【应急响应】Linux入侵排查思路

作者：Bypass

原文链接：https://mp.weixin.qq.com/s?__biz=MzA3NzE2MjgwMg==&mid=2448903857&idx=1&sn=53232e146731c66685d7a3b7423e58aa&chksm=8b55deecbc2257fada792de3c3ad677c3e50a2350d75cdd0f00421c6156963846ea9474ba4a3&scene=21#wechat_redirect

---

0x00 前言

当企业发生黑客入侵、系统崩溃或其它影响业务正常运行的安全事件时，急需第一时间进行处理，使企业的网络信息系统在最短时间内恢复正常工作，进一步查找入侵来源，还原入侵事故过程，同时给出解决方案与防范措施，为企业挽回或减少经济损失。

针对常见的攻击事件，结合工作中应急响应事件分析和解决的方法，总结了一些Linux服务器入侵排查的思路。

0x01 入侵排查思路

一、账号安全

基本使用：

```
1、用户信息文件/etc/passwd
root:x:0:0:root:/root:/bin/bash
account:password:UID:GID:GECOS:directory:shell
用户名：密码：用户ID：组ID：用户说明：家目录：登陆之后shell
注意：无密码只允许本机登陆，远程不允许登陆

2、影子文件/etc/shadow
root:$6$oGs1PqhL2p3ZetrE$X7o7bzoouHQVSEmSgsYN5UD4.kMHx6qgbTqwNVC5oOAouXvcjQSt.Ft7ql1WpkopY0UV9ajBwUt1DpYxTCVvI/:16809:0:99999:7:::
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

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
```

入侵排查：

```
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、查询可以远程登录的帐号信息
[root@localhost ~]# awk '/\$1|\$6/{print $1}' /etc/shadow

3、除root帐号外，其他帐号是否存在sudo权限。如非管理需要，普通帐号应删除sudo权限
[root@localhost ~]# more /etc/sudoers | grep -v "^#\|^$" | grep "ALL=(ALL)"

4、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
```

二、历史命令

基本使用：

```
通过.bash_history查看帐号执行过的系统命令
1、root的历史命令
histroy


2、打开/home各帐号目录下的.bash_history，查看普通帐号的历史命令
为历史的命令增加登录的IP地址、执行命令时间等信息：
```

1）保存1万条命令
```
sed -i 's/^HISTSIZE=1000/HISTSIZE=10000/g' /etc/profile
```

2）在/etc/profile的文件尾部添加如下行数配置信息：
```
######jiagu history xianshi#########
USER_IP=`who -u am i 2>/dev/null | awk '{print $NF}' | sed -e 's/[()]//g'`
if [ "$USER_IP" = "" ]
then
USER_IP=`hostname`
fi
export HISTTIMEFORMAT="%F %T $USER_IP `whoami` "
shopt -s histappend
export PROMPT_COMMAND="history -a"
######### jiagu history xianshi ##########
```

3）source /etc/profile让配置生效

生成效果： 1 2018-07-10 19:45:39 192.168.204.1 root source /etc/profile

3、历史操作命令的清除：history -c
但此命令并不会清除保存在文件中的记录，因此需要手动删除.bash_profile文件中的记录。

入侵排查：

进入用户目录下
```
cat .bash_history >> history.txt
```

三、端口

使用netstat 网络连接命令，分析可疑端口、IP、PID

```
netstat -antlp|more
```

查看下pid所对应的进程文件路径，
运行ls -l /proc/$PID/exe或file /proc/$PID/exe（$PID 为对应的pid 号）

四、进程

使用ps命令，分析进程

```
ps aux | grep pid
```

五、开机启动项

基本使用：

系统运行级别示意图：

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

查看运行级别命令
runlevel

系统默认允许级别

```
vi  /etc/inittab
id=3：initdefault  系统开机后直接进入哪个运行级别
```

开机启动配置文件

```
/etc/rc.local
/etc/rc.d/rc[0~6].d
```

例子: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

```
root@localhost ~]# ln -s /etc/init.d/sshd /etc/rc.d/rc3.d/S100ssh
```

此处sshd是具体服务的脚本文件，S100ssh是其软链接，S开头代表加载时自启动；如果是K开头的脚本文件，代表运行级别加载时需要关闭的。

入侵排查：

启动项文件：
more /etc/rc.local
/etc/rc.d/rc[0~6].d
ls -l /etc/rc.d/rc3.d/

六、定时任务

基本使用

1、利用crontab创建计划任务

- 基本命令

crontab -l 列出某个用户cron服务的详细内容

Tips：默认编写的crontab文件会保存在 (/var/spool/cron/用户名 例如: /var/spool/cron/root

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

如：*/1 * * * * echo "hello world" >> /tmp/test.txt 每分钟写入文件

2、利用anacron实现异步定时任务调度

- 使用案例

每天运行 /home/backup.sh脚本：
vi /etc/anacrontab
@daily 10 example.daily /bin/bash /home/backup.sh

