EJERCICIO 1: LIME Y AVML

Eric Serrano Marín

ANÁLISIS FORENSE CETI

Contenido

1. Instalación de LiME

Clonar el respositorio de LiME

```
usuario@Ubuntu21MV:~/ejercicio1$ git clone https://github.com/504ensicsLabs/LiME

Clonando en '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
Recibiendo objetos: 100% (370/370), 1.61 MiB | 6.43 MiB/s, listo.
Resolviendo deltas: 100% (199/199), listo.
```

Compilación de LiME

Como podemos observar nos da un error que nos indica que indica que el compilador gcc-12 no está instalado en nuestro sistema y es necesario para compilar el módulo LiME

```
usuario@Ubuntu21MV:~/ejercicio1/LiME/src$ make
make -C /lib/modules/6.5.0-14-generic/build M="/home/usuario/ejercicio1/LiME/src
" modules
make[1]: se entra en el directorio '/usr/src/linux-headers-6.5.0-14-generic'
warning: the compiler differs from the one used to build the kernel
  The kernel was built by: x86_64-linux-gnu-gcc-12 (Ubuntu 12.3.0-1ubuntu1~22.04
) 12.3.0
  You are using:
  CC [M]  /home/usuario/ejercicio1/LiME/src/tcp.o
/bin/sh: 1: gcc-12: not found
make[3]: *** [scripts/Makefile.build:251: /home/usuario/ejercicio1/LiME/src/tcp.
o] Error 127
make[2]: *** [/usr/src/linux-headers-6.5.0-14-generic/Makefile:2037: /home/usuar
io/ejercicio1/LiME/src] Error 2
make[1]: *** [Makefile:234: __sub-make] Error 2
make[1]: se sale del directorio '/usr/src/linux-headers-6.5.0-14-generic'
make: *** [Makefile:35: default] Error 2
```

- **Update**

Para arreglar esto hacemos un update.

```
usuario@Ubuntu21MV:~/ejercicio1/LiME/src$ sudo apt update
Obj:1 http://security.ubuntu.com/ubuntu jammy-security InRelease
Obj:2 http://es.archive.ubuntu.com/ubuntu jammy InRelease
Obj:3 http://es.archive.ubuntu.com/ubuntu jammy-updates InRelease
Obj:4 http://es.archive.ubuntu.com/ubuntu jammy-backports InRelease
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Se pueden actualizar 6 paquetes. Ejecute «apt list --upgradable» para verlos.
```

- **Instalamos gcc -12**

```
usuario@Ubuntu21MV:~/ejercicio1/LiME/src$ sudo apt install gcc-12
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Los paquetes indicados a continuación se instalaron de forma automática y ya no
son necesarios.
  app-install-data-partner cpp-10 gcc-10-base gir1.2-clutter-1.0
  gir1.2-clutter-gst-3.0 gir1.2-cogl-1.0 gir1.2-coglpango-1.0
  gir1.2-gnomebluetooth-1.0 gir1.2-gst-plugins-base-1.0 gir1.2-gtkclutter-1.0
```

- **Correcta compilación**

Como podemos observar ya nos ha compilado correctamente.

```
usuario@Ubuntu21MV:~/ejercicio1/LiME/src$ make
make -C /lib/modules/6.5.0-14-generic/build M="/home/usuario/ejercicio1/LiME/src
" modules
make[1]: se entra en el directorio '/usr/src/linux-headers-6.5.0-14-generic'
warning: the compiler differs from the one used to build the kernel
  The kernel was built by: x86_64-linux-gnu-gcc-12 (Ubuntu 12.3.0-1ubuntu1~22.04
) 12.3.0
  You are using:           gcc-12 (Ubuntu 12.3.0-1ubuntu1~22.04) 12.3.0
  CC [M]  /home/usuario/ejercicio1/LiME/src/tcp.o
  CC [M]  /home/usuario/ejercicio1/LiME/src/disk.o
  CC [M]  /home/usuario/ejercicio1/LiME/src/main.o
  CC [M]  /home/usuario/ejercicio1/LiME/src/hash.o
  CC [M]  /home/usuario/ejercicio1/LiME/src/deflate.o
  LD [M]  /home/usuario/ejercicio1/LiME/src/lime.o
  MODPOST /home/usuario/ejercicio1/LiME/src/Module.symvers
  CC [M]  /home/usuario/ejercicio1/LiME/src/lime.mod.o
  LD [M]  /home/usuario/ejercicio1/LiME/src/lime.ko
  BTF [M] /home/usuario/ejercicio1/LiME/src/lime.ko
Skipping BTF generation for /home/usuario/ejercicio1/LiME/src/lime.ko due to una
vailability of vmlinux
make[1]: se sale del directorio '/usr/src/linux-headers-6.5.0-14-generic'
strip --strip-unneeded lime.ko
mv lime.ko lime-6.5.0-14-generic.ko
```

