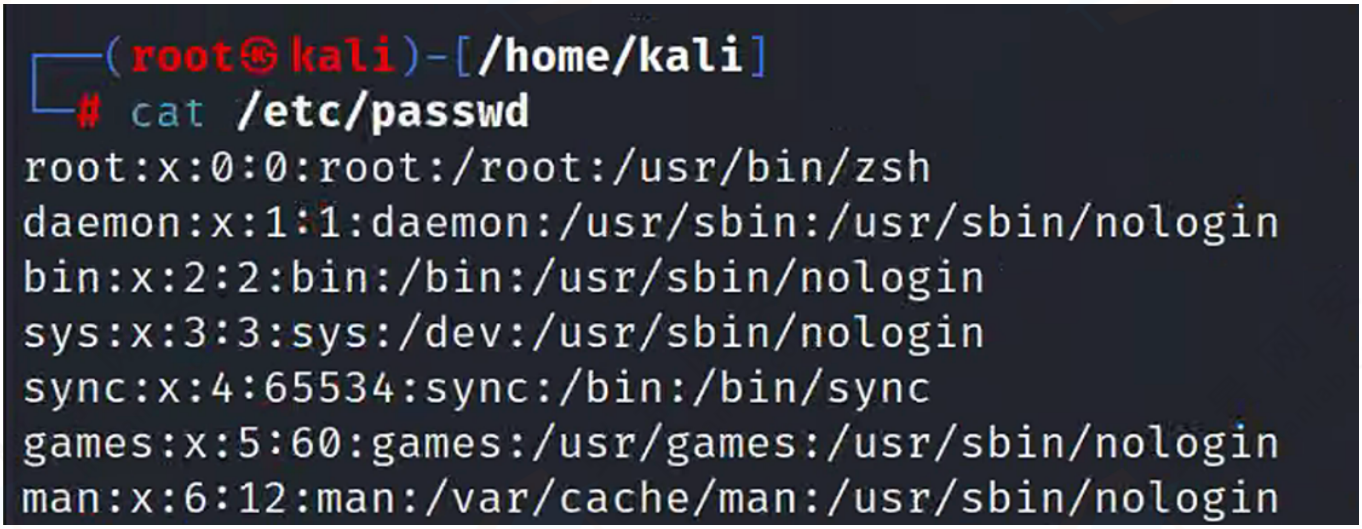
一、入侵排查思路

1. 账号安全

- 用户信息文件 /etc/passwd
  - 

  - account:password:UID:GID:GECOS:directory:shell
  - 用户名：密码（x代表密码占位符，表示该密码在/etc/shadow中）：用户ID：组ID：用户说明：家目录：登陆之后shell
  - Tips
  - /etc/passwd 任何用户都能查看，但仅有 root 用户可以更改
  - /usr/sbin/nologin 代表用户无法通过系统登录界面及ssh远程终端登陆，也无法通过su命令进行用户切换
  - 除root用户家目录在/root目录外，其他可登陆普通用户家目录在 /home/用户名 ，特殊的无法登陆用户，如apache服务用户www-data，家目录在 /var/www
  - /bin/zsh 、/bin/bash 、 /bin/sh 都是常见的登陆shell，当然也会见到带/usr前缀的目录，例如 /usr/bin/bash
  - 排查思路：是否存在可以用户，是否存在除root外其他uid=0的用户
- 用户影子文件 /etc/shadow
  - 

  - kali:\$y\$j9T\$thVUCcCzQozwQh.2JyVRs.$T0FS1BRAcGSTCGldig/Ji2CbWc3bLVV8Ym1wEPDcIw1:19590:0:99999:7:::
  - 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：密码修改到期到的警告天数：密码过期之后的宽限天数：账号失效时间：保留
  - Tips：

