关于CTF中的取证分析

原创

白海客 于 2020-12-05 20:21:40 发布 1438 收藏 15

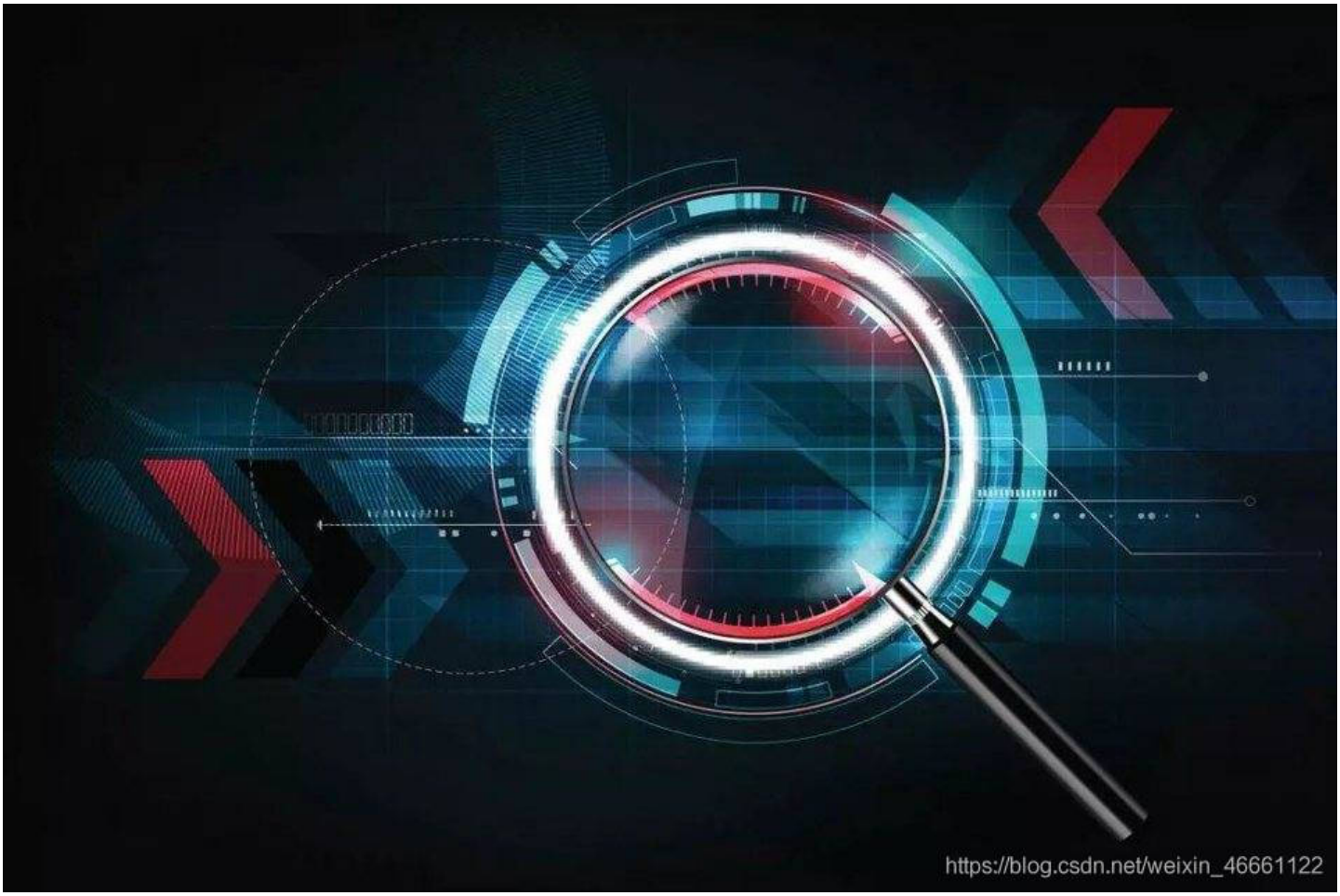
分类专栏： 笔记

本文链接：https://blog.csdn.net/weixin_46661122/article/details/110719331

什么是计算机取证？

计算机取证（Computer Forensics，又名计算机取证技术、计算机鉴识、计算机法医学）是指运用计算机辨析技术，对计算机犯罪行为进行分析以确认罪犯及计算机证据，并据此提起诉讼。也就是针对计算机入侵与犯罪，进行证据获取、保存、分析和出示。计算机证据指在计算机系统运行过程中产生的以其记录的内容来证明案件事实的电磁记录物。从技术上而言。计算机取证是一个对受侵计算机系统进行扫描和破解，以对入侵事件进行重建的过程。可理解为“从计算机上提取证据”即：获取、保存、分析、出示、提供的证据必须可信；

