An Introduction to Linux Memory Forensics

proneer

http://forensic-proof.com

Security is a people problem…

JK Kim

Outline

1. Live Forensics

2. Memory Forensics

Live Forensics

Live LISTs (aimed at Ubuntu)

- **Storage/Partition/File System Information**
  - fdisk –l
  - cat /proc/scsi/scsi
  - cat /proc/ide
  - cat /proc/diskstats
  - cat /proc/partitions
  - df -h
- **Mudules**
  - cat /proc/modules
  - lsmod

Live LISTs (aimed at Ubuntu)

- **System Information**
  - uname –a
  - uptime
  - cat /proc/version
  - cat /proc/cpuinfo

- **Installed Software**
  - dpkg --get-selections,
  - cat /var/log/dpkg.log

Live LISTs (aimed at Ubuntu)

- **Process Status**
  - ps -elf
- **Scheduling, Start programs**
  - cat /etc/crontab
  - ls /etc/init.d/*
- **Routing Table**
  - netstat –rn
- **Network Interface, Hosts**
  - ifconfig -a
  - cat /etc/hosts

Live LISTs (aimed at Ubuntu)

- **ARP Table**
  - arp -a

- **Network Status**
  - netstat -anp

- **Open Files & Sockets**
  - lsof –i -P –n

- **Recent Command**
  - cat bash_history

Live LISTs (aimed at Ubuntu)

- **Account**
  - cat /etc/passwd
  - cat /etc/shadow
  - cat /etc/group
- **User Activity**
  - w
  - finger –lmsp
  - Last
- **Boot Message**
  - dmesg

Live LISTs (aimed at Ubuntu)

- **Print Queues**
  - /var/spool/lpd/lp/*
- **Run Level**
  - runlevel
- **Swap Partition**
  - cat /proc/swaps

Live LISTs (aimed at Ubuntu)

- **Memory Information**
  - cat /proc/meminfo
  - cat /proc/<pid>/maps
  - cat /proc/iomem
  - cat /proc/slabinfo
  - cat /proc/vmallocinfo
  - cat /proc/vmstat
  - vmstat

Memory Forensics

Memory Forensics

Targets

- **System Memory**
  - /dev/mem ➔ It have limits to access whole physical memory area.

- **Kernel Memory**
  - /dev/kmem

Memory Dump Tools

- **fmem** (http://hysteria.sk/~niekt0/foriana/fmem_current.tgz)
  - fmem is LKM(Linux Kernel Module) to access /dev/fmem without limitations.
  - The tool behave direct access to physical memory similarly /dev/mem.
  - The physical memory can be copied using dd-like tools.

- **LiME** (http://code.google.com/p/lime-forensics/)
  - LiME is LKM(Linux Kernel Module) to acquire volatile memory.
  - The tools also supports acquiring Android and dumping over the network.

- **Second Look®: The Linux Memory Forensic Acquisition** (http://secondlookforensics.com/)
  - This tool is commercial forensic solution with modified crash driver and a script dumping memory using driver.

fmem

- **fmem** (**http://hysteria.sk/~niekt0/foriana/fmem_current.tgz**)

1. **wget** http://hysteria.sk/~niekt0/foriana/fmem_current.tgz
2. **tar –xvf** fmem_current.tgz
3. **$ make** (➔compile)
4. **$ ./run.sh (➔** load LKM)
5. **$ dd** if=/dev/fmem of=/var/tmp/fmem_dump.dd bs=1MB count…

```
root@ubuntu:/var/tmp# lsmod | grep fmem
fmem                  13001  0
root@ubuntu:/var/tmp# dd if=/dev/fmem of=./fmem_dump.dd bs=1MB
535+0 records in
535+0 records out
535000000 bytes (535 MB) copied, 20.8761 s, 25.6 MB/s
root@ubuntu:/var/tmp# ll
total 522472
-rw-r--r--  1 root root 535000000 2012-05-12 09:32 fmem_dump.dd
```

