排查分析

> 这段时间陆陆续续开始`hvv`，而这里就简单的介绍一下`hvv`中对应急响应中可能存在问题进行介绍和分析。

windows排查分析

开机启动项

一般情况下，各个木马等恶意程序，都会在计算机开机的时候自动运行。

所以我们就需要排查一下windows中的开机启动项。

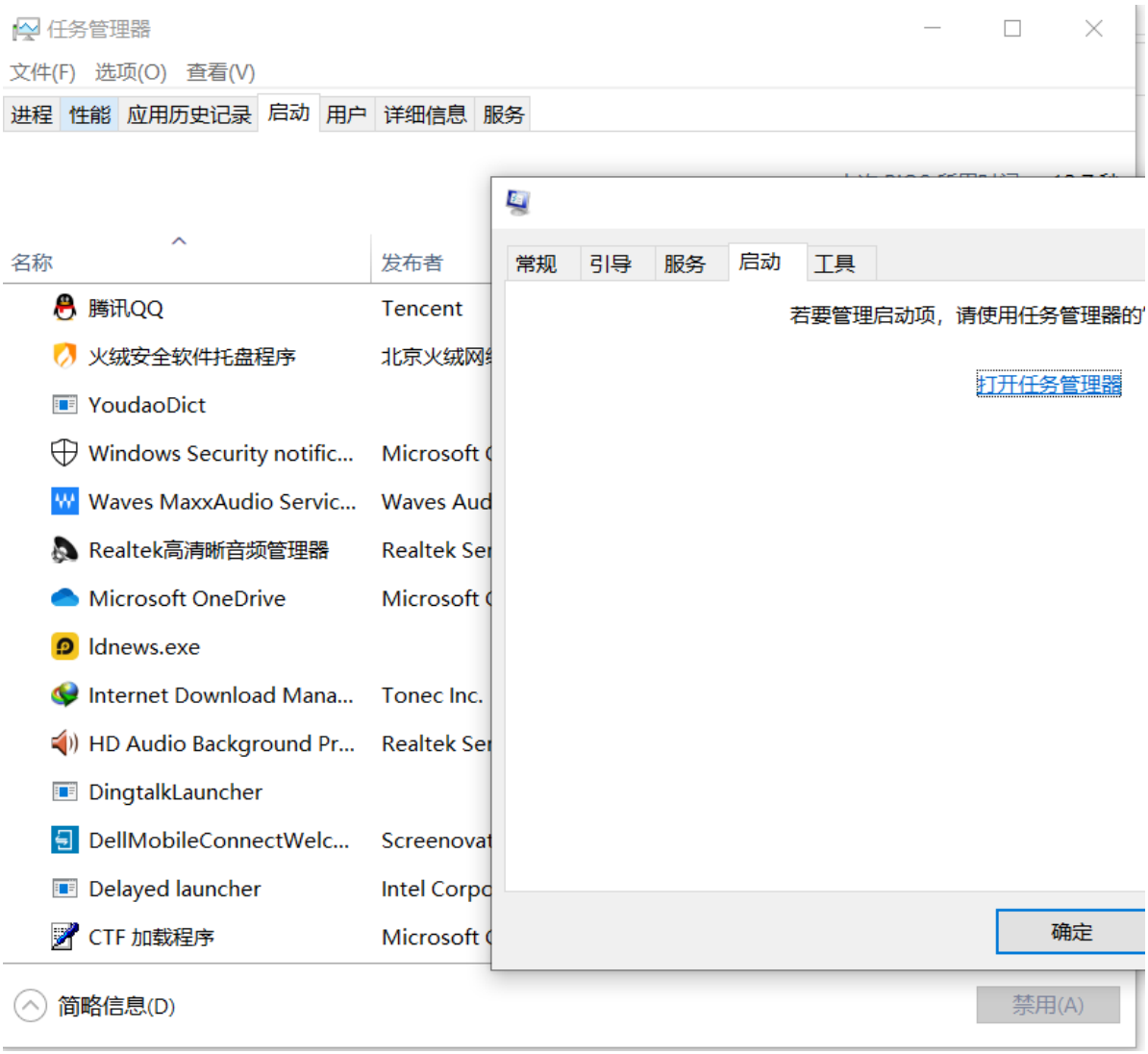
查看方法：

1.利用操作系统的启动菜单

`C:\Users\dell\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup`

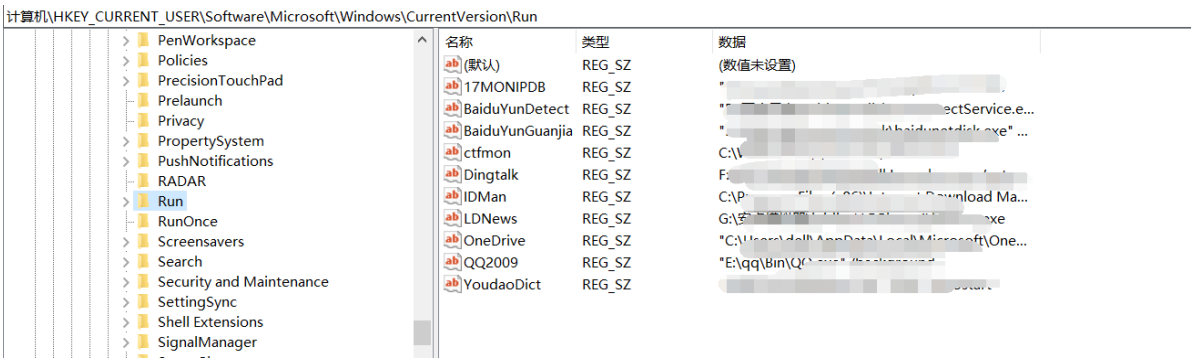
dell为自己电脑的用户名

2.利用系统配置`msconfig`



3.利用注册表`regedit`

`HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run`



temp临时异常文件

temp（临时文件），是位于`C:\Users\dell\AppData\Local\Temp`

可以通过`%temp%`打开，用于收藏夹，浏览器的临时文件，编辑文件等等。

检查思路：因为该文件夹下面是有很高的权限对于登录用户，（写入文件等等），而我们检查的思路就是检查该文件夹下面是不是有异常的文件（`exe，dll，sys`）等等，或者是特别大的`temp`文件.

可以通过在线病毒分析网站进行分析，或者通过杀毒软件进行分析。

病毒分析网址

temp文件夹介绍

浏览器信息分析

这部分主要是，当攻击者拿下了服务器，并且需要通过访问自己的vps，来下载一下恶意程序，就可能是通过浏览器。而这部分就可能是存在游戏信息了，就可以通过浏览器的记录信息进行查看。

浏览器浏览痕迹查看，浏览器文件下载查看，查看浏览器的cookie等等

文件时间属性分析

在windows系统中,文件属性的时间属性具有：创建时间，修改时间，访问时间（默认情况下禁止）。默认情况下，计算机是以修改时间作为展示。

而一般黑客拿下了服务器，一般来说会修改时间来隐藏shell文件，而当黑客修改的时间早于文件创建的时间那么这个文件就有非常大的问题？？？（因为一般来说创建时间的最早的）

