《电子证据分析》课程实验报告

|  |  |  |  |
| --- | --- | --- | --- |
| 实验名称 |  | 姓名 |  |
| 班级 |  | 学号 |  |
| 实验日期 |  | 指导老师 |  |
| 实验环境  (实验软硬件要求) | Win10、cmd、volatility | | |
| 实验目的 | （给出本次实验所涉及并要求掌握的知识点）  *了解并且掌握volatility的相关基础插件的操作和使用*  *掌握内存取证的基本步骤和实际操作* | | |

|  |  |
| --- | --- |
| 实验内容 | 使用volatility对内存镜像进行操作。并且使用pslist、psscan、pstree、timeliner插件，并且描述对应的结果  先进入对应的路径，打出以下命令可以查看帮助    -f就是要输入的文件镜像    因为还需要知道文件对应的系统到底是什么，可以使用imageinfo这个插件    故，先使用的命令如下：  volatility\_2.6\_win64\_standalone.exe -f 内存镜像.dd imageinfo  这里要注意内存镜像一定要放在和volatility软件一个目录下才能这样，不知道为啥我用绝对路径会出错。    要注意imageinfo这个插件只有对windows系列系统才有效，对于其他的系统是无效的。    pslist插件:遍历EPROCESS结构体来输出所有运行的进程到屏幕上。（EPROCESS是一种双链表结构体，每有一个进程运行就会将其加入这个结构体中）PS.双链表结构体这里就是一个有分别指向着前、后两个结构体的指针  psscan插件:扫描所有的进程项。  对两者的结合使用：      上面的是对pslist里面的内容的解释，这里面的句柄数可以理解为是占用了的资源数。会话数（上面打错了……是会话）是与网络的交互，Exit是内核里这个进程结束的时间。      比较内容结果之后就可以发现了，差异就是有一个进程id为712的进程隐藏起来了    如果觉得这样的排列看着不方便找到进程之间的父子关系，还可以用pstree插件。它会把所有的没有被隐藏的进程都以树的方式来表示出来，看起来会更加直观。    这样就可以让这些内容显示的更加清楚了。  另外，还有一个插件tiimeliner也需要了解。  这个插件可以记录所有的进程的所有的操作。      如果内容过多，则可以使用管道命令重定向到对应的文件中去    这样就会在对应的路径下出现一个233.txt的文档，里面的内容就是之前在命令行里面出现的那些内容 |
| 实验总结 | （对本次实验涉及到的知识点的重难点归纳、实验心得、思考与建议）  这个主要是了解内存取证的相关知识，并且掌握对应的工具的使用，在查找隐藏起来的恶意进程的时候比较麻烦……看起来比较累。 |
| 评分 |  |