- /etc/shadow 仅root用户可读写
- $\y$j9T$thVUCcCzQozwQh.2JyVRs.$
  T0FS1BRAcGSTCGldig/Ji2CbWc3bLVV8Ym1wEPDclw1 是加密后的用户密码，无法逆向破解
- 密码有效期、密码修改到期的警告天数等策略可以为空，或默认的99999（无限制）
- /etc/shadow 并不是用户配置文件，如果仅把后门用户插入到此文件是无法生效的。

- 一些排查命令

```
1、查询特权用户特权用户(uid 为0)
[root@localhost ~]# awk -F: '$3==0{print $1}' /etc/passwd
2、除root帐号外，是否有其他未知帐号存在sudo权限
[root@localhost ~]# more /etc/sudoers | grep -v "^#\|^$" | grep "ALL=(ALL"
3、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
4、常见命令
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
uptime  查看登陆多久、多少用户，负载
```

(1) 历史命令

- Linux系统里，执行过命令的用户会在自己的家目录下，生成相应的历史命令记录文件
  如.bash_history、.zsh_history 、.sh_history
- 打开各帐号目录下的 .bash_history 、.zsh_history，查看帐号的历史命令
  - cat /root/.*_history | more

```
┌──(root㉿kali)-[/home/kali]
└─#   cat /root/.*_history | more
git
git clone  https://ghproxy.com/https://github.com/maurosoria/dirsearch.git
cd dirsearch
pip3 install -r requirements.txt -i https://mirrors.aliyun.com/pypi/simple
python3 dirsearch.py
```

- cat /home//._history | more

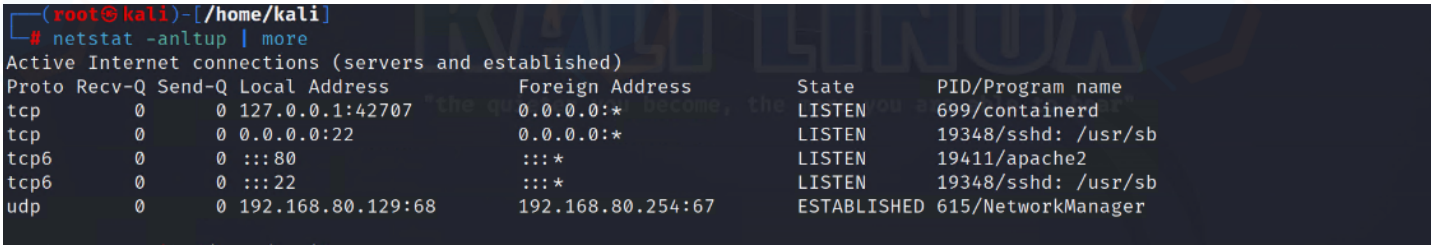
```
┌──(root㉿kali)-[/home/kali]
└─#   cat /home/*/.*_history | more
ls
exit
sudo su
sudo su
```

- 主要分析是否有账户执行过恶意操作
- 当安全事件发生的时候，就可以通过查看每个用户所执行过的命令，来分析该用户是否有执行恶意命令，如果发现哪个用户执行过恶意命令，那么我们就可以锁定这个线索，去做下一步的排查

(2) 异常端口与进程

- 使用 netstat 网络连接命令，查看服务器是否有未被授权的端口被监听，分析可疑端口、IP、PID
- 检查服务器是否存在恶意进程，恶意进程往往会开启监听端口，与外部控制机器进行连接

  netstat –anltup | more
  - 解释：a 所有状态连接、n 十进制数字显示IPv4地址、l 显示监听连接、t 显示TCP协议、u 显示UDP协议、p 显示PID