通过查看文件属性可以查看到具体的时间、

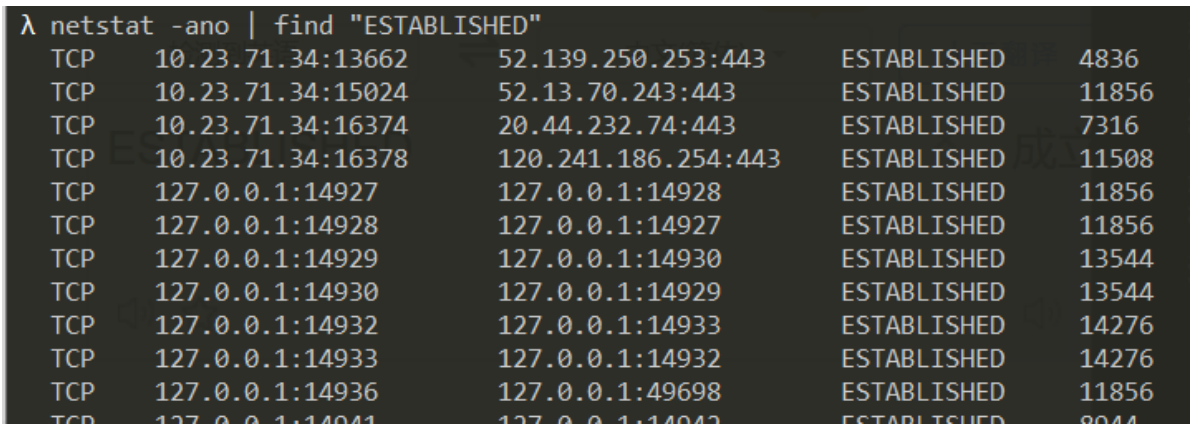
最近打开文件分析

windows系统中默认记录系统中最近打开使用的文件信息，可以在目录`C:\Users\dell\Recent`下打开，或者`recent`打开。我们就可以查看一下最近打开的文件，如果一些黑客打开了一下文件并且忘记关闭就可能有留下信息。

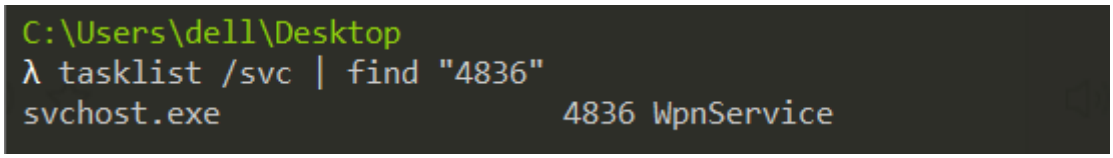
进程分析

计算机与外部网络通信是建立在TCP/UDP协议上的，并且每一次通信都是具有不同的端口（0-65535）。如果计算机被木马了，肯定会与外部网络进行通信，那么此时就可以通过查看网络连接情况，找到对应的进程ID，然后关闭进程ID就可以关闭连接状态。

```
netstat -ano | find "ESTABLISHED"  #寻找建立的连接
```




```
tasklist /svc | find "4836"  #寻找pid=4836对应的程序
```



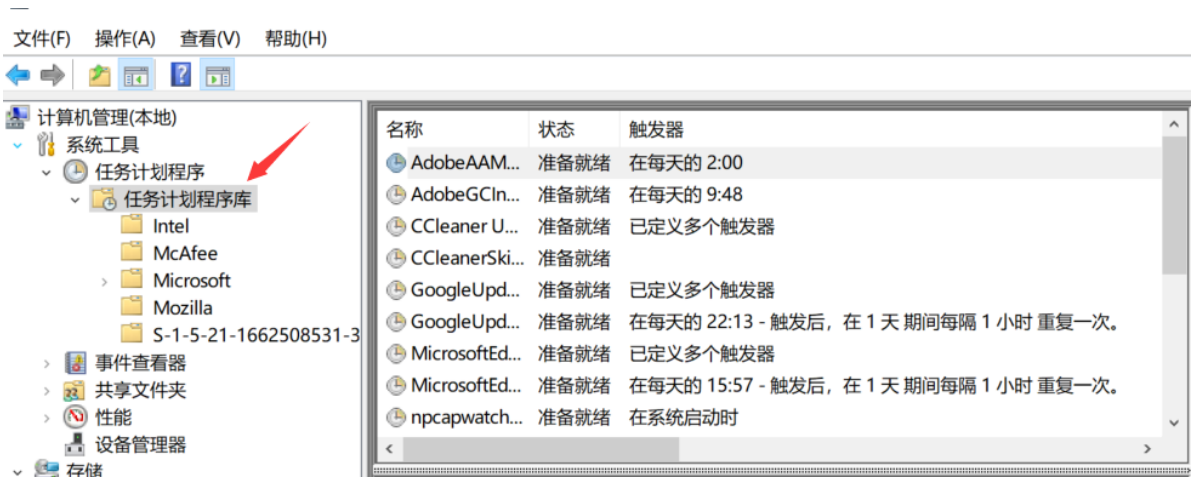

```
tasklist /PID id值 /T  #关闭进程
```

系统信息windows计划任务

在计算机中可以通过设置计划任务，在固定的时间执行固定的操作。一般情况下，恶意代码也可能在固定的时间设置执行。

在windows之前的系统使用`at`命令对计划进行管理。

提示使用`schtasks.exe`或者使用图形化界面。



如果发现恶意的计划任务，应该删除。

系统信息隐藏账号发现与删除

隐藏账号是指黑客入侵了系统之后为了可以持续的保存于该计算机的访问，而在计算机系统中建立了不轻易被发现的计算机用户。

最简单的隐藏账号建立：

```
net user test$ test /add && net localgroup administrator test$ /add
```

