【取证分析】CentOS_5.5_安装GCC编译LiME

zzzhhh / 2018-05-20 22:22:10 / 浏览数 1798

---

1 概述

近期遇到个使用CentOS 5.5的系统，生产环境没有GCC、GDB。要对这台机器抓取关键内存回去用volatility分析。

思路1：使用工具Dump某个进程的内存。使用cat /proc/[进程PID]maps抓出进程关键内存。

在github有相似的工程可以参考：https://github.com/WangYinuo/MemDump

但由于进程太多，这个方案被否定了。

思路2：使用受害系统同样版本的CentOS系统编译好LiME再去加载.ko模块抓取内存。

由于这个版本的yum源停止更新，所以只好使用安装盘自带的RPM包手动安装GCC，编译LiME，制作元数据用volatility分析。

光盘地址：http://vault.centos.org/5.5/isos/x86_64/CentOS-5.5-x86_64-bin-DVD.torrent

1.1 安装GCC

- 打开VMWare界面，选择菜单VM--Settings，在对话框中选择CDROM，设置参数为Use ISO image，选择CentOS镜像安装文件；
- 启动虚拟机中的CentOS系统，用root登录，在桌面上用鼠标右键新建一终端窗口；
- 在终端中输入 cd /media/CentOS_5.5_Final/CentOS 回车

```
[root@localhost malware]# cd /media/CentOS_5.5_Final/CentOS
[root@localhost CentOS]# rpm -ivh cpp-4.1.2-48.el5.x86_64.rpm
[root@localhost CentOS]# rpm -ivh kernel-headers-2.6.18-194.el5.x86_64.rpm
[root@localhost CentOS]# rpm -ivh libgomp-4.4.0-6.el5.x86_64.rpm
[root@localhost CentOS]# rpm -ivh glibc-headers-2.5-49.x86_64.rpm
[root@localhost CentOS]# rpm -ivh libgomp-4.4.0-6.el5.x86_64.rpm
[root@localhost CentOS]# rpm -ivh kernel-devel-2.6.18-194.el5.x86_64.rpm
[root@localhost CentOS]# rpm -ivh glibc-devel-2.5-49.x86_64.rpm
[root@localhost CentOS]# rpm -ivh gcc-4.1.2-48.el5.x86_64.rpm
```

1.2 编译LiME

```
[root@localhost CentOS]# tar -zxvf LiME.tar.gz
[root@localhost CentOS]# cd /home/yunwei/Desktop/malware/LiME/src/
[root@localhost src]# make
make -C /lib/modules/2.6.18-194.el5/build M="/home/yunwei/Desktop/malware/LiME/src" modules
make[1]: Entering directory `/usr/src/kernels/2.6.18-194.el5-x86_64'
 Building modules, stage 2.
 MODPOST
 LD [M]  /home/yunwei/Desktop/malware/LiME/src/lime.ko
make[1]: Leaving directory `/usr/src/kernels/2.6.18-194.el5-x86_64'
strip --strip-unneeded lime.ko
mv lime.ko lime-2.6.18-194.el5.ko
[root@localhost src]# ll
total 1176
-rw-r--r-- 1 root root   2557 Sep 28  2017 disk.c
-rw-r--r-- 1 root root 168240 May 20 10:44 disk.o
-rw-r--r-- 1 root root  41984 May 20 11:46 lime-2.6.18-194.el5.ko
-rw-r--r-- 1 root root   1920 Sep 28  2017 lime.h
-rw-r--r-- 1 root root   1151 May 20 10:44 lime.mod.c
-rw-r--r-- 1 root root  81632 May 20 10:44 lime.mod.o
-rw-r--r-- 1 root root 505173 May 20 10:44 lime.o
-rw-r--r-- 1 root root   6614 Sep 28  2017 main.c
-rw-r--r-- 1 root root 175408 May 20 10:44 main.o
-rw-r--r-- 1 root root   1661 Sep 28  2017 Makefile
-rw-r--r-- 1 root root   1722 Sep 28  2017 Makefile.sample
-rw-r--r-- 1 root root      0 May 20 10:44 Module.markers
-rw-r--r-- 1 root root      0 May 20 10:44 Module.symvers
-rw-r--r-- 1 root root   3889 Sep 28  2017 tcp.c
-rw-r--r-- 1 root root 166152 May 20 10:44 tcp.o
```

