**Linux应急响应**

**什么是应急响应:**

**当我们的网站或者系统正常运行过程中,为了应对攻击发生所做的准备以及在发生攻击事件后所采取的措施。更多的还是偏侧与攻击后的阻止和排查.**

**应急响应流程:http://www.shangusec.net/sitesources/webs/page\_pc/xwzx/aqdt/article4af735e804424ca4badc5c7d3dd9b1dd.html**

**常见的应急响应事件分类：**

**web入侵：网页挂马、主页篡改、Webshell**

**系统入侵：病毒木马、勒索软件、远控后门**

**网络攻击：DDOS攻击、DNS劫持、ARP欺骗**

**网页挂马:**

**挂马,就是黑客通过各种手段获得网站管理员账号,然后登陆网站后台,向页面中加入恶意转向代码。也可以直接通过弱口令获得服务器或者网站FTP,然后直接对网站页面直接进行修改。当用户访问被加入恶意代码的页面时,就会自动的访问被转向的地址或者下载木马病毒。**

**解决办法:**

**第一是找到根源,堵住根源,因为这条很难办,无法快速定位病原。**

**大多数情况先从第二条措施做起,比如删除被挂马页面的恶意代码.**

**主页篡改:**

**很多时间，当然我们打开某个网时，会跳出一个恶意对话框，无论你点任何地方，你浏览器的主页都会被篡改 . 木马病毒所致**

**解决:**

**临时:打开浏览器，点工具-->Internet选项，在常规标签下把主页地址改成你的原主页即可。**

**永久:找到木马进行删除**

**病毒木马:**

**常见的就是系统中上传木马 , 进行挖矿 ,让主机访问恶意链接等.主要表现CPU长时间使用率非常高或者系统卡顿.**

**勒索软件:**

**勒索软件（ransomware）是一种流行的木马，通过骚扰、恐吓甚至采用绑架用户文件等方式，使用户数据资产或计算资源无法正常使用，并以此为条件向用户勒索钱财。**

**感染后表现形式，包括：**

**1. 锁定计算机或移动终端屏幕 。**

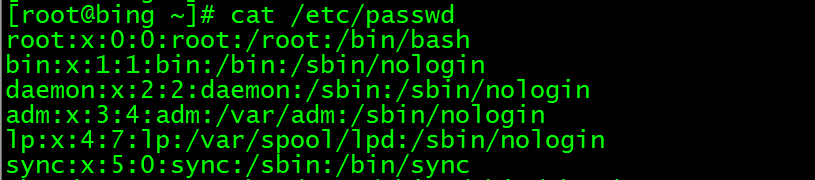
**2. 借杀毒软件之名，假称在用户系统发现了安全威胁，令用户感到恐慌， 从而购买所谓的“杀毒软件”。**

