网络安全溯源指南

V 1.0

寸光网络安全工作室

商务合作（微信）：Signboards

2023 年 11 月 19 日

寸光网络安全工作室

目录

一、 window 系统溯源 4
1、 检查系统账号安全 4
1.1 查看服务器是否存在可疑账号、新增账号 4
1.2 查看服务器是否存在隐藏账号、克隆账号 4
1.3 查看 window 日志，检查登入时间，是否存在暴力破解等行为 5
2、 检查异常端口、进程 5
2.1 检查端口连接情况，查看是否有可疑 IP 外连。 5
2.2 查看进程 6
3、 检查启动项、计划任务、服务 8
3.1 检查启动项 8
3.2 查看计划任务 9
3.3 排查服务自启动 9
4、 检查系统相关信息 10
4.1 查看系统补丁信息 10
4.2 查看近期创建修改的文件 10
二、 Linux 系统溯源 11
1、 系统排查 11
1.1 系统信息 11
1.2 用户账号 11
1.3 启动项 12
1.4 定时任务 12
2、 服务排查 13
2.1 进程查看 13
2.2 线程查看 13
2.3 进程查杀 13
2.4 调试分析 14
2.5 查看服务 14
3、 网络排查 14
3.1 分析可疑端口、可疑 IP、可疑 PID 及程序进程 14
4、 文件排查 15
4.1find 命令的使用 15
4.2 敏感目录 16
4.3 基于时间点查找 16
三、日志分析 17
1、window 日志分析 17
1.1 安全日志分析 17
2、Linux 日志分析 22
2.1 分析 secure 日志 23
2.2 分析应用日志 23
四、文件恢复 24

1、 Window 24
1.1WinFR 24
1.2Windows File Recovery 24
2、 Linux 25
2.1losf 命令 25
2.2extundelete 26
2.3testdisk 27
五、溯源到人 32
1、IP 溯源 32
2、ID 溯源 33
3、手机号溯源 33
4、EMail 溯源 33
5、域名溯源 33
6、木马分析（云沙箱） 34

一、window 系统溯源

1、检查系统账号安全

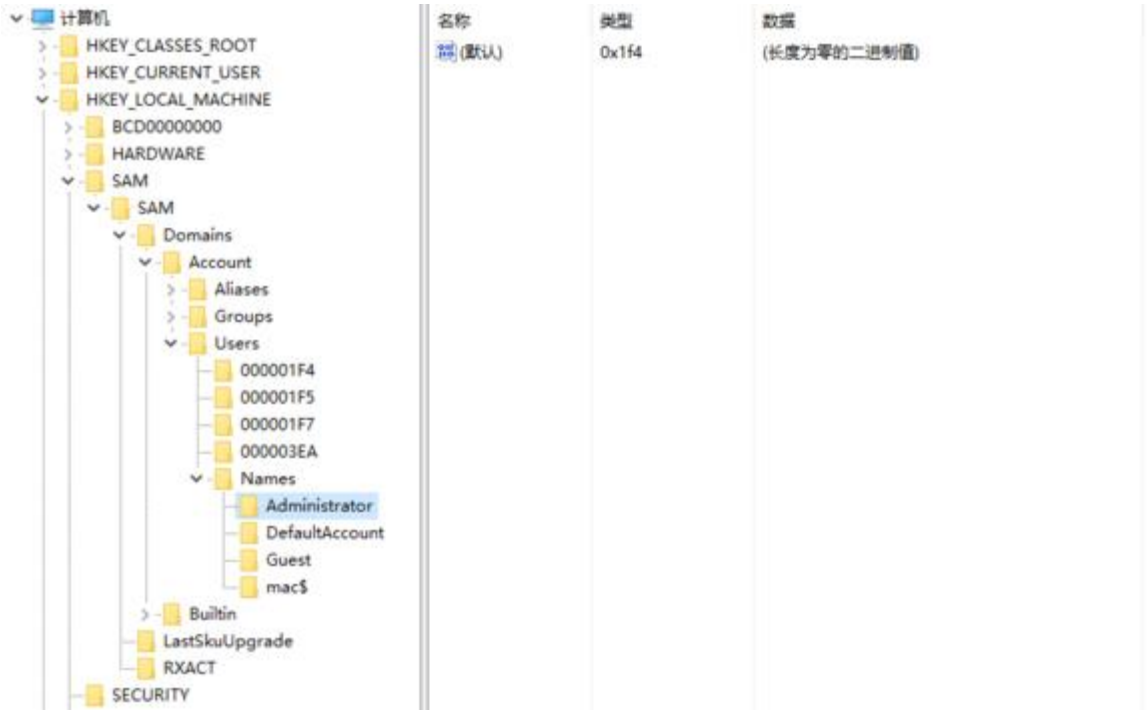
1.1 查看服务器是否存在可疑账号、新增账号

打开 cmd 窗口，输入 lusrmgr.msc 命令，查看是否有新增/可疑的账号，如有管理员群组的（Administrators）里的新增账户，如有，请立即禁用或删除掉。

lusrmgr.exe（无法找到注册表方式建立的用户）

net user（无法列出$用户）

HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users\（查看注册表最准确）



1.2 查看服务器是否存在隐藏账号、克隆账号

使用 D 盾_web 查杀工具，集成了对克隆账号检测的功能。

1.3 查看 window 日志，检查登入时间，是否存在暴力破解等行为

日志位置：

Windows 2000 / Server2003 / Windows XP：

%SystemRoot%\System32\Winevt\Logs*.evtx

Windows Vista / 7 / 10 / Server2008 及以上版本：

%SystemRoot%\System32\Config*.evtx

Windows 事件日志中，它记录为事件 ID=4625 表示失败，记录为事件 ID=4624 表示成功。

属性	描述
审计失败（4625）：	这是事件 ID 4625 的审核失败。
登录类型：3：	登录类型 3 表示这是一次远程登录尝试。
帐户名称：AZUREUSER	那是用户尝试过的（AZUREUSER）。
源网络地址：164.92.82.228	攻击者使用的IP地址。

命令行提取：

wevtutil qe security /q:"*[EventData[Data[@Name='LogonType']='10'] and System[(EventID=4624)]]" /f:text /rd:true /c:10

2、检查异常端口、进程

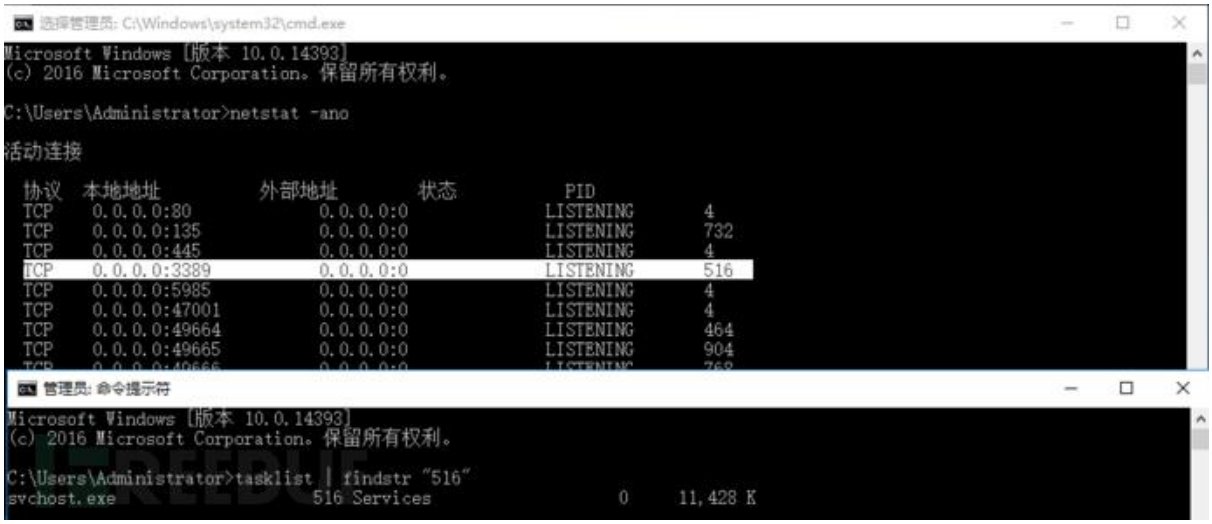
2.1 检查端口连接情况，查看是否有可疑 IP 外连。

重点观察状态是 ESTABLISHED 的可疑 IP

netstat -ano 查看目前的网络连接

重点看状态是 ESTABLISHED 的端口：netstat -ano | findstr 'estab'

再通过 tasklist 命令进行进程定位 tasklist | findstr “PID”