当机器在 backup.sh 期望被运行时是关机的，anacron会在机器开机十分钟之后运行它，而不用再等待 7天。

入侵排查

重点关注以下目录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/*
```

小技巧：

```
 more /etc/cron.daily/*  查看目录下所有文件
```

七、服务

服务自启动

第一种修改方法：

```
chkconfig [--level 运行级别] [独立服务名] [on|off]
chkconfig -level  2345 httpd on  开启自启动
chkconfig httpd on （默认level是2345）
```

第二种修改方法：

```
修改/etc/re.d/rc.local 文件
加入 /etc/init.d/httpd start
```

第三种修改方法：

使用ntsysv命令管理自启动，可以管理独立服务和xinetd服务。

入侵排查

1、查询已安装的服务：

RPM包安装的服务

```
chkconfig  --list  查看服务自启动状态，可以看到所有的RPM包安装的服务
ps aux | grep crond 查看当前服务
```

```
系统在3与5级别下的启动项
中文环境
chkconfig --list | grep "3:启用\|5:启用"
英文环境
chkconfig --list | grep "3:on\|5:on"
```

源码包安装的服务

```
查看服务安装位置 ，一般是在/user/local/
service httpd start
搜索/etc/rc.d/init.d/  查看是否存在
```

八、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

日志分析技巧：

1、定位有多少IP在爆破主机的root帐号：
```
grep "Failed password for root" /var/log/secure | awk '{print $11}' | sort | uniq -c | sort -nr | more
```

定位有哪些IP在爆破：
```
grep "Failed password" /var/log/secure|grep -E -o "(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)"|uniq -c
```

爆破用户名字典是什么？
```
 grep "Failed password" /var/log/secure|perl -e 'while($_=<>){ /for(.*?) from/; print "$1\n";}'|uniq -c|sort -nr
```

2、登录成功的IP有哪些：
```
grep "Accepted " /var/log/secure | awk '{print $11}' | sort | uniq -c | sort -nr | more
```

登录成功的日期、用户名、IP：
```
grep "Accepted " /var/log/secure | awk '{print $1,$2,$3,$9,$11}'
```

3、增加一个用户kali日志：
```
Jul 10 00:12:15 localhost useradd[2382]: new group: name=kali, GID=1001
Jul 10 00:12:15 localhost useradd[2382]: new user: name=kali, UID=1001, GID=1001, home=/home/kali
, shell=/bin/bash
Jul 10 00:12:58 localhost passwd: pam_unix(passwd:chauthtok): password changed for kali
#grep "useradd" /var/log/secure
```

4、删除用户kali日志：
```
Jul 10 00:14:17 localhost userdel[2393]: delete user 'kali'
Jul 10 00:14:17 localhost userdel[2393]: removed group 'kali' owned by 'kali'
Jul 10 00:14:17 localhost userdel[2393]: removed shadow group 'kali' owned by 'kali'
# grep "userdel" /var/log/secure
```

5、su切换用户：
```
Jul 10 00:38:13 localhost su: pam_unix(su-l:session): session opened for user good by root(uid=0)
```

sudo授权执行：
```
sudo -l
Jul 10 00:43:09 localhost sudo:    good : TTY=pts/4 ; PWD=/home/good ; USER=root ; COMMAND=/sbin/shutdown -r now
```

0x03 工具篇

一、Rootkit查杀

- chkrootkit

  网址： http://www.chkrootkit.org

```
使用方法：
wget ftp://ftp.pangeia.com.br/pub/seg/pac/chkrootkit.tar.gz
tar zxvf chkrootkit.tar.gz
cd chkrootkit-0.52
make sense
#编译完成没有报错的话执行检查
./chkrootkit
```

- rkhunter

  网址： http://rkhunter.sourceforge.net

```
使用方法：
Wget https://nchc.dl.sourceforge.net/project/rkhunter/rkhunter/1.4.4/rkhunter-1.4.4.tar.gz
tar -zxvf rkhunter-1.4.4.tar.gz
cd rkhunter-1.4.4
./installer.sh --install
rkhunter -c
```

二、病毒查杀

- Clamav

  ClamAV的官方下载地址为： http://www.clamav.net/download.html

  安装方式一：