- Proto：表示网络协议，如TCP或UDP。
- Recv-Q：表示接收队列中的数据包数量，Send-Q：表示发送队列中的数据包数量
- Local Address：表示本地地址（IP地址和端口号），格式为"IP地址:端口号"。
  - 127.0.0.1 代表端口只监听在本地，其他机器无法连接
  - 192.168.80.129 代表端口只监听在192.168.80.129 IP（eth0网卡）上，只有能访问到192.168.80.129 的机器（如192.168.80.x 网段下的其他局域网计算机）才能访问
  - 0.0.0.0 代表端口监听在所有的接口IP上，表明所有IPv4地址计算机均可访问（当然前提是目标能连通该计算机）
  - ：：：等价于 0.0.0.0 ， 他是IPv6地址
- Foreign Address：表示远程地址（IP地址和端口号），格式同样为"IP地址:端口号"。
  - 如果以"-"或"::"开头，则表示没有远程地址（即尚未建立或已断开连接）。
- State：表示连接状态，通常包括已建立（ESTABLISHED）、监听（LISTEN）、等待（WAIT）、关闭等。
- PID/Program name：表示与网络连接相关联的进程的ID和名称。有些时候可能显示进程的ID而不显示进程的名称。
- 排查思路
  - 发现可疑IP，上报或检测威胁情报，确认后停止进程 kill -9 PID
  - 发现可以连接进程，ls -l /proc/PID/exe 或 file /proc/PID/exe 查看进程具体运行的文件路径，如果发现是病毒文件，及时上报并进行留存与删除。

```
┌──(root㉿kali)-[/home/kali]
└─# netstat -anltup | more
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.1:42707         0.0.0.0:*               LISTEN      699/containerd
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      19348/sshd: /usr/sb
tcp6       0      0 :::80                   :::*                    LISTEN      19411/apache2
tcp6       0      0 :::22                   :::*                    LISTEN      19348/sshd: /usr/sb
udp        0      0 192.168.80.129:68       192.168.80.254:67       ESTABLISHED 615/NetworkManager

┌──(root㉿kali)-[/home/kali]
└─# ls -l /proc/19411/exe
lrwxrwxrwx 1 root root 0 Sep 24 10:39 /proc/19411/exe -> /usr/sbin/apache2
```

```
┌──(root㉿kali)-[/home/kali]
└─# file /proc/19411/exe
/proc/19411/exe: symbolic link to /usr/sbin/apache2
```

- 检查异常进程
  - ps aux

```
┌──(root㉿kali)-[/home/kali]
└─# ps aux
USER         PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root           1  0.0  0.6  21052 12748 ?        Ss   09:57   0:00 /sbin/init splash
root           2  0.0  0.0      0     0 ?        S    09:57   0:00 [kthreadd]
root           3  0.0  0.0      0     0 ?        I<   09:57   0:00 [rcu_gp]
root           4  0.0  0.0      0     0 ?        I<   09:57   0:00 [rcu_par_gp]
root           5  0.0  0.0      0     0 ?        I<   09:57   0:00 [slub_flushwq]
root           6  0.0  0.0      0     0 ?        I<   09:57   0:00 [netns]
root           9  0.0  0.0      0     0 ?        I    09:57   0:01 [kworker/u64:0-events_unbound]
root          10  0.0  0.0      0     0 ?        I<   09:57   0:00 [mm_percpu_wq]
root          11  0.0  0.0      0     0 ?        I    09:57   0:00 [rcu_tasks_kthread]
root          12  0.0  0.0      0     0 ?        I    09:57   0:00 [rcu_tasks_rude_kthread]
root          13  0.0  0.0      0     0 ?        I    09:57   0:00 [rcu_tasks_trace_kthread]
root          14  0.0  0.0      0     0 ?        S    09:57   0:00 [ksoftirqd/0]
root          15  0.0  0.0      0     0 ?        I    09:57   0:00 [rcu_preempt]
root          16  0.0  0.0      0     0 ?        S    09:57   0:00 [migration/0]
```