Volcado de memoria

```
usuario@Ubuntu21MV:~/ejercicio1/LiME/src$ sudo insmod lime-6.5.0-14-generic.ko "path=/home/usu
ario/volcado_memoria/memoria format=raw"
usuario@Ubuntu21MV:~/ejercicio1/LiME/src$
```

```
usuario@Ubuntu21MV:~/volcado_memoria$ ls -lh
total 2,0G
-r--r--r-- 1 root root 2,0G ene 21 12:22 memoria
usuario@Ubuntu21MV:~/volcado_memoria$
```

2. Instalación por segunda vez de LiME

Quitar módulo de LiME anterior

```
usuario@Ubuntu21MV:~/ejercicio1/LiME/src$ sudo rmmod lime
usuario@Ubuntu21MV:~/ejercicio1/LiME/src$ lsmod | grep lime
usuario@Ubuntu21MV:~/ejercicio1/LiME/src$
```

Compilación de LiME

```
usuario@Ubuntu21MV:~/ejercicio1/LiME/src$ make
make -C /lib/modules/6.5.0-14-generic/build M="/home/usuario/ejercicio1/LiME/src" modules
make[1]: se entra en el directorio '/usr/src/linux-headers-6.5.0-14-generic'
warning: the compiler differs from the one used to build the kernel
  The kernel was built by: x86_64-linux-gnu-gcc-12 (Ubuntu 12.3.0-1ubuntu1~22.04) 12.3.0
  You are using:           gcc-12 (Ubuntu 12.3.0-1ubuntu1~22.04) 12.3.0
  LD [M]  /home/usuario/ejercicio1/LiME/src/lime.ko
  BTF [M] /home/usuario/ejercicio1/LiME/src/lime.ko
Skipping BTF generation for /home/usuario/ejercicio1/LiME/src/lime.ko due to unavailability of
 vmlinux
make[1]: se sale del directorio '/usr/src/linux-headers-6.5.0-14-generic'
strip --strip-unneeded lime.ko
mv lime.ko lime-6.5.0-14-generic.ko
usuario@Ubuntu21MV:~/ejercicio1/LiME/src$
```

Volcado de la memoria

```
usuario@Ubuntu21MV:~/ejercicio1/LiME/src$ sudo insmod lime-6.5.0-14-generic.ko "path=/home/usu
ario/volcado_memoria/memoria2 format=raw"
```

```
usuario@Ubuntu21MV:~/ejercicio1/LiME/src$ ls -lh /home/usuario/volcado_memoria
total 4,0G
-r--r--r-- 1 root root 2,0G ene 21 12:22 memoria
-r--r--r-- 1 root root 2,0G ene 21 12:33 memoria2
usuario@Ubuntu21MV:~/ejercicio1/LiME/src$
```