$就是隐藏用户的意思

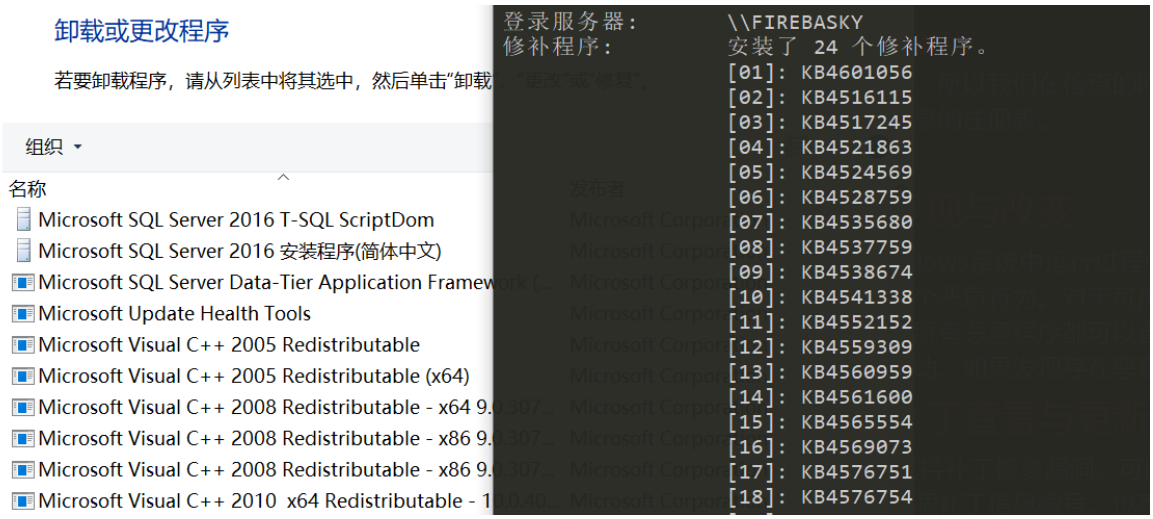
或者修改注册表，所以我们在检查的时候一定要所以图形化界面检查，并且检查用户信息的注册表。

恶意进程发现与改变

恶意程序在Windows系统中运行过程中，将以进程的方式展示，其中恶意进程执行着各个恶意行为。对于可执行程序，可以直接使用杀毒软件查杀，但是并非所有恶意程序都可以查杀，因此需要手工检查，或者使用其他的工具辅助。如果发现存在恶意程序，应立即将其改变。

系统信息补丁查看与更新

Windows系统支持补丁修复漏洞。可以通过 `systeminfo` 查看系统信息，并展示对应的漏洞补丁信息编号。也可以在卸载软件中查看系统补丁和第三方软件补丁。



hacker可以通过查看系统补丁情况来进行利用。

网站webshell查杀

『D盾_防火墙』专为IIS设计的一个主动防御的保护软件,以内外保护的方式防止网站和服务器给入侵,在正常运行各类网站的情况下，越少的功能，服务器越安全的理念而设计! 限制了常见的入侵方法，让服务器更安全!

http://www.d99net.net/

我们可以通过D盾_防火墙来对我们的网站进行查杀

Linux排查分析

文件分析敏感文件信息

`/tmp目录`

黑客在攻击Linux系统中为了进行提权操作，需要有写入执行权限的文件夹，而在Linux中`/tmp`目录下就有这个功能，`/tmp`是一个特别的临时文件，每个用户都可以对其进行读写操作。

```
root@iZbp1aovfjqdgqvjl2au7iZ:~# ls -lat /
total 140
drwx------  34 root root  4096 Mar 26 12:52 root
drwxr-xr-x  23 root root   800 Mar 26 12:52 run
drwxrwxrwt   7 root root  4096 Mar 26 12:45 tmp
```