    - USER：表示进程所属的用户。
    - PID：表示进程的ID（即进程号）。
    - %CPU：表示进程使用的CPU资源百分比。
    - %MEM：表示进程使用的内存资源百分比。
    - VSZ：表示进程的虚拟内存大小（以KB为单位）。
    - RSS：表示进程的实际内存大小（以KB为单位）。
    - TTY：表示进程关联的TTY设备。
    - STAT：表示进程的状态，通常包括运行（R）、睡眠（S）、停止（T）、僵死（Z）等。
    - START：表示进程的启动时间。TIME：表示进程的累计CPU占用时间。
    - COMMAND：表示进程的命令名称和参数。
  - top

```
top - 11:00:47 up  1:03,  2 users,  load average: 0.10, 0.13, 0.09
Tasks: 189 total,   1 running, 188 sleeping,   0 stopped,   0 zombie
%Cpu(s):  0.3 us,  0.3 sy,  0.0 ni, 99.4 id,  0.0 wa,  0.0 hi,  0.0 si,  0.0 st
MiB Mem :   1958.2 total,    567.5 free,    934.0 used,    639.0 buff/cache
MiB Swap:   1024.0 total,   1024.0 free,      0.0 used.   1024.3 avail Mem

    PID USER      PR  NI    VIRT    RES    SHR S  %CPU  %MEM     TIME+ COMMAND
    972 root      20   0  730968 223360  82328 S   0.7  11.1   0:08.63 Xorg
   1670 kali      20   0  363780  42824  30348 S   0.3   2.1   0:03.03 vmtoolsd
      1 root      20   0   21052  12748   9420 S   0.0   0.6   0:00.64 systemd
      2 root      20   0       0      0      0 S   0.0   0.0   0:00.00 kthreadd
      3 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 rcu_gp
      4 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 rcu_par_gp
      5 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 slub_flushwq
      6 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 netns
      9 root      20   0       0      0      0 I   0.0   0.0   0:01.15 kworker/u64:0-flush-8:0
     10 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 mm_percpu_wq
     11 root      20   0       0      0      0 I   0.0   0.0   0:00.00 rcu_tasks_kthread
     12 root      20   0       0      0      0 I   0.0   0.0   0:00.00 rcu_tasks_rude_kthread
     13 root      20   0       0      0      0 I   0.0   0.0   0:00.00 rcu_tasks_trace_kthread
     14 root      20   0       0      0      0 S   0.0   0.0   0:00.34 ksoftirqd/0
     15 root      20   0       0      0      0 I   0.0   0.0   0:00.43 rcu_preempt
     16 root      rt   0       0      0      0 S   0.0   0.0   0:00.00 migration/0
     17 root     -51   0       0      0      0 S   0.0   0.0   0:00.00 idle_inject/0
     19 root      20   0       0      0      0 S   0.0   0.0   0:00.00 cpuhp/0
     21 root      20   0       0      0      0 S   0.0   0.0   0:00.00 kdevtmpfs
```

    - 按 q 即可退出
- 运行以上命令，如果发现有名称不断变化的非授权进程占用大量系统CPU或内存资源时，则可能为恶意程序
- 确认该进程为恶意进程后，可以使用 kill -9 进程PID 命令结束，或使用防火墙限制进程外联