2.2 查看进程

可以重点观察以下内容：

1、CPU 或内存资源占用长时间过高的进程

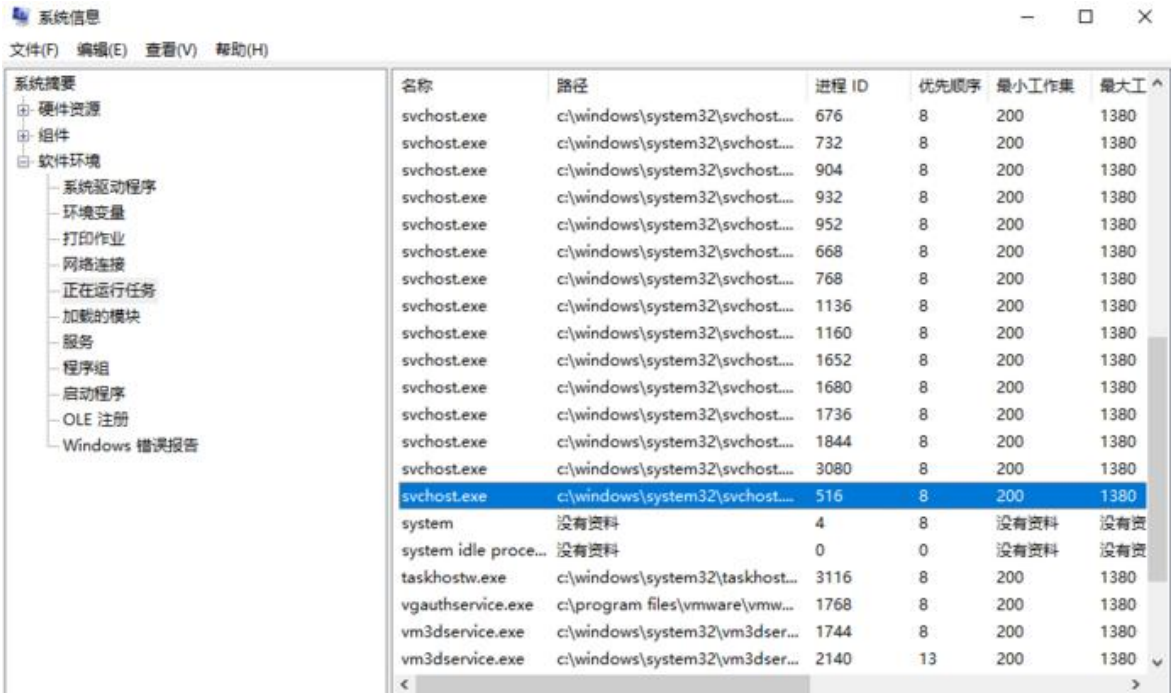
2、没有签名验证信息的进程

3、进程的路径是否合法、常规

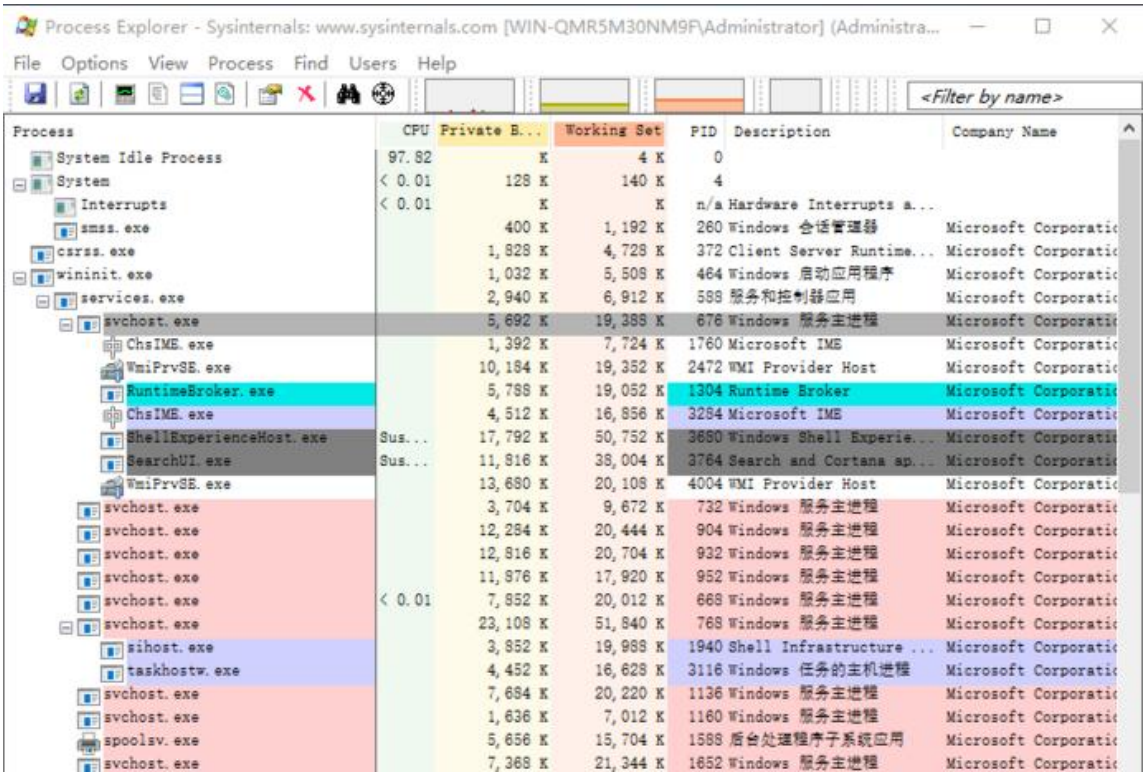
4、没有描述信息的进程

显示 进程--PID--服务： tasklist /svc

开始--运行--输入 msinfo32，依次点击“软件环境→正在运行任务”就可以查看到进程的详细信息，比如进程路径、进程 ID、文件创建日期、启动时间等。



通过微软官方提供的 Process Explorer 等工具进行排查

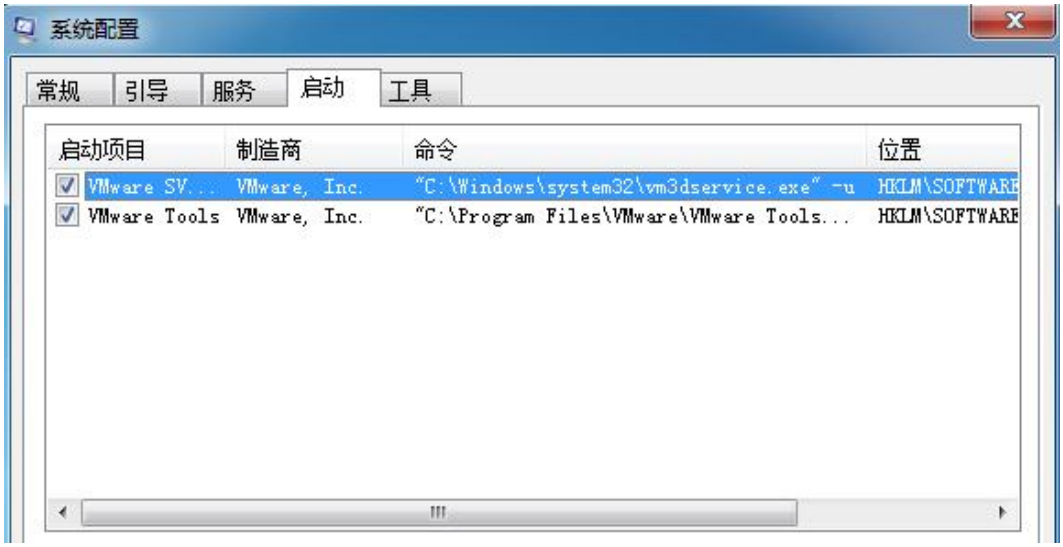


3、检查启动项、计划任务、服务

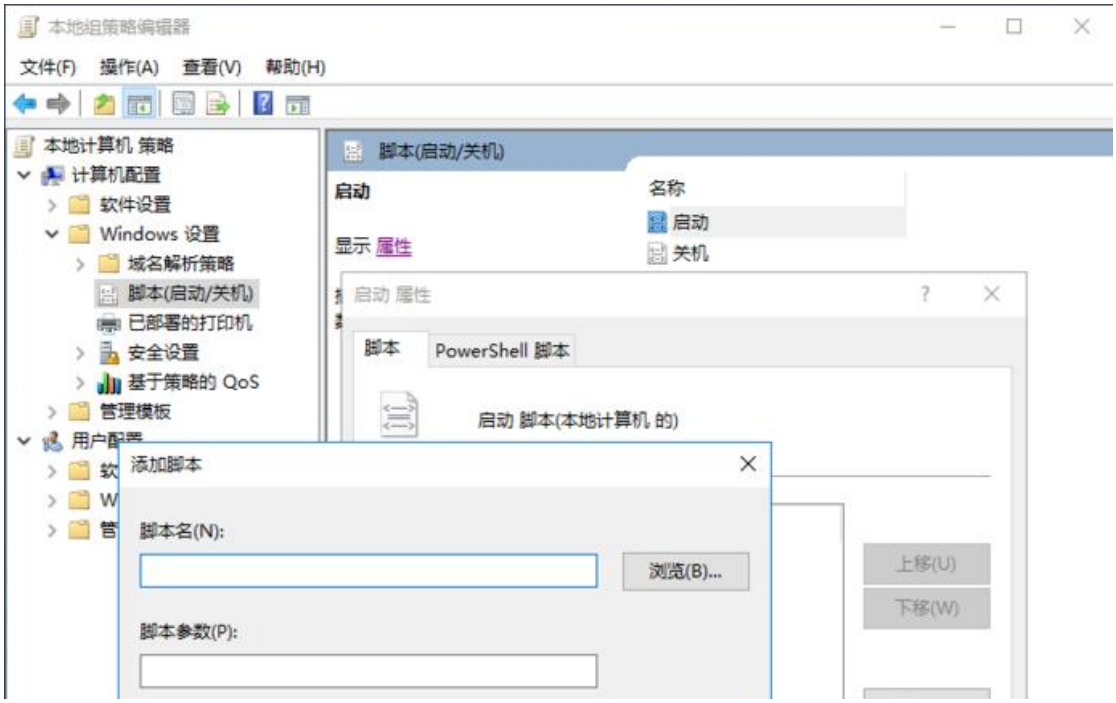
3.1 检查启动项

3.1.1 单击【开始】>【所有程序】>【启动】，默认情况下此目录在是一个空目录，确认是否有非业务程序在该目录下。

3.1.2 单击开始菜单 >【运行】(快捷键 win+R)，输入 msconfig，查看是否存在命名异常的启动项目，是则取消勾选命名异常的启动项目，并到命令中显示的路径删除文件。



3.1.3 桌面打开运行（可使用快捷键 win+R），输入 gpedit.msc 查看组策略



3.2 查看计划任务

在控制面板里面的系统与安全中查看计划任务属性。

3.3 排查服务自启动

在桌面打开运行（可使用快捷键 win+R），输入 services.msc

、

4、检查系统相关信息

4.1 查看系统补丁信息

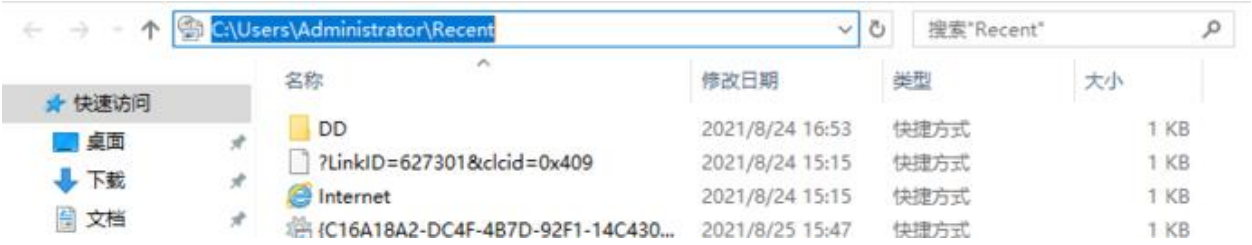
在桌面打开运行（可使用快捷键 win+R）输入 systeminfo

4.2 查看近期创建修改的文件

利用计算机自带文件搜索功能，指定修改时间进行搜索。

利用 Registry Workshop 注册表编辑器的搜索功能，可以找到最后写入时间区间的文件。

单击【开始】>【运行】，输入%UserProfile%\Recent，分析最近打开分析可疑文件



二、Linux 系统溯源

Linux 入侵溯源分析分系统、服务、文件、网络四个部分

1、系统排查

1.1 系统信息

```
$ lscpu                    #查看 CPU 信息
$ uname -a                 #操作系统信息
$ cat /proc/version #系统版本信息
$ cat /etc/redhat-release   #查看系统发行版
$ lsmod                    #查看模块信息
$ lsblk                    #列出块设备信息
$ ifconfig eth0 | grep -w inet   #显示网卡 IP 信息
$ curl cip.cc         #查看主机公网 IP 信息
$ hostname            #查看系统主机名称
$ cat /etc/resolv.conf     #DNS 配置查看
```

1.2 用户账号

(1) 查看系统用户信息

```
$ cat /etc/passwd
```

用户名:密码加密:用户 ID:用户组 ID:注释:用户主目录:默认登录 shell

最后一列：/bin/bash 表示用户状态可登录; /sbin/nologin 表示账户状态不可登录

```
$ history 查看用户历史操作命令
```

(2) 查询超级权限账户: UID 为 0

```
$ awk -F: '{if($3==0)print $1}' /etc/passwd
```

(3) 查看可登录账户

```
$ grep '/bin/bash' /etc/passwd
```

(4) 查看空口令账户

```
$ awk -F: 'length($2)==0 {print $1}' /etc/shadow
```

(5) 登录信息查看

```
