**Volatility全部插件**

vol.py --plugin=/home/kali/桌面/volatility/volatility/plugins -f memdump.mem --profile=Win7SP1x64 mimikatz

usbstor 从注册表中读取Usb设备插入信息

lastpass 从浏览器内存空间中读取账户密码信息

ndispktscan 搜索内核的网络流量包信息

powersh 对内存中的（隐藏）powershell进程进行分析

systeminfo 自动获取取证所需基本系统信息，例如系统名称、时区、关机时间等

bitlocker 提取BitLocker全卷加密密钥(FVEK)，可以用来解密BitLocker卷

autoruns 列出自启动程序

osint 解析出不同进程中的url和ip

chrome\_ragamuffin 分析内存中的chrome浏览器运行实例，可以分析正在浏览的页面

volatility --plugins=/home/kali/桌面/volatility/volatility/plugins -f Adv.raw chrome\_ragamuffin --analysis history

volatility --plugins=/home/kali/桌面/volatility/volatility/plugins -f Adv.raw chrome\_ragamuffin --analysis renderer

LinuxFirefox 分析内存中的firefox浏览器

linux\_ffhis 查看历史记录

linux\_ffcookies 查看cookie

1、amcache 查看AmCache应用程序痕迹信息

2、apihooks 检测内核及进程的内存空间中的API hook

3、atoms 列出会话及窗口站atom表

4、atomscan Atom表的池扫描(Pool scanner)

5、auditpol 列出注册表HKLMSECURITYPolicyPolAdtEv的审计策略信息

6、bigpools 使用BigPagePoolScanner转储大分页池(big page pools)

7、bioskbd 从实时模式内存中读取键盘缓冲数据(早期电脑可以读取出BIOS开机密码)

8、cachedump 获取内存中缓存的域帐号的密码哈希

9、callbacks 打印全系统通知例程

10、clipboard 提取Windows剪贴板中的内容

11、cmdline 显示进程命令行参数

12、cmdscan 提取执行的命令行历史记录（扫描\_COMMAND\_HISTORY信息）

13、connections 打印系统打开的网络连接(仅支持Windows XP 和2003)

14、connscan 打印TCP连接信息

15、consoles 提取执行的命令行历史记录（扫描\_CONSOLE\_INFORMATION信息）

16、crashinfo 提取崩溃转储信息

17、deskscan tagDESKTOP池扫描(Poolscaner)

18、devicetree 显示设备树信息

19、dlldump 从进程地址空间转储动态链接库

20、dlllist 打印每个进程加载的动态链接库列表

21、driverirp IRP hook驱动检测

22、drivermodule 关联驱动对象至内核模块

23、driverscan 驱动对象池扫描

24、dumpcerts 提取RAS私钥及SSL公钥

25、dumpfiles 提取内存中映射或缓存的文件

26、dumpregistry 转储内存中注册表信息至磁盘

27、editbox 查看Edit编辑控件信息 (Listbox正在实验中)

28、envars 显示进程的环境变量

29、eventhooks 打印Windows事件hook详细信息

30、evtlogs 提取Windows事件日志（仅支持XP/2003)

31、filescan 提取文件对象（file objects）池信息

32、gahti 转储用户句柄（handle）类型信息

33、gditimers 打印已安装的GDI计时器(timers)及回调(callbacks)

34、gdt 显示全局描述符表(Global Deor Table)

35、getservicesids 获取注册表中的服务名称并返回SID信息

36、getsids 打印每个进程的SID信息

37、handles 打印每个进程打开的句柄的列表

38、hashdump 转储内存中的Windows帐户密码哈希(LM/NTLM)

39、hibinfo 转储休眠文件信息

40、hivedump 打印注册表配置单元信息

41、hivelist 打印注册表配置单元列表

42、hivescan 注册表配置单元池扫描

43、hpakextract 从HPAK文件（Fast Dump格式）提取物理内存数据

44、hpakinfo 查看HPAK文件属性及相关信息

45、idt 显示中断描述符表(Interrupt Deor Table)

