Linux安全:三个细节体现Unix系统安全性Linux认证考试 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/555/2021_2022_Linux_E5_AE_89_E5_85_c103_555830.htm Unix操作系统的安全性是众所周知的。但是如果要你说出Unix系统到底安全在哪里，估计也没有人能够说出一个所以然来。笔者也一下子不能够把Unix系统的安全特性向大家娓娓道来。笔者这里仅仅举Unix系统安装设计方面的三个小细节。估计从这个三个小细节中，大家看到Unix工程师在系统安全性与便利性方面所做的努力。一、同一个命令不同用户不同的权限。 Date命令是Unix系统的一个常用命令，其显示了系统的日期与时间。但是不同的用户角色其具有不同的功能。如是系统管理员用户，则可以通过这个命令来更改系统时间。但是如果执行这个命令的用户是系统普通用户，那么这个命令则只能够显示时间，而无法更改时间。也就是说，默认情况下，只有系统管理员才可以更改系统时间，但是修改时间与查看时间用的是同一个命令。系统会自动去判断当前用户是否有修改时间的权利。 这就是Unix系统中一个很有用的安全特性。一方面类似的功能采用同一个命令，方便了系统管理员的操作与维护.另一方面系统会自动对命令的权限进行审查，以保障用户只能够利用命令进行与自己权限相符合的操作。从这里可以看出，Unix系统不仅在安全上有保障，其更加看重与安全和便利的一种结合。不会为了安全，而牺牲管理维护的便利性。 大家都知道，随意更改系统的日期可能会给系统造成很大的负面影响，会使得一些作业计划混乱。如系统当前可能有多个进程在后台运行，此时系统会根据进程的优先性、管理员定义的作

业计划等等安排好了这些命令进程执行的时间进度表，规定在某个特定的时刻启动这些作业或者进程。此时如果允许一个非管理员员用户随意更改系统时间，则系统中的作业可能会乱了套。如系统管理员为了系统的安全，设置了每天中午12点30分对系统中的重要文件进行备份。如果在中午 12点的时候普通用户修改了时间，把时间从12点改为了1点。那么此时系统就不会对系统重要文件进行备份。若不幸的是，在第二天上午由于一些意外导致系统硬盘损坏或者其他系统故障，那么由于前一天没有正常备份，则损坏的文件将无法修复。可以随意更改系统时间会导致很多难以预料的结果。 所以从这个date命令中就可以看出，Unix系统在安全设计上确实比其他操作系统略高一筹。同一个命令不同帐户具有不同的操作功能，这让Unix系统在安全与便利上达到了同一。 二、不提示具体的出错信息。 Unix系统跟其他操作系统一样，也是通过账户名与密码来保证操作系统的基本安全性。但是，笔者认为Unix在这方面可能考虑的更全面一点。 Unix系统是一个多用户操作系统。通常情况下，Unix系统只允许拥有帐号和密码的用户登录。用户的帐号列表往往有系统管理员来进行维护。系统管理员授予用户使用计算机的权限，并为其计统帐号、口令等信息。当系统出现提示信息要求用户登录时，用户只能够输入系统管理员所提供的正确用户名与密码之后才能够登陆到操作系统。如当系统出现了logon提示符之后，就表示该系统终端允许某个用户通过帐号与密码进行登录。在输入账户名之后，按下回车键之后，就需要输入密码。系统会要求用户输入准确的密码来进行身份验证。万一用户输入密码错误后(用户名准确)，此时系统只会含糊的提示

“ login incorrect ” (登陆不准确)。而不会提示用户到底错在哪里，是错在密码错误又或者是用户名输入错误。 这个含糊的提示，将会给非法攻击者造成一定的障碍。由于非法攻击者不知道到底是密码错误又或者是账户名错误，这会增加对方攻击的成本。或者说，这个提示对于攻击者来说，或多或少有一些欺骗性。但是，这个措施却可以很明显的提高系统的安全性。或许有些员工会抱怨这么设计友好性太差。不仅会欺骗攻击者，而且也会欺骗普通的用户。不过从安全性来说，这个安全措施仍然是必要的。 另外值得一提的是，在用户登录时，Unix系统还跟其他操作系统一样，提供了一种更高级别的安全措施。即当用户登录到Unix系统时，根据系统安全策略，可以让用户强制更改管理员所赋予的口令。此时用户最好能够立即更改默认口令，设置一个只有自己知道的口令(连管理员可能都不知道)。毕竟账户名或者口令若太多人知道的话，会给操作系统带来一定的安全隐患。 当Unix系统在登陆时如果用户名或者密码验证错误，系统不会提供详细的出错信息，从而不让非法攻击者找到出错的原因，增加其攻击的难度。其实这些类似的安全措施，在Unix系统中是比比皆是。在后续的文章中，笔者可能还会多次谈到这个安全特性。从这个小小的安全设计中，就可以看出Unix操作系统的安全确实不是吹的。 三、输出中不带有相应的表头。 利用命令who可以显示当前登陆用户的详细信息，如用户名、登陆的途径、登陆时间等内容。在Linux系统中也有类似的功能。不过两个系统有差异。 在Unix系统中如果执行了who命令之后，会以如下类似的格式显示。 $who Oracle console May 10 12:05(:0) Oracle pts/1 May 10 12:15(:0:0) 这个结果表示当前系统

的登陆者有两个，都为Oracle(操作系统允许同一个账户通过不同的渠道登陆到操作系统，这也是Unix系统的一个特性。在Linux操作系统中也可以实线类似的功能，但是在微软操作系统中好像不行。)后面会显示用户登录的途径、登陆系统的时间等等。但是让很多Unix系统的初学者感到困扰的就是，在输出结果中竟然没有一个相应的表头来说明各个列的含义。这一点可能让人看起来觉得Unix操作系统不怎么友好，但是却可以保障Unix系统的安全性。如一些Unix系统的高级安全策略都是基于这个特性所实现的。 另外，由于这个用户信息具有非常重要的价值，故对此进行一些安全的防护就具有更大的现实意义。如系统管理员可以从who命令的输出结果中抽取一部分数据供下一个命令使用。如笔者笔者经常利用这个内容给系统当前登陆的用户发送邮件。为此笔者设计了一个小程序，在每个星期五的时候(利用date命令从输出结果中抽取每个星期五的日期)向系统当前登陆的账户(利用who命令抽取其中的user-id一列的数值)，然后通过mailx命令可以给当前所有已登陆的账户发送邮件。系统工程师可以通过一些简单的命令实现类似负责的维护功能，这也是Unix系统跟其他操作系统的优势所在。 除了发送邮件，系统工程师还可以利用这个who命令显示的结果实现其他一些功能，如发送信息给当前登陆用户要求起保存当前作业并注销操作系统、甚至强制断开用户与本机的连接等等。故如果不对who的结果信息作一定程度的保护的话，那么就将给Unix系统带来很大的安全威胁。 其实除了who命令之外，Unix系统类似的情况还有很多。正是这一个个的细节考虑，才保障了整个Unix系统的安全。从这一方面来说，Unix系统有时候即使牺牲了界

面的友好性，来实现系统的安全性，也是可以接受的。 更多优质资料尽在百考试题论坛 百考试题在线题库 linux认证更多详细资料 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com