3. Instalación AVML

https://github.com/microsoft/avml/releases

```
usuario@Ubuntu21MV:~/ejercicio1$ wget https://github.com/microsoft/avml/releases/download/v0.13.0/avml
--2024-01-21 13:53:33--  https://github.com/microsoft/avml/releases/download/v0.13.0/avml
Resolviendo github.com (github.com)... 140.82.121.4
Conectando con github.com (github.com)[140.82.121.4]:443... conectado.
Petición HTTP enviada, esperando respuesta... 302 Found
Ubicación: https://objects.githubusercontent.com/github-production-release-asset-2e65be/190660866/c1425d9f-0b3c-4a63-b25c-1571068c694d?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAVCODYLSA53PQK4ZA%2F20240121%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20240121T125333Z&X-Amz-Expires=300&X-Amz-Signature=84ba422d16a63a65dd5de58dff25fd638f34f9d8f58ca12aa959c284db24e723&X-Amz-SignedHeaders=host&actor_id=0&key_id=0&repo_id=190660866&response-content-disposition=attachment%3B%20filename%3Davml&response-content-type=application%2Foctet-stream [siguiente]
--2024-01-21 13:53:33--  https://objects.githubusercontent.com/github-production-release-asset-2e65be/190660866/c1425d9f-0b3c-4a63-b25c-1571068c694d?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAVCODYLSA53PQK4ZA%2F20240121%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20240121T125333Z&X-Amz-Expires=300&X-Amz-Signature=84ba422d16a63a65dd5de58dff25fd638f34f9d8f58ca12aa959c284db24e723&X-Amz-SignedHeaders=host&actor_id=0&key_id=0&repo_id=190660866&response-content-disposition=attachment%3B%20filename%3Davml&response-content-type=application%2Foctet-stream
Resolviendo objects.githubusercontent.com (objects.githubusercontent.com)... 185.199.108.133, 185.199.109.133, 185.199.110.133, ...
Conectando con objects.githubusercontent.com (objects.githubusercontent.com)[185.199.108.133]:443... conectado.
Petición HTTP enviada, esperando respuesta... 200 OK
```

Permisos de ejecución

```
Guardando como: ‘avml’

avml                    100%[============================>]   6,30M  --.-KB/s    en 0,1s

2024-01-21 13:53:34 (48,6 MB/s) - ‘avml’ guardado [6609568/6609568]

usuario@Ubuntu21MV:~/ejercicio1$ ls
avml  LiME
usuario@Ubuntu21MV:~/ejercicio1$ chmod +x AVML
chmod: no se puede acceder a 'AVML': No existe el archivo o el directorio
usuario@Ubuntu21MV:~/ejercicio1$ chmod +x avml
```

Volcado de memoria

```
usuario@Ubuntu21MV:~/ejercicio1$ sudo ./avml ejercicio1.mem
usuario@Ubuntu21MV:~/ejercicio1$ ls
avml  ejercicio1.mem  LiME
usuario@Ubuntu21MV:~/ejercicio1$ ls -lh ejercicio1.mem
-rw------- 1 root root 2,0G ene 21 14:05 ejercicio1.mem
```

4. Comparación de LiME frente a AVML. Pros y contras

LiME

- **Pros**

1. Amplia compatibilidad con sistemas Linux.
2. Soporte para varios modos de volcado.
3. Desarrollo activo y configurabilidad.

- **Contras**

1. Configuración compleja, sobretodo después de usar AVML.
2. Dependiente de la versión del kernel.

AVML

- **Pros**

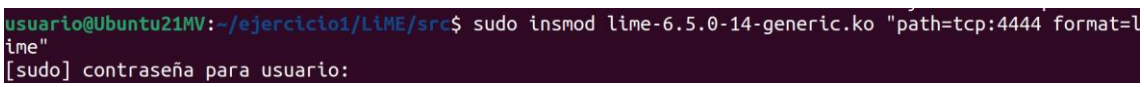
1. Diseñado para sistemas Linux.
2. Simplificación del proceso de volcado de memoria.
3. Integración potencial con Volatility.

- **Contras**

1. Limitado a sistemas Linux (no tan versátil como LiME)
2. Puede depender de la versión del kernel.

5. Descarga de una memoria RAM con LiME o AVML directamente a un equipo en red y no en el disco duro local de la máquina a analizar (scp o nc)

En la máquina en la que queremos la memoria RAM, vamos a hacer el siguiente comando. ***Sudo insmod lime-6.5.0-14-generic.ko "path=tcp:4444 format=lime.***



En la máquina en la que queremos recibirlo: ***sudo nc 172.22.231.14 4444 > <nombre que queremos darle>***

Podemos observar que se ha pasado la totalidad del archivo, ya que ocupa exactamente lo mismo que la primera que hice.