链滴

centos 系统安全方面设置

作者：An
原文链接：https://ld246.com/article/1358910192154
来源网站：链滴

1.修改SSH端口号，这个很有必要，把默认端口号22改成其他的之后，一些专门扫描22端口的黑软件可以拒之门外了。
操作方法：
<pre>vi /etc/ssh/sshd_config</pre>
找到#port 22
将前面的#去掉,然后修改端口 port 123 （123可以根据个人情况自定义）
2、禁用root登录
注意，采用此方法前必须要先建立好一个普通用户：
操作方法：
<pre>useradd abc
passwd abc</pre>
然后在/etc/ssh/sshd_config这个文件里设置是否禁用root登录，这个看个人需要了，我暂时没。
操作方法：找到其中的PermitRootLogin yes 将其修改为 PermitRootLogin no（如果PermitRotLogin前面有#的话也要删除掉）
以后用普通用户登陆后，如果需要root权限就采用 su root 命令即可。
完成以上两步之后重启sshd服务：service sshd restart
3.简单配置一下防火墙规则
1）安装iptables防火墙：yum install iptables
2）清除已有iptables规则
<pre>iptables -F
iptables -X
iptables -Z</pre>
3）设置防火墙规则
#允许本地回环接口(即运行本机访问本机)：
<pre>iptables -A INPUT -s 127.0.0.1 -d 127.0.0.1 -j ACCEPT</pre>
允许已建立的或相关连的通行：
<pre>iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT</pre>
#允许所有本机向外的访问 ：
<pre>iptables -A OUTPUT -j ACCEPT</pre>
允许访问22端口（ssh远程连接端口，如果已修改为其他端口，此处要注意填写新的端口），8端口（开网页用的），20，21端口（ftp用的）
<pre>iptables -A INPUT -p tcp --dport 22 -j ACCEPT
iptables -A INPUT -p tcp --dport 80 -j ACCEPT
iptables -A INPUT -p tcp --dport 21 -j ACCEPT
iptables -A INPUT -p tcp --dport 20 -j ACCEPT</pre>
#如果需要远程连接数据库，还需要开启3306端口，设置方法同上。
#禁止其他未允许的规则访问
<pre>iptables -A INPUT -j REJECT #（注意：如果22端口或者更已经更改的ssh端口未加入允许规，SSH链接会直接断开。）
iptables -A FORWARD -j REJECT</pre>
完成这步之后，发现无法ping了，还需要添加如下命令：
<pre>iptables -L -n --line-numbers</pre>
将INPUT里面的reject-with icmp-port-unreachable那一条删除
如果要删除的INPUT里的reject-with icmp-port-unreachable这条规则的序号为8，则执行：
<pre>iptables -D INPUT 8</pre>
4）查看已添加的iptables规则
<pre>iptables -L -n</pre>
5）iptables的开机启动及规则保存
<pre>chkconfig --level 345 iptables on</pre>
将其加入开机启动：
<pre>service iptables save</pre>
保存规则。

转自：http://www.dreamxyt.net/692.html