$ lastlog | more   #查看用户最后登录信息
$ lastb | more      #显示用户错误的登录信息
$ last | more       #查看用户最近登录信息
$ uptime   #查看登陆多久、多少用户，负载
$ who     #查看当前登录用户（tty 本地登陆   pts 远程登录）
$ w        #查看系统信息，想知道某一时刻用户的行为
```

/var/log/wtmp: 存储登录成功的信息
/var/log/btmp: 存储登录失败的信息
/var/log/utmp: 存储当前正在登录的信息

(6) 查看除 root 账号外其他帐号是否存在 sudo 权限

```
$ more /etc/sudoers | grep -v "^#\|^$" | grep "ALL=(ALL)"
```

(7) 禁用或删除多余及可疑的帐号

```
$ usermod -L user      #禁用帐号，帐号无法登录，/etc/shadow 第二栏为!开头
$ userdel user          #删除 user 用户
$ userdel -r user      #将删除 user 用户，并且将/home 目录下的 user 目录一并删除
```

1.3 启动项

```
$ cat /etc/init.d/rc.local
$ cat /etc/rc.local
$ ls -alt /etc/init.d/ | head
```

1.4 定时任务

```
crontab -u <-l, -r, -e>
```

-u 指定一个用户
-l 列出某个用户的任务计划
-r 删除某个用户的任务
-e 编辑某个用户的任务

```
$ crontab -u root -l   # 列出 root 用户的任务计划
```

2、服务排查

2.1 进程查看

```
$ ps -elf | grep pid   # 以长格式显示系统中的进程信息
$ ps -aux --sort -pcpu | less     # 根据 cpu 使用率进行排序
$ ps -aux --sort -pmem | less     # 根据内存使用来升序排序
$ ps -axjf   # 以树形结构显示进程
$ top 动态查看进程状态，可分析 CPU 占用较高的进程，排查挖矿木马

<查看进程打开的文件>
$ lsof -p pid     # 查看指定进程 ID 已打开的内容
$ lsof -i         # 显示所有连接
$ lsof -i:port   # 查看与指定端口相关的网络信息
$ lsof -i@ip      # 查看与指定 IP 相关的网络信息
$ lsof -i -sTCP:LISTEN     # 找出正等待连接的端口
$ lsof -i | grep -i ESTABLISHED   # 找出已经建立的连接
$ lsof -u user        # 使用-u 显示指定用户打开哪些文件
$ lsof -u ^root       # 查看除指定用户以外的其它所有用户所做的事情
$ lsof -c command   # 查看指定的命令正在使用的文件和网络连接
$ lsof | grep deleted          # 查看被删除的文件信息
$ kill -9 `lsof -t -u user` # 杀死指定用户运行的所有进程
$ lsof -u user -i @ip          # 显示用户 user 连接到指定 IP 所做的一切
```

2.2 线程查看

```
<根据 pid 查看由进程起的线程>
$ ps H -T -p pid
$ ps -Lf pid
$ top -H -p pid -H 选项可以显示线程
$ pstree -acU 推荐，非常全面展示进程与线程间的关系
$ ps -eLFa   # 查看全部线程
```

2.3 进程查杀

```
<kill 进程>
$ kill -9 pid        #强制终止进程
$ killall name       #依据进程名称杀死进程
$ killall -u user #杀死指定用户的进程
```

