Linux 木马清除过程

作者：euphrat1ca
原文链接：https://ld246.com/article/1563854014620
来源网站：链滴

首先啰嗦一下，关于linux主机，高危端口真得万万不能全网开放。看了日志后，发现黑客真是时时刻在爆破。

关于linux入侵的排查思路，总结如下：

1. 查看异常进程活动-查找是否有异常进程和端口占用

    1. 查找占用cpu最多的进程，相关命令：运行top命令后，键入大写字母P按cpu排序；
    2. 查找占用内存最多的进程，相关命令：运行top命令后，键入大写字母M

```
ps aux | sort -k4nr
```

    3. 查找进程文件：

```
ls -la /proc/$pid/exe
```

    4. 跟踪异常进程运行情况：

```
strace -tt -T -e trace=all -p $pid
```

    5. 查看进程打开的文件

```
lsof -p $pid
```

    6. 查看进程端口情况

```
netstat -anltp | grep $pid
```

2. 查看账号安全

    1. 查看是否有存在新增异常账号：

```
a.查找特权用户
awk -F ":" '$3==0{print $1}' /etc/passwd
b.查找可以远程登录的账号信息
awk '/\$1|\$6/{print $1}' /etc/shadow
c.查找sudo权限账户
cat /etc/sudoers | grep -v "^#\|^$" | grep "ALL=(ALL)"
```

    2. 查看是否有账号异常登录情况：

```
a.查看当前登录用户和其行为
w
b.查看所有用户最后一次登录的时间
lastlog
c.查看所有用户的登录注销信息及系统的启动、重启及关机事件
last
d.查看登录成功的日期、用户名及ip
grep "Accepted " /var/log/secure* | awk '{print $1,$2,$3,$9,$11}'
e.查看试图爆破主机的ip
grep refused /var/log/secure* | awk {'print $9'} | sort | uniq -c |sort -nr | moregrep "Failed pas
word" /var/log/secure* | grep -E -o "(([0-9]{1,3})\.([0-9]{1,3})\.([0-9]{1,3})\.([0-9]{1,3}))" | uniq -c

f.查看有哪些ip在爆破主机的root账号
grep "Failed password for root" /var/log/secure | awk '{print $11}' | sort
g.查看爆破用户名字典
```

```
grep "Failed password" /var/log/secure | awk {'print $9'} | sort | uniq -c | sort -nr
```

3. 查找异常文件

    1. 查找cron文件中是否存在恶意脚本

```
/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/*
```

    2. 查看最近一段时间内被修改的系统文件

```
find /etc/ /usr/bin/ /usr/sbin/ /bin/ /usr/local/bin/ -type f -mtime -T | xargs ls -la
```

    3. 按时间排序，确认最近是否有命令被替换，可以结合rpm -Va命令

```
ls -alt /usr/bin /usr/sbin /bin /usr/local/binrpm -Va>rpm.log
```

    4. 确认是否有异常开机启动项

```
cat /etc/rc.localchkconfig --list
```

4. 借助工具查杀病毒和rootkit

    1. 查杀rootkit

```
chkrootkit (下载地址-http://www.chkrootkit.org)rkhunter (下载地址-http://rkhunter.sourceforge.net)
```

    2. 查杀病毒

```
clamav(下载地址-http://www.clamav.net/download.html)
```

    3. 查杀webshell

```
cloudwalker(下载地址-http://github.com/chaitin/cloudwalker)
```