**3. 计算机屏幕弹出的提示消息，称用户文件被加密，要求支付赎金。**

**1.检查密码是否为弱口令登录**

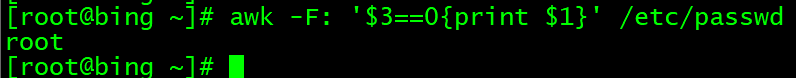
**2.判断是否有新添加的用户，并排查**

**cat /etc/passwd**

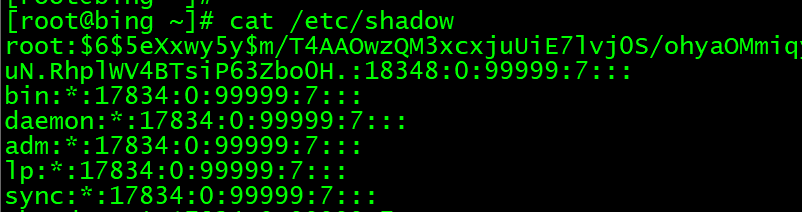


**查看uid为零的用户（管理员用户） awk -F: 以:为分隔符查找 $3表示第三列 $1表示第一列**

**awk -F: '$3==0{print $1}'**

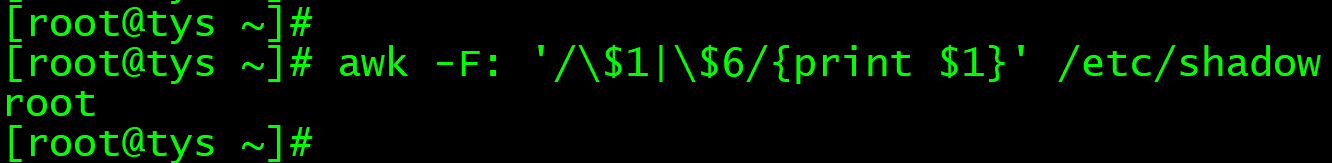


**cat /etc/shadow**



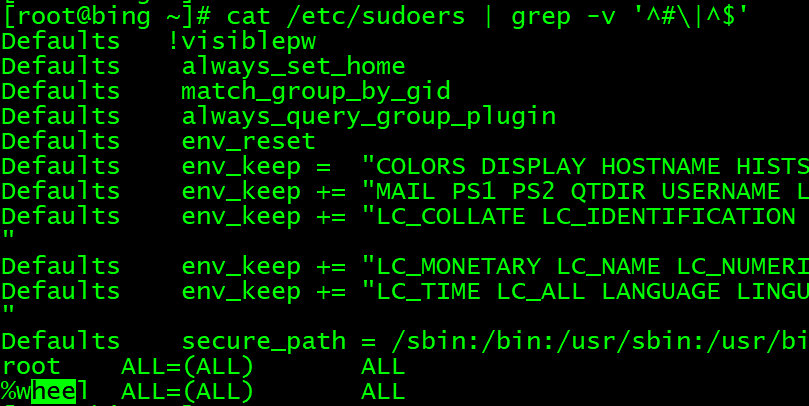
**查看能够远程登录的用户：有密码即可远程登录 有密码的$1或者$6开头**

**awk -F: '/\$1|\$6/{print $1}' /etc/shadow**



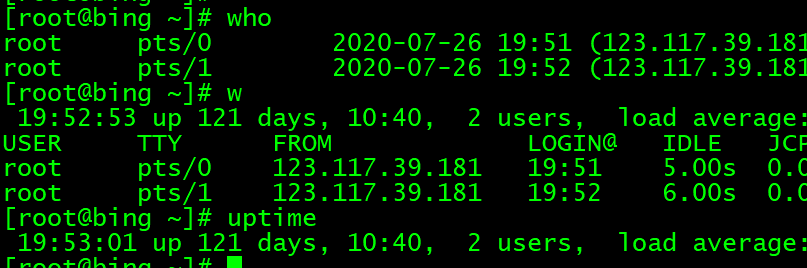
**查看sudo信息：看是否有超级管理员存在 过滤#开头的或者过滤空白**

**cat /etc/sudoers | grep -v '^#\|^$'**



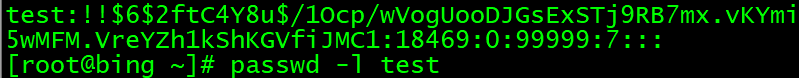
**2.1查看远程登录用户有哪些**

**w,who,uptime(登录多久，多少用户，负载)**

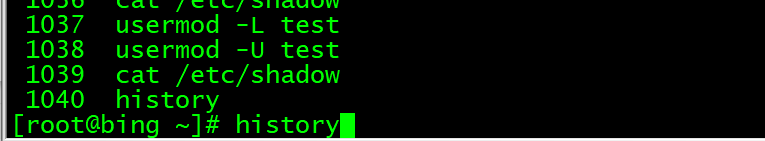


**3.账户禁用 (将可疑账户禁用)**

**usermod -L 账号 或 passwd -l 账号 解除passwd -u**

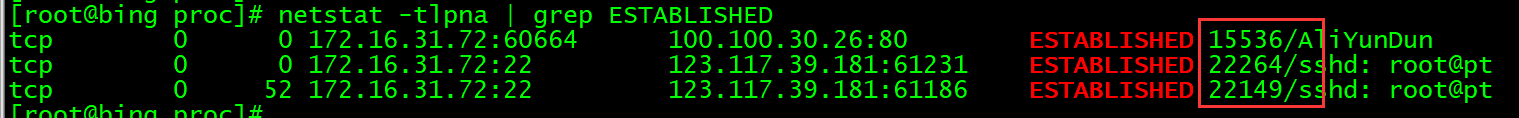


**4.查看历史命令 看看入侵者做了什么样的操作**

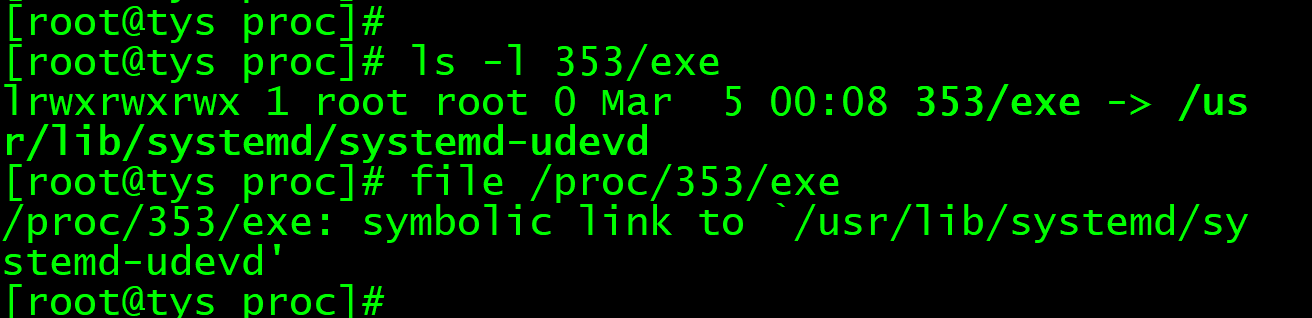


