Linux服务器安全运维

# 账号和登录安全

## 删除特殊的用户和用户组

系统安装时候，默认安装了很多不必要的用户和用户组。有的时候，有的用户要禁止登录功能。可以使用命令，usermod –s /sbin/nologin/用户名。

* 可删除的用户：adm,lp,sync,shutdown,shutdown,halt,news,uucp,operator,games,gopher
* 可删除的用户组：adm,lp,news,uucp,games,dip,pppusers,popusers,slipusers等

## 关闭系统不需要的服务

系统运行必须的服务：

acpid:用于电源管理。

apmd:高级电源管理服务，可以监控电池的性能。

kudzu:检测硬件是否变化的服务。

crond:为linux下自动安排的进程提供服务。

atd:指定时间做指定事情的服务。

keytables:用于装载镜像键盘。

iptables:linux中内置的防火墙。

xinetd:支持多种网络服务的核心守候进程。

xfs:使用X windows桌面系统的必须的服务

network:网络服务。

sshd:提供远程登录Linux上的服务。

syslog:记录系统日志的服务。

## 密码安全策略(使用ssh服务)

|  |
| --- |
| #启用公钥认证  PubkeyAuthentication yes  #publicKey文件路径  AuthorizedKeysFile .ssh/authorized\_keys  #不使用口令认证  PasswordAuthentication no |

## 合理使用su、sudo命令

|  |
| --- |
| #普通用户user可以在任意ip地址不输入密码的情况使用命令  user ALL=NOPASSWD:service iptables start  #普通用户user可以在任意ip地址不输入密码的情况使用任意命令  user ALL=NOPASSWD: ALL |

## 删减系统登录欢迎信息

虽然系统的一些欢迎信息或者版本信息能够给系统管理员带来一些便利，但是这些信息有时候可能成为黑客利用。为了保证系统的安全，可以修改或者删除某些系统文件。

/etc/issue和/etc/issue.net：文件记录了操作系统的名称和版本号，用户通过本地总段或者本地与你控制台登录系统时候，就会显示/etc/issue中的文件内容，当用户通过ssh或者telnet等远程工具登录时候，会显示/etc/issue.net的文件内容。默认ssh登录后，/etc/issue.net的内容不会显示出来。可以修改/etc/ssh/sshd\_config文件。在文件中添加Banner /etc/issue.net

/etc/redhat-release：记录了操作系统的名称和版本号。

/etc/motd：使系统的公告信息。用词用户登录后，/etc/motd文件的内容就会显示在用户总段。其中包括一些警告信息，容易被黑客窃取。

# 远程访问和认证安全

## 远程登录使用ssh方式

Port 22 #设置sshd监听端口，为了安全，建议使用22默认端口

AddressFamily any

ListenAddress 0.0.0.0 #用来设置sshd服务器绑定端口

ListenAddress ::

Protocol 2 #ssh协议的版本

HostKey /etc/ssh/ssh\_host\_rsa\_key

HostKey /etc/ssh/ssh\_host\_dsa\_key #是指服务器密钥文件的路径

KeyRegenerationInterval 1h #多少秒后系统重新生成密钥

ServerKeyBits 1024 #定义服务器密钥长度

#用来设定在记录来自sshd的消息时候，是否给出facility code

SyslogFacility AUTHPRIV

LogLevel INFO #记录sshd日志消息的级别

#设置用户登录失败，在切断连接服务前服务器等待时间(s)