$ kill -9 -pid　　# 如果进程起子进程，可以使用此命令，这里 pid 前有个减号，表示杀掉这个进程组

$ pkill name　　#杀死指定进程名的进程

2.4 调试分析

<跟踪进程执行时的系统调用和所接收的信号,可跟踪用户进程与 Linux 内核之间的交互>

$ strace -p `pidof AliYunDun`　# 依据 pid 跟踪进程正在进行的系统调用

$ strace -o trace.log ls testdir/　　#将输出记录到文件中

$ strace -v ls testdir　#在每个系统调用中提供附加信息\

$ strace -f ls testdir　#对当前正在跟踪的进程创建的任何子进程进行跟踪

$ strace -e open ls testdir　　#使用-e 标志跟上系统调用的名称

$ strace -e write,getdents ls testdir　#查看多个系统调用

$ strace -t ls testdir/　　#查看所有的系统调用的时间戳

$ strace -r ls testdir/　　#显示执行每个系统调用所花费的时间

<显示每个进程的栈跟踪>

$ pstack pid

2.5 查看服务

$ chkconfig　--list　#查看系统运行的服务

0-6 表示等级

1 单用户模式

2 无网络连接的多用户命令模式

3 有网络连接的多用户命令模式

4 表示不可用

5 带图形界面的多用户模式

6 重新启动

$ service --status-all | grep running　|　more　　#显示正在运行的服务

$ systemctl list-unit-files | grep enabled | more　#列出 systemd 下正在运行服务

3、网络排查

3.1 分析可疑端口、可疑 IP、可疑 PID 及程序进程

$ sudo netstat -ltpe | more # 查看监听中的网络连接并显示进程 ID、进程所有者用户名

$ sudo netstat -antp | grep "ESTABLISHED'' # 查看正在通信中的连接信息

$ sudo netstat -antpe # -n 和 -e 选项连用，显示进程所有者的用户 ID 号

$ netstat -ts # 打印出 tcp 协议下的收发包数量等统计数据

$ watch -d -n0 "netstat -atnp | grep "ESTA" # 监视 active 状态的连接

$ ss -plat # 检查哪些进程在监听端口

<网络占用查看>

Debian/Ubuntu

apt-get install nethogs

Centos/RHEL

yum -y install epel-release

yum -y install nethogs

4、文件排查

4.1find 命令的使用

基础使用

find / -name evil.sh

忽略大小写

find / -iname evil.sh

查找时排除某个/类文件

find / -name *evil* ! -name *.log

查找时排除目录

find / -name *evil* -path "/root/home/aaa" -prune

查找目录

find / -type d -name eval

<根据文件大小搜索>

$ find / -size -1223124c -size +1223122c -exec ls -id {} \; #搜索 1223123 大小的文件

$ find /usr/bin -type f -size 2k # 查找大小等于 2KB 的文件

$ find / -size +10MB -20M # 寻找 10M 到 20M 之间的文件

<特殊文件匹配>

$ find /var/www/ -name "*.php" |xargs egrep 'assert|phpspy|c99sh|milw0rm|eval|\(gunerpress|\(base64_decoolcode|spider_bc|shell_exec|passthru|\(\$_\POST\[|eval \(str_rot13|\.chr\(|\$\{\"_P|eval\(\$_R|file_put_contents\(\.*\$_|base64_decode'

匹配 webshell

$ find /tmp -perm 777 # 打印出权限为 777 的文件, -perm 选项指明 find 应该只匹配具有特定权限值的文件

$ find / -type f -user root -print # 打印出用户 root 拥有的所有文件，选项-user USER 找出由某个特定用户所拥有的文件

$ find / -type f -perm -04000 -ls -uid 0 2>/dev/null # 查找具有 SUID 位文件

$ find / -perm -u=s -type f 2>/dev/null

$ find / -perm -g=s -type f 2>/dev/null # 查看具有 SGID 位文件

4.2 敏感目录

(1) 临时目录/tmp、/var/tmp、/dev/shm 下的文件，目录权限是 1777，容易被上传木马文件

(2) 命令目录/usr/bin、/usr/sbin 等下的二进制文件容易被替换, 替换后可下载 busybox 使用被替换命令

$ ls -alt /usr/bin | head #按照最新修改时间显示，排查可疑文件

(3) ~/.ssh、/etc/ssh 经常作为一些后门配置的路径，需重点排查

$ cat ~/.ssh/authorized_keys #检查公钥是存在否异常写入

4.3 基于时间点查找

<列出攻击日志内变动的文件,排查恶意软件>

$ ls --full-time ./ | sed -n '/2019-01-01/p' #查找当前文件夹下的某个日期产生的文件

$ find / -ctime 0 -name ".sh" #查找一天内新增的 sh 文件

-type b/c/d/f/l/p: 查找快设备、字符设备、目录、普通文件、符号链接、管道

-mtime -n +n # 按文件更改时间来查找文件，-n 指 n 天以内，+n 指 n 天前

-atime -n +n # 按文件访问时间来查找文件，-n 指 n 天以内，+n 指 n 天前

-ctime -n +n # 按文件创建时间来查找文件，-n 指 n 天以内，+n 指 n 天前

$ find /tmp -type f -amin -10 -print #打印出 10 分钟内访问的所有文件

三、日志分析

1、window 日志分析

Windows 主要有以下三类日志记录系统事件：应用程序日志、系统日志和安全日志。

系统日志：记录操作系统组件产生的事件，主要包括驱动程序、系统组件和应用软件的崩溃以及数据丢失错误等。系统日志中记录的时间类型由 Windows NT/2000 操作系统预先定义。

默认位置： %SystemRoot%\System32\Winevt\Logs\System.evtx

应用程序日志：包含由应用程序或系统程序记录的事件，主要记录程序运行方面的事件，例如数据库程序可以在应用程序日志中记录文件错误，程序开发人员可以自行决定监视哪些事件。如果某个应用程序出现崩溃情况，那么我们可以从程序事件日志中找到相应的记录，也许会有助于你解决问题。

默认位置：%SystemRoot%\System32\Winevt\Logs\Application.evtx

安全日志：记录系统的安全审计事件，包含各种类型的登录日志、对象访问日志、进程追踪日志、特权使用、帐号管理、策略变更、系统事件。安全日志也是调查取证中最常用到的日志。默认设置下，安全性日志是关闭的，管理员可以使用组策略来启动安全性日志，或者在注册表中设置审核策略，以便当安全性日志满后使系统停止响应。

默认位置：%SystemRoot%\System32\Winevt\Logs\Security.evtx

1.1 安全日志分析

Windows 安全日志存储在 C:\Windows\System32\winevt\Logs，该目录下存在许多 evtx 日志文件。Windows 2000 / Server2003 / Windows XP 安全日志默认位置在 C:\WINDOWS\System32\config。

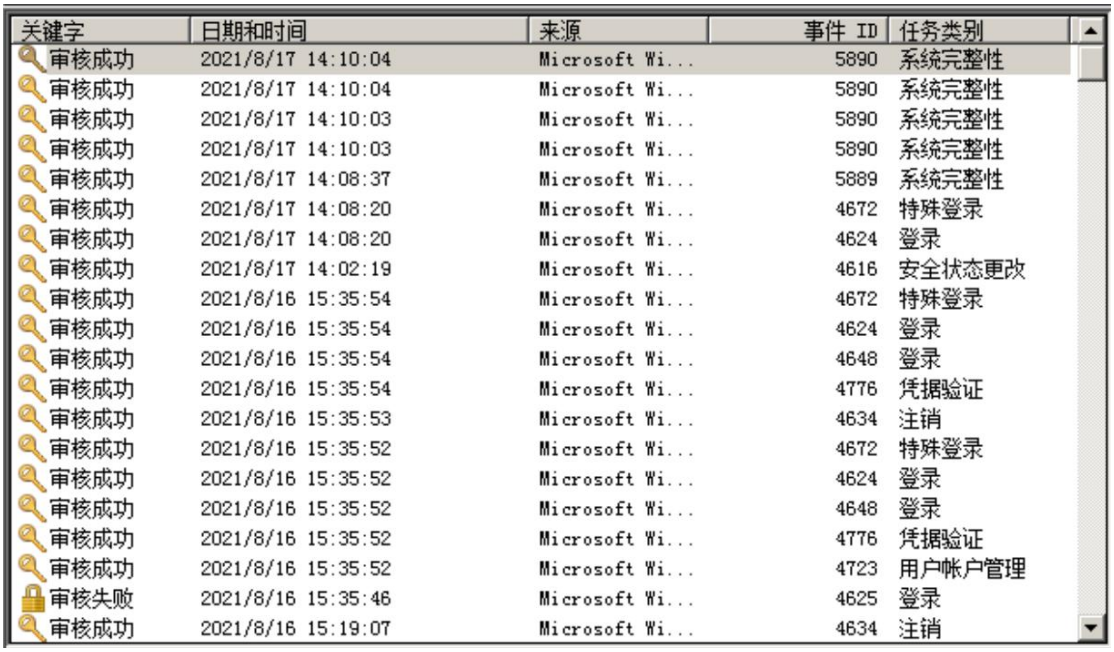
在默认情况下， Windows 日志仅仅记录一些特定日志，因为 Windows 日志中每种日志的大小默认为 20M，超过大小之后会覆盖最早的日志记录。如果我们需要记录详细的安全日志，则需要通过修改本地策略或者在高级审核策略配置 (gpedit.msc) 中来启用其他项的日志记录功能。

