**磁盘内存分析**

**概念**

在CTF中，内存取证一般指对计算机及相关智能设备运行时的物理内存中存储的临时数据进行获取与分析，提取flag或者与flag相关重要信息

常见的内存文件格式有：img、dmp、raw、vmem。对应格式找对应系统

## **磁盘**

常见的磁盘分区格式有以下几种

Windows: FAT12 -> FAT16 -> FAT32 -> NTFS

Linux: EXT2 -> EXT3 -> EXT4

FAT 主磁盘结构

IMG_256

删除文件：目录表中文件名第一字节 e5。

## **VMDK**

VMDK 文件本质上是物理硬盘的虚拟版，也会存在跟物理硬盘的分区和扇区中类似的填充区域，我们可以利用这些填充区域来把我们需要隐藏的数据隐藏到里面去，这样可以避免隐藏的文件增加了 VMDK 文件的大小（如直接附加到文件后端），也可以避免由于 VMDK 文件大小的改变所带来的可能导致的虚拟机错误。而且 VMDK 文件一般比较大，适合用于隐藏大文件。

**内存**

①解析 Windows / Linux / Mac OS X 内存结构

②分析进程，内存数据

③根据题目提示寻找线索和思路，提取分析指定进程的特定内存数据

**常用工具**

**Volatility**

Volatility是开源的Windows，Linux，MaC，Android的****内存取证分析工具****，由python编写成，命令行操作，支持各种操作系统。Volatility可以用来获取内存图像，查找可疑文件等。

**基本用法**

1. 当我们拿到内存文件后，一般会做的便是先识别一下该内存文件一些信息（一般会去识别配置文件，然后通过对应的配置文件进行其他操作）

命令：volatility -f [内存文件] imageinfo

1. 查看系统注册表（获取主机名、IP等信息）

找到system注册表—hivelist：

命令:volatility -f [内存文件] --profile=[配置文件] hivelist

1. 读注册表中的信息—printkey

命令:volatility -f [内存文件] --profile=[配置文件] printkey -o [虚拟地址] -K [注册表路径]

1. 查看剪切版中的信息（获取复制剪切的内容）：

命令:volatility -f [内存文件] --profile=[配置文件] clipboard

1. 查看进程信息（发现可疑进程）：

无法显示隐藏/终止的进程—pslist

命令:volatility -f [内存文件] --profile=[配置文件] pslist

1. 显示隐藏/终止的进程—psscan

命令:volatility -f [内存文件] --profile=[配置文件] psscan

1. 把进程以树的形式显示—pstree

命令:volatility -f [内存文件] --profile=[配置文件] pstree

1. 查看DLL文件（当我们发现可疑进程后，可通过此命令进行深度查看）：

命令:volatility -f [内存文件] --profile=[配置文件] dlllist -p [PID]

1. 查看IE浏览器历史记录(获取IE浏览器浏览历史信息)：

命令:volatility -f [内存文件] --profile=[配置文件] iehistory

1. 查看文件（获取可疑文件）：

命令:volatility -f [内存文件] --profile=[配置文件] filescan

1. 查看命令行历史记录（获取执行的可疑命令）

命令:volatility -f [内存文件] --profile=[配置文件] cmdscan

1. 查看进程命令行参数（具体查看一些可疑进程的参数指令）

命令:volatility -f [内存文件] --profile=[配置文件] cmdline

1. 查看notepad文件（只能查看进程中的notepad.exe中的内容）

命令:volatility -f [内存文件] --profile=[配置文件] notepad

1. 得到了一些信息有时候往往不过，有可能还需要我们提取内存中的数据再进行二次操作才可以得到flag

①获取密码hash 命令：volatility -f [内存文件] --profile=[配置文件] hashdum

②获取对应进程（当我们发现某个进程中可能会存在我们所需的flag） 命令： volatility -f [内存文件] --profile=[配置文件] memdump -n [文件名（不带后缀）] -D [保存路径]

Or volatility -f [内存文件] --profile=[配置文件] memdump -p [PID] -D [保存路径]

③打印注册表中的对应表的数据： 命令：volatility -f [内存文件] --profile=[配置文件] hivedump -o [虚拟地址]

④转储内存中的文件 命令：volatility -f [内存文件] --profile=[配置文件] dumpfiles -Q [偏移地址] -D [保存路径]

⑤转储内存中的进程里exe文件 命令：volatility -f [内存文件] --profile=[配置文件] procdump -p [PID] -D [保存路径]