|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **版本** | **更改日期** | **要点说明** | **编制** | **审核** | **批准** |
| V1.0 | 2018-04-23 | 拟定数广侧Linux OS加固配置标准 | Cheungwu |  |  |
| 文档保密等级： | | □机密 ■内部 □公开 | | | |

# 定期升级内核

查看内核版本方法:[root@q1test01 ~]# cat /proc/version

当前最新稳定的Linux 内核版本是4.16.1;

禁止使用Linux kernel < 4.15的内核版本。原因是

1. Linux kernel 2.5.69 - Linux kernel 4.11：存在Phoenix Talon远程DOS和RCE漏洞。具体漏洞编号是：CVE-2017-8890、CVE-2017-9075、CVE-2017-9076、CVE-2017-9077
2. Linux kernel 2.6.22 - Linux kernel 4.8.3：存在脏牛本地提权漏洞。漏洞具体编号：CVE-2016-5195
3. Linux kernel < 4.15：存在Meltdown/Spectre CPU缓存泄露漏洞。漏洞具体编号：CVE-2017-5754、CVE-2017-5753、CVE-2017-5715

# 软件安全要求：

2.1 安装的软件必须是官网渠道下载，安装的版本必须是最新稳定版本；

2.2自启动服务：

开机自启动服务最多包括atd、bootlocal、crond、iptables、irqbalance、kdump、messagebus、netirqaffinity、network、nscd、rsyslog、sshd、udev-post，其中bootlocal为执行/etc/rc.d/boot.local脚本，该脚本启动的daemon进程最多包括洋葱Agent、网管Agent 和TscAgent。

设置方法：

[root@localhost ~]# chkconfig --list     显示开机可以自动启动的服务

[root@localhost ~]# chkconfig --add \*\*\* 添加开机自动启动\*\*\*服务

[root@localhost ~]# chkconfig --del \*\*\*   删除开机自动启动\*\*\*服务

/etc/rc.d/boot.local脚本启动的daemon进程最多包括洋葱Agent、网管Agent 和TscAgent

2.3 RPM软件安装包使用最新版本，并定期更新。

# 密码策略

1. 密码长度和期限：

编辑/etc/login.defs  指定如下参数的值。

PASS\_MAX\_DAYS   90

 PASS\_MIN\_DAYS   0

 PASS\_MIN\_LEN   8

 PASS\_WARN\_AGE   7

说明：用户密码长度大于8位，3个月过期，失效前7天提醒

2)设置账户锁定登陆失败锁定次数、锁定时间

编辑/etc/pam.d/system- auth

auth required pam\_tally.so onerr=fail deny=10 unlock\_time=600

说明：设置位密码连续10次锁定，锁定时间600秒

3)设置密码的复杂程度

编辑/etc/pam.d/system- auth

找到pam\_cracklib.so 在后面加一些参数，

如：password requisite pam\_cracklib.so minlen=8 ucredit=-1 lcredit=-1 dcredit=-1 ocredit=-1

说明：最少有1个大写字母，2个小写字符，5个数字， 1个符号

4)  用户第一次登录成功后强制修改密码：

强制账户帐号过期 chage -d 0 username

# 网络安全要求

* 1. Iptables默认策略设置drop.

4.2. 除必要的对外网开放的业务外，默认禁止外网访问本机，即iptables屏蔽eth0通讯。

查看iptables，输入命令 iptables –L，显示

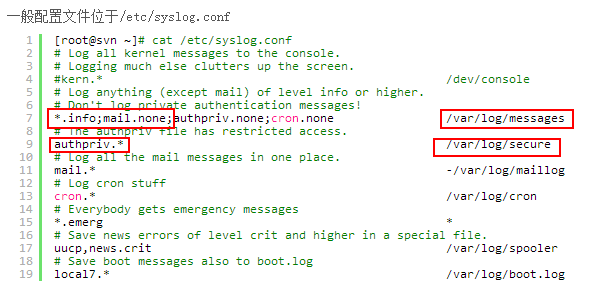
4.2.iptable设置入站方向，仅允许指定的业务端口被指定的来源IP访问。

# 日志审计要求

5.1 /var/log/secure记录用户验证、密码修改等相关信息。

5.2 /var/log/messages记录系统相关信息。

/var/log/secure 和/var/log/messages日志文件都是由syslog日志服务驱动。/etc/syslog.conf配置文件中, /var/log/secure 和/var/log/messages设置需符合以下



5.3 history 记录最少保存3000条，并输出操作时间。

# 编辑/etc/bashrc，添加以下内容



# 让系统记录每条历史命令的执行时间。注意最后的"号前面要放个空格



# 保存历史命令条数



# 执行下面的命令使配置立即生效



# 简明checklist

|  |  |  |  |
| --- | --- | --- | --- |
| 分类 | 检查点 | 检查方法 | 检查结果 |
| 定期升级内核 | 禁止使用Linux kernel < 4.15的版本 | 使用uname –a检查内核版本 |  |
| 软件安全要求 | 安装的软件必须是官网渠道下载 | 管理员自检安装的软件是否都来自官方渠道 |  |
| 删除无效的自启动服务 | chkconfig –list查看自启动服务 |  |
| 删除不用的自启动脚本 | 查看/etc/rc.d/boot.local配置文件 |  |
| 密码策略 | 设置密码长度和期限 | 设置/etc/login.defs配置  PASS\_MAX\_DAYS 90  PASS\_MIN\_DAYS 0  PASS\_MIN\_LEN 8  PASS\_WARN\_AGE 7 |  |
| 设置账户锁定登陆失败锁定次数、锁定时间 | 设置/etc/pam.d/system- auth配置  auth required pam\_tally.so onerr=fail deny=10 unlock\_time=600 |  |
| 设置密码的复杂程度 | 设置/etc/pam.d/system- auth配置  password requisite pam\_cracklib.so minlen=8 ucredit=-1 lcredit=-1 dcredit=-1 ocredit=-1 |  |
| 网络安全要求 | 仅允许指定的业务端口被指定的来源IP访问 | iptables –L检查配置 |  |
| **日志审计要求** | 记录认证等重要日志 | /etc/syslog.conf检查配置  \*.info;mail.none;authpriv.none;cron.none /var/log/message  authpriv.\* /var/log/secure |  |
| history 记录最少保存3000条 | /etc/bashrc检查  export HISTTIMEFORMAT=”%Y-$m-%d %H:%M:%S”  export HISTSIZE=3000 |  |