МІНІСТЕРСТВО ОСВІТИ І НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ІМЕНІ ІГОРЯ СІКОРСЬКОГО»
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
Кафедра Інформаційної Безпеки

Аналіз та моніторинг кібербезпеки

Практичне завдання №2

Аналіз пам’яті у системі Linux

Перевірив:
Козленко О. В.

Виконав:
студент IV курсу
групи ФБ-01
Сахній Н. Р.

Київ 2024

Мета: Отримання практичних навичок з пошуку та збору цифрових артефактів в ОС Linux.

Завдання: Отримати повну інформацію про стан файлової системи у Linux, створити образ та проаналізувати його. Створити за допомогою утиліти LiME образ оперативної пам'яті системи. Проаналізувати стан працюючої системи за допомогою утіліти SysScout.

1. Перелік та отримання розділів

- Після отримання списку усіх доступних дисків та інформації про їх наявні розділи, створимо **dd** образ жорсткого диска (**/dev/sda**):

```
lab@ua:~$ sudo fdisk -l | grep -in "sda" -A 10
49:Disk /dev/sda: 25 GiB, 26843545600 bytes, 52428800 sectors
50-Disk model: VBOX HARDDISK
51-Units: sectors of 1 * 512 = 512 bytes
52-Sector size (logical/physical): 512 bytes / 512 bytes
53-I/O size (minimum/optimal): 512 bytes / 512 bytes
54-Disklabel type: dos
55-Disk identifier: 0xa45a9db6
56-
57-Device     Boot   Start      End  Sectors  Size Id Type
58:/dev/sda1  *       2048  1050623  1048576  512M  b W95 FAT32
59:/dev/sda2       1052670 52426751 51374082 24,5G  5 Extended
60:/dev/sda5       1052672 52426751 51374080 24,5G 83 Linux
61-
62-
63-Disk /dev/loop8: 91,7 MiB, 96141312 bytes, 187776 sectors
64-Units: sectors of 1 * 512 = 512 bytes
65-Sector size (logical/physical): 512 bytes / 512 bytes
66-I/O size (minimum/optimal): 512 bytes / 512 bytes
67-
68-
69-Disk /dev/loop9: 50,98 MiB, 53432320 bytes, 104360 sectors
70-Units: sectors of 1 * 512 = 512 bytes
```

```
lab@ua:~$ sudo dd if=/dev/sda of=tpext.img bs=2M status=progress count=4096
8388608000 bytes (8,4 GB, 7,8 GiB) copied, 275 s, 30,5 MB/s
4096+0 records in
4096+0 records out
8589934592 bytes (8,6 GB, 8,0 GiB) copied, 276,368 s, 31,1 MB/s
```

```
lab@ua:~$ ls -l ./tpext.img
-rw-r--r-- 1 root root 8589934592 лют 14 15:10 ./tpext.img
```

2. Отримання пам'яті системи Linux

- За допомогою утиліти **LiME** отримаємо вміст RAM після побудови деякого бінарника із використанням команди **make**:

```
lab@ua:~/Downloads$ git clone https://github.com/504ensicsLabs/LiME/
Cloning into 'LiME'...
remote: Enumerating objects: 370, done.
remote: Counting objects: 100% (21/21), done.
remote: Compressing objects: 100% (17/17), done.
remote: Total 370 (delta 10), reused 12 (delta 4), pack-reused 349
Receiving objects: 100% (370/370), 1.61 MiB | 4.99 MiB/s, done.
Resolving deltas: 100% (199/199), done.
```

```
lab@ua:~/Downloads/LiME/src$ make
make -C /lib/modules/5.15.0-91-generic/build M="/home/lab/Downloads/LiME/src" modules
make[1]: Entering directory '/usr/src/linux-headers-5.15.0-91-generic'
  CC [M]  /home/lab/Downloads/LiME/src/tcp.o
  CC [M]  /home/lab/Downloads/LiME/src/disk.o
  CC [M]  /home/lab/Downloads/LiME/src/main.o
  CC [M]  /home/lab/Downloads/LiME/src/hash.o
  CC [M]  /home/lab/Downloads/LiME/src/deflate.o
  LD [M]  /home/lab/Downloads/LiME/src/lime.o
  MODPOST /home/lab/Downloads/LiME/src/Module.symvers
  CC [M]  /home/lab/Downloads/LiME/src/lime.mod.o
  LD [M]  /home/lab/Downloads/LiME/src/lime.ko
  BTF [M] /home/lab/Downloads/LiME/src/lime.ko
Skipping BTF generation for /home/lab/Downloads/LiME/src/lime.ko due to unavailability of vmlinux
make[1]: Leaving directory '/usr/src/linux-headers-5.15.0-91-generic'
strip --strip-unneeded lime.ko
mv lime.ko lime-5.15.0-91-generic.ko
```

```
lab@ua:~/Downloads/LiME/src$ ls
deflate.c  disk.c  hash.c  lime-5.15.0-91-generic.ko  lime.mod    lime.mod.o  main.c  Makefile         modules.order   tcp.c
deflate.o  disk.o  hash.o  lime.h                     lime.mod.c  lime.o      main.o  Makefile.sample  Module.symvers  tcp.o
```

```
lab@ua:~/Downloads/LiME/src$ sudo insmod ./lime-5.15.0-91-generic.ko "path=../Linux_Memory.mem format=raw"
lab@ua:~/Downloads/LiME/src$ ls -lah ../Linux_Memory.mem
-r--r--r-- 1 root root 4,0G лют 14 15:29 ../Linux_Memory.mem
lab@ua:~/Downloads/LiME/src$
```