LoginGraceTime 2m

PermitRootLogin yes #是否允许root用户登录

#设置ssh在接受登录请求之前是否检查用户根目录和rhosts文件权限。

StrictModes yes

MaxAuthTries 6 #最大失败尝试次数

#MaxSessions 10

RSAAuthentication yes #是否启用RSA密钥验证

PubkeyAuthentication yes #是否开启公钥验证

AuthorizedKeysFile .ssh/authorized\_keys #设置公钥验证文件的路径

#AuthorizedKeysCommand none

#AuthorizedKeysCommandRunAs nobody

#RhostsRSAAuthentication no

#HostbasedAuthentication no

#设置进行RhostsRSAAuthentication验证时，忽略~.ssh/known\_hosts

IgnoreUserKnownHosts no

IgnoreRhosts yes #验证的时候是否使用~/.rhosts和~/.shosts

PasswordAuthentication yes #用来设置是否开启密码验证机制

#PermitEmptyPasswords no #是否允许口令为空的用户登录

#PasswordAuthentication yes

#ChallengeResponseAuthentication yes #是否启用s/key密码

UsePAM yes #是否通过PAM认证

X11Forwarding yes #是否允许x11转发

PrintMotd yes #用来设置sshd是否在用户登录时候显示/etc/motd中内容

PrintLastLog yes #是否显示上一次登录信息、

#TCPKeepAlive yes

UseDNS yes #是否使用DNS反向解析

## 合理使用shell历史命令记录功能

Linux可以通过history命令查看用户所有的历史操作记录，同时shell命令保存在用户~/.bash\_history中。编辑/etc/bashrc文件：

|  |
| --- |
| HISTFILESIZE=4000  HISTSIZE=4000  HISTTIMEFORMAT='%F %t'  export HISTTIMEFORMAT |

为了确保服务器的安全，保留shell命令的执行历史是非常有用的技巧。以下代码详细记录用户，操作日志的shell脚本。/etc/profile代码如下：

|  |
| --- |
| #Record history operation  USER\_IP=`who -u am i 2>/dev/null |awk '{print $NF}' |sed -e 's/[()]//g'`  LOGNAME=`who -u am i |awk '{print $1}'`  HISTDIR=/user/share/.history  if [ -z $USER\_IP ]  then  USER\_IP=`hostname`  fi  if [ ! -d $HISTDIR ]  then  mkdir -p $HISTDIR  chmod 777 $HISTDIR  fi  if [ ! -d $HISTDIR/${LOGNAME} ]  then  mkdir -p $HISTDIR/${LOGNAME}  chmod 300 $HISTDIR/${LOGNAME}  fi  export HISTSIZE=4000  DT=`date +"%Y%m%d\_%H%M%S"`  export HISTFILE="$HISTDIR/${LOGNAME}/${USER\_IP}.history.$DT"  export HISTTIMEFORMAT="[%Y.%m.%d %H:%M:%S]"  chmod 600 $HISTDIR/${LOGNAME}/\*.history\* 2>/dev/null |

## 启用tcp\_wrappers防火墙

tcp\_wrappers是一个来自分析tcp/ip封包的软件，类似于iptables。作为一个安全的系统，linux本身包括两层防火墙。第一层是通过ip过滤机制的iptables。第二层是tap\_wrappers,tongguo tcp\_wrrappers可以实现对系统中提供的某些服务的开放与关闭、允许与禁止。

### 查看是否安装tcp\_wrappers

rpm -qa | grep tcp

### tcp\_wrappers防火墙的局限性

linux中某些服务可以使用tcp\_wrappers防火墙，取决于服务是否应用libwrapped库。系统中默认的服务，如sshd，portmap，sendmail，xinetd,vsftpd,tcpd等都可以使用tcp\_wrappers。

### tcp\_wrappers设定的规则

tcp\_wrappers防火墙的实现是通过/etc/hosts.allow和/etc/hosts.deny两个文件夹来完成的。格式：service:hosts [:action]

* service ：代表服务名，例如sshd,vsftpd,sendmail等
* hosts：主机名或者ip地址，可以多个。例如192.168.12.0、[www.ixdba.net](http://www.ixdba.net)
* action：动作，符合条件后，采取的动作。

配置文件中常用关键字：

ALL:所有服务或者ip

ALL EXCEPT：从所有的服务或者所有IP中除去指定的。

例如：

#除了指定ip地址这台机器，其他任何机器执行搜有服务是都被允许或者拒绝。

ALL:ALL EXCEPT 192.168.12.189

一般情况下，linux会先判断/etc/hosts.allow这个文件，如果远程登录计算机满足设定，就不会使用/etc/hosts.deny文件。相反，如果不满足hosts.allow文件的设定，就会使用hosts.deny文件，如果满足就限制为不可访问linux服务器。如果两者都不满足设定，主机默认是可以访问Linux服务器的。因此，在设定/etc/hosts.allow文件访问规则后，只需设置/etc/hosts.deny为所有计算机都不能登录状态。sshd:ALL