查看方法：

win+R 输入 eventvwr.msc 或者 事件查看器，查看 windows 日志（包括应用程序、安全、Setup、系统、事件）

每条安全日志由以下结构组成：

关键字(审核成功/审核失败)	日期和时间(事件发生的时间)	来源	事件ID	任务类别



关键字	日期和时间	来源	事件 ID	任务类别
审核成功	2021/8/17 14:10:04	Microsoft Wi...	5890	系统完整性
审核成功	2021/8/17 14:10:04	Microsoft Wi...	5890	系统完整性
审核成功	2021/8/17 14:10:03	Microsoft Wi...	5890	系统完整性
审核成功	2021/8/17 14:10:03	Microsoft Wi...	5890	系统完整性
审核成功	2021/8/17 14:08:37	Microsoft Wi...	5889	系统完整性
审核成功	2021/8/17 14:08:20	Microsoft Wi...	4672	特殊登录
审核成功	2021/8/17 14:08:20	Microsoft Wi...	4624	登录
审核成功	2021/8/17 14:02:19	Microsoft Wi...	4616	安全状态更改
审核成功	2021/8/16 15:35:54	Microsoft Wi...	4672	特殊登录
审核成功	2021/8/16 15:35:54	Microsoft Wi...	4624	登录
审核成功	2021/8/16 15:35:54	Microsoft Wi...	4648	登录
审核成功	2021/8/16 15:35:54	Microsoft Wi...	4776	凭据验证
审核成功	2021/8/16 15:35:53	Microsoft Wi...	4634	注销
审核成功	2021/8/16 15:35:52	Microsoft Wi...	4672	特殊登录
审核成功	2021/8/16 15:35:52	Microsoft Wi...	4624	登录
审核成功	2021/8/16 15:35:52	Microsoft Wi...	4648	登录
审核成功	2021/8/16 15:35:52	Microsoft Wi...	4776	凭据验证
审核成功	2021/8/16 15:35:52	Microsoft Wi...	4723	用户帐户管理
审核失败	2021/8/16 15:35:46	Microsoft Wi...	4625	登录
审核成功	2021/8/16 15:19:07	Microsoft Wi...	4634	注销

事件属性的解释：

属性名	描述
源	记录事件的软件，可以是程序名（如“SQL Server”），也可以是系统或大型程序的组件（如驱动程序名）。例如，“Elnkii”表示 EtherLink II 驱动程序。
事件 ID	标识特定事件类型的编号。描述的第一行通常包含事件类型的名称。例如，6005 是在启动事件日志服务时所发生事件的 ID。此类事件的描述的第一行是“事件日志服务已启动”。产品支持代表可以使用事件 ID 和来源来解决系统问题。
级别	以下事件严重性级别可能出现在安全日志中： 审核成功。指明用户权限操作成功。审核失败。指明用户权限操作失败。 在事件查看器的正常列表视图中，这些分类都由符号表示。
用户	事件发生所代表的用户的名称。如果事件实际上是由服务器进程所引起的，则此名称为客户端 ID；如果没有发生模仿的情况，则为主 ID。如果适用，安全日志项同时包含主 ID 和模仿 ID。当服务器允许一个进程采用另一个进程的安全属性时就会发生模拟的情况。
操作代码	包含标识活动或应用程序引起事件时正在执行的活动中的点的数字值。例如，初始化或关闭。
日志	已记录事件的日志的名称。
任务类别	用于表示事件发布者的子组件或活动。
关键字	可用于筛选或搜索事件的一组类别或标记。示例包括“网络”、“安全”或“未找到资源”。
计算机	发生事件的计算机的名称。该计算机名称通常为本地计算机的名称，但是它可能是已转发事件的计算机的名称，或者可能是名称更改之前的本地计算机的名称。
日期和时间	记录事件的日期和时间。

登录类型：

登录类型	描述	说明
2	交互式登录（Interactive）	用户在本地进行登录。
3	网络（Network）	最常见的情况就是连接到共享文件夹或共享打印机时。
4	批处理（Batch）	通常表明某计划任务启动。
5	服务（Service）	每种服务都被配置在某个特定的用户账号下运行。
7	解锁（Unlock）	屏保解锁。
8	网络明文（NetworkCleartext）	登录的密码在网络上是通过明文传输的，如FTP。
9	新凭证（NewCredentials）	使用带/Netonly参数的RUNAS命令运行一个程序。
10	远程交互，（RemoteInteractive）	通过终端服务、远程桌面或远程协助访问计算机。
11	缓存交互（CachedInteractive）	以一个域用户登录而又没有域控制器可用。

子状态码：

子状态码	描述(针对失败的原因的检查)
0xc0000064	用户名不存在
0xc000006a	用户名是正确的,但密码是错误的
0xc0000234	用户当前锁定
0xc0000072	帐户目前禁用
0xc000006f	用户试图登录天的外周或时间限制
0xc0000070	工作站的限制
0xc0000193	帐号过期
0xc0000071	过期的密码
0xc0000133	时钟之间的直流和其他电脑太不同步
0xc0000224	在下次登录用户需要更改密码
0xc0000225	显然一个缺陷在Windows和不是一个风险
0xc000015b	没有被授予该用户请求登录类型(又名登录正确的)在这台机器
0xc000006d	似乎是由于系统问题和不安全

事件 ID 分析:

事件ID	说明	事件ID	说明
1102	清理审计日志	4720	创建用户
4624	账号成功登录	4726	删除用户
4625	账户登录失败	4728	一个成员被添加到启用安全的全局组中
4768	已请求 Kerberos 身份验证票证 (TGT)。	4729	成员已从启用安全的全局组中删除
4771	Kerberos 预身份验证失败。	4732	一个成员被添加到启用安全的本地组
4772	Kerberos 身份验证票证请求失败。	4733	成员已从启用安全的本地组中删除
4769	已请求 Kerberos 服务票证。	4634	帐户已注销。
4776	域控制器尝试验证帐户的凭据。	4756	一个成员被添加到启用安全的通用组。
4770	更新了 Kerberos 服务票证	4672	分配给新登录的特殊权限
4672	分配给新登录的特殊权限	4757	成员已从启用安全的通用组中删除
5156	出站连接记录	4719	系统审核策略已更改
4698	已创建计划任务	5158	入站连接记录
4699	计划任务被删除	4702	已更新计划任务
4700	已启用计划任务	4688	已创建新进程
4701	计划任务被禁用	4689	一个进程已经退出

2、Linux 日志分析

日志类型大致可以分为三类：内核和系统日志、用户日志、应用日志。

内核和系统日志：这种日志主要由 syslog 管理、根据其配置文件/etc/syslog.conf 中的设置决定内核消息和各种系统程序信息记录到哪个位置。

用户日志：用户日志主要记录系统用户登录或者退出的信息，包括用户名账号、登录时间、源 IP 等。

应用日志：记录应用程序运行过程中的各种事件信息。

常见的日志文件：

日志文件	说明
/var/log/messages	记录系统重要信息日志
/var/log/secure	记录验证和授权方面的信息，例如ssh登录、su切换用户、添加用户等
/var/log/maillog	记录系统运行电子邮件服务器的日志信息。
/var/log/cron	记录系统定时任务相关日志
/var/log/boot.log	记录系统启动时候的日志，包括自启动的服务
/var/log/dmesg	记录内核缓冲信息
/var/log/bmtp	记录所有登录失败的日志
/var/log/wtmp	用户每次登录进入和退出时间的永久记录
/var/log/lastlog	记录所有用户的最近信息。

2.1 分析 secure 日志

2.1.1 定位有多少 IP 在爆破主机的 root 帐号：

grep "Failed password for root" /var/log/secure | awk '{print $11}' | sort | uniq -c | sort -nr | more

定位有哪些 IP 在爆破：

grep "Failed password" /var/log/secure|grep -E -o "(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)"|uniq -c

爆破用户名字典是什么？

grep "Failed password" /var/log/secure|perl -e 'while($_=<>){ /for(.*?) from/; print "$1\n";}'|uniq -c|sort -nr

2.1.2 登录成功的 IP 有哪些：

grep "Accepted " /var/log/secure | awk '{print $11}' | sort | uniq -c | sort -nr | more

登录成功的日期、用户名、IP：

grep "Accepted " /var/log/secure | awk '{print $1,$2,$3,$9,$11}'