3. SysScout Tool

- Проведемо аналіз системи Linux в реальному часі та отримаємо інформацію про операційну систему, часові позначки, інформацію про **HOST** і **DNS**, інформацію про пам’ять, користувача, який увійшов у систему, та останніх користувачів, які ввійшли в систему:

```
lab@ua:~/Downloads$ git clone https://github.com/joshbrunty/SysScout
Cloning into 'SysScout'...
remote: Enumerating objects: 108, done.
remote: Total 108 (delta 0), reused 0 (delta 0), pack-reused 108
Receiving objects: 100% (108/108), 27.11 KiB | 1.00 MiB/s, done.
Resolving deltas: 100% (50/50), done.
```

```
lab@ua:~/Downloads$ cd SysScout/
lab@ua:~/Downloads/SysScout$
lab@ua:~/Downloads/SysScout$ bash ./SysScout.sh
```

```
-----------------------------------------


  _____                 _____                  _
 / ____|               / ____|                | |
| (___   _   _  ___   | (___    ___  ___   _  | |_
 \___ \ | | | |/ __|  \___ \  / __|/ _ \ | | | || __|
 ____) || |_| |\__ \  ____) || (__| (_) || |_| || |_
|_____/  \__, ||___/ |_____/  \___|\___/  \__,_| \__|
          __/ |v.1.0.3
         |___/
-----------------------------------------
A Network Forensics/Incident Response Tool
By: Josh Brunty: josh [dot] brunty [at] marshall [dot] edu
-----------------------------------------
Current Local Machine Date & Time : середа, 14 лютого 2024 15:52:52 +0200
--------------------------
   Main Menu
--------------------------
1. Operating System Info
2. Time Info
3. HOST and DNS Info
4. Network Info
5. Who is Online
6. Last Logged In Users
7. Memory Information
8. Exit
```

```
Enter your choice [ 1 - 8 ]: 1
-------------------------------------------------------------
      Operating System Information
-------------------------------------------------------------
Operating system : ua.sakhnii.com GNU/Linux
Operating System Version : #101~20.04.1-Ubuntu SMP Thu Nov 16 14:22:28 UTC 2023 x86_64
```

```
Enter your choice [ 1 - 8 ]: 2
-------------------------------------------------------------
      Time Information
-------------------------------------------------------------
Local Machine Time : 15:48
Local Machine Timezone : EET
Local Machine Date : 02-14-24
```

```
Enter your choice [ 1 - 8 ]: 3
-------------------------------------------------------------
      Hostname and DNS information
-------------------------------------------------------------
Hostname : ua
DNS domain : sakhnii.com
Fully qualified domain name : ua.sakhnii.com
Network address (IP) :  192.168.50.22
DNS name servers (DNS IP) : 127.0.0.53
```

```
Enter your choice [ 1 - 8 ]: 4
-------------------------------------------------------------
      Network information
-------------------------------------------------------------
Total network interfaces found : 1
----------------------
--- IP Address Info ---
----------------------
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    inet 192.168.50.22/24 brd 192.168.50.255 scope global dynamic noprefixroute enp0s3
       valid_lft 80752sec preferred_lft 80752sec
----------------------
--- Network Routing ---
----------------------
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
0.0.0.0         192.168.50.1    0.0.0.0         UG        0 0          0 enp0s3
169.254.0.0     0.0.0.0         255.255.0.0     U         0 0          0 enp0s3
192.168.50.0    0.0.0.0         255.255.255.0   U         0 0          0 enp0s3
-----------------------------------
--- Interface Traffic information  ---
-----------------------------------