1.3 抓取内存

/home/yunwei/Desktop/malware/centos5.lime为自定义路径

```
## ■■■■■■■■■■
[root@localhost src]# insmod lime-`uname -r`.ko path=/home/yunwei/Desktop/malware/centos5.lime format=lime
## ■■■■■■■■■■■■■■■■■■■■■■
[root@localhost src]# rmmod lime
```

1.4 制作元数据

1.4.1 dwarfdump使用

安装调试文件导出工具dwarfdump：

- 1) 下载与编译libdwarf

```
## ■■Libdwarf
[root@localhost src]# git clone https://github.com/tomhughes/libdwarf.git
[root@localhost src]# tar -zxvf libdwarf.tar.gz

## ■■■■■■■■
[root@localhost src]# cd /media/CentOS_5.5_Final/CentOS/
[root@localhost src]# rpm -ivh /media/CentOS_5.5_Final/CentOS/elfutils-libelf-0.137-3.el5.x86_64.rpm
[root@localhost libdwarf]# rpm -ivh elfutils-libelf-devel-static-0.137-3.el5.x86_64.rpm elfutils-libelf-devel-0.137-3.el5.x86_

## ■■■■ libdwarf
[root@localhost CentOS]# cd /home/yunwei/Desktop/malware/libdwarf
[root@localhost CentOS]# ./configure
[root@localhost libdwarf]# make

### ■■■■■■■■■■■■■■■
[root@localhost libdwarf]# cd dwarfdump/
[root@localhost dwarfdump]# make install
cp dwarfdump /usr/local/bin/dwarfdump
cp ./dwarfdump.conf /usr/local/lib/dwarfdump.conf
cp ./dwarfdump.1 /usr/local/share/man/man1/dwarfdump.1
[root@localhost dwarfdump]# dwarfdump -h
### ■■dwarfdump -h■■■■■■■■■■■■■■■
```

- 2) 生成内存镜像

```
[root@localhost malware]# tar -zxvf volatility.tar.gz
[root@localhost malware]# cd volatility/tools/linux/
## ■■
[root@localhost linux]# make
make -C //lib/modules/2.6.18-194.el5/build CONFIG_DEBUG_INFO=y M="/home/yunwei/Desktop/malware/volatility/tools/linux" modules
make[1]: Entering directory `/usr/src/kernels/2.6.18-194.el5-x86_64'
 CC [M]  /home/yunwei/Desktop/malware/volatility/tools/linux/module.o
/home/yunwei/Desktop/malware/volatility/tools/linux/module.c:214: error: redefinition of ‘struct module_sect_attr’
/home/yunwei/Desktop/malware/volatility/tools/linux/module.c:221: error: redefinition of ‘struct module_sect_attrs’
/home/yunwei/Desktop/malware/volatility/tools/linux/module.c:375:5: warning: "STATS" is not defined
/home/yunwei/Desktop/malware/volatility/tools/linux/module.c:391:5: warning: "DEBUG" is not defined
make[2]: *** [/home/yunwei/Desktop/malware/volatility/tools/linux/module.o] Error 1
make[1]: *** [_module_/home/yunwei/Desktop/malware/volatility/tools/linux] Error 2
make[1]: Leaving directory `/usr/src/kernels/2.6.18-194.el5-x86_64'
make: *** [dwarf] Error 2

### ■■■ 198,7 ~ 221,7,■■■■■■■■
/*
#if LINUX_VERSION_CODE == KERNEL_VERSION(2,6,18)
....
struct module_sections module_sect_attrs;

#endif
*/

## ■■■■■■■■■■■■■■

[root@localhost linux]# make
```

```
make -C //lib/modules/2.6.18-194.el5/build CONFIG_DEBUG_INFO=y M="/home/yunwei/Desktop/malware/volatility-2.6/tools/linux" mod
make[1]: Entering directory `/usr/src/kernels/2.6.18-194.el5-x86_64'
 CC [M]  /home/yunwei/Desktop/malware/volatility-2.6/tools/linux/module.o
/home/yunwei/Desktop/malware/volatility-2.6/tools/linux/module.c:354:5: warning: "STATS" is not defined
/home/yunwei/Desktop/malware/volatility-2.6/tools/linux/module.c:370:5: warning: "DEBUG" is not defined
 Building modules, stage 2.
 MODPOST
 CC      /home/yunwei/Desktop/malware/volatility-2.6/tools/linux/module.mod.o
 LD [M]  /home/yunwei/Desktop/malware/volatility-2.6/tools/linux/module.ko
make[1]: Leaving directory `/usr/src/kernels/2.6.18-194.el5-x86_64'
dwarfdump -di module.ko > module.dwarf
make -C //lib/modules/2.6.18-194.el5/build M="/home/yunwei/Desktop/malware/volatility-2.6/tools/linux" clean
make[1]: Entering directory `/usr/src/kernels/2.6.18-194.el5-x86_64'
 CLEAN   /home/yunwei/Desktop/malware/volatility-2.6/tools/linux/.tmp_versions
make[1]: Leaving directory `/usr/src/kernels/2.6.18-194.el5-x86_64'
```