计算机取证在打击计算机和网络犯罪中作用十分关键，它的目的是要将犯罪者留在计算机中的“痕迹”作为有效的诉讼证据提供给法庭，以便将犯罪嫌疑人绳之以法。因此，计算机取证是计算机领域和法学领域的一门交叉科学，被用来解决大量的计算机犯罪和事故，包括网络入侵、盗用知识产权和网络欺骗等。



取证意义:还原黑客入侵痕迹,尽可能得到黑客入侵渗透证据

取证方法

活取证

抓取文件metadata、创建时间线、命令历史、分析日志文件、哈希摘要、转存内存信息

使用未受感染的干净程序执行取证，U盘/网络存储收集数据

死取证

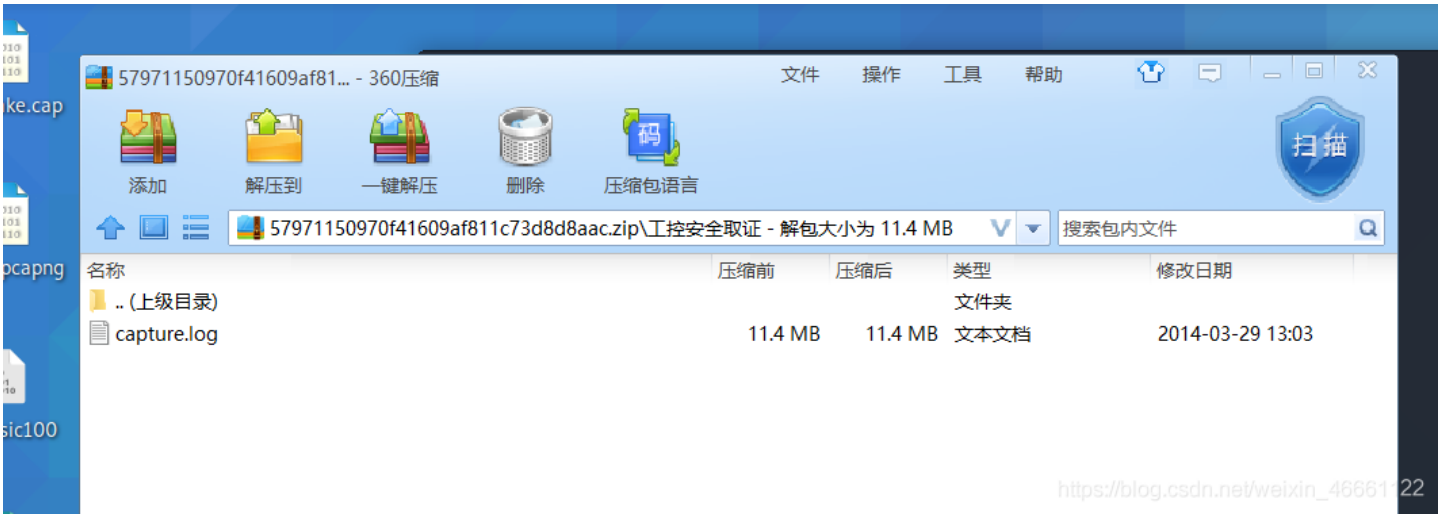
关机后制作硬盘镜像、分析镜像(MBR、GPT、LVM)