LiME

- **LiME** (**http://code.google.com/p/lime-forensics/**)

1. **svn** checkout ***http***://lime-forensics.googlecode.com/svn/trunk/ lime-forensics-read-only
2. **$ make** (➔compile)
3. **$ insmod lime.ko path=<target dir> (➔** load LKM)

```
root@ubuntu:/var/tmp# ls
lime.ko
root@ubuntu:/var/tmp# insmod  lime.ko  path=/var/tmp
root@ubuntu:/var/tmp# ll
total 1046256
-r--r--r--  1 root root 534708224 2012-05-12 09:42 1336840920_100000_1feeffff.pdump
-r--r--r--  1 root root    587776 2012-05-12 09:42 1336840920_10000_9f7ff.pdump
-r--r--r--  1 root root   1048576 2012-05-12 09:42 1336840920_1ff00000_1fffffff.pdump
root@ubuntu:/var/tmp# lsmod | grep lime
lime                   12686  0
root@ubuntu:/var/tmp#
```

Memory Analysis Tools

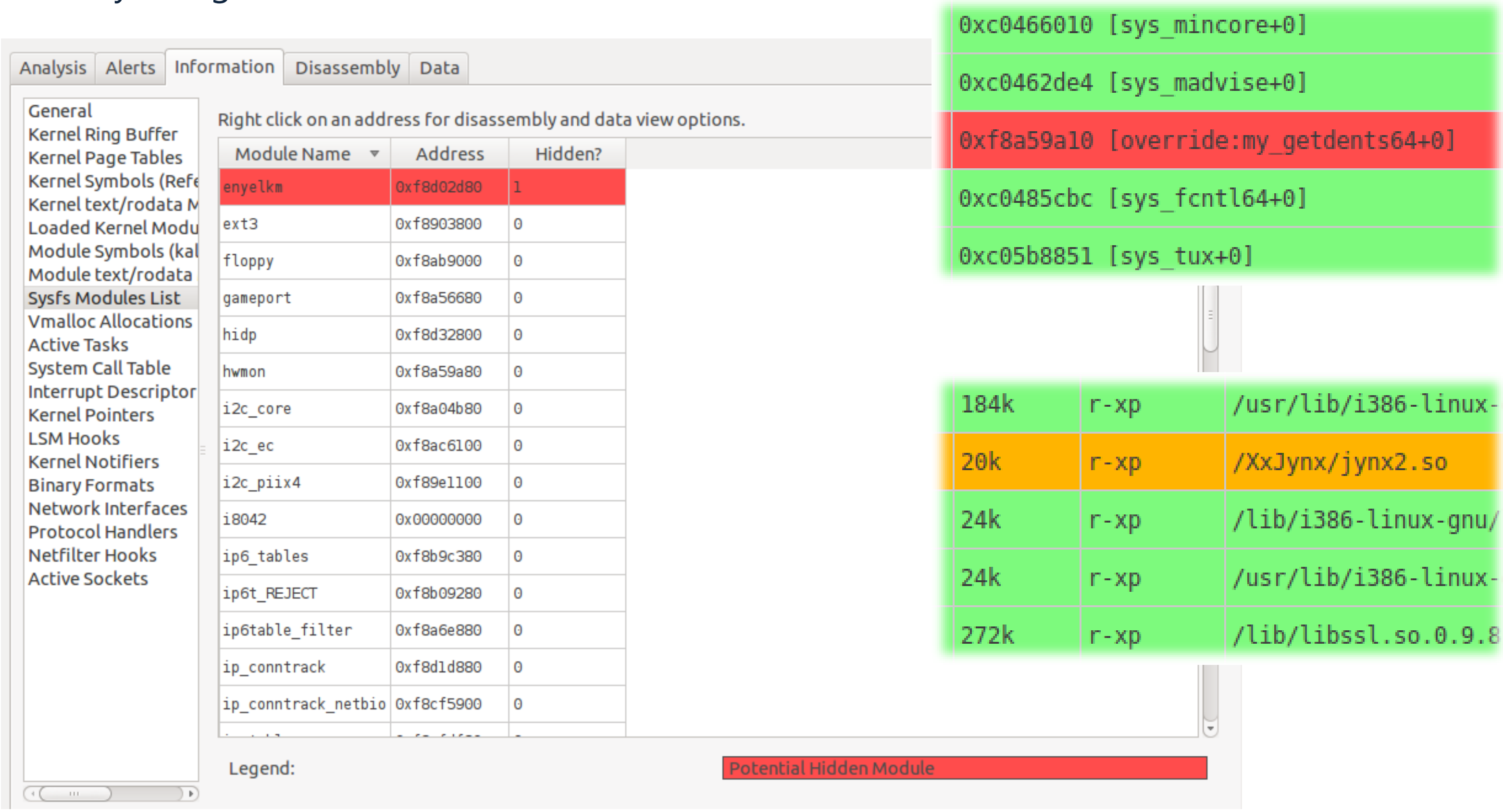
- **Foriana** (http://hysteria.sk/~niekt0/foriana/)
  - Foriana is tool for extracts such as process, modules, … from physical memory image (fmem).
  - Commands
    - ✓ --list-modules
    - ✓ --list-processes
    - ✓ --list-files
    - ✓ --magic-module
    - ✓ --magic-process
    - ✓ --magic-user-process
    - ✓ --create-process/module-pattern
    - ✓ --debug
    - ✓ … …