Kernel Interface table
Iface      MTU    RX-OK RX-ERR RX-DRP RX-OVR    TX-OK TX-ERR TX-DRP TX-OVR Flg
enp0s3    1500   201051      0      0 0         18331      0      0      0 BMRU
lo       65536     1723      0      0 0          1723      0      0      0 LRU
-----------------------------
--- MAC/Hardware Addresses ---
-----------------------------
08:00:27:56:13:cc
00:00:00:00:00:00
```

```
Enter your choice [ 1 - 8 ]: 5
-------------------------------------------------------------
      Who is online
-------------------------------------------------------------
NAME     LINE         TIME             COMMENT
lab      :0           2024-02-14 14:19 (:0)
```

```
Enter your choice [ 1 - 8 ]: 6
------------------------------------------------------------
      List of last logged in users
------------------------------------------------------------
lab      :0           :0               Wed Feb 14 14:19   still logged in
reboot   system boot  5.15.0-91-generi Wed Feb 14 14:16   still running
reboot   system boot  5.15.0-91-generi Wed Feb 14 14:14   still running
alice    :0           :0               Thu Jan  4 21:35 - crash (40+16:38)
reboot   system boot  5.15.0-91-generi Thu Jan  4 21:31   still running
lab      :0           :0               Thu Jan  4 21:30 - crash  (00:01)
alice    pts/0                         Thu Jan  4 21:28 - 21:28  (00:00)
alice    pts/0                         Thu Jan  4 21:26 - 21:26  (00:00)
lab      :0           :0               Thu Jan  4 14:41 - 21:29  (06:47)
reboot   system boot  5.15.0-91-generi Thu Jan  4 14:32   still running
lab      :0           :0               Thu Jan  4 14:25 - down   (00:07)
reboot   system boot  5.15.0-91-generi Thu Jan  4 14:22 - 14:32  (00:09)

wtmp begins Thu Jan  4 14:22:39 2024
```

```
Enter your choice [ 1 - 8 ]: 7
------------------------------------------------------------
      Free and used memory
------------------------------------------------------------
              total        used        free      shared  buff/cache   available
Mem:           3912         832         130          19        2949        2780
Swap:          1162           2        1160
---------------------------------
--- Virtual Memory Statistics ---
---------------------------------
procs -----------memory---------- ---swap-- -----io---- -system-- ------cpu-----
 r  b   swpd   free   buff  cache   si   so    bi    bo   in   cs us sy id wa st
 0  0   2060 133364  46952 2973692    0    0  3297  3649  247  232  3  3 76 18  0
---------------------------------------
--- Top 5 Memory Utilizing Processes ---
---------------------------------------
lab         1784  1.2  9.5 4254684 381848 ?      Ssl  14:19   1:10  \_ /usr/bin/gnome-shell
lab         1575  0.8  2.2 874160 90300 tty2     Sl+  14:19   0:50          \_ /usr/lib/xorg/Xorg vt2 -
ty -verbose 3
lab         2659  0.2  1.1 818060 47588 ?        Ssl  14:33   0:11  \_ /usr/libexec/gnome-terminal-serv
lab         2117  0.0  1.1 827992 45664 ?        Sl   14:20   0:00  |   \_ update-notifier
lab         1975  0.0  1.3 714456 54184 ?        Sl   14:19   0:00  |   \_ /usr/libexec/evolution-data-
```

```
Enter your choice [ 1 - 8 ]: 8
Happy Forensicating. Go Herd! Follow us on Twitter: @joshbrunty @MUDigForensics
lab@ua:~/Downloads/SysScout$
```

4. Аналіз необробленого зображення

```
lab@ua:~$ sudo dd if=/dev/sda1 of=fat32.img bs=4k status=progress
131072+0 records in
131072+0 records out
536870912 bytes (537 MB, 512 MiB) copied, 0,92417 s, 581 MB/s
```

