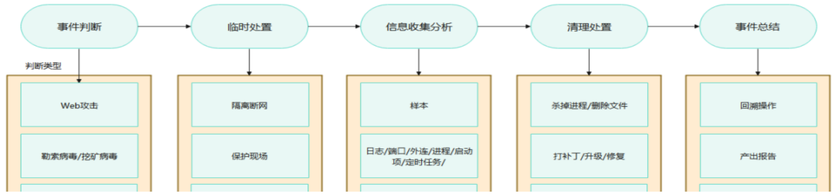
Linux应急检查项&命令			
排查项	思路	命令	拓展
排查项	• 查看账户 • 查看端口 • 查看进程 • 启动项与定时任务 • 日志分析 • 文件分析 • 历史命令	#查看资源（进程）占用情况 top #查看进程 ps -aux #查看网络连接 netstat -pantu #查看开123端口的进程 lsof -i:123 #显示错误的登录信息 lastb #显示系统用户最近的的登录信息 last #显示所有用户最近的登录信息 lastlog #查看定时任务 crontab -l	相关工具： 1、sysdig：系统行为监测类软件，抓进程和系统核心日志
查看账号	查看用户信息文件，查看是否存在UID为0的用户、新增的用户 查看当前已登录用户及会话时常 查看用户登录信息 查看sudo用户列表，除去Root账号外，是否存在其他账号拥有sudo权限 禁用和删除可以用户账号	用户信息文件：cat /etc/passwd 用户组信息文件：/etc/group （注意：无密码只允许本机登陆，远程不允许登陆） 可查询可登录账户UID为0的账户。root是UID为0的可登录账户（su，ssh密钥登陆），如果出现其他为0的账户，账号重点排查 sudo awk -F: '($3==0) print $1}' /etc/passwd 用户密码文件/etc/shadow cat /etc/shadow sudo awk '/\$1|\$6/{print $1}' /etc/shadow //*查看具有远程登录权限的账户 #查看目前登录系统的用户信息，一共有五列，其每一列对应的含义如下 #第一列显示用户名词 #第二列显示用户的连接方式。tty:0代表用户直接连接电脑，pts代表远程登录 #root pts/0 2023-05-29 11:28 (xxx.xxx.xxx.xxx) who//当前在本地系统上的所有用户的登陆信息。 w //查看已经登陆的用户信息 #提出用户,如果想提出以上的用户则 pkill -kill -t pts/0 #查看用户登录的信息 last #显示系统中所有用户最近一次登录信息 lastlog #显示登录失败用户的信息 lastb	一、cat /etc/shadow命令介绍 root:6oGs1PqhL2p3ZetrE$X7o7bzoouHQY5EmSgsYN5UD4.kMHx6qgbTqw NVC5oOAouXvcjQSt.Ft7qI1WpkopY0UV9ajBwUt1DpYxTCVvI/:16809:0:99999:7::: 分别代表的是： 用户名：加密密码：密码最后一次修改日期：两次密码的修改时间间隔：密码有效期： 密码修改到期前的警告天数：密码过期之后的宽限天数：账号失效时间：保留 所有伪用户的密码都是“!!”或“*” ，代表没有密码是不能登录的。当然，新创建的 用户如果不设定密码，那么它的密码项也是“!!”，代表这个用户没有密码，不能登录。 允许登陆。
查看端口和进程	查看端口外连情况，分析可疑进程 查看本地有无重要端口被连接 查看有无可疑IP外连，可以用微步在线检测 查看当前运行那些进程，分析可疑的进程	#查看端口连接情况 netstat -pantu （如果netstat没安装的话，可以用ss命令） #查看进程，分析异常的进程名、PID、可疑的命令行 ps -aux #查看异常进程 ps -aux | grep $PID ps aux --sort=-pcpu,+pmem 显示当前系统中运行进程的命令，并按照 CPU 使用率（降序）和内存使用率（升序）进行排序。 ps a(显示当前终端会话中的所有进程，包括其他用户的进程) #查看pid所对应的进程文件路径 ls -l /proc/$PID/exe #结束进程 kill -9 $PID #查看指定端口对应的进程 lsof -i:80 #查看指定PID的调用情况 lsof -p 666 #动态展示系统整体运行情况，查看有无资源占用过高的进程 top命令能够查看当前主机CPU使用率，在挖矿场景能够快速定位相关进程 top lsof列出当前系统打开的文件（该命令常被用于定位进程运行的文件，可用于定位恶意进程的真实文件） lsof -p pid、lsof -c sshd 网络数据包截获分析工具。