数字取证技术(Digital Forensics Technology)笔记I

数字取证技术概述

👉**知识点(数字取证技术)** 数字取证是信息安全领域的一个重要分支,关注收集、分析、保存电子数据证据,用于法律诉讼程序.数字取证的基本步骤:

- 电子数据获取(Acquire):包括截获或解码解密数据(常用工具如Wireshark,Autopsy);
- 数据的鉴定,恢复和保护(Maintenance):包括修复损坏的数据或复制保护已有的数据(常用工具如Guymager,dd,Recuvan,PhotoRec,TestDisk,R-Studio,Runtime's GetDataBack,Ontrack EasyRecovery);
- 数据的分析(Analyze):应用数学或计算机算法更清晰地呈现数据的内涵(常用工具如c++,python,opencv,numpy,SageMath...);
- 数据的报告展示(Present):撰写报告使普通人能理解取证的客观结论(常用工具如Markdown);

▧**例子(数字取证技术的历史)** 不限于使用计算机取证的历史(Forensics Timeline):

- 1835年:Henry Goddard使用物理方法分析子弹和凶杀案的关联性(物理方法);
- 1836年:James Marsh设计了化学检测手段用于检测凶杀案中的砒霜成分(化学方法);
- 1930年:Karl Landsteiner因为血液鉴定分类方法获得了诺贝尔奖(生物方法);
- 1988年:国际计算机调查专家协会(International Association of Computer Investigative Specialists,IACIS)成立,标志着数字取证技术成为刑事调查的主流手段;

(♞**思考)** 计算机取证是否只能应对计算机领域的犯罪?请列举反例;

Linux基本知识

👉**知识点(grep)** 用于查找含有某个字段的文件(比如在文件夹"/home/doc"中迭代地查找含有"name"字段的文件):

```
$ grep -ri /home/doc "name"
```

👉**知识点(find)** 用于查找含有某个名字的文件(比如在文件夹"/home/code"中迭代地查找c++文件):

```
$ find /home/code -name *.cpp
```

👉**知识点(管道)** "管道"(pipe)是一种强大的功能,允许将一个命令的输出作为另一个命令的输入(比如在展示的进程里过滤出含"GameName"的进程):

```
$ ps -aux | grep "GameName"
```

(🐴**思考**) Linux的关机命令是什么,为什么不提倡直接关闭电源来关机;

(🐴**思考**) 作为系统管理员,需要定期检查位于/var/log/auth.log的系统认证日志文件,以识别所有失败的sudo尝试;编写一个管道命令,筛选出所有包含"sudo"和"失败"关键字的日志条目,并计算这类事件的总数;

```
$ grep "sudo" /var/log/auth.log | grep "失败" | wc -l
```

(🐴**思考**) 在一台运行Linux的服务器上,有一个位于/var/www/html目录下的大型网站,该目录包含数千个.php和.html文件;如何找出所有文件内容中包含字符串"deprecated"(表示使用了不推荐的代码)的文件,并将这些文件的完整路径和文件名输出到/home/user/deprecated-list.txt文件中;

```
$ grep -rl "deprecated" /var/www/html/ --include=\*.{php,html} >
 /home/user/deprecated-list.txt
```

(🐴**思考**) 现在怀疑某个不明确的进程可能在不适当的时间进行网络连接,试图发送敏感数据;编写一个命令或脚本来监控和记录过去一小时内所有尝试通过TCP端口443(HTTPS)建立外部连接的进程名称和它们的PID,保留这些信息以供日后分析;

```
$ netstat -tunapl | awk '/:443/ {print $7}' | sort |
uniq -c | sort | tail -n +1
```

命令行使用netstat列出所有活动的连接,awk '/:443/ {print $7}'筛选出目标端口为443的连接,并打印出其进程ID和名称。然后通过排序和统计每个进程的连接数,显示了在过去一小时内尝试建立外部连接的独特进程(tail命令用于查看文件末尾内容,它通常与标准输入或文件相关联,并将其最后一部分输出到屏幕或其他设备上);