- Перевіримо, чи належить образ до типу диска чи розділу, скориставшись командою **mmls**:

```
lab@ua:~$ mmls fat32.img
Cannot determine partition type
```

```
lab@ua:~$ mmls tpext.img
DOS Partition Table
Offset Sector: 0
Units are in 512-byte sectors

      Slot      Start        End          Length       Description
000:  Meta      0000000000   0000000000   0000000001   Primary Table (#0)
001:  -------   0000000000   0000002047   0000002048   Unallocated
002:  000:000   0000002048   0001050623   0001048576   Win95 FAT32 (0x0b)
003:  -------   0001050624   0001052671   0000002048   Unallocated
004:  Meta      0001052670   0052426751   0051374082   DOS Extended (0x05)
005:  Meta      0001052670   0001052670   0000000001   Extended Table (#1)
006:  001:000   0001052672   0052426751   0051374080   Linux (0x83)
```

- За допомогою команди **fsstat** визначимо типу розділу:

```
lab@ua:~$ fsstat fat32.img
FILE SYSTEM INFORMATION
--------------------------------------------
File System Type: FAT32

OEM Name: mkfs.fat
Volume ID: 0xe929e05c
Volume Label (Boot Sector): NO NAME
Volume Label (Root Directory):
File System Type Label: FAT32
Next Free Sector (FS Info): 2080
Free Sector Count (FS Info): 1046488

Sectors before file system: 2048

File System Layout (in sectors)
Total Range: 0 - 1048575
* Reserved: 0 - 31
** Boot Sector: 0
** FS Info Sector: 1
** Backup Boot Sector: 6
* FAT 0: 32 - 1055
* FAT 1: 1056 - 2079
```

```
* Data Area: 2080 - 1048575
** Cluster Area: 2080 - 1048575
*** Root Directory: 2080 - 2087

METADATA INFORMATION
------------------------------------------
Range: 2 - 16743942
Root Directory: 2

CONTENT INFORMATION
------------------------------------------
Sector Size: 512
Cluster Size: 4096
Total Cluster Range: 2 - 130813

FAT CONTENTS (in sectors)
------------------------------------------
2080-2087 (8) -> EOF
```

- Використаємо команду “**ils –a**”, щоб вивести інформацію про inode та знайти список записів MFT:

```
lab@ua:~$ ils -a fat32.img
class|host|device|start_time
ils|ua.sakhnii.com||1707920231
st_ino|st_alloc|st_uid|st_gid|st_mtime|st_atime|st_ctime|st_crtime|st_mode|st_nlink|st_size
2|a|0|0|0|0|0|0|0|1|4096
16743939|a|0|0|0|0|0|0|0|1|512
16743940|a|0|0|0|0|0|0|0|1|524288
16743941|a|0|0|0|0|0|0|0|1|524288
16743942|a|0|0|0|0|0|0|0|1|0
```

- Переглянемо файли та каталоги за допомогою **fls**:

```
lab@ua:~$ fls fat32.img
v/v 16743939:   $MBR
v/v 16743940:   $FAT1
v/v 16743941:   $FAT2
V/V 16743942:   $OrphanFiles
```

- Із використанням команди “**istat … 12**” переглянемо часові позначки, коли файл був створений, доступний та змінений:

```
lab@ua:~$ istat fat32.img 12
Invalid metadata address (fatxxfs_inode_lookup: 12 is not an inode)
```

```
lab@ua:~$ istat tpext.img 12
Cannot determine file system type
```

- Введемо команду “**fls –v**”:

```
lab@ua:~$ fls -v fat32.img
tsk_img_open: Type: 0   NumImg: 1  Img1: fat32.img
aff_open: Error determining type of file: fat32.img
aff_open: No such file or directory
tsk_img_findFiles: fat32.img found
tsk_img_findFiles: 1 total segments found
raw_open: segment: 0  size: 536870912  max offset: 536870912  path: fat32.img
fsopen: Auto detection mode at offset 0
raw_read: byte offset: 0 len: 65536
raw_read: found in image 0 relative offset: 0 len: 65536
raw_read_segment: opening file into slot 0: fat32.img
```

- Використовуючи “**istat … 13**” зобразимо часові мітки видалених записів:

```
lab@ua:~$ istat fat32.img 13
Invalid metadata address (fatxxfs_inode_lookup: 13 is not an inode)
```

```
lab@ua:~$ istat tpext.img 13
Cannot determine file system type
```