支持针对网络层、协议、主机、网络或端口的过滤。并提供and、or、not等逻辑语句帮助去除无用的信息。 命令：tcpdump 监听特定主机：tcpdump host 182.254.38.55	一、定位进程在哪个目录 首先，使用ps命令或top命令获取你要查找的进程的进程ID。例如，假设进程ID是1234。 ps -ef | grep 1234 进入/proc/<PID>/目录，将<PID>替换为你要查找的进程的进程ID。 cd /proc/1234/ 在该目录下，你可以找到一个名为exe的符号链接文件，它指向进程的执行文件。使用ls命令来查看该符号链接文件 ls -l exe（该命令的输出将显示进程的执行文件的绝对路径）
启动项与定时任务	系统运行级别 运行级别 含义 0 关机 1 单用户模式，可以想象为windows的安全模式，主要用于系统修复 2 不完全的命令行模式，不含NFS服务 3 完全的命令行模式，就是标准字符界面 4 系统保留 5 图形模式 6 重启	#查看自启动服务 cat /etc/cron* #查看某个用户的计划任务 crontab -l #编辑定时任务 crontab -e #删除当前用户的定时任务 crontab -r #查看有无异常开机启动命令 more /etc/rc.local #查看服务自启动状态 chkconfig #当我们需要开机启动自己的脚本时，只需要将可执行脚本丢在/etc/init.d目录下，然后在/etc/rc.d/rc*.d中建立软链接即可,S开头代表加载时自启动 ln -s /etc/init.d/sshd /etc/rc.d/rc3.d/S100ssh	
日志分析	查看ssh登录日志 查看登录成功的IP 查看有多少IP尝试登录root账号	关键日志文件 日志文件 说明 /var/log/cron 记录系统定时任务相关日志 /var/log/massage 记录Linux操作系统常见的系统和服务错误信息 /var/log/btmp 记录登录失败的信息 ，也可以使用命令lastb /var/log/lastlog 记录系统中所有用户最后一次成功登录的时间 ，也可以使用命令lastlog /var/log/wtmp 永久记录所有用户的登录、注销信息，同时记录系统的启动、重启、关机事件，也可以使用命令last /var/log/utmp 只记录当前用户的信息，也可以使用命令w,who,user /var/log/secure 记录验证和授权方面的信息，如SSH登录，用户切换、SUDO授权的部分操作 /var/log/yum.log 查看Centos软件安装日志 /var/log/apt 查看Ubuntu软件安装日志 last# 显示所有登录用户的信息	日志分析的时候，先对涉事时间段的日志进行排查，排查时间维度大于
文件分析&历史命令分析	查看敏感目录下是否存在影藏文件 发现可疑文件使用`stat`查看创建修改时间 如果前期信息收集知道木马的创建时间，可疑根据时间查找文件 （根据文件修改时间和HASH值来寻找可疑的文件、后门程序） 查看历史命令	关键文件： 文件名 说明 /etc/passwd 用户信息文件 /etc/crontab 定时任务文件 /etc/anacrontab 异步定时任务文件 /etc/rc.d/rc.local 开机启动项 #查找近7天内修改的文件 find / -mtime -7 -ls | more find是查找文件名的命令， find / -name "*frp" 可以用grep命令 grep hello file.txt（在文件 file.txt 中查找字符串 "hello"，并打印匹配的行：） stat filename //查看文件状态stat filename md5sum filename //计算文件hash值 #查看历史命令 cat .bash_history cat ~/.bash_history cat /root/.bash_history（或者是/home/用户名/.bash_history） history stat 查看文件信息，该命令可以查看文件的基本信息，如创建时间、查看时间、修改时间等 stat /etc/passwd	



