

And when the connection are sucessfull we connect to another server using:

```
$ ssh root@lsd.segfault.net
```

Some tor ip address are blocked because are used for illegal purposes, so all we can do are connecting first to the server adm.segfault using torify and no torify on the other connections.

After the final test of efficiency we got some latency but we are navigating into 12 layers of tor connections; a high level of privacy and anonymity for research.

References

[1] OpenSSH History on OpenBSD website;*visited 18/02/2024*.