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

> 在数字取证领域,Linux操作系统被认为是强大且灵活的环境,具备许多适用于分析和应对复杂取证任务的工具.与Windows操作系统取证相比,Linux取证具有一些独特的特点和优势.Linux操作系统取证更加依赖技术知识和命令行工具的使用,而在Windows中,则更侧重用户界面的灵活性和易用性.Linux操作系统的开源特性为取证分析提供了更深入的可见性,但也意味着需要较高的技术熟练程度.两种环境上的取证均要求对系统特有的文件结构、日志机制和工具集有所了解.

Linux操作系统取证技术

👉**知识点(dd)**:用于创建磁盘或分区的位镜像.

示例:

```
dd if=/dev/sda1 of=/tmp/disk_image.iso bs=4096 conv=noerror,sync
```

- `if`:输入文件(input file),这里是指磁盘设备.
- `of`:输出文件(output file),即创建的磁盘镜像位置.
- `bs`:块大小(block size),每次读取/写入的字节数.
- `conv`:转换选项,`noerror` 继续操作发生错误的读取,`sync` 使用空字节填充块.

结果示例:

```
20480+0 records in
20480+0 records out
104857600 bytes (105 MB, 100 MiB) copied, 10.0253 s, 10.5 MB/s
```

- 显示了读取和写入的块数量、总字节数、花费的时间及平均速率.

👉**知识点(strings)**:从二进制文件中提取可打印的字符序列.

示例:

```
strings -n 10 /bin/bash
```

- `-n`:输出长度至少为10的字符串序列.

结果示例:

```
/usr/lib/locale
LC_CTYPE
POSIX
```

- 这是从`/bin/bash`中提取出的字符串序列清单,通常更长,这里只展示了部分.

👉**知识点**(hexdump):以十六进制格式查看文件内容.

示例:

```
hexdump -C -n 100 /bin/bash
```

- `-C`:规范格式显示,展示十六进制和ASCII内容.
- `-n`:指定查看文件的前100个字节.

结果示例:

```
00000000  7f 45 4c 46 02 01 01 00  00 00 00 00 00 00 00 00  |.ELF............|
00000010  03 00 3e 00 01 00 00 00  60 09 40 00 00 00 00 00  |..>.....`.@.....|
...
```

- 每行包含了十六进制的字节表示和相应的ASCII字符.

👉**知识点**(find):搜索文件系统中的文件.

示例:

```
find / -name "*.log" -mtime -7 -print
```

- `/`:从根目录开始搜索.
- `-name`:搜索符合给定模式的文件名.
- `-mtime`:搜索在最近7天内被修改的文件.
- `-print`:打印找到的文件全路径.

结果示例:

```
/var/log/syslog
/var/log/kern.log
...
```

- 输出最近7天内被修改过的`.log`文件列表.

👉**知识点(grep)**:搜索文件内容.

示例:

```
grep "Failed password" /var/log/auth.log
```

- 搜索`/var/log/auth.log`中包含"Failed password"的行.

结果示例:

```
Feb 15 10:17:31 ubuntu sshd[2898]: Failed password for invalid user root from
192.168.1.101 port 22 ssh2
...
```

- 输出所有包含"Failed password"的日志行,显示登录失败的尝试.

👉**知识点(netstat)**:显示网络连接、路由表、接口统计等信息,有助于理解发生在系统上的网络事件.

示例:

```
netstat -antup
```

- `-a` 显示所有选项,默认情况下不显示监听的服务器套接字.
- `-n` 显示数字形式的地址(默认显示域名).
- `-t` 显示TCP连接.
- `-u` 显示UDP连接.
- `-p` 显示监听端口的程序名.

结果示例:

```
Proto Recv-Q Send-Q Local Address           Foreign Address         State
PID/Program name
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
1234/sshd
...
```

- 列出了系统上的所有TCP网络连接和监听状态,以及关联的进程.

👉**知识点(df)**:显示文件系统的磁盘空间使用情况,有助于发现异常的数据存储模式.

示例:

```
df -h
```

- `-h` 以易读的格式(如 MB、GB)显示信息.

结果示例:

```
Filesystem      Size  Used Avail Use% Mounted on
/dev/sda1        20G   13G  6.0G  65% /
...
```

- 显示了每个文件系统的总大小、已使用空间、可用空间和使用百分比.