在Linux系统中，进程的执行文件通常位于`/proc/<PID>/`目录下，其中`<PID>`是进程的进程ID（Process ID）。你可以使用以下步骤来定位特定进程的执行文件所在的目录：

1. 首先，使用`ps`命令或`top`命令获取你要查找的进程的进程ID。例如，假设进程ID是1234。

```perl
ps -ef | grep 1234
```

2. 进入`/proc/<PID>/`目录，将`<PID>`替换为你要查找的进程的进程ID。

```bash
cd /proc/1234/
```

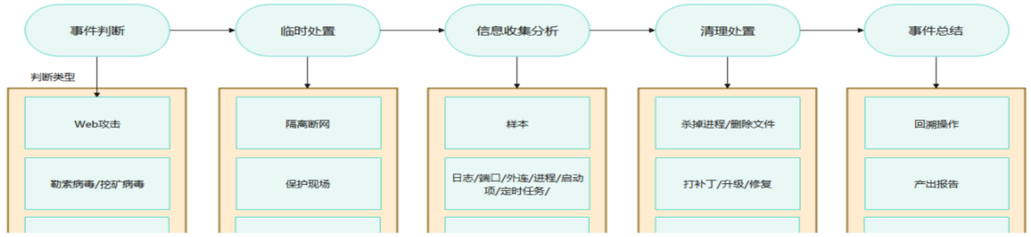
3. 在该目录下，你可以找到一个名为`exe`的符号链接文件，它指向进程的执行文件。使用`ls`命令来查看该符号链接文件。

```bash
ls -l exe
```