1.5 volatility使用内存镜像分析

将module.dwarf文件和/boot中对应目标系统内核版本的System.map文件打包成.zip文件，放入/volatility/volatility/plugins/overlays/linux/目录中

```
## ■■■■■■CentOS5.5_2.6.18-194.el5-x86_64.zip

[root@localhost linux]# zip CentOS5.5_2.6.18-194.el5-x86_64.zip module.dwarf /boot/System.map-`uname -r`

## ■CentOS5.5_2.6.18-194.el5-x86_64.zip■■volatility-master\volatility\plugins\overlays\linux■■■

## ■■■■-■■■■

D:\malware\volatility-master>vol.py -f "D:\malware\CentOS5.5_2.6.18-194.el5_test.lime" --profile=LinuxCentOS5_5_2_6_18-194_el5
Volatility Foundation Volatility Framework 2.6
Offset             Name                 Pid             PPid            Uid             Gid    DTB                Start Time
------------------ -------------------- --------------- --------------- --------------- ------ ------------------ ----------
0xffff81003fe3a7a0 init                 1               0               0               0      0x0000000013332000 2018-05-20 1
0xffff81003fe3a040 migration/0          2               1               0               0      ------------------ 2018-05-20 1
0xffff81003fe3e7e0 ksoftirqd/0          3               1               0               0      ------------------ 2018-05-20 1
0xffff81003fe3e080 events/0             4               1               0               0      ------------------ 2018-05-20 1
0xffff810037fe7820 khelper              5               1               0               0      ------------------ 2018-05-20 1
0xffff810037fd90c0 kthread              14              1               0               0      ------------------ 2018-05-20 1
0xffff810037cdc040 kblockd/0            18              14              0               0      ------------------ 2018-05-20 1
0xffff81003f4ea7e0 kacpid               19              14              0               0      ------------------ 2018-05-20 1
```

1.6 参考

Linux安装GCC的一系列问题的解决

https://blog.csdn.net/yvanboyang/article/details/73274004

CentOS 5.5 安装GCC与g++步骤

https://www.linuxidc.com/Linux/2011-07/38657.htm

CentOS 6.5使用安装盘自带的RPM包手动安装gcc

https://blog.csdn.net/testcs_dn/article/details/41727767

Volatility学习笔记二-制作SLES11SP2的profile

https://www.jianshu.com/p/28848d3d9c1b

Build Volatility profile on Centos 5

http://vdchuyen.com/blog/2016/01/01/build-volatility-centos-profile.html

上一篇：windows本地提权漏洞cve-... 下一篇：RCTF 2018 Writeup...

1. 0 条回复

- 动动手指，沙发就是你的了！

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板