**5.检查异常端口**

**netstat -antp | grep ESTABLISHED （看怪ip，端口）**

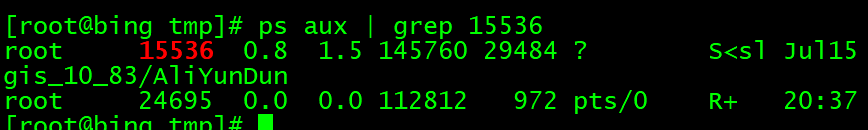


**查看pid所对应的进程文件路径,将可能为病毒文件上传微步情报社区或着virus total**





**6.检查异常进程 定位登录账号**



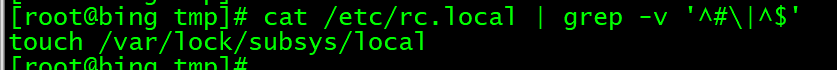
**7.检查开机自启项**

**/etc/rc.local**

**/etc/rc.d/rc[0~6].d**

**ls -alt /etc/init.d/**

**cat /etc/rc.local | grep -v '^#\|^$'**



**8.检查定时任务**

**/var/spool/cron/\***

**/etc/crontab**

**/etc/cron.d/\***

**/etc/cron.daily/\***

**/etc/cron.hourly/\***

**/etc/cron.monthly/\***

**/etc/cron.weekly/**

**/etc/anacrontab**

**/var/spool/anacron/\***

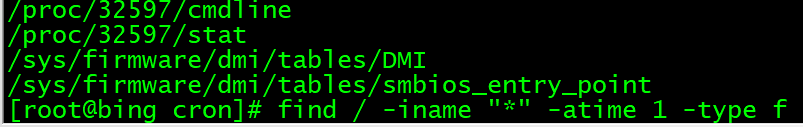
**9.检查异常文件**

**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**

**3、针对可疑文件可以使用stat进行查看文件修改时间。**

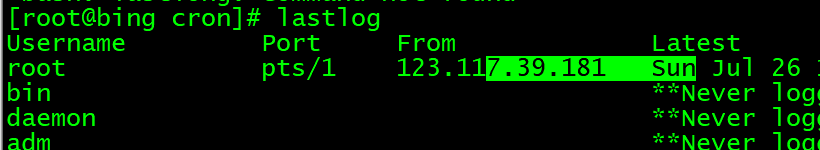


**10.检查系统日志**

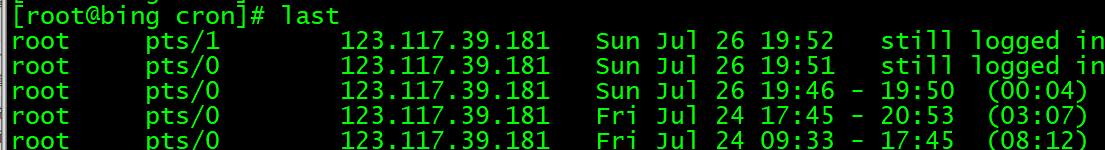


