Kali Linux 渗透测试

The quieter you become，the more you are able to hear

第十八章 计算机取证

苑房弘 Fanghong.yuan@163.com

取证科学简介

- Forensic investigations
- 法庭取证调查
- 事件响应调查
  - 黑客攻击、渗透测试留痕

取证科学

- 什么是 Forensic 科学
  - 法医的、用于法庭的、辩论学、法医学
  - 为了侦破案件还原事实真相，收集法庭证据的一系列科学方法
    - 参考本地区法律要求
    - 实践操作通用原则
- CSI：物理取证
  - 指纹、DNA、弹道、血迹、
  - 物理取证的理论基础是物质交换原则
- 本章关注：数字取证 / 计算机取证 / 电子取证
  - 智能设备、计算机、手机平板、IoT、有线及无线通信、数据存储

通用原则

- 维护证据完整性
  - 数字取证比物理取证幸运的多，可以有无限数量的拷贝进行分析
  - 数字HASH值验证数据完整性
- 维护监管链
  - 物理证物保存在证物袋中，每次取出使用严格记录，避免破坏污染
  - 数字证物原始版本写保护，使用拷贝进行分析
- 标准的操作步骤
  - 证物使用严格按照按照规范流程，即使事后证明流程有误（免责）
- 取证分析全部过程记录文档

通用原则

- 数字取证者的座右铭
  - 不要破坏数据现场（看似简单，实际几乎无法实现）
  - 寄存器、CPU缓存、I/O设备缓存等易失性数据几乎无法获取
  - 系统内存是主要的非易失性存储介质取证对象，不修改无法获取其中数据
  - 非易失性存储介质通常使用完整镜像拷贝保存
  - 正常关机还是直接拔掉电源（数据丢失破坏）
- 证据搜索
  - 数据
  - 信息
  - 证据

取证科学

- 作为安全从业者
  - 通过取证还原黑客入侵的轨迹
  - 作为渗透测试和和黑客攻击区分标准
    - 世纪佳缘事件
    - 印象笔记渗透测试事件

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 存储收集到的数据
- 死取证
  - 关机后制作硬盘镜像、分析镜像（MBR、GPT、LVM）

取证工具

- 不考虑法律因素、法庭证据、监管链、文档记录等取证环节
- 只介绍Kali当中部分取证工具的使用方法
- 内存dump工具
  - Dumpit：http://www.moonsols.com/wp-content/uploads/downloads/2011/07/DumpIt.zip
  - 内存文件与内存大小接近或者稍微大一点，raw格式

取证工具

- 分析内存文件
  - volatility imageinfo -f xp.raw　　#文件信息，关注profile
  - volatility hivelist -f XP.raw --profile=WinXPSP3x86　#数据库文件
  - volatility -f XP.raw --profile=WinXPSP3x86 hivedump -o 0xe124f8a8
  - # 按虚内存地址查看注册表内容
  - volatility -f XP.raw --profile=WinXPSP3x86 printkey -K "SAM\Domains\Account\Users\Names"　　# 用户账号
  - volatility -f xp.raw --profile=WinXPSP3x86 printkey -K "SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon"　#最后登陆的用户
  - volatility -f XP.raw --profile=WinXPSP3x86 userassist　　#正在运行的程序、运行过多少次、最后一次运行时间等

取证工具

- 分析内存文件
  - volatility -f XP.raw --profile=WinXPSP3x86 pslist #进程列表及物理内存位置
    - volatility -f 7.raw --profile=Win7SP1x64 memdump -p 1456 -D test #dump进程内存
    - strings 1456.dmp > 1111.txt # 提取字符串 grep password / @
  - volatility cmdscan -f 7.raw --profile=Win7SP1x64 #命令行历史
  - volatility netscan -f 7.raw --profile=Win7SP1x64 #网络连接
  - volatility iehistory -f 7.raw --profile=Win7SP1x64 #
  - volatility -f 7.raw --profile=Win7SP1x64 hivelist #提取HASH
    - volatility -f 7.raw --profile=Win7SP1x64 hashdump -y system -s SAM