```
1、安装zlib：
wget http://nchc.dl.sourceforge.net/project/libpng/zlib/1.2.7/zlib-1.2.7.tar.gz
tar -zxvf  zlib-1.2.7.tar.gz
cd zlib-1.2.7
#安装一下gcc编译环境： yum install gcc
CFLAGS="-O3 -fPIC" ./configure --prefix= /usr/local/zlib/
make && make install

2、添加用户组clamav和组成员clamav：
groupadd clamav
useradd -g clamav -s /bin/false -c "Clam AntiVirus" clamav

3、安装Clamav
tar -zxvf clamav-0.97.6.tar.gz
cd clamav-0.97.6
./configure --prefix=/opt/clamav --disable-clamav -with-zlib=/usr/local/zlib
make
make install

4、配置Clamav
mkdir /opt/clamav/logs
mkdir /opt/clamav/updata
touch /opt/clamav/logs/freshclam.log
touch /opt/clamav/logs/clamd.log
cd /opt/clamav/logs
chown clamav:clamav clamd.log
chown clamav:clamav freshclam.log

5、ClamAV 使用：
 /opt/clamav/bin/freshclam 升级病毒库
./clamscan -h 查看相应的帮助信息
./clamscan -r /home  扫描所有用户的主目录就使用
./clamscan -r --bell -i /bin  扫描bin目录并且显示有问题的文件的扫描结果
```

  安装方式二：

```
#安装
yum install -y clamav
#更新病毒库
freshclam
```

```
#扫描方法
clamscan -r /etc --max-dir-recursion=5 -l /root/etcclamav.log
clamscan -r /bin --max-dir-recursion=5 -l /root/binclamav.log
clamscan -r /usr --max-dir-recursion=5 -l /root/usrclamav.log
#扫描并杀毒
clamscan -r  --remove  /usr/bin/bsd-port
clamscan -r  --remove  /usr/bin/
clamscan -r --remove  /usr/local/zabbix/sbin
#查看日志发现
cat /root/usrclamav.log |grep FOUND
```

三、webshell查杀

linux版：

河马webshell查杀：http://www.shellpub.com
深信服Webshell网站后门检测工具：http://edr.sangfor.com.cn/backdoor_detection.html

四、RPM check检查

系统完整性可以通过rpm自带的-Va来校验检查所有的rpm软件包，查看哪些命令是否被替换了：

```
./rpm -Va > rpm.log
```

如果一切均校验正常将不会产生任何输出，如果有不一致的地方，就会显示出来，输出格式是8位长字符串，每个字符都用以表示文件与RPM数据库中一种属性的比较结果 ，如果是. (点) 则表示测试通过。

验证内容中的8个信息的具体内容如下：

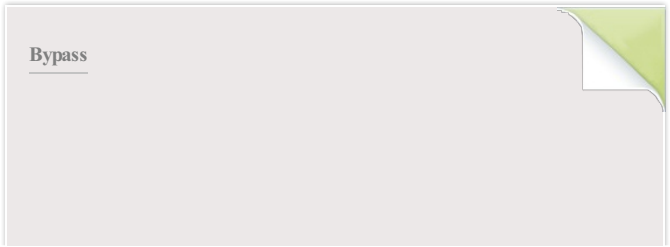
S	文件大小是否改变
M	文件的类型或文件的权限（rwx）是否被改变
5	文件MD5校验是否改变（可以看成文件内容是否改变）
D	设备中，从代码是否改变
L	文件路径是否改变
U	文件的属主（所有者）是否改变
G	文件的属组是否改变
T	文件的修改时间是否改变

如果命令被替换了，如何去还原回来：

文件提取还原过程：
rpm -qf /bin/ls 查询ls命令属于哪个软件包
mv /bin/ls /tmp 先把ls转移到tmp目录下，造成ls命令丢失的假象
rpm2cpio /mnt/cdrom/Packages/coreutils-8.4-19.el6.i686.rpm | cpio -idv ./bin/ls 提取rpm包中ls命令到当前目录的/bin/ls下
cp /root/bin/ls /bin/ 把ls命令复制到/bin/目录 修复文件丢失

文件提权还原实例：

本文由Bypass原创发布，转载请保留出处。欢迎关注我的个人微信公众号：Bypass--，浏览更多精彩文章。



About Me

一个网络安全爱好者，对技术有着偏执狂一样的追求。致力于分享原创高质量干货，包括但不限于：渗透测试、WAF绕过、代码审计、安全运维。