计算机取证工具主要可以分为以下几种不同类别:

```
磁盘和数据捕获工具
文件查看器
文件分析工具
注册表分析工具
互联网分析工具
电子邮件分析工具
移动设备分析工具
网络取证工具
数据库取证工具
```

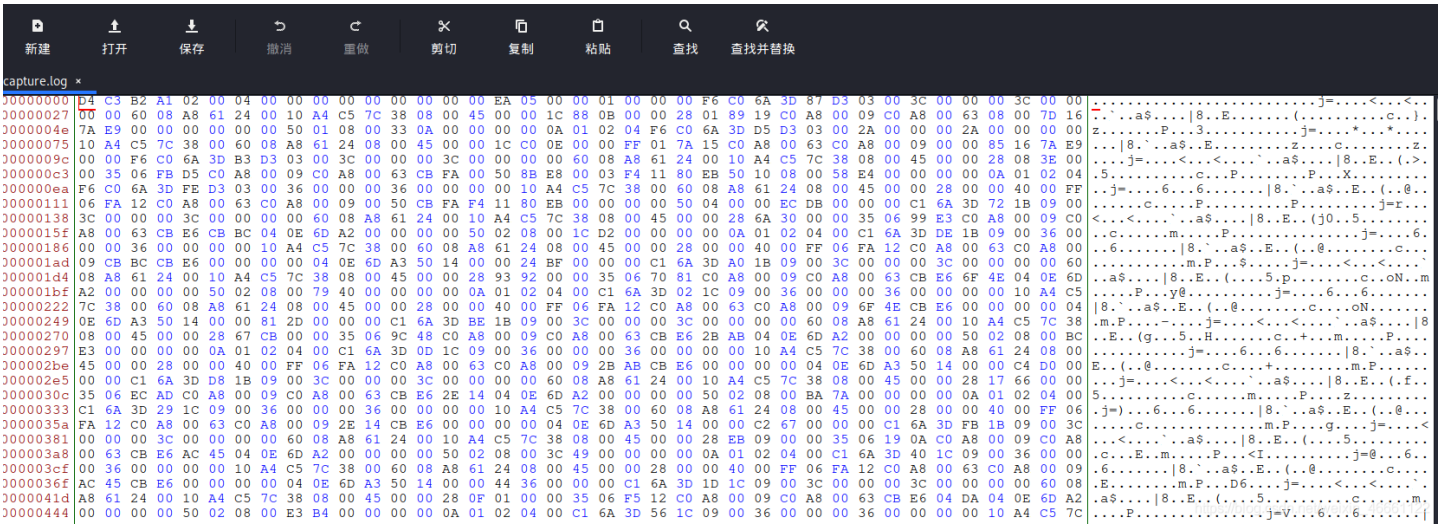
CTF中三种常见的取证场景，及流量分析，内存镜像取证和磁盘镜像取证。