# 文件系统安全

## 锁定系统重要文件

为了系统安全，linux提供了一个锁定文件的命令chattr,通过这个命令可以修改ext2,ext3,ext4文件系统下文件的属性，并且这个命令必须由root来执行。和这个命令对应的是lsattr,后者用来查询文件的属性。

chattr命令格式:chattr [-RV] [-v version] [mode] 文件或者目录

参数含义：

-R：递归修改所有的文件及子目录、

-V：详细显示修改内容。

Mode用来控制文件属性

* +(在原有参数上，追加参数) -(在原有参数基础上，移除参数) =(更新参数)
* a(append,该参数说明只能往文件中添加内容，不能删除，一般用于日志文件)
* i(immutable,设定文件不能修改，删除，重命名，设定链接。)
* c(compress,设定文件是否经压缩后在存储)
* s(安全的删除文件或目录，及文件被删除后全部回收硬盘空间)
* u(与s相反，系统会保留删除的数据块以便以后恢复删除这个文件)

例如：chattr -R +I /bin

lsattr命令格式：lsattr [-adlRvV] 文件或者目录

参数说明：

-a：列出目录的所有文件，包括以“.”开头的文件

-d：显示指定目录的属性

-R：以递归方式列出目录下所有文件及子目录以及属性值

-v：显示文件或者目录版本

虽然通过chattr命令可以修改文件的属性能够提高文件系统的安全性，但是不适合所有的目录，如/,/dev,/tmp,/var。这些目录系统都会被用到。

## 文件权限的修改和检查

### 查找系统中任何用户都有写权限的文件或者目录

|  |
| --- |
| find / -type f -perm -2 -o -perm -20 | xargs ls –al  find / -type d -perm -2 -o -perm -20 | xargs ls –ad |

### 查看程序中含s位的程序

|  |
| --- |
| find / -type f -perm -4000 -o -perm -2000 -print | xargs ls –al |

### 检查系统中所有suid及sgid文件

|  |
| --- |
| find / -user root -perm -2000 -print -exec md5sum {} \;  find / -user root -perm -4000 -print -exec md5sum {} \; |

### 检查系统没有属主的文件

|  |
| --- |
| find / -nouser -o -nogroup |

## /tmp,/var/tmp,/dev/shm安全设定

/dev/shm是linux系统中一个共享内存设备，在启动时候会默认加载/dev/shm,被加载的/dev/shm使用的是tmpfs文件系统，它属于内存文件系统，会完全驻留在RAM中。可以使用一下设置优化：

|  |
| --- |
| tmpfs /dev/shm tmpfs defaults,nosuid,noexec,rw 0 0 |

# 系统软件安全管理

80%以上的系统攻击是由于软件或者应用程序的漏洞所导致的。

# Linux后门入侵检测工具

rootkit是Linux平台下最常见的一种木马后门工具，它主要通过替换系统文件来达到入侵和和隐蔽的目的，这种木马比普通木马后门更加危险和隐蔽，普通的检测工具和检查手段很难发现这种木马。rootkit攻击能力极强，对系统的危害很大，它通过一套工具来建立后门和隐藏行迹，从而让攻击者保住权限，以使它在任何时候都可以使用root权限登录到系统。rootkit主要有两种类型：文件级别和内核级别。

## rootkit后门检测工具chkrootkit

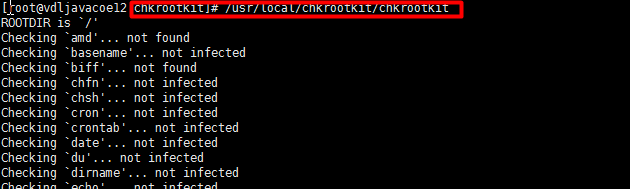
### 安装和使用

|  |
| --- |
| --安装和使用  yum -y install gcc  yum -y install gcc-c++  yum -y install make  tar zxvf chkrootkit.tar.gz  cd chkrootkit-0.50/  make sense  cd ..  cp -r chkrootkit-0.50/ /usr/local/chkrootkit |