`/etc/init.d`目录中存放的是一系列系统服务的管理（启动与停止）脚本。而黑客很有可能在该目录下放了一下恶意代码和恶意程序。我们还有可以通过`stat`命令查看文件时间属性。

```
root@iZbp1aovfjqdgqvjl2au7iZ:/etc/init.d# ls
aegis                  cron                  mountall.sh            procps      ssh
apache2                dbus                  mountdevsubfs.sh       rc          sysstat
apache-htcacheclean    docker                mountkernfs.sh         rc.local    udev
apparmor               grub-common           mountnfs-bootclean.sh  rcS         ufw
atd                    halt                  mountnfs.sh            README      umountfs
bootmisc.sh            hostname.sh           mysql                  reboot      umountnfs.sh
cgroupfs-mount         hwclock.sh            networking             resolvconf  umountroot
checkfs.sh             irqbalance            ntp                    rsync       urandom
checkroot-bootclean.sh keyboard-setup.dpkg-bak ondemand             rsyslog     uuidd
checkroot.sh           killprocs             php7.0-fpm             sendsigs    vsftpd
chrony                 kmod                  plymouth               single
console-setup          mountall-bootclean.sh plymouth-log           skeleton
```

```
root@iZbp1aovfjqdgqvjl2au7iZ:/etc/init.d# stat apache2
  File: 'apache2'
  Size: 8087            Blocks: 16         IO Block: 4096   regular file
Device: fd01h/64769d    Inode: 1055670     Links: 1
Access: (0755/-rwxr-xr-x)  Uid: (    0/    root)   Gid: (    0/    root)
Access: 2021-03-26 06:25:02.433734664 +0800
Modify: 2020-07-16 06:29:16.000000000 +0800
Change: 2020-09-29 17:43:28.358284064 +0800
 Birth: -
```

一般来说黑客入侵了服务器基本上会修改一些文件和代码来达到更好的利用。而我们检查的时候就需要去检查在一定时间修改的文件。

```
find ./ -mtime 0 -name "*.php"
#查看24小时内被修改的文件。
#0不是24小时 1表示48小时。。。
```

```
root@iZbp1aovfjqdgqvjl2au7iZ:~# find ./ -mtime 0 -name "*.php"
./1.php
```

或者黑客会创建文件等等。

```
find ./ -ctime 3 -name "*.php"
#查看72小时内新增的文件
```

```
root@iZbp1aovfjqdgqvjl2au7iZ:~# find ./ -ctime 0 -name "*.php"
./1.php
./test.php
```

权限查看

在linux系统中，如果是777权限，那么该文件就非常可能是有问题。

因为这样黑客就可以非常操作。

```
find ./ -iname "*.php" -perm 777
#其中-iname忽略大小写，-perm 筛选权限
```

进程分析网络连接分析

一般来说黑客在攻击一个服务器的时候基本上会使用反弹shell，来建立tcp连接，而我们就需要分析网络连接进行查看是不是被黑客攻击了。

在linux系统中可以使用`netstat`查看网络连接。

`man netstat` 查看帮助文档

常用的命令`netstat -pantl`查看处于tcp网络套节字相关信息。

```
root@iZbp1aovfjqdgqvjl2au7iZ:~# netstat -pantl
Active Internet connections (servers and established)
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      881/sshd
tcp        0      0 127.0.0.1:6010          0.0.0.0:*               LISTEN      6946/0
tcp        0      0 172.16.1.33:33418       100.100.45.186:80       TIME_WAIT   -
tcp        0      0 172.16.1.33:56208       100.100.30.26:80        ESTABLISHED 947/AliYunDun
tcp        0    332 172.16.1.33:22          222.18.126.99:52231     ESTABLISHED 6946/0
tcp6       0      0 :::80                   :::*                    LISTEN      1303/apache2
tcp6       0      0 :::81                   :::*                    LISTEN      2163/docker-proxy
tcp6       0      0 :::82                   :::*                    LISTEN      2183/docker-proxy
tcp6       0      0 :::21                   :::*                    LISTEN      848/vsftpd
```

```
ESTABLISHED 表示建立了连接
LISTEN      表示监听状态
```