流量分析的话，这里以攻防世界的工控安全取证，题目描述是设备受到了大量的扫描，扫描不止一次，分析日志，找出黑客的第4次扫描编号。

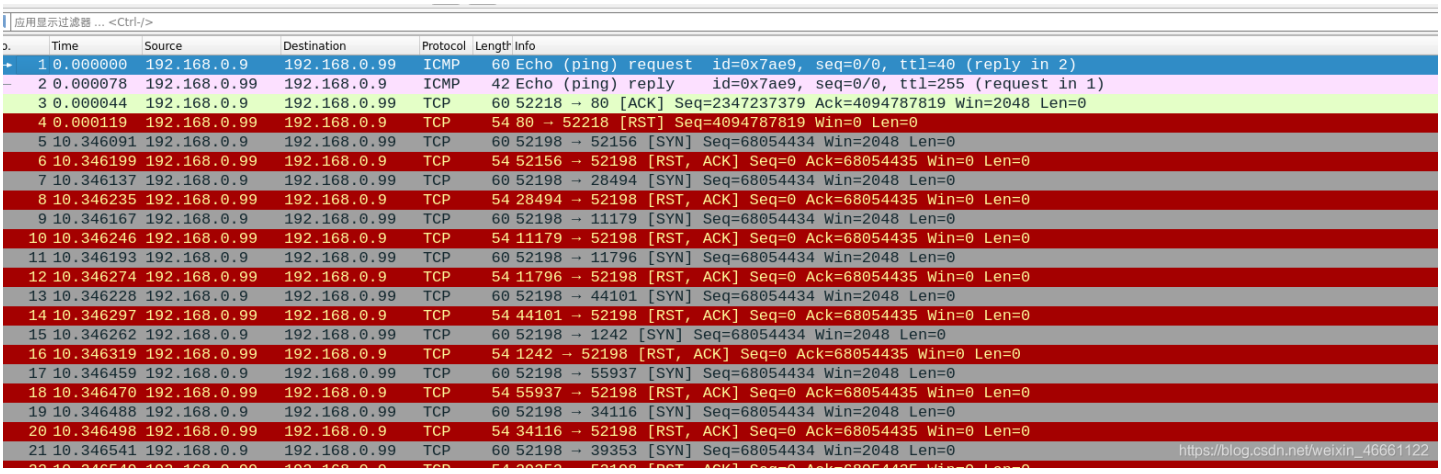


log日志文件

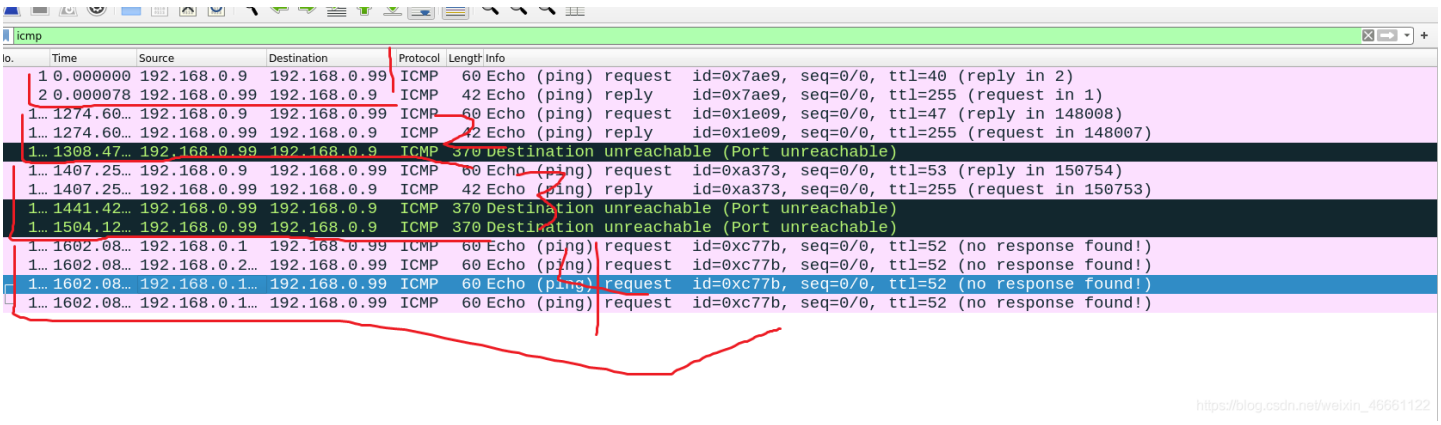
尝试binwalk分离无果



查看该文件16进制数据,文件头D4 C3 B2 A1可知是pcap文件，将log文件重命名后缀为pcap