### 使用chkrootkit

chkrootkit各个参数的含义如下所示。参数含义：

* -h显示帮助信息
* -v显示版本信息
* -l显示测试内容
* -ddebug模式，显示检测过程的相关指令程序
* -q安静模式，只显示有问题的内容
* -x高级模式，显示所有检测结果
* -r dir设置指定的目录为根目录
* -p dir1:dir2:dirN指定chkrootkit检测时使用系统命令的目录
* -n跳过NFS连接的目录



### chkrootkit的缺点

chkrootkit在检查rootkit的过程中使用了部分系统命令，因此，如果服务器被黑客入侵，那么依赖的系统命令可能也已经被入侵者替换，此时chkrootkit的检测结果将变得完全不可信。

## rootkit后门检测工具RKHunter

RKHunter是一款专业的检测系统是否感染rootkit的工具，它通过执行一系列的脚本来确认服务器是否已经感染rootkit。在官方的资料中，RKHunter可以作的事情有：MD5校验测试，检测文件是否有改动；检测rootkit使用的二进制和系统工具文件；检测特洛伊木马程序的特征码；检测常用程序的文件属性是否异常；检测系统相关的测试；检测隐藏文件；检测可疑的核心模块LKM；检测系统已启动的监听端口。

### 安装RKHunter

|  |
| --- |
| tar -zxvf rkhunter-1.4.0.tar.gz  cd rkhunter-1.4.0  ./installer.sh --layout default --install |

