Practica 2
Análisis forense de sistemas Linux

Partimos de una máquina virtual con Debian 10, ejecutando la versión del kernel 4.19.0-16-amd64. Utilizaremos esta máquina para realizar volcados de memoria utilizando diversas herramientas disponibles. Es importante destacar que estas herramientas deben estar compiladas específicamente para la versión del kernel que estamos utilizando. En nuestro caso, nos aseguraremos de usar una compilación compatible con el kernel 4.19.0-16-amd64 para garantizar la efectividad y precisión de los volcados de memoria en el entorno Linux.

```
alumno@debian:~$ lsb_release -a
No LSB modules are available.
Distributor ID: Debian
Description:    Debian GNU/Linux 10 (buster)
Release:        10
Codename:       buster
alumno@debian:~$ uname -a
Linux debian 4.19.0-16-amd64 #1 SMP Debian 4.19.181-1 (2021-03-19) x86_64 GNU/
Linux
alumno@debian:~$
```

fmem

Con esta herramienta, se nos ha proporcionado el archivo de código compilado '**fmem.ko**', configurado específicamente para la versión exacta del kernel que estamos utilizando, junto con un script '**fmem.sh**'.

```
alumno@debian:/media/alumno/E86A-FD87$ ls -l
total 768
-rwxrwxrwx 1 alumno alumno 450680 abr  8  2021  fmem.ko
-rwxrwxrwx 1 alumno alumno    429 abr  8  2021  fmem.sh
drwxrwxrwx 1 alumno alumno 131072 mar 19 21:17 'System Volume Information'
alumno@debian:/media/alumno/E86A-FD87$
```

Ejecutaremos el script que, como podemos observar en la línea 11, utiliza el módulo de kernel compilado '**fmem.ko**'.

```
1  | #!/bin/bash
2  |
3  | a1="0x"`cat /proc/kallsyms | grep ' page_is_ram' | head -1 |cut -d ' ' -f 1`
4  |
5  |
6  | if [ "$a1" == "0x" ]; then
7  |     echo "Cannot find symbol 'page_is_ram'";
8  |     exit;
9  | fi
10 |
11 | echo -n "Module: insmod fmem.ko a1=$a1 : ";
12 | insmod fmem.ko a1="$a1" || exit;
13 | echo "OK";
14 | echo -n "Device: "; sleep 1;ls /dev/fmem
15 | echo "----Memory areas: -----"
16 | cat /proc/mtrr;
17 | echo "----------------------"
18 | echo "!!! Don't forget add \"count=\" to dd !!!";
```

Procedemos a ejecutar el script con permisos de root. Observamos que este script monta un dispositivo llamado /dev/fmem, el cual utilizaremos para la adquisición de datos.

```
alumno@debian:/media/alumno/E86A-FD87$ sudo ./fmem.sh
[sudo] password for alumno:
Module: insmod fmem.ko a1=0xffffffffbb07f650 : OK
Device: /dev/fmem
----Memory areas: -----
----------------------
!!! Don't forget add "count=" to dd !!!
alumno@debian:/media/alumno/E86A-FD87$
```

Una vez que hayamos montado el dispositivo, utilizaremos el comando '**free -m**' para determinar la cantidad de RAM disponible en el sistema. Luego procederemos a adquirir los datos del dispositivo utilizando el comando '**dd**', especificando el tamaño de la RAM obtenido en el parámetro 'count'.

```
alumno@debian:/media/alumno/E86A-FD87$ free -m
              total        used        free      shared  buff/cache   availabl
e
Mem:           1995         264        1420           7         310         158
2
Swap:           974           0         974
alumno@debian:/media/alumno/E86A-FD87$ sudo dd if=/dev/fmem of=/media/alumno/E
86A-FD87/volcado2.raw bs=1MB count=1995
1995+0 registros leídos
1995+0 registros escritos
1995000000 bytes (2,0 GB, 1,9 GiB) copied, 314,227 s, 6,3 MB/s
alumno@debian:/media/alumno/E86A-FD87$
```

Lime

En el caso de LIME, solo se nos proporciona el código compilado compatible con la versión del kernel. Sin embargo, esta herramienta ofrece dos métodos para realizar volcados de memoria. Uno de ellos es similar al caso anterior, donde se ejecuta en la misma computadora objetivo. Pero también permite realizar el volcado a través de la red hacia nuestra estación forense.

Volcado de RAM en el objetivo

Simplemente usamos el comando **insmod** con el código compilado proporcionado para la versión específica del kernel, y especificamos una ruta donde se almacenará el volcado de memoria.

```
alumno@debian:/media/alumno/E86A-FD87$ sudo insmod lime-4.19.0-16-amd64.ko "pa
th=/media/alumno/E86A-FD87/volcado3.lime format=lime"

alumno@debian:/media/alumno/E86A-FD87$
alumno@debian:/media/alumno/E86A-FD87$
```

Volcado de RAM por red

En este caso, lo primero que haremos será asegurarnos de estar en la misma red que el objetivo y luego verificar la dirección IP que tiene asignada el objetivo.

```
alumno@debian:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defa
ult qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state U
P group default qlen 1000
    link/ether 08:00:27:f8:9f:ce brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.153/24 brd 192.168.1.255 scope global dynamic noprefixroute
 enp0s3
       valid_lft 86380sec preferred_lft 86380sec
    inet6 2a0c:5a82:2615:4d00:f4c2:aa93:fee4:d4e4/64 scope global temporary dy
namic
       valid_lft 604780sec preferred_lft 85834sec
    inet6 2a0c:5a82:2615:4d00:a00:27ff:fef8:9fce/64 scope global mngtmpaddr no
prefixroute
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fef8:9fce/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
alumno@debian:~$
```

Al igual que en el método anterior, utilizaremos el comando insmod con el código compilado. Sin embargo, en esta ocasión, en el parámetro de la ruta (path), usaremos "**tcp**" junto con el puerto al cual deseamos enviar el volcado de memoria.

```
alumno@debian:/media/alumno/E86A-FD87$ sudo insmod lime-4.19.0-16-amd64.ko "pa
th=tcp:4444 format=raw"
[sudo] password for alumno:
alumno@debian:/media/alumno/E86A-FD87$
```

Una vez que tengamos el módulo insmod escuchando en un puerto específico, utilizaremos Netcat desde nuestra estación forense para recibir el volcado de memoria. Para ello, especificaremos la dirección IP del objetivo junto con el puerto correspondiente, y también especificaremos el nombre que deseamos asignar al volcado.

```
Archivo  Acciones  Editar  Vista  Ayuda
┌──(jose㉿kali)-[~]
└─$ nc 192.168.1.153 4444 > volcado3-b.raw

┌──(jose㉿kali)-[~]
```

AVML

Por último, tenemos la herramienta AVML. En este caso, no es necesario compilar ningún código específico para el kernel. La herramienta ya está preparada para realizar el volcado de memoria sin necesidad de compilaciones adicionales.