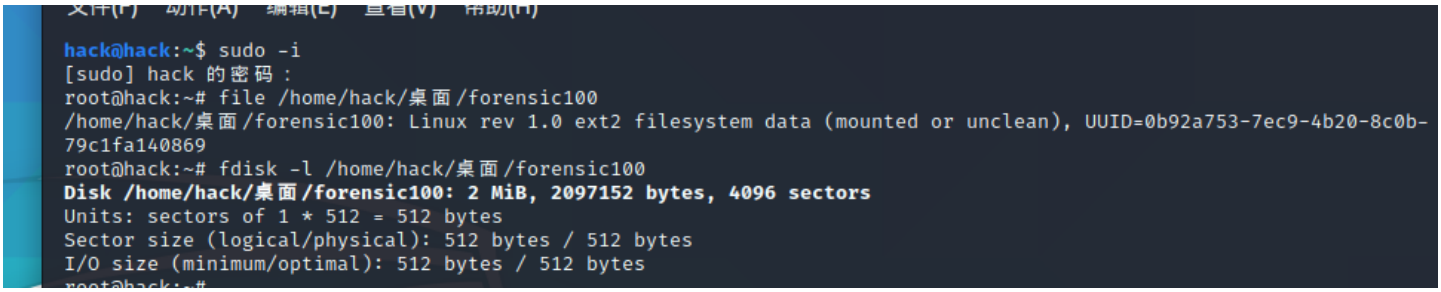
使用wireshark进行流量分析,只有ICMP数据包和大量的TCP复位数据包，通过题目提示，黑客是实施了对设备的ping扫描,显示过滤器过滤ICMP数据包。



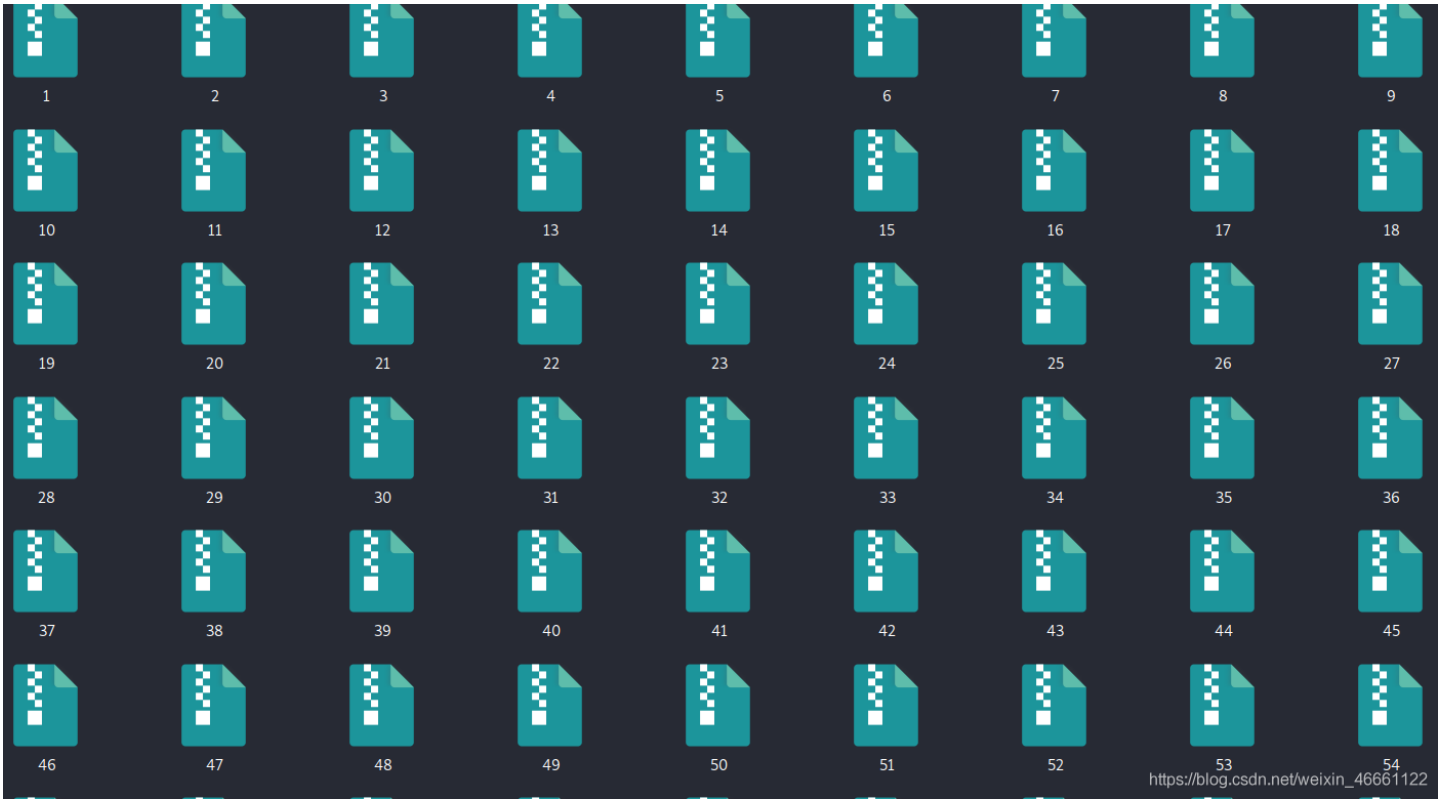
通过一问一答的方式，第4次ping扫描的数据包编号是155989,即flag为flag{155989}。