Memory Analysis Tools

- **Volatilitux** (http://code.google.com/p/volatilitux/)
  - Volatilitux is to analyzing linux physical memory with python-based.
  - Supports Architectures
    - ✓ ARM, x86, x86 with PAE enabled
  - Commands
    - ✓ pslist, memmap, memdmp, filelist, filedmp
  - Tested Machines
    - ✓ Android 2.1
    - ✓ Fedora 5 and 8
    - ✓ Debian 5
    - ✓ CentOS 5
    - ✓ Ubuntu10.10 with and without PAE

Memory Analysis Tools

- **Second Look®: The Linux Memory Forensic Analysis** (http://secondlookforensics.com/)
  - This tool is commercial forensic solution with modified crash driver and a script dumping memory using driver.



Right click on an address for disassembly and data view options.

Module Name	Address	Hidden?
enyelkm	0xf8d02d80	1
ext3	0xf8903800	0
floppy	0xf8ab9000	0
gameport	0xf8a56680	0
hidp	0xf8d32800	0
hwmon	0xf8a59a80	0
i2c_core	0xf8a04b80	0
i2c_ec	0xf8ac6100	0
i2c_piix4	0xf89e1100	0
i8042	0x00000000	0
ip6_tables	0xf8b9c380	0
ip6t_REJECT	0xf8b09280	0
ip6table_filter	0xf8a6e880	0
ip_conntrack	0xf8d1d880	0
ip_conntrack_netbio	0xf8cf5900	0

Legend: 🟥 Potential Hidden Module

```
0xc0466010 [sys_mincore+0]
0xc0462de4 [sys_madvise+0]
0xf8a59a10 [override:my_getdents64+0]
0xc0485cbc [sys_fcntl64+0]
0xc05b8851 [sys_tux+0]
```

```
184k   r-xp   /usr/lib/i386-linux-
20k    r-xp   /XxJynx/jynx2.so
24k    r-xp   /lib/i386-linux-gnu/
24k    r-xp   /usr/lib/i386-linux-
272k   r-xp   /lib/libssl.so.0.9.8
```

Memory Analysis Tools

- **In addition to that …**
  - **Volatility Framework for Linux** (http://code.google.com/p/volatility/wiki/LinuxMemoryForensics)
  - **Draugr** (http://code.google.com/p/draugr/)
  - **Read Hat Crash Utility** (http://people.redhat.com/anderson/)
  - **Idetect** (http://forensic.seccure.net/)
  - **Forensic Analysis Toolkit (FATKit)**

Question?