2.1.3 增加和删除用户

grep “useradd”or “userdel”/var/log/secure

2.2 分析应用日志

1、把应用程序的 access.log 日志中状态码为 200 的记录，grep 定向到文本中，再进行整理分析，这样能快速地入侵定位 IP、攻击载荷、木马路径等。

grep " 200 " *.log > *.log

2、访问量前 10 的 IP

cat access.log | cut -f1 -d " " | sort | uniq -c |sort -k 1 -n -r | head -10

cut 部分表示取第 1 列即 IP 列，取第 4 列则为 URL 的访问量

3、统计一个文本中包含字符个数

cat access.log |grep /2023/ |wc -l

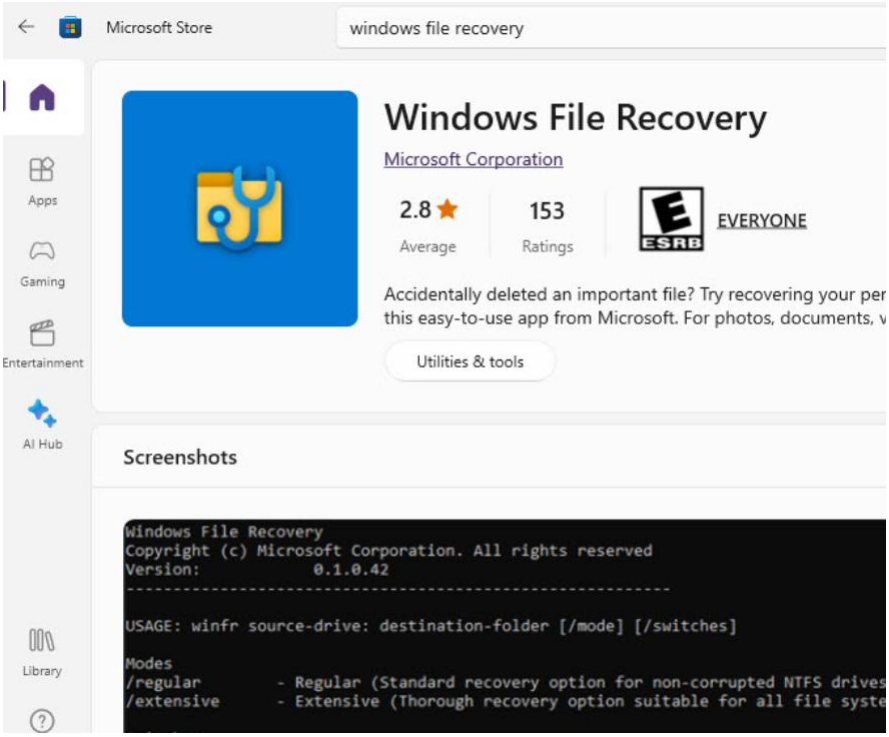
四、文件恢复

1、Window

1.1WinFR

https://www.winfr.com.cn/

1.2Windows File Recovery

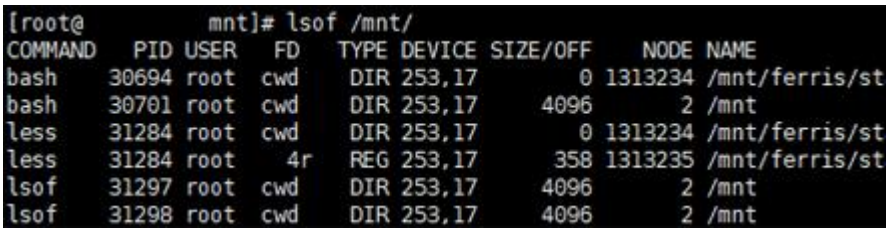


2、Linux

2.1losf 命令

（这个命令实际上并不能直接用来恢复文件，不过它可以列出被各种进程打开的文件信息）

lsof /mnt 查看正在使用删除文件的进程号



切换到/proc 下，删除文件对应的进程的 pid 下的文件描述符中的目录中；将对应的内容重定向或 cp 到其他文件中。

重点关注：PID 与 FD

cd /proc/31284/fd/

cat 4 > /mnt/ferris_train.less

```
[root@          fd]# cd /proc/31284/fd/
[root@          fd]# ll
总用量 0
lrwx------ 1 root root 64 12月  4 14:55 0 -> /dev/pts/0
lrwx------ 1 root root 64 12月  4 14:55 1 -> /dev/pts/0
lrwx------ 1 root root 64 12月  4 14:55 2 -> /dev/pts/0
lr-x------ 1 root root 64 12月  4 14:55 3 -> /dev/tty
lr-x------ 1 root root 64 12月  4 14:55 4 -> /mnt/ferris/static
```

2.2extundelete

原理：使用存储在分区日志中的信息，尝试恢复已从 ext3 或 ext4 的分区中删除的文件

优点：相比于 ext3grep 只能恢复 ext3 文件系统的文件，其适用范围更广，恢复速度更快

extundelete 官方地址(官方文档)：http://extundelete.sourceforge.net

#centos 安装操作
yum install e2fsprogs-devel e2fsprogs* gcc*
#ubuntu 安装操作
apt-get install build-essential e2fslibs-dev e2fslibs-dev

恢复文件操作：
（执行 extundelete 命令的当前目录必须是可写的。）

1、查看要恢复文件的分区的文件系统
df -Th

```
[root@          ~]# df -Th
文件系统        类型      容量  已用  可用 已用% 挂载点
/dev/vda2       ext4       20G  8.9G  9.6G   49% /
devtmpfs        devtmpfs  3.9G     0  3.9G    0% /dev
tmpfs           tmpfs     3.9G     0  3.9G    0% /dev/shm
tmpfs           tmpfs     3.9G  329M  3.5G    9% /run
tmpfs           tmpfs     3.9G     0  3.9G    0% /sys/fs/cgroup
/dev/vda1       ext4      190M   92M   85M   52% /boot
```

2、对要恢复文件的分区解除挂载
umount /mnt

```
[root@localhost ~]# umount /mnt
[root@localhost ~]# lsblk
NAME   MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
vda    253:0    0   20G  0 disk
├─vda1 253:1    0  200M  0 part /boot
└─vda2 253:2    0 19.8G  0 part /
```

3、查看可以恢复的数据
（指定误删文件的分区进行查找,最后一列标记为 Deleted 的文件, 即为删除了的文件。）
extundelete /dev/vdb1 --inode 2 （根分区的 inode 值是 2）

```
File name                                       | Inode number | Deleted status
.                                                 2
..                                                2
ferris                                            1310721        Deleted
nfs01                                             4718593        Deleted
test2.txt                                         12             Deleted
```

4、恢复单个目录

（指定要恢复的目录名，如果是空目录，则不会恢复。 ）

extundelete /dev/vdb1 --restore-directory ferris

```
[root@    ~]# extundelete /dev/vdb1 --restore-directory ferris
NOTICE: Extended attributes are not restored.
Loading filesystem metadata ... 800 groups loaded.
Loading journal descriptors ... 576 descriptors loaded.
Searching for recoverable inodes in directory ferris ...
```

（当执行恢复文件的命令后，会在执行命令的当前的目录下生成 RECOVERED_FILES 目录，恢复的文件都会放入此目录中。如未生成目录，即为失败。）

5、恢复全部删除的文件

extundelete /dev/vdb1 --restore-all

```
[root@    ~]# extundelete /dev/vdb1 --restore-all
NOTICE: Extended attributes are not restored.
Loading filesystem metadata ... 800 groups loaded.
Loading journal descriptors ... 582 descriptors loaded.
Searching for recoverable inodes in directory / ...
9 recoverable inodes found.
```

2.3testdisk

安装：

apt install testdisk

yum install testdisk

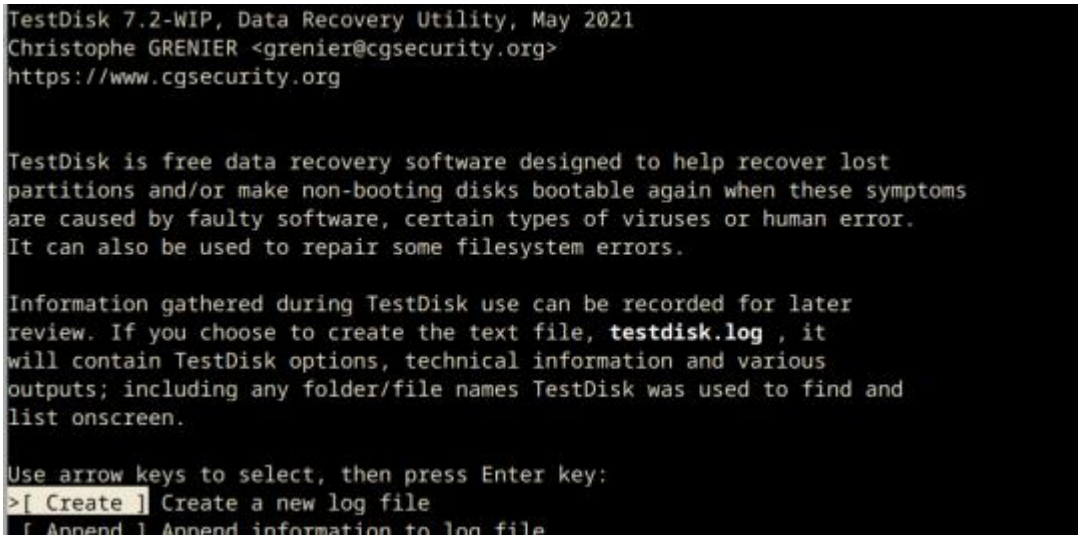
首先，你必须以 root 身份登录，或者有 sudo 权限才能使用 testdisk。