磁盘镜像取证

没有任何提示，但由题目可知需要获取key.txt



磁盘取证的第1步是确定磁盘的类型,这道题的磁盘类型是ext2,然后通过fdisk -l可查看磁盘中的卷信息,大小,偏移量等。
然后将磁盘镜像进行挂载
mount -o loop -t 文件系统类型 镜像路径 挂载点路径
如果有多分区镜像,也就是该磁盘信息有偏移量的时候,还需要加上offset,指定偏移量的值。



磁盘挂载之后，可看到大量的压缩包

```
hack@hack:~$ sudo -i
[sudo] hack 的密码：
root@hack:~# ls
1    111  124  137  15   162  175  188  20   212  225  238  30  43  56  69  81  94
10   112  125  138  150  163  176  189  200  213  226  239  31  44  57  7   82  95
100  113  126  139  151  164  177  19   201  214  227  24   32  45  58  70  83  96
101  114  127  14   152  165  178  190  202  215  228  240  33  46  59  71  84  97
102  115  128  140  153  166  179  191  203  216  229  241  34  47  6   72  85  98
103  116  129  141  154  167  18   192  204  217  23   242  35  48  60  73  86  99
104  117  13   142  155  168  180  193  205  218  230  243  36  49  61  74  87  lost+found
105  118  130  143  156  169  181  194  206  219  231  244  37  5   62  75  88
106  119  131  144  157  17   182  195  207  22   232  25   38  50  63  76  89
107  12   132  145  158  170  183  196  208  220  233  26   39  51  64  77  9
108  120  133  146  159  171  184  197  209  221  234  27   4   52  65  78  90
109  121  134  147  16   172  185  198  21   222  235  28   40  53  66  79  91
11   122  135  148  160  173  186  199  210  223  236  29   41  54  67  8   92
110  123  136  149  161  174  187  2    211  224  237  3    42  55  68  80  93
root@hack:~# grep -r key.txt
匹配到二进制文件 1
root@hack:~# gunzip < 1
SECCON{@]NL7n+-s75FrET]vU=7Z}
root@hack:~#
```


可通过grep -r查找我们要的key.txt,匹配到二进制文件名，然后gunzip < 文件名 ,即可得到flag。

内存镜像分析

https://yq.aliyun.com/articles/85909取证工具集

CTF题目链接:https://www.cnblogs.com/wrnan/p/12572263.html

内存镜像分析使用到的工具是Volatility,当我们拿到一个内存镜像时,首先需要确定这个内存镜像的基本信息,判断这个镜像是哪种操作系统,通过imageinfo命令获取镜像的信息,之后查看进程使用命令pslist,当查找到某个文件或者进程的可疑行为时,通过命令dumpfile和memdump将相关数据导出。