**最为重要的是**

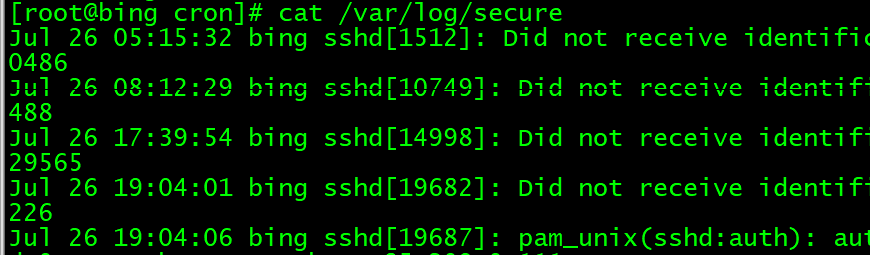
**/var/log/lastlog**



**/var/log/wtmp**



**/var/log/secure**



**11.安装杀毒软件**

**# Ubuntu安装Clamav**

**mark@ubuntu:~$ sudo apt-get install clamav**

**mark@ubuntu:~$ sudo apt-get install clamav-daemon**

**mark@ubuntu:~$ sudo freshclam**

**mark@ubuntu:~$ sudo lsof /var/log/clamav/freshclam.log**

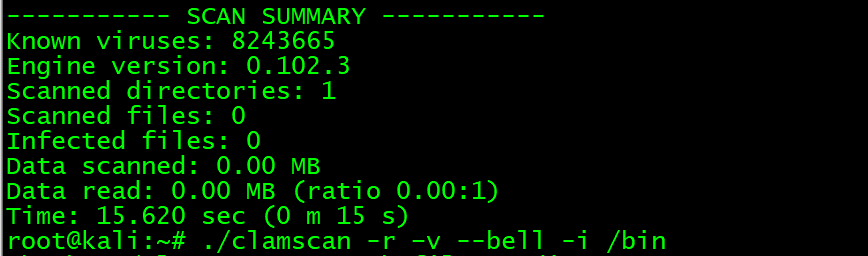
**mark@ubuntu:~$ sudo systemctl stop clamav-freshclam.service**

**mark@ubuntu:~$ sudo freshclam**

**mark@ubuntu:~$ clamscan -r /home # 扫描用户文件夹**

**./clamscan -r –v --bell -i /bin 扫描bin目录并且显示有问题的文件的扫描结果**

**clamscan -r -i /home --move=/opt/infected -l /var/log/clamscan.log**



**12.安全检查脚本**

**Github项目地址：**

**<https://github.com/grayddq/GScan>**

**<https://github.com/ppabc/security_check>**

**<https://github.com/T0xst/linux>**

案例分享:https://www.freebuf.com/articles/system/208804.html