(3) 开机启动项

- Linux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	重启动

- 恶意程序往往会添加在系统的启动项，在用户关机重启后再次运行
- 添加服务为开机自启动
    - update-rc.d ssh enable
- 关闭服务开机自启动
    - update-rc.d ssh disable
- 了解/etc/rc*.d 目录
    - ls -l /etc/ |grep rc

```
┌──(root㉿kali)-[/home/kali/Downloads]
└─# ls -l /etc/ |grep rc
-rw-r--r--   1 root     root      1994 Aug  5 10:57 bash.bashrc
drwxr-xr-x   2 root     root      4096 Aug 21 14:58 ettercap
-rw-r--r--   1 root     root      3886 Jul 15 10:58 gprofng.rc
-rw-r--r--   1 root     root      1875 Jan  3  2023 inputrc
-rw-r--r--   1 root     root     41525 Jan 18  2023 matplotlibrc
-rw-r--r--   1 root     root     11399 Jan 18  2023 nanorc
drwxr-xr-x   2 root     root      4096 Jun 16 08:44 ODBCDataSources
drwxr-xr-x   2 root     root      4096 Sep 24 11:21 rc0.d
drwxr-xr-x   2 root     root      4096 Sep 24 11:21 rc1.d
drwxr-xr-x   2 root     root      4096 Sep 25 03:19 rc2.d
drwxr-xr-x   2 root     root      4096 Sep 25 03:19 rc3.d
drwxr-xr-x   2 root     root      4096 Sep 25 03:19 rc4.d
drwxr-xr-x   2 root     root      4096 Sep 25 03:19 rc5.d
drwxr-xr-x   2 root     root      4096 Sep 24 11:21 rc6.d
drwxr-xr-x   2 root     root      4096 Aug 21 16:27 rcS.d
-rw-r--r--   1 root     root      3663 Jun  9  2015 screenrc
-rw-r--r--   1 root     root       694 Aug  7 11:46 searchsploit_rc
-rw-r--r--   1 root     root      4942 May 14  2022 wgetrc
```

- 在UNIX和UNIX-like操作系统中，/etc/rc是一个目录，用于存放系统启动过程中需要执行的脚本文件。其中包含了一些不同级别的文件夹，每个文件夹代表了不同的运行级别（runlevel）或者系统状态。以下是通常在/etc/rc目录中找到的文件夹：

1. rc0.d：用于关机时的脚本。例如，关闭各个服务、卸载文件系统等。
2. rc1.d：单用户模式时所执行的脚本。也叫进入恢复模式，用于修复系统问题。
3. rc2.d：多用户文本模式下运行的脚本。该级别下一般不含图形界面。
4. rc3.d：完全的多用户文本模式下运行的脚本。
5. rc4.d：未使用，可以根据需求自定义。
6. rc5.d：多用户图形模式下运行的脚本。系统启动后，会进入图形用户界面桌面环境。
7. rc6.d：用于重新启动时执行的脚本。例如，启动一些必备服务。
8. rcS.d目录中的脚本文件在系统启动进入单用户模式时自动运行，用于配置系统的初始化任务和适应单用户环境所需的必要设置

在每个运行级别文件夹中，以特定的顺序执行脚本文件。文件名以字母"K"或"S"开头，加上两位数字。以"S"开头的脚本用于启动服务，而以"K"开头的脚本用于停止服务。这些脚本文件会在系统启动和关机过程中自动运行，并根据各个级别的需求来启动或停止相应的服务。

- ls -l /etc/rc*.d

```
lrwxrwxrwx 1 root root 23 Aug 21 16:27 S01open-vm-tools → ../init.d/open-vm-tools
lrwxrwxrwx 1 root root 15 Aug 21 14:53 S01pcscd → ../init.d/pcscd
lrwxrwxrwx 1 root root 18 Aug 21 14:53 S01plymouth → ../init.d/plymouth
lrwxrwxrwx 1 root root 37 Aug 21 14:53 S01pulseaudio-enable-autospawn → ../init.d/pulseaudio-ena
ble-autospawn
lrwxrwxrwx 1 root root 22 Aug 21 14:58 S01redis-server → ../init.d/redis-server
lrwxrwxrwx 1 root root 15 Aug 21 14:58 S01rsync → ../init.d/rsync
lrwxrwxrwx 1 root root 15 Aug 21 14:53 S01saned → ../init.d/saned
lrwxrwxrwx 1 root root 23 Aug 21 14:57 S01smartmontools → ../init.d/smartmontools
lrwxrwxrwx 1 root root 13 Aug 21 14:53 S01ssh → ../init.d/ssh
lrwxrwxrwx 1 root root 14 Aug 21 14:53 S01sudo → ../init.d/sudo
lrwxrwxrwx 1 root root 17 Aug 21 14:58 S01sysstat → ../init.d/sysstat
```