常用参数

-f 指定文件名

imageinfo：

用于查看我们正在分析的内存样本的摘要信息。具体来说显示主机所使用的操作系统版本、服务包以及硬件结构(32位或64位)、页目录表的起始地址和该获取该内存镜像的时间等基本信息
其中以.raw后缀的文件名就是本机的内存镜像。>imageinfo.txt是把imageinfo命令取得的信息定向的存在imageinfo.txt的文件中。

kpcrscan：

用于查找内存中用于定义内核处理器控制区域（KPCR）的_KPCR结构体信息，具体来说，可以显示每个处理器的详细信息，包括IDT（线程控制符）和GDT（全局段描述符表）地址，当前运行的线程和空闲线程，CPU数量、制造厂商及其速度，CR3寄存器或页目录表基地址的值等信息。该命令的使用方法要用到imageinfo取得的profile信息

dlllist：

能够显示一个进程装载的动态链接库的信息，其显示列表主要包括加载的动态链接库文件的基地址、文件大小以及文件所在路径。

filescan：

此命令将显示系统上的打开的文件，包括已被恶意软件隐藏的文件

handles：

显示在一个进程中打开的处理

modscan：

扫描_ldr_data_table_entry对象的物理内存。显示内核的驱动程序，包括已隐藏/链接的

netscan：

发现TCP / UDP端点和监听器。这个命令将显示一个主动网络连接的列表

pslist：

可以枚举系统中的进程，这条命令通过遍历PsActiveProcessHead指针指向的双向链表枚举当前内存中活跃的所有进程信息，主要包括偏移地址、进程ID号、父进程ID号、线程数量、句柄数量、进程会话ID号以及进程开始和退出的时间

pstree：

这个命令显示跟pslist一样的信息，以树的形式

connscan：

查看网络连接

实例：

查询文件信息，关注 profile

volatility imageinfo -f win.dmp imageinfo

查询数据库文件

volatility hivelist -f win.dmp --profile=Win7SP1x86

volatility hivelist -f win.dmp --profile=Win7SP1x86 pslist

volatility hivelist -f win.dmp --profile=Win7SP1x86 pstree

按虚内存地址查看注册表内容

volatility -f win.dmp --profile=Win7SP1x86 hivelist

volatility -f win.dmp --profile=Win7SP1x86 hivedump -o 0x91fa1648

查看用户账号

volatility -f win.dmp --profile=Win7SP1x86 printkey -K “SAM\Domains\Account\Users\Names”

最后登录的用户

volatility -f win.dmp --profile=Win7SP1x86 printkey -K "SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon

正在运行的程序、运行过多少次、最后一次运行时间等

volatility -f win.dmp --profile=Win7SP1x86 userassist

进程列表及物理内存

volatility -f win.dmp --profile=Win7SP1x86 pslist

dump 进程内存

volatility -f win.dmp --profile=Win7SP1x86 memdump -p 3684 -D dumpdir/

root@Hitman47:~/dumpdir# hexeditor 3684.dmp

root@Hitman47:~/dumpdir# strings 3684.dmp > 1111.txt

root@Hitman47:~/dumpdir# strings 3684.dmp | grep password

root@Hitman47:~/dumpdir# strings 3684.dmp | grep /

root@Hitman47:~/dumpdir# strings 3684.dmp | grep @

命令历史

volatility cmdscan -f win.dmp --profile=Win7SP1x86

网络连接

volatility netscan -f win.dmp --profile=Win7SP1x86

IE 历史

volatility iehistory -f win.dmp --profile=Win7SP1x86

提取hash

volatility -f win.dmp --profile=Win7SP1x86 hivelist

volatility命令说明手册:https://github.com/volatilityfoundation/volatility/wiki/Command-Reference

https://www.freebuf.com/column/152545.html
这也是一篇非常有价值的文章

在kali2020最新版本没有了该工具,github安装地址https://github.com/volatilityfoundation/volatility