如果发现异常ip。应使用`kill -9 pid`关闭进程。而获得了PID就可以配合`ps`查看信息。使用`ps`查看进程信息。使用`ps aux|grep PID`筛选具体的PID进程信息，`lsof -i :端口`也可以。

登录分析

在Linux系统中做的使用操作都记录到系统日志中，对于登录也可以查看日志文件信息，查看是否异常。（黑客可以异常登录我们的服务器）

```
last -i | grep -v 0.0.0.0
#筛选非本地登录
```

`w`命令实时登录查看

```
root@iZbp1aovfjqdgqvjl2au7iZ:~# w
 16:36:08 up 18:51,  1 user,  load average: 0.00, 0.01, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
root     pts/0    2[redacted]      16:09    0.00s  0.06s  0.00s w
```

异常用户分析排查

一般黑客进入了系统会创建用户保证下次方便操作。

而在Linux系统中root用户是一个最高管理员，可以在linux上做任何事情。

新建用户：`useradd username`

设置密码：`passwd usernaem 输入密码`

当`/etc/passwd`有修改权限就可以修改`/etc/passwd`文件中的uid和gid等于0（root用户其uid和gid是为0）

所有我们就找要不要异常用户和异常用户的权限问题。

```
cat /etc/passwd
grep "0:0" /etc/passwd
ls -l /etc/passwd
awk -F: '$3==0{print $1}' /etc/passwd
awk -F: '$2==""{print $1}' /etc/passwd
awk -F: 'length($2)==0 {print $1}' /etc/shadow
```

在`/etc/shadow`文件中`!`表示空密码。

历史文件分析history

当黑客入侵了系统，肯定会执行一些命令，而这些命令就会记录到Linux系统中，我们就可以通过`/root/.bash_history`查看，或者直接使用`history`。

特别注意的时：黑客可以进行了wget（下载木马），ssh（连接内网主机），tar zip等命令（数据打包），系统配置等（命令修改 如：修改ps netstat命令）

计划任务排查 crontab

在黑客拿下了系统，可能会写入一些计划任务进行利用。而这时候我们就可以查看计划任务来检查。

在linux 系统中可以使用crontab命令进行计划任务的设置。

`crontab -h`

```
^C^Xroot@iZbp1aovfjqdgqvjl2au7iZ:~# crontab -h
crontab: invalid option -- 'h'
crontab: usage error: unrecognized option
usage:  crontab [-u user] file
        crontab [ -u user ] [ -i ] { -e | -l | -r }
                (default operation is replace, per 1003.2)
        -e      (edit user's crontab)
        -l      (list user's crontab)
        -r      (delete user's crontab)
        -i      (prompt before deleting user's crontab)
```

特别注意计划任务中的未知的内容

开机自动项

在linux(debian)系统中`/etc/init.d/`目录下保存着开机自动启动的程序。

黑客可能在其中添加了一下恶意程序来利用。

用户可以直接使用`/etc/init.d/ 程序名 status`查看状态

使用`update-rc.d 程序名` disable 取消开机自动　enable是开启

```
root@iZbp1aovfjqdgqvjl2au7iZ:/etc/init.d# update-rc.d
update-rc.d: error: not enough arguments
usage: update-rc.d [-n] [-f] <basename> remove
       update-rc.d [-n] <basename> disable|enable [S|2|3|4|5]
                -n: not really
                -f: force

The disable|enable API is not stable and might change in the future.
```

$PTAH变量异常

决定shell将到那个地方执行，PATH的值是一系列目录，当用户执行程序的时候，linux在那些目录下进行搜索编译链接，如ls cd等等

```
root@iZbp1aovfjqdgqvjl2au7iZ:/etc/init.d# echo $PATH
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games
```

修改PATH `export PATH=$PATH:/usr/local/new/bin`，但是这样只能在本次有效果，系统重新启动就会失去效果。

解决方法就是在`/etc/profile`或`/home/.bashrc`(source ~/.bashrc)。

而我们就需要查看有没有异常的环境变量。

后门排查工具-rkhunter

`rkhunter`是一个自动的工具进行排查

安装：`apt install rkhunter`

具有的功能

- 系统命令的检测，md5校验
- rookit检测
- 本机敏感目录，系统配置异常检测

基本使用`rkhunter --check --sk`