该命令的输出将显示进程的执行文件的绝对路径。

注意：在某些情况下，你可能需要具有足够的权限才能访问`/proc`目录下的某些文件。

Window应急检查项&命令			
排查项	思路	命令	工具
排查项	• 查看日志 • 查看端口/外连情况**(netstat -pantu)** • 查看进程**(tasklist)** • 查看系统账户 • 查看启动项 • 查看注册表 • 查看定时任务	#获取本地用户列表 net user #查看当前会话 net session #查看当前运行的服务 net start #远程连接 net use #查看当前用户下的共享目录 net share #查看网络连接 netstat -ano #查看操作系统的详细配置信息 systeminfo #获取进程信息wmic process #获取系统进程信息tasklist	更多工具详情请根据实际应急需要在工具包中使用
查看账号	查看是否存在弱口令 查看lusrmgr用户列表，是否存在未知用户、影藏用户（特征为用户名后存在$符） 查看lusrmgr组列表，查看是否存在未知账户。	query user //查看当前系统登录的会话 logoff ID //把指定用户踢出会话 net user //查看本地用户 lusrmgr.msc //查看账号 whoami whoami //查看当前用户 net user net user-常用命令 net user //以下示例显示本地计算机的所有用户帐户列表 net user $用户名 //显示用户账号<用户名>的登陆历史等信息 wmic useraccount //用户帐户管理（可审影子账户） 注册表方式查询影子账户 HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users\Names 点击"开始"—>"运行"，输入"regedt32.exe"后回车,需要到"HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users\Names"查看； 注意在SAM\SAM\获取所有权限。	D盾 Pchunter
查看端口	查看有无异常端口连接 使用netstat查看异常进程，并查找到PID 查看异常外连IP 查看有无重要的端口外连，类似于22(SSH)、3389(RDP) 被注入的进程属性里会多出**.NET Assemblies和.NET Performance**两个菜单	netstat //查看端口网络外连情况 -an -a 显示所有连接和监听端口 -n 以数字形式显示地址和端口号 -o 显示与每个连接相关的进程ID -t 显示TCP协议的连接情况 -u 显示UDP协议的连接情况 -p proto 显示proto指定的协议的连接 proto有TCP、UDP、TCPv6、UDPv6。如果与-s选项一起使用以显示按协议统计信息 Established的意思是确定的 正在连接 用tasklist | findstr "pid" 如果感觉netstat -aonb查出的外联IP有异常的话，可以拿到威胁情报平台上查询看看。如果是恶意IP，可以直接做下一步处理。在最后得到PID后。可以在任务管理器或者Porsess工具去查看进程 ，命令行也行 tasklist /svc netstat-ano | find"ESTABLISHED"查看网络建立连接状态 tasklist /svc | find "PID" 查看具体PID进程对应的程序 taskkill /PID pid值 /T 关闭进程	火绒剑 #着重关注未知文件、外部IP DNSQuerySniffer #着重关注红色端口号、A记录、状态码
查看进程	打开任务管理器，查看资源占用情况 运行msinfo32查看正在运行任务	taskmgr.exe #任务管理器 tasklit #列出所有进程 tasklist /svc #列出每个进程所调用的服务 taskkill /T /F /PID #结束某进程 分析可疑进程技巧： 1、查看应用程序是否有签名【工具上可以查看到（如微软的工具procexp64.exe）有的工具需要开启才能看到】 2、把所有的进程一建发送到VT平台上进行批量扫描【procexp64.exe也有这个功能】 3、把当前所有的程序的DLL文件显示出来 查看没有签名的进程的window命令： Win+R，输入"sigverif"显示系统中所有没有签名的程序	火绒剑 Pchunter #关注无厂商名、签名验证、描述信息的可疑进程
启动项与计划任务	运行msconfig，打开系统配置，查看是否存在异常的启动项（win7以后取消） 可以在任务管理器中打开（taskmgr.exe）查看启动项	net statistics workstation #查看系统开机事件 schtasks #CMD查看系统计划任务 taskschd.msc #win+r运行，查看任务计划程序 wmic startup get command,caption #查看程序启动信息 wmic service list brief #查看主机服务信息 注册表regedit HKEY CURRENT USERS/software/Microsoft/Windows/CurrentVersion/Run 操作系统中的启动菜单 C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup	autoruns #查看启动项、计划任务 PChunter #查看启动项，黑色-微软进程；蓝色-非微软进程；红色-可疑进程、隐藏服务；
日志分析	打开事件查看器，如果存在大量的登录失败事件ID则代表对相关的账号进行了爆破	主要日志： #系统日志 %SystemRoot%\System32\Winevt\Logs\System.evtx #安全日志 %SystemRoot%\System32\Winevt\Logs\Security.evtx #应用程序日志 %SystemRoot%\System32\Winevt\Logs\Application.evtx	eventvwr.msc #win+r 打开事件查看器 事件日志分析： 事件ID 说明 4624 登录成功 4625 登录失败 4634 注销成功 4647 用户启动的注销 4672 使用超级用户进行登录 4720 创建用户 7045 服务创建
文件分析	查看有无新键的文件夹 （时间排序，查看事件发生时间段修改过的文件,c盘和web应用目录为主）	%UserProfile%\Recent #win+r运行，分析最近打开的可疑文件 #查看有无新键的用户文件夹 Window 2003 C:\Documents and Settings Window 2007及以后 C:\Users\ msinfo32 #查看系统信息	下载的软件来 回收站 临时文件(temp)： 1、系统临时文件主要在：C:\Windows\Temp 2、系统临时用户文件夹位置为：C:\Documents and Settings\用户名\Local Settings\Temp。 3、IE临时文件夹位置一般为：C:\Documents and Settings\用户名\Local Settings\Temporary Internet Files。这里的用户名是指登陆计算机的用户名，一般默认为：Administrator。 需要注意的是：临时下载的文件是放在系统临时用户文件中，具体位置为：C:\Documents and Settings\用户名\Local Settings\Temp。并且Local Settings文件是隐藏的，需要设置下显示隐藏文件才可以看到。 历史文件记录(history) 应用程序打开历史记录
	分析最近打开的可疑文件 （时间排序，查看事件发生时间段修改过的文件）	分析最近打开的可疑文件 可以在目录C:\Documents and Settings\Administrator Recent 下查看， 也可以使用 win+R打开运行%userprofile%\recent查看。	



检查点

- 系统版本和补丁、防火墙状态；
- Webshell、病毒、后门、攻击痕迹；
- 端口开放、连接情况、CPU、进程、启动项；
- 文件修改、时间变动；
- 应用日志、系统日志；
- 配置修改、计划任务、用户；
- 安全设备等防护设备；
- 问题现状点；

注册表方式查询账户
HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users\Names

点击“开始”→“运行”，输入“regedt32.exe”后回车,需要到“HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users\Names”查看；注意在SAM\SAM\获取所有权限。