（当你用 testdisk 恢复被删除的文件时，你最终会将恢复的文件放在你启动该工具的目录下）

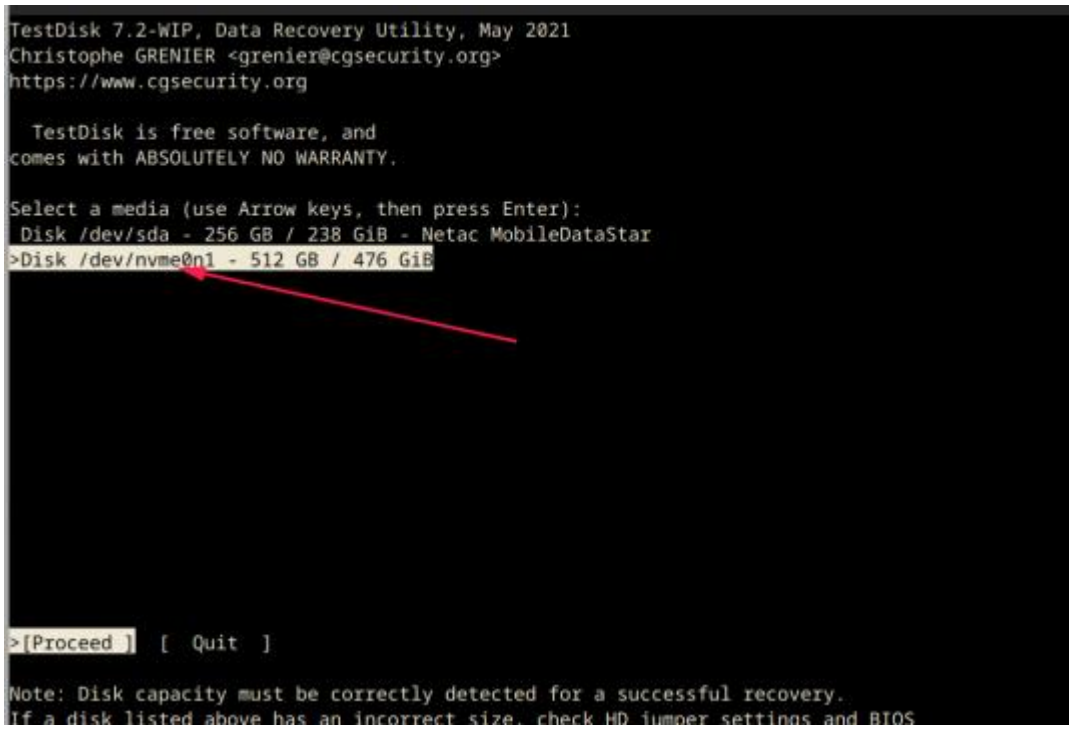
启动：

$ sudo testdisk

1、这里选择创建了一个日志文件

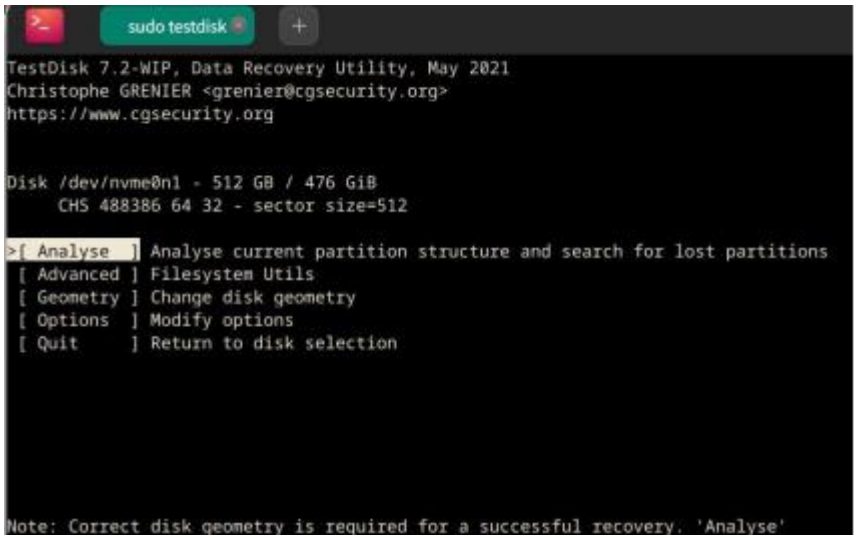


1、下一步是选择被删除文件所存储的磁盘分区(如果没有高亮显示的话)。根据需要使用上下箭头移动到它。然后点两次右箭头，当 “Proceed” 高亮显示时按回车键。

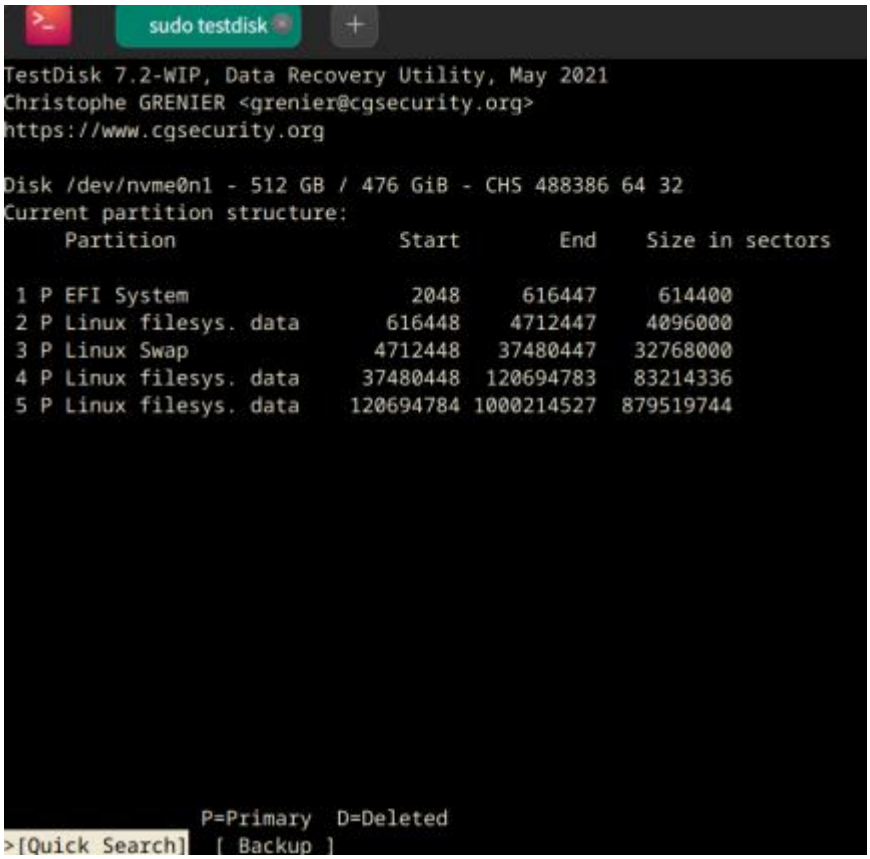


2、此时，testdisk 应该已经选择了合适的分区类型。回车

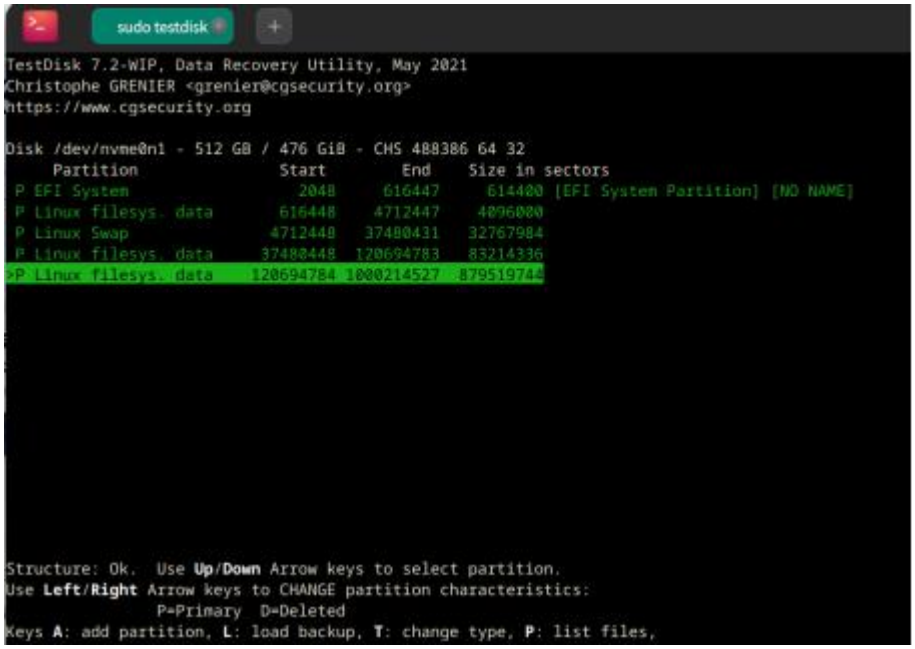
4、在下一步中，按向下箭头指向 >[Analyse]



