如何来量身定制安全的Linux系统服务平台 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/252/2021_2022__E5_A6_82_E4_BD_95_E6_9D_A5_E9_c103_252997.htm 如何保证安全的最大化呢？量体裁衣，有的放矢，取舍得当是关键。现从以下几个方面加以详述。 控制文件的属性和权限 密切关注文件的属性和权限设置是保证主机文件系统完整性的至关紧要的操作。 两种特殊的文件访问权限分别是SUID(八进制为4000)和SGID（八进制为2000）。设置这两种权限的文件，将使其它用户在执行它们时拥有所有者的权限。也就是说，如果一个设置为SUID的程序，即使是普通用户使用也是作为root来运行的。因此，SUID/SGID文件是安全的隐患。 SUID和SGID攻击方式的预防： 1．严格审查系统内的文件权限。可以找出系统内使用SUID/SGID的文件，列出清单保存，做到心中有数。命令如下： [root#] find / -type f -perm 6000 -ls | less [root#] find / -type f -perm 6000 > Suid-Sgid.txt 2．对于一部分程序必须设置为SUID的，可以让它们自成一组，集中管理。但是绝对不允许在用户的家目录下有SUID程序存在。 3．确保重要的SUID脚本不可写。命令如下： [root#] find / -perm -2 ! -type l -ls 4．对于并非绝对需要被设置成SUID的程序，改变它们的访问权限或者卸载程序。如： [root#] chmod -s [program] 5．查找系统内所有不属于任何用户和组的文件。因为这些文件很容易被利用来获得入侵主机的权限，造成潜在的威胁。命令如下： [root#] find / -nouser -o -nogroup 6．善于使用lsattr和chattr这两个ext2/3的属性命令。本文将主要讨论a属性和i属性，因为这两个属性对于提高文件系统的安全性和保障文件

系统的完整性有很大的好处。a属性（Append-only），系统只允许在这个文件之后追加数据，不允许任何进程覆盖或截断这个文件。如果目录具有这个属性，系统将只允许在这个目录下建立和修改文件，而不允许删除任何文件。i属性（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，那么任何进程只能修改目录之下的文件，不允许建立和删除文件。 如果主机直接暴露在因特网或者位于其它危险（如其它非管理员亦可接触服务器）环境，有很多Shell账户或提供HTTP和FTP等网络服务，一般应该在安装配置完成后使用如下命令，便于保护这些重要目录：[root#] chattr -R i /bin /boot /etc /lib /sbin [root#] chattr -R i /usr/bin /usr/include /usr/lib /usr/sbin [root#] chattr a /var/log/messages /var/log/secure..... 如果很少对账户进行添加、变更或删除操作，把/home本身设置为Immutable属性也不会造成什么问题。 在很多情况下，整个/usr目录树也应该具有不可改变属性。实际上，除了对/usr目录使用chattr -R i /usr/命令外，还可以在/etc/fstab文件中使用ro选项，使/usr目录所在的分区以只读的方式加载。 另外，把系统日志文件设置为只能添加属性(Append-only)，将使入侵者无法擦除自己的踪迹，以便于执法人员取证、分析。 文件系统的完整性检查 完整性是安全系统的核心属性。管理员需要知道是否有文件被恶意改动过。攻击者可以用很多方法破坏文件系统，例如，可以利用错误配置获得权限，也可以修改文件植入特洛伊木马和病毒。Linux中常用如下工具进行校验检查。 1．md5sum md5sum 命令可以用来创建长度为128位的文件指纹信息。通过md5sum -c命令可以反向检查文件是否被修改过。黑客进入

到系统后，会用修改后的文件来取代系统上某些特定的文件，如netstat命令等。于是当使用 netstat -a命令查看系统状态时，不会显示系统攻击者存在的信息。攻击者还可能会替代所有可能泄露其存在的文件，一般来说包括：/bin/ps、/bin/netstat、/bin/login、/bin/ls、 /usr/bin/top、/usr/bin/passwd、/usr/bin/top、 /sbin/portmap、/etc/xinetd.conf、/etc/services。 这些文件都是替代的对象。由于这些文件已经被取代，那么简单地利用ls命令是查看不出这些文件有什么破绽的。因此你需要用md5sum工具在系统安装前期为这些文件做好指纹认证并保存，以备日后检测所用。 2．RPM安装包 如果使用的是基于RPM的安装包（Red Hat公司开发并包含在其Linux产品之中的多功能软件安装管理器，现有多种版本的Linux使用此管理器，如Red Hat、TurboLinux），它可以用来建立、安装、查询、检验、升级和卸载独立的软件包。一个完整的RPM包包括压缩文件和包信息。当使用RPM安装软件时，RPM为每个被安装的文件向数据库中添加信息，包括MD5校验和、文件大小、文件类型、拥有者、组和权限模式。当RPM以-verify标志运行时，将把初始文件的值与当前安装的文件进行比较并报告差异。例如，下面是对一个被黑站点的运行结果：# rpm -qf /bin/ps（或# rpm -qf /usr/bin/top 查看命令隶属哪个RPM包） procps.2.0.2-2 # rpm -V procps（-V MD5检验） SM5..UGT /bin/ps SM5..UGT /usr/bin/top（有消息表示此文件已被修改） 由上可以看出，攻击者已经入侵到系统中，并且用自己的ps及top命令替代了原来系统中的命令，从而使管理员看不到其运行的进程。RPM的使用方法很多，具体操作方法参见man rpm文档。 3

. Tripwire Tripwire是一个用来检测整个系统是否存在恶意代码和检验文件完整性的有用工具。它采用MD5算法生成128位的“ 指纹 ”，通过命令自动保存系统快照，再产生相应的MD5数值以供日后比较判断。 使用Tripwire可以定义哪些文件/目录需要被检验。一般默认设置能满足大多数的要求。该工具运行在四种模式下：数据库生成模式、数据库更新模式、文件完整性检查模式、互动式数据库更新模式。当初始化数据库生成的时候，它生成对现有文件各种信息的数据库文件。为预防以后系统文件或者配置文件被意外地改变、替换或删除，它将每天基于原始数据库对现有文件进行比较，以发现哪些文件被更改、是否有系统入侵等意外事件发生。当然，如果系统中的配置文件或程序被更改，则需要再次生成数据库文件，保持最新的系统快照。此软件功能强大，使用方便。具体的安装和使用，可以通过Google搜索获得。