□□一、安装和升级

□□
使用custom自定义安装，不必要的软件包尽量不装，如有必要给lilo/grub引导器加入口令限制，安装完成后使用up2date或是apt(Debian)升级系统软件，有时升级内核也是必要的。

□□编辑 /etc/sudoers 添加下面内容 jinshuai ALL=NOPASSWD:ALL

□□二、帐号安全

□□
1、一般服务器都是放在IDC机房，需要通过远程访问进行管理，要限制root的远程访问，管理员通过普通帐号远程登录，然后su到root，开发人员只使用普通帐号权限。

□□1) 在/etc/default/login 文件，增加一行设置命令：CONSOLE = /dev/tty01

□□2)可以通过下面的脚本禁止对控制台的访问：# !/bin/sh cd /etc/pam.d for i in * do

□□sed '/[^#].*pam_console.so/s/^/#/' foo && mv foo $I done

□□3) 通过下面的措施可以防止任何人都可以su为root，在/etc/pam.d/su中添加如下两行。
auth sufficient /lib/security/$ISA/pam_rootok.so debug 网管网ofAdmin.Com auth required /lib/security/$ISA/pam_wheel.so group=wheel

□□然后把您想要执行su成为root的用户放入wheel组：usermod -G10 admin

□□
2、编辑/etc/securetty，注释掉所有允许root远程登录的控制台，然后禁止使用所有的控制台程序，其命令如下:

□□rm -f /etc/security/console.apps/servicename

□□
三、采用最少服务原则，凡是不需要的服务一律注释掉。在/etc/inetd.conf中不需要的服务前加"#"，较高版本中已经没有inetd，而换成了Xinetd;取消开机自动运行服务，把/etc/rc.d/rc3.d下不需要运行的肥务的第一个字母"S"改成"K",其他不变.

□□四、文件系统权限

□□1)
找出系统中所有含s"位的程序,把不必要的"s"位去掉,或者把根本不用的直接删除,这样可以防止用户滥用及提升权限的可能性,其命令如下:

□□find / -type f -perm -4000 -o -perm -2000 -print | xargs ls -lg

□□2) 把重要文件加上不可改变属性(一般情况不用这么做): chattr +i /etc/passwd

□□

Immutable，系统不允许对这个文件进行任何的修改。如果目录具有这个属性，那么任何的进程只能修改目录之下的文件，不允许建立和删除文件。

□□3) 找出系统中没有属主的文件: find / -nouser -o -nogroup

□□4) 找出任何都有写权限的文件和目录:

□□find / -type f -perm -2 -o -perm -20 |xagrs ls -lg find / -type d -perm -2 -o -perm -20 |xagrs ls -ldg

□□5)
ftp的上传目录不能给与执行权限,如提供可运行CGI的虚拟主机服务,应该做额外安全配置.
编/etc/security/limits.conf,加入或改变如下行: hard core 0 hard rss 5000 hard nproc 20

□□五.Banner伪装

□□1)
入侵者通常通过操作系统、服务及应用程序版本来攻击，漏油列表和攻击程也是按此来分类，所以我们有必要作点手脚来加大入侵的难度。

□□所以编辑/etc/rc.d/rc.local如下:

□□echo "Kernel $(uname -r) on $a $(uname -m)" >/etc/issue echo "Kernel \r on an \m" >> /etc/issue cp -f /etc/issue /etc/issue.net echo >> /etc/issue

□□2)
对于Apache的配置文件，找到ServerTokens和ServerSignature两个directive，修改其默认属性如下，使用不回显版本号: ServerTokens prod ServerSignature Off

□□六、IPTABLES防火墙规则:

□□iptables -A INPUT -p --dport 22 -j ACCEPT

□□iptables -A INPUT -i eth0 -p tcp --dport 80 -j ACCEPT

□□iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT iptables -A INPUT -j DROP

□□
以上规则将阻止由内而外的TCP主动选接。上面是一个简单例子，IPTABLES功能十分强大，可以根据具体情况设置防火墙规则。

□□
七、tripwire是一个比较有名的工具，它能帮你判断出一些重要系统文件是否被修改过。现在

的Linux发行版中一般部带有该工具的开源版本，在默认的校验对象配置文件中加入一些敏感文件就可以使用。

□□八.自行扫描

□□普通的安全加固基本上是做完了，我们可以自己做一个风险评估，推荐使用nessus latest version.

□□九.日志策略

□□
主要就是创建对人侵相关的重要日志的硬拷贝，不致于应急响应的时候连最后的黑匣子都没有。可以把它们重定向到打印机，管理员邮件，独立的日志服务器及其热备份。
十.Snort入侵检测系统

□□
对人侵响应和安全日志要求较高的系统有此必要;对于一般的系统而言，如果管理员根本不会去看一大堆日志，那么它白白占用系统资源，就如同鸡肋一样。
对Linux平台下病毒的防范总结出以下几条建议，仅供参考:

□□(1)做好系统加固工作。

□□(2)留心安全公告，及时修正漏洞。

□□(3)日常操作不要使用root权限进行。

□□(4)不要随便安装来历不明的各种设备驱动程序。

□□(5)不要在重要的服务器上运行一些来历不明的可执行程序或脚本。

□□(6)尽量安装防毒软件，并定期升级病毒代码库。

□□(7)对于连接到Internet的Linux服务器，要定期检测Linux病毒、蠕虫和木马是否存在。

□□
(8)对于提供文件服务的Linux服务器，最好部署一款可以同时查杀Windows和Linux病毒的软件。

□□(9)对于提供邮件服务的Linux服务器，最好配合使用一个E-mail病毒扫描器。
网管网ofAdmin.Com

□□
总而言之，对于Linux平台下病毒的防范要采取多种手段，决不可因为现在Linux病毒很少就掉以轻心

□□一、安装和升级

□□

使用custom自定义安装，不必要的软件包尽量不装，如有必要给lilo/grub引导器加入口令限制，安装完成后使用update、yum或是apt可以通过下面的脚本禁止对控制台的 # !/bin/sh cd /etc/pam.d for i in; do

□□sed ‘/[^#].pam_console.so/s/^/#/‘ foo mv foo $I done

□□3) 通过下面的措施可以防止任何人都可以su为root，在/etc/pam.d/su中添加如下两行。auth sufficient /lib/security/$ISA/pam_rootok.so debug

□□auth required /lib/security/$ISA/pam_wheel.so group=wheel

□□然后把您想要执行su成为root的用户放入wheel组:

□□usermod -G10 admin

□□

2、编辑/etc/securetty，注释掉所有答应root远程登录的控制台，然后禁止使用所有的控制台程序，其命令如下:

□□rm -f /etc/security/console.apps/servicename

□□

三、采用最少服务原则，凡是不需要的服务一律注释掉。在/etc/inetd.conf中不需要的服务前加"#"，较高版本中已经没有inetd，而换成了Xinetd;取消开机自动运行服务，把/etc/rc.d/rc3.d下不需要运行的服务的第一个字母"S"改成"K"，其他不变.

□□四、文件系统权限

□□1)

找出系统中所有含s"位的程序，把不必要的"s"位去掉，或者把根本不用的直接删除，这样可以防止用户滥用及提升权限的可能性，其命令如下: find / -type f -perm -4000 -o -perm -2000 -print xargs ls -lg

□□2) 把重要文件加上不可改变属性: chattr +i /etc/passwd

□□

Immutable，系统不答应对这个文件进行任何的修改。假如目录具有这个属性，那么任何的进程只能修改目录之下的文件，不答应建立和删除文件。

□□3) 找出系统中没有属主的文件: find / -nouser -o -nogroup

□□4) 找出任何都有写权限的文件和目录: find / -type f -perm -2 -o -perm -20 xagrs ls -lg

□□find / -type d -perm -2 -o -perm -20 xagrs ls -ldg

□□5)
ftp的上传目录不能给与执行权限，如提供可运行CGI的虚拟主机服务，应该做额外安全配置.编/etc/security/limits.conf，加入或改变如下行: hard core 0 hard rss 5000 hard nproc 20

□□五、Banner伪装

□□1)
入侵者通常通过操作系统、服务及应用程序版本来攻击，漏油列表和攻击程也是按此来分类，所以我们有必要作点手脚来加大入侵的难度。所以编辑/etc/rc.d/rc.local如下：echo "Kernel $ on $a $" /etc/issue echo "Kernel “r on an “m" /etc/issue cp -f /etc/issue /etc/issue.net echo /etc/issue

□□2)
对于Apache的配置文件，找到ServerTokens和ServerSignature两个directive，修改其默认属性如下，使用不回显版本号：

□□ServerTokens prod

□□ServerSignature Off

□□六、IPTABLES防火墙规则：

□□iptables -A INPUT -p --dport 22 -j ACCEPT

□□iptables -A INPUT -i eth0 -p tcp --dport 80 -j ACCEPT

□□iptables -A INPUT -m state --state ESTABLISHED，RELATED -j ACCEPT iptables -A INPUT -j DROP

□□
以上规则将阻止由内而外的TCP主动选接。上面是一个简单例子，IPTABLES功能十分强大，可以根据具体情况设置防火墙规则。

□□
七、tripwire是一个比较有名的工具，它能帮你判定出一些重要系统文件是否被修改过。现在的Linux发行版中一般部带有该工具的开源版本，在默认的校验对象配置文件中加入一些敏感文件就可以使用。

□□八、自行扫描

□□普通的安全加固基本上是做完了，我们可以自己做一个风险评估，推荐使用nessus latest version.

□□九、日志策略

□□
主要就是创建对人侵相关的重要日志的硬拷贝，不致于应急响应的时候连最后的黑匣子都没有。可以把它们重定向到打印机，治理员邮件，独立的日志服务器及其热备份。

□□十、Snort入侵检测系统

□□
对人侵响应和安全日志要求较高的系统有此必要;对于一般的系统而言，假如治理员根本不会去看一大堆日志，那么它白白占用系统资源，就如同鸡肋一样。
对Linux平台下病毒的防范总结出以下几条建议，仅供参考：做好系统加固工作。

□□留心安全公告，及时修正漏洞。日常操作不要使用root权限进行。

□□不要随便安装来历不明的各种设备驱动程序。

□□不要在重要的服务器上运行一些来历不明的可执行程序或脚本。
尽量安装防毒软件，并定期升级病毒代码库。

□□对于连接到Internet的Linux服务器，要定期检测Linux病毒、蠕虫和木马是否存在。

□□
对于提供文件服务的Linux服务器，最好部署一款可以同时查杀Windows和Linux病毒的软件。

□□对于提供邮件服务的Linux服务器，最好配合使用一个E-mail病毒扫描器。

□□
总而言之，对于Linux平台下病毒的防范要采取多种手段，决不可因为现在Linux病毒很少就掉以轻心。