### 使用rkhunter指令

Rkhunter常用参数以及含义如下所示。

 参数             含义

-c, --check：必选参数，表示检测当前系统

--configfile <file>：使用特定的配置文件

--cronjob：作为cron任务定期运行

--sk, --skip-keypress：自动完成所有检测，跳过键盘输入

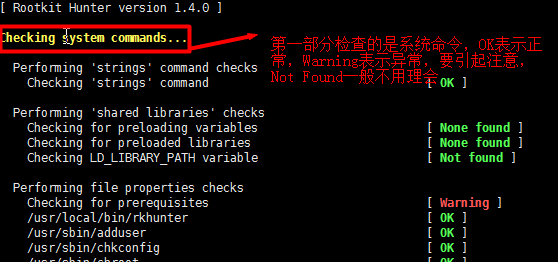
--summary：显示检测结果的统计信息

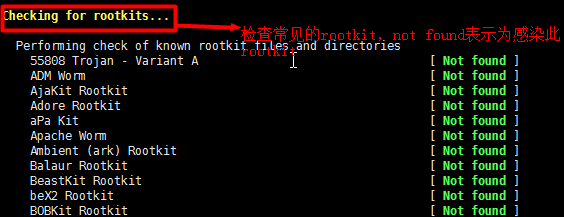
--update：检测更新内容

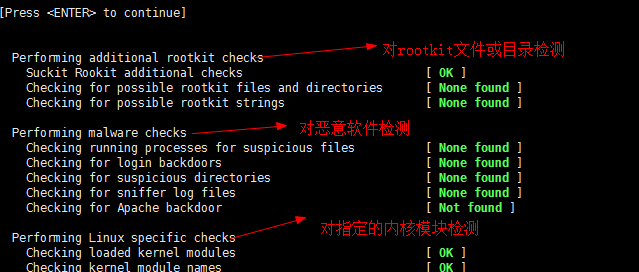
-V, --version：显示版本信息

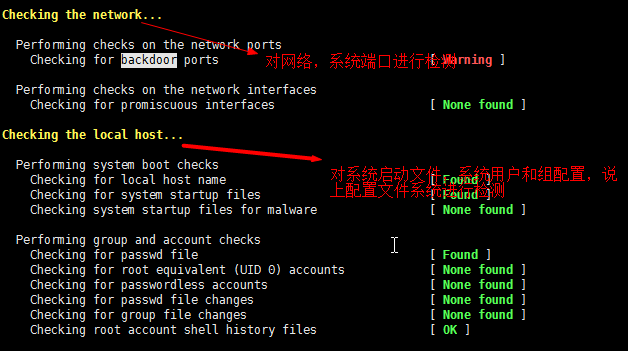
--versioncheck：检测最新版本

/usr/local/bin/rkhunter -c

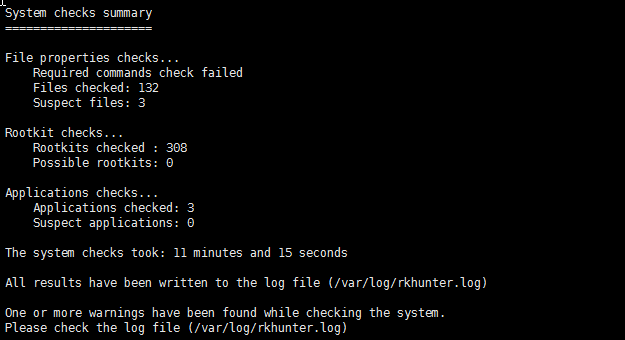












注意：使用HKHunter来检测系统如果发现是红色，就要引起注意。如果想每天定时运行可以配置定时任务/etc/crontab

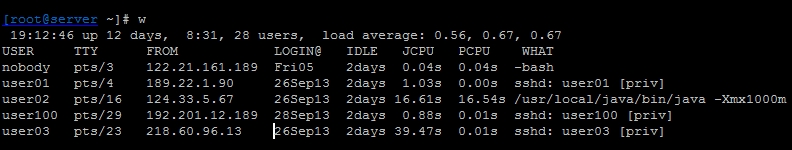
|  |
| --- |
| 30 09 \* \* \* root /usr/local/bin/rkhunter --check --cronjob |

# 服务器遭受攻击后处理过程

切断网络->查找攻击源(通过查看日志)-> 分析入侵原因和途径->备份用户数据->重新安装系统->修复程序或系统漏洞->恢复数据和连接网络

## 检查并锁定可疑用户

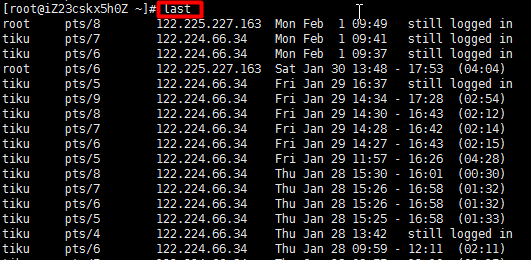
#w命令即可列出所有登录过系统的用户



#锁定可疑用户并剔除

|  |
| --- |
| passwd -l nobody  ps -ef|grep @pts/3  kill -9 6051 |

#last命令查看用户登录事件



## 查看系统日志

可以查看系统日志/var/log/messages,/var/log/secure等，这两个这两个日志文件可以记录软件的运行状态以及远程用户的登录状态，还可以查看每个用户目录下的.bash\_history文件，特别是/root目录下的.bash\_history文件，这个文件中记录着用户执行的所有历史命令。

## 检查并关闭系统可疑进程

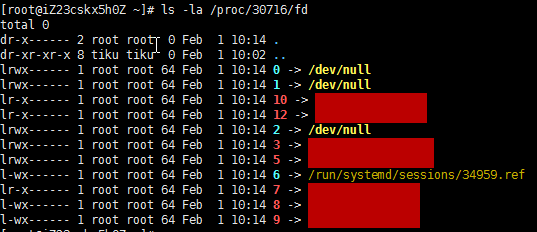
#通过pidof命令可以查找正在运行的进程PID



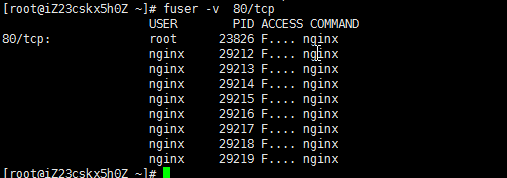
#查看对应PID目录下exe文件的信息



#查看文件的句柄



#指定端口或者tcp、udp协议找到进程PID，进而找到相关进程



## 检查文件系统的完好性

对文件系统的检查也可以通过chkrootkit、RKHunter这两个工具来完成。