👉**知识点(lsof)**:列出当前系统打开文件的工具,用于发现正在运行的进程及其文件使用情况.

示例:

```
lsof -u username
```

- `-u` 按指定用户的进程列出文件.

结果示例:

```
COMMAND  PID   USER   FD   TYPE DEVICE SIZE/OFF     NODE NAME
sshd     1234  user   cwd  DIR  8,1    4096          2   /home/user
...
```

- 显示了用户`username`所运行进程的文件使用情况.

👉**知识点(mount/umount)**:挂载(mount)和卸载(umount)文件系统,常用于访问存储设备或磁盘镜像.

示例:

```
mount /dev/sdb1 /mnt/usb
```

- 将 `sdb1` 设备挂载到 `/mnt/usb`.

```
umount /mnt/usb
```

- 卸载 `/mnt/usb` 处的设备.

结果示例:通常不产生输出.

👉**知识点(fsck)**:检查和维护完整性和一致性的文件系统工具.

示例:

```
fsck /dev/sdb1
```

- 对设备 `sdb1` 进行文件系统检查.

结果示例:

```
fsck from util-linux 2.31.1
e2fsck 1.44.1 (24-Mar-2018)
/dev/sdb1: clean, 11/128016 files, 14221/512000 blocks
```

- 输出显示 `/dev/sdb1` 的文件系统检查结果.

👉**知识点(md5sum /sha256sum)**:计算和校验文件的 MD5 或 SHA-256 哈希值,用于验证文件的完整性.

示例:

```
md5sum example.txt
```

- 计算并显示 `example.txt` 文件的 MD5 哈希值.

```
sha256sum example.txt
```

- 计算并显示 `example.txt` 文件的 SHA-256 哈希值.

结果示例:

```
9e107d9d372bb6826bd81d3542a419d6  example.txt
```

- 显示了 `example.txt` 文件的 MD5 哈希值.

```
e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855  example.txt
```

- 显示了 `example.txt` 文件的 SHA-256 哈希值.

👉**知识点(注册表的功能)**:...

思考题

(🐴**思考**):作为取证分析师,您怀疑某个犯罪分子修改了系统上的某些图片文件来隐藏信息.这些图片文件的后缀名为".png".请问如何使用Linux命令来计算特定目录下所有PNG图片文件的SHA-256哈希值,以便稍后进行检查和验证?

参考答案:

```
find /suspect/directory -name "*.png" -exec sha256sum {} + > image_hashes.txt
```

该命令使用 `find` 来搜索 `suspect/directory` 目录下所有 `.png` 文件,然后对每个找到的文件执行 `sha256sum` 命令,并将结果重定向输出到文件 `image_hashes.txt` 中.借助 `-exec` 参数, `{}` 代表当前处理的文件名, `+` 表示对找到的所有文件一起执行 `sha256sum` 命令.

(🐴**思考**):如果您需要查找最近7天内修改过的可疑脚本文件,这些脚本位于特定用户的home目录下,例如用户"bob",并且具有".sh"扩展名,您将如何使用Linux命令行来完成这项任务?

参考答案:

```
find /home/bob -name "*.sh" -mtime -7 -ls
```

- 这个 `find` 命令检查了用户"bob"的home目录(`/home/bob`)下所有 `.sh` 文件,在过去7天内修改过的文件会被列出,选项 `-ls` 会显示出每个找到文件的详细信息.

(🐴**思考**):如何使用单个Linux命令行,从系统中已经删除（但磁盘上尚未被覆盖的数据）的文件中恢复可能存在的可打印字符串?

参考答案:

```
grep --binary-files=text -a -C 200 '特定字符串' /dev/sda1 > recovered_text.txt
```

命令 `grep` 用于搜索磁盘 `/dev/sda1` 中含有'特定字符串'的数据,选项 `-a` 把二进制文件当作文本处理, `-C 200` 表示在找到的字符串周围包含200字节的内容,这有助于找到完整的字符串或文本段落,

输出重定向到了文件`recovered_text.txt`中.

(♞思考):对一次安全事件中某服务器的网络连接情况进行调查,如何使用命令行列出所有当前的TCP连接,以及每个连接的源地址和目的地址?

参考答案:

```
netstat -atn
```

`netstat`命令用于显示网络连接,选项`-a`显示所有连接和监听端口,`-t`表示仅显示TCP连接,`-n`显示数字地址,不进行主机名解析.