链滴

centos 系统加固脚本

作者：yuanhenglizhen

原文链接：https://ld246.com/article/1545662053586

来源网站：链滴

运行

curl -L https://github.com/mufengcoding/shell/releases/download/1.1/security.sh | bash

注意只运行一次， 多次运行可能会gg

github地址：https://github.com/mufengcoding/shell/blob/master/security.sh

```
#!/bin/sh
# desc: setup linux system security
# author:mufengs
# powered by blog.mufengs.com
# version 0.1.2 written by 2018.11.24
#account setup


#锁定以下用户

passwd -l xfs

passwd -l news

passwd -l nscd

passwd -l dbus

passwd -l vcsa

passwd -l games

passwd -l nobody

passwd -l avahi

passwd -l haldaemon

passwd -l gopher

passwd -l ftp

passwd -l mailnull

passwd -l pcap

passwd -l mail

passwd -l shutdown

passwd -l halt

passwd -l uucp

passwd -l operator
```

```
passwd -l sync

passwd -l adm

passwd -l lp


#将帐号相关文件设为只读属性

\# chattr /etc/passwd /etc/shadow

chattr +i /etc/passwd

chattr +i /etc/shadow

chattr +i /etc/group

chattr +i /etc/gshadow


#系统登陆失败3次锁定5分钟

\# add continue input failure 3 ,passwd unlock time 5 minite

sed -i 's#auth required pam\_env.so#auth required pam\_env.so \\n auth required pam\_tally.
o onerr=fail deny=3 unlock\_time=300 \\n auth required /lib/security/$ISA/pam\_tally.so one
r=fail deny=3 unlock\_time=300#' /etc/pam.d/system-auth


#5分钟超时登出

\# system timeout 5 minite auto logout

echo  "TMOUT=300"  \>>/etc/profile


#设置历史命令为10条

\# will system save history command list to 10

sed -i "s/HISTSIZE=1000/HISTSIZE=10/" /etc/profile


#让以上配置生效

\# enable /etc/profile go!

source /etc/profile
```

```
#防范SYN Flood攻击
\# add syncookie enable /etc/sysctl.conf
echo  "net.ipv4.tcp\_syncookies=1"  \>> /etc/sysctl.conf
sysctl -p \# exec sysctl.conf enable

\# optimizer sshd\_config

sed -i "s/#MaxAuthTries 6/MaxAuthTries 6/" /etc/ssh/sshd\_config
sed -i "s/#UseDNS yes/UseDNS no/" /etc/ssh/sshd\_config

#限制重要命令的权限
\# limit chmod important commands
chmod 700 /bin/ping
chmod 700 /usr/bin/finger
chmod 700 /usr/bin/who
chmod 700 /usr/bin/w
chmod 700 /usr/bin/locate
chmod 700 /usr/bin/whereis
chmod 700 /sbin/ifconfig
chmod 700 /usr/bin/pico
chmod 700 /bin/vi
chmod 700 /usr/bin/which
chmod 700 /usr/bin/gcc
chmod 700 /usr/bin/make
chmod 700 /bin/rpm
```

```
\# history security

chattr +a /root/.bash\_history
chattr +i /root/.bash\_history

\# write important command md5
cat \> list << "EOF" &&
/bin/ping
/bin/finger
/usr/bin/who
/usr/bin/w
/usr/bin/locate
/usr/bin/whereis
/sbin/ifconfig
/bin/pico
/bin/vi
/usr/bin/vim
/usr/bin/which
/usr/bin/gcc
/usr/bin/make
/bin/rpm
/bin/ls
/bin/top
/bin/ps
EOF
```

```
for  i  in  \`cat list\`
do
if \[ !  \-x  $i \];then
echo  "$i not found,no md5sum!"
else
md5sum $i  \>> /var/log/\`hostname\`.log
fi
done
rm -f list

\# 修改默认umask
perl -npe 's/umask\\s+0\\d2/umask 077/g' -i /etc/bashrc
perl -npe 's/umask\\s+0\\d2/umask 077/g' -i /etc/csh.cshrc


#cron加固
echo  "Locking down Cron"

touch /etc/cron.allow

chmod 600 /etc/cron.allow

awk -F: '{print $1}' /etc/passwd | grep -v root \> /etc/cron.deny

echo  "Locking down AT"

touch /etc/at.allow
```

原文链接：centos 系统加固脚本

```
chmod 600 /etc/at.allow

awk -F: '{print $1}' /etc/passwd | grep -v root \> /etc/at.deny


#内核加固
cat <<  EOF >> /etc/sysctl.conf
net.ipv4.ip\_forward = 0

net.ipv4.conf.all.send\_redirects = 0

net.ipv4.conf.default.send\_redirects = 0

net.ipv4.tcp\_max\_syn\_backlog = 1280

net.ipv4.icmp\_echo\_ignore\_broadcasts = 1

net.ipv4.conf.all.accept\_source\_route = 0

net.ipv4.conf.all.accept\_redirects = 0

net.ipv4.conf.all.secure\_redirects = 0

net.ipv4.conf.all.log\_martians = 1

net.ipv4.conf.default.accept\_source\_route = 0
```

```
net.ipv4.conf.default.accept\_redirects = 0

net.ipv4.conf.default.secure\_redirects = 0

net.ipv4.icmp\_echo\_ignore\_broadcasts = 1

net.ipv4.icmp\_ignore\_bogus\_error\_responses = 1

net.ipv4.tcp\_syncookies = 1

net.ipv4.conf.all.rp\_filter = 1

net.ipv4.conf.default.rp\_filter = 1

net.ipv4.tcp\_timestamps = 0
EOF

\# 禁止所有TCP Wrappers
echo  "ALL:ALL"  \>> /etc/hosts.deny
echo  "sshd:ALL"  \>> /etc/hosts.allow

#防止缓冲区溢出
sysctl -w kernel.exec-shield=1
sysctl -q -n -w kernel.randomize\_va\_space=2
echo  "kernel.exec-shield = 1"\>>/etc/sysctl.conf
echo  "kernel.randomize\_va\_space = 2"\>>/etc/sysctl.conf
```

```
#禁止空密码登陆
sed -i 's/\\<nullok\\>//g' /etc/pam.d/system-auth

#定时更新
yum -y install yum-cron
chkconfig yum-cron on
```

原文链接：centos 系统加固脚本