链滴

centos 系统安全配置十五点建议

作者：huwei1108

原文链接：https://ld246.com/article/1533801243995

来源网站：链滴

1防止攻击

1、禁用ping，vi /etc/rc.d/rc.local下添加一行:echo 1 > /proc/sys/net/ipv4/icmp_echo_ignore_al，0表示运行，1表示禁用

2、防止DOS攻击,所有用户设置资源限制，vi /security/limits.conf添加以下几行，hard core 0，har rss 5000，hard nproc 50，禁止调试文件；检查/etc/pam.d/login文件，必须存在session required /lib/security/pam_limits.so

2注释不需要的用户和用户组

vi /etc/passwd 注释不需要的用户，“#”注释，如下：

#games□x12□100games:/usr/games:/sbin/
ologin

#gopher□x13:30:gopher:/var/gopher:/sbin/nologin

#ftp□x14:50:FTP User:/var/ftp:/sbin/nologin

#adm□x3:4:adm:/var/adm:/sbin/nologin

#lp□x4:7:lp:/var/spool/lpd:/sbin/nologin

#sync□x5:0:sync:/sbin:/bin/sync

#shutdown□x6:0:shutdown:/sbin:/sbin/shutdown

#halt□x7:0:halt:/sbin:/sbin/halt

#uucp□x10:14:uucp:/var/spool/uucp:/sbin/nologin

#operator□x11:0:operator:/root:/sbin/nologin

vi /etc/group 注释不需要的用户组，如下:

#adm□x4:root,adm,daemon

#lp□x7:daemon,lp

#uucp□x14:uucp

#games□x20:

#dip□x40:

#news□x9:13:news:/etc/news

3禁止使用Ctrl+Alt+Del快捷键重启服务器

vi /etc/inittab #注释这一行

#ca::ctrlaltdel:/sbin/shutdown -t3 -r now

4使用yum update更新系统时不升级内核，只更新软件包

由于系统与硬件的兼容性问题，有可能升级内核后导致服务器不能正常启动，这是非常可怕的，没有别的需要，建议不要随意升级内核。

cp /etc/yum.conf /etc/yum.confbak

1、修改yum的配置文件 vi /etc/yum.conf 在[main]的最后添加 exclude=kernel*

2、直接在yum的命令后面加上如下的参数：

yum --exclude=kernel* update

查看系统版本 cat /etc/issue

查看内核版本 uname -a

5关闭自动更新

chkconfig --list yum-updatesd #显示当前系统状态

service yum-updatesd stop #关闭 开启参数为start

chkconfig --level 35 yum-updatesd off #禁止开启启动）

chkconfig yum-updatesd off #禁止开启启动（所有启动模式全部禁止）

chkconfig --list yum-updatesd #显示当前系统状态

6隐藏系统信息

在缺省情况下，当你登陆到linux系统，会显示linux发行版的名称、版本、内核版本、服务器的名称这些信息不能泄露，需隐藏起来。

修改下面两文件的命名。

mv /etc/issue /etc/issuebak

mv /etc/issue.net /etc/issue.netbak

7关闭系统不需要的服务

service acpid stop chkconfig acpid off #停止服务，取消开机启动

service autofs stop chkconfig autofs off #停用自动挂载档案系统与周边装置

service bluetooth stop chkconfig bluetooth off #停用Bluetooth蓝牙

service cpuspeed stop chkconfig cpuspeed off #停用控制CPU速度主要用来省电

service cups stop chkconfig cups off #停用Common UNIX Printing System 使系统支援印表机

service ip6tables stop chkconfig ip6tables off #禁止IPv6

8禁止非root用户执行/etc/rc.d/init.d/下的系统命令

chmod -R 700 /etc/rc.d/init.d/*

9重要文件加上不可更改属性，从而防止非授权用户获得权限

给系统服务端口列表文件加锁,防止未经许可的删除或添加服务:

chattr +a .bash_history

chattr +i .bash_history

chattr +i /etc/shadow
chattr +i /etc/group

chattr +i /etc/passwd
chattr +i /etc/gshadow
chattr +i /etc/services

重新添加删除用户需解锁，解锁命令为:chattr -i 对应文件

10限制文件的权限

700权限表示只有属主才能去操作
chmod 700 /usr/bin
chmod 700 /bin/ping
chmod 700 /usr/bin/vim
chmod 700 /bin/netstat
chmod 700 /usr/bin/tail
chmod 700 /usr/bin/less
chmod 700 /usr/bin/head
chmod 700 /bin/cat
chmod 700 /bin/uname
chmod 500 /bin/ps

恢复文件权限命令:chmod 755 对应文件

11关闭多余的虚拟控制台

系统默认定义了 6 个虚拟控制台，关闭多余的控制台，只留一个控制台，可以节省内存，防止从不同控制台登录，修改如下:
vi /etc/inittab
Run gettys in standard runlevels*
1:2345:respawn:/sbin/mingetty tty1
#2:2345:respawn:/sbin/mingetty tty2
#3:2345:respawn:/sbin/mingetty tty3
#4:2345:respawn:/sbin/mingetty tty4
#5:2345:respawn:/sbin/mingetty tty5
#6:2345:respawn:/sbin/mingetty tty6

12优化内核参数

vi /etc/sysctl.conf
net.ipv4.tcp_max_syn_backlog = 65536

net.core.netdev_max_backlog = 32768

net.core.somaxconn = 32768

net.core.wmem_default = 8388608

net.core.rmem_default = 8388608

net.core.rmem_max = 16777216

net.core.wmem_max = 16777216

net.ipv4.tcp_timestamps = 0

net.ipv4.tcp_synack_retries = 2

net.ipv4.tcp_syn_retries = 2

net.ipv4.tcp_tw_recycle = 1

#net.ipv4.tcp_tw_len = 1

net.ipv4.tcp_tw_reuse = 1

net.ipv4.tcp_mem = 94500000 915000000 927000000

net.ipv4.tcp_max_orphans = 3276800

#net.ipv4.tcp_fin_timeout = 30

#net.ipv4.tcp_keepalive_time = 120

net.ipv4.ip_local_port_range = 10024 65535 #（表示用于向外连接的端口范围。缺省情况下很小：2768到61000 注意：这里不要将最低值设的太低，否则可能会占用掉正常的端口！ ）

13 限制shell命令记录大小

每个用户的主目录下都存放着/home/axjsms/.bash_history文件，可存放多大500条命令，为了系统全，需限制该文件大小，可修改为50，vi /etc/profile添加HISTSIZE=50;

14 修改ssh服务的root登录权限

修改ssh服务配置文件，使的ssh服务不允许直接使用root用户来登录，这样减少系统被恶意登录攻击机会。

vi /etc/ssh/sshd_config

PermitRootLogin no

15修改ssh默认的端口

ssh默认会监听22端口，可以修改至8822端口以避过常规的扫描

1、修改22端口为8822端口，vi /etc/ssh/sshd_config把port 22改为port 8822

2、service sshd restart

3、查看端口是否正确，netstat -lnp|grep ssh

4、防火墙开放8822端口，vi /etc/sysconfig/iptables,添加-A RH-Firewall-1-INPUT -m state --stat NEW -m tcp -p tcp --dport 8822 -j ACCEPT

重启iptables服务，service iptables restart