Volatility插件

- Firefoxhistory 插件
  - http://downloads.volatilityfoundation.org/contest/2014/DaveLasalle_ForensicSuite.zip
  - /usr/lib/python2.7/dist-packages/volatility/plugins/
  - volatility -f 7.raw --profile=Win7SP1x64 firefoxhistory
- USN日志记录插件
  - NTFS特性，用于跟踪硬盘内容变化（不记录具体变更内容）
  - https://raw.githubusercontent.com/tomspencer/volatility/master/usnparser/usnparser.py
  - volatility -f 7.raw --profile=Win7SP1x64 usnparser --output=csv --output-file=usn.csv #

Volatility插件

- Timeline 插件
  - volatility -f 7.raw --profile=Win7SP1x64 timeliner
  - 从多个位置收集大量系统活动信息
- 内存取证发现恶意软件
  - https://github.com/volatilityfoundation/volatility/wiki/Memory-Samples
  - https://code.google.com/archive/p/volatility/wikis/SampleMemoryImages.wiki

Volatility插件

- 内存取证发现恶意软件
  - XP：建立 meterpreter session 后 dump 内存分析
  - volatility -f xp.raw --profile=WinXPSP3x86 pstree
  - volatility connscan # 网络连接
  - volatility getsids -p 111,222 # SID
  - volatility dlllist -p 111,222 # 数量
  - volatility malfind -p 111,222 -D test # 检查结果查毒

活取证

- 从内存还原文字
  - https://technet.microsoft.com/en-us/sysinternals/dd996900.aspx
  - https://technet.microsoft.com/en-us/sysinternals/bb897439.aspx
  - procdump -ma notepad.exe notepad.dmp
  - strings notepad.dmp > notepad.txt
  - 其他文字处理程序也适用
- 从内存还原图片
  - 远程桌面、画图工具、Virtualbox 虚拟机
  - volatility -f 7.raw --profile=Win7SP1x64 memdump -p 1456 -D test
  - mv mstsc.dmp mstsc.data
  - Gimp -> open -> Raw Image Data -> 调整参数

活取证

- 从内存中提取明文密码
  - procdump -ma lsass.exe lsass.dmp
  - Mimikatz
  - sekurlsa::minidump lsass.dmp
  - sekurlsa::logonPasswords
- Volatility 的 mimikatz 插件
  - https://github.com/sans-dfir/sift-files/blob/master/volatility/mimikatz.py
- Firefox 浏览器审计工具
  - dumpzilla /root/.mozilla/firefox/bvpenhsu.default/ --All

死取证

- 硬盘镜像
  - 使用 kali 光盘启动计算机创建硬盘镜像文件
  - 留足存储镜像文件的存储空间
  - Dc3dd 来自美国空军计算机犯罪中心
  - Dcfldd
  - Guymager
  - 计算机取证技术参考数据集
    - http://www.cfreds.nist.gov/Controlv1_0/control.dd
- DFF（Digital Forensics Framework）
  - Open Evidence　　# 红色表示已经删除的文件
  - 发现恢复已经删除和隐藏的文件

死取证

- Autopsy
  - 非常流行的硬盘镜像分析工具
  - WebServer + 客户端 架构
- Extundelete
  - 适用于ext3、ext4文件系统的反删除工具
  - Extundelete [device-file] --restore-file [restore location]
- iPhone Backup Analyzer
  - 分析 iTunes 生成的 iPhone 手机备份文件，并非电话image
- Foremost （美国政府开发）
  - 从内存dump中恢复文档图片，支持raw、dd、iso、vmem等格式
  - foremost -t jpeg,gif,png,doc -i 7.raw

死取证

- 网络取证请看《协议分析》
  - 全流量镜像可以还原历史

Kali Linux 渗透测试 < 完 >

- 自我评价
  - 内容全面、结构系统；
  - 我已经尽力了，自己很满意，希望大家都听懂了！
  - 不断被抄袭，一定程度上促进了行业发展；
  - 过去共同学习，来日各自探索！