46、iehistory 重建IE缓存及访问历史记录

47、imagecopy 将物理地址空间导出原生DD镜像文件

48、imageinfo 查看/识别镜像信息

49、impscan 扫描对导入函数的调用

50、joblinks 打印进程任务链接信息

51、kdbgscan 搜索和转储潜在KDBG值

52、kpcrscan 搜索和转储潜在KPCR值

53、ldrmodules 检测未链接的动态链接DLL

54、lsadump 从注册表中提取LSA密钥信息（已解密）

55、machoinfo 转储Mach-O 文件格式信息

56、malfind 查找隐藏的和插入的代码

57、mbrparser 扫描并解析潜在的主引导记录(MBR)

58、memdump 转储进程的可寻址内存

59、memmap 打印内存映射

60、messagehooks 桌面和窗口消息钩子的线程列表

61、mftparser 扫描并解析潜在的MFT条目

62、moddump 转储内核驱动程序到可执行文件的示例

63、modscan 内核模块池扫描

64、modules 打印加载模块的列表

65、multiscan 批量扫描各种对象

66、mutantscan 对互斥对象池扫描

67、notepad 查看记事本当前显示的文本

68、objtypescan 扫描窗口对象类型对象

69、patcher 基于页面扫描的补丁程序内存

70、poolpeek 可配置的池扫描器插件

71、printkey 打印注册表项及其子项和值

72、privs 显示进程权限

73、procdump 进程转储到一个可执行文件示例

74、pslist 按照EPROCESS列表打印所有正在运行的进程

75、psscan 进程对象池扫描

76、pstree 以树型方式打印进程列表

77、psxview 查找带有隐藏进程的所有进程列表

78、qemuinfo 转储 Qemu 信息

79、raw2dmp 将物理内存原生数据转换为windbg崩溃转储格式

80、screenshot 基于GDI Windows的虚拟屏幕截图保存

81、servicediff Windows服务列表(ala Plugx)

82、sessions \_MM\_SESSION\_SPACE的详细信息列表(用户登录会话)

83、shellbags 打印Shellbags信息

84、shimcache 解析应用程序兼容性Shim缓存注册表项

85、shutdowntime 从内存中的注册表信息获取机器关机时间

86、sockets 打印已打开套接字列表

87、sockscan TCP套接字对象池扫描

88、ssdt 显示SSDT条目

89、strings 物理到虚拟地址的偏移匹配(需要一些时间，带详细信息)

90、svcscan Windows服务列表扫描

91、symlinkscan 符号链接对象池扫描

92、thrdscan 线程对象池扫描

93、threads 调查\_ETHREAD 和\_KTHREADs

94、timeliner 创建内存中的各种痕迹信息的时间线

95、timers 打印内核计时器及关联模块的DPC

96、truecryptmaster 恢复TrueCrypt 7.1a主密钥

添加参数 –D 保存密钥文件

97、truecryptpassphrase 查找并提取TrueCrypt密码

98、truecryptsummary TrueCrypt摘要信息

99、unloadedmodules 打印卸载的模块信息列表

100、userassist 打印注册表中UserAssist相关信息

101、userhandles 转储用户句柄表

102、vaddump 转储VAD数据为文件

103、vadinfo 转储VAD信息

104、vadtree 以树形方式显示VAD树信息

105、vadwalk 显示遍历VAD树

106、vboxinfo 转储Virtualbox信息（虚拟机）

107、verinfo 打印PE镜像中的版本信息

108、vmwareinfo 转储VMware VMSS/VMSN 信息

109、volshell 内存镜像中的shell

110、windows 打印桌面窗口(详细信息)

111、wintree Z顺序打印桌面窗口树

112、wndscan 池扫描窗口站

113、yarascan 以Yara签名扫描进程或内核内存