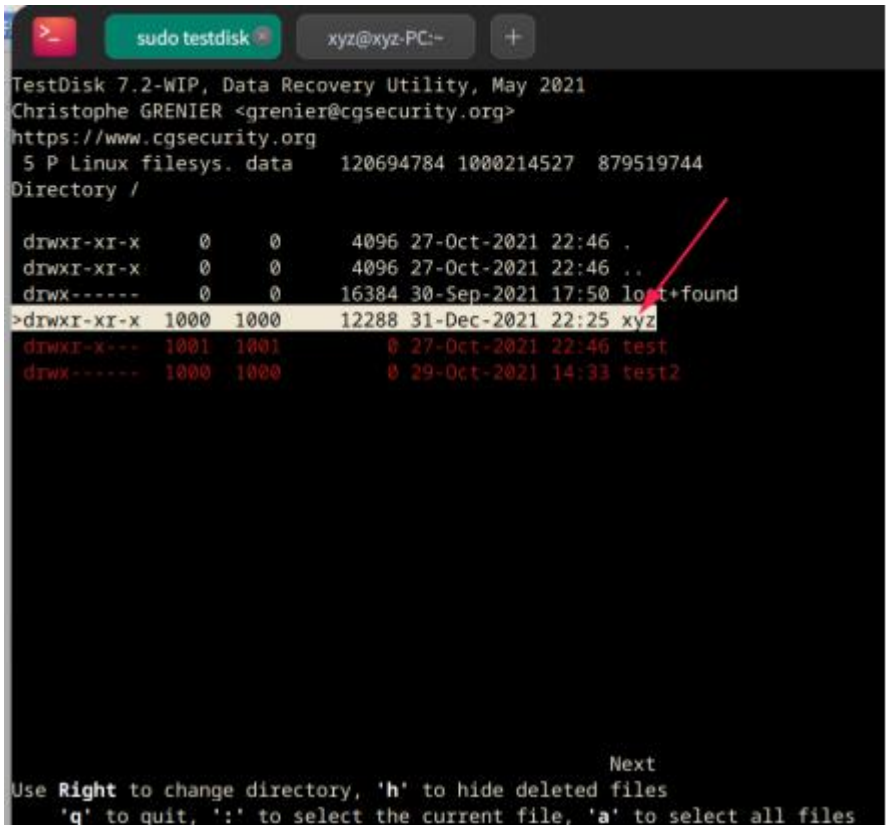
3、通过方向键选择“Quick Search” 选择“快速搜索”，或者回车后选择“深度搜索”， 然后运行搜索直到扫描完所有 inode。



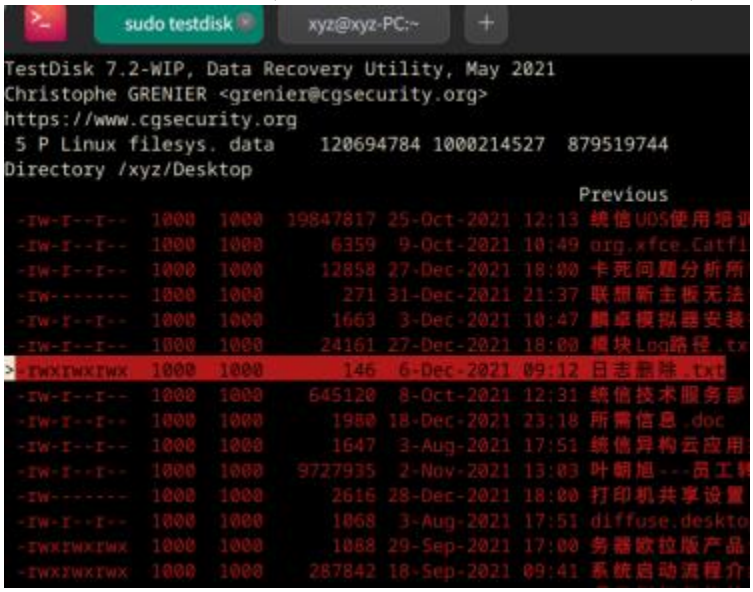
6、选择中需要的查找的分区，按 p 列出文件
（下方按键说明 A:添加分区，L:加载备份，T:更改类型，P:列出文件）



7、进入到这里，就要开始查找误删除的数据了。

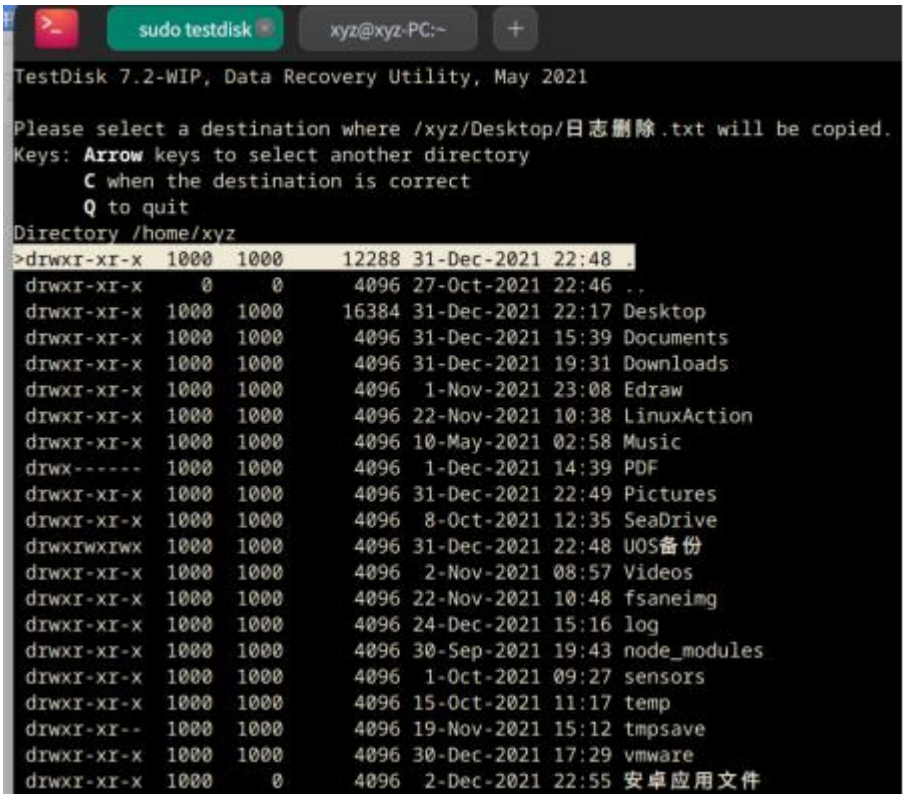


4、进入目标目录后，一旦你找到需要恢复的文件，按 c 选择它。



9、选择需要恢复的文件后，会提示选择保存的恢复文件的目录。

选定后按 c 确定选择的目录，选定保存目录后，后面的恢复文件都会保存这里。



五、溯源到人

1、IP 溯源

利用 IP 进行定位查询：

https://www.ipplus360.com/

https://www.chaipip.com

https://www.opengps.cn/

https://www.ipip.net/ip.html

利用 IP 查询安全情报

https://x.threatbook.com/

https://ti.360.net/
https://tix.qq.com/
https://ti.qianxin.com/
https://ti.dbappsecurity.com.cn/
https://ti.nsfocus.com/
https://www.venuseye.com.cn/
https://redqueen.tj-un.com/IntelHome.html

2、ID 溯源

https://whatsmyname.app/
https://privacy.aiuys.com/
https://github.com/p1ngul1n0/blackbird
https://github.com/sherlock-project/sherlock
搜索引擎、SRC 排名、QQ 群、微信群、抖音、快手、微博、知乎、脉脉、牛客网、 github、gitee、csdn、cnblogs

3、手机号溯源

https://www.reg007.com/
https://privacy.aiuys.com/
https://zy.xywlapi.cc/emoh.html
http://www.newx007.com/
https://fee.icbc.com.cn/index.jsp
支付宝转账、钉钉通讯录导入、微信搜索

4、EMail 溯源

https://epieos.com/
https://emailrep.io/

5、域名溯源

https://whois.chinaz.com/
https://beian.miit.gov.cn/
https://www.beian.gov.cn/portal/registerSystemInfo

6、木马分析（云沙箱）

https://s.threatbook.com/
https://sandbox.ti.qianxin.com/sandbox/page
https://www.virscan.org/
https://www.virustotal.com/
https://opentip.kaspersky.com/
https://habo.qq.com/