默认情况下，update-rc.d ssh enable将SSH服务添加到运行级别为2、3、4和5的文件夹中，也就是在/etc/rc2.d、/etc/rc3.d、/etc/rc4.d和/etc/rc5.d目录中创建符号链接，链接到与SSH服务相关的启动

脚本。这些目录代表多用户文本模式和多用户图形模式的运行级别, 作用是在系统启动时自动启动SSH服务，并在运行级别切换时自动重新启动。

(4) 定时任务

- **基本命令**
  - crontab -l 列出某个用户cron服务的详细内容
  - crontab -r 删除每个用户cront任务(谨慎：删除所有的计划任务)
  - crontab -e 使用编辑器编辑当前的crontab文件
- 进入 cron 文件目录，查看是否存在非法定时任务脚本
  - 重点关注以下目录中是否存在恶意脚本

```
/var/spool/cron/*
/var/spool/cron/crontabs/*
/etc/crontab
/etc/cron.d/*
/etc/cron.daily/*
/etc/cron.hourly/*
/etc/cron.monthly/*
/etc/cron.weekly/*
```

- 如果发现有不认识的计划任务，可以定位脚本确认是否是正常业务脚本
- 如果是非正常业务脚本，直接注释掉任务内容或删除脚本

(5) 第三方软件漏洞

- 及时升级修复应用程序漏洞
  - 检查说明：机器被入侵，部分原因是系统使用的应用程序软件版本较老，存在较多的漏洞没有修复，导致可以被利用
  - 解决方法：用户可以通过软件官方发布的安全通告，通过yum、 apt 等方式进行直接升级修复
  - apt update
  - apt upgrade ssh （！这个命令慎用，一般不需要更新软件，且更新软件相关依赖也会同步更新，可能导致系统错误）

(6) 检查异常文件

1、查看敏感目录，如/tmp目录下的文件，同时注意隐藏文件夹，以“..”为名的文件夹具有隐藏属性
2、得到发现WEBSHELL、远控木马的创建时间，如何找出同一时间范围内创建的文件?
可以使用find命令来查找，如 find /opt -iname "*" -atime 1 -type f 找出 /opt 下一天前访问过的文件

(7) 检查系统日志

日志默认存放位置：/var/log/
查看日志配置情况：more /etc/rsyslog.conf

日志文件	说明
/var/log/cron	记录了系统定时任务相关的日志
/var/log/cups	记录打印信息的日志
/var/log/dmesg	记录了系统在开机时内核自检的信息，也可以使用dmesg命令直接查看内核自检信息
/var/log/mailog	记录邮件信息
/var/log/message	记录系统重要信息的日志。这个日志文件中会记录Linux系统的绝大多数重要信息，如果系统出现问题时，首先要检查的就应该是这个日志文件
/var/log/btmp	记录错误登录日志，这个文件是二进制文件，不能直接vi查看，而要使用lastb命令查看
/var/log/lastlog	记录系统中所有用户最后一次登录时间的日志，这个文件是二进制文件，不能直接vi，而要使用lastlog命令查看
/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。同样这个文件也是一个二进制文件，不能直接vi，而需要使用last命令来查看
/var/log/utmp	记录当前已经登录的用户信息，这个文件会随着用户的登录和注销不断变化，只记录当前登录用户的信息。同样这个文件不能直接vi，而要使用w,who,users等命令来查询
/var/log/secure	记录验证和授权方面的信息，只要涉及账号和密码的程序都会记录，比如SSH登录，su切换用户，sudo授权，甚至添加用户和修改用户密码都会记录在这个日志文件中

(8) Linux杀毒软件

- Clamav
  - ClamAV的官方下载地址为： http://www.clamav.net/download.html
  - 安装ClamAV：
  - apt install clamav
  - clamscan -r /home