用PAM认证加强Linux服务器安全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_ti2020/644/2021_2022__E7_94_A8PAM_E8_AE_A4_E8_c103_644816.htm PAM(Pluggable Authentication Modules)即可插拔式认证模块，它是一种高效而且灵活便利的用户级别的认证方式，它也是当前Linux服务器普遍使用的认证方式。当然，在不同版本的Linux统中部署PAM认证是有所不同的，本文将以RHEL4版本为例进行解析。 1.部署PAM认证的必要性 我们知道一台Linux服务器会开许多不同的服务，这些服务中很多服务本身并没有认证功能，只是把认证交给用户名及密码。如果这样的话，那么所有服务都用Linux系统的用户名及密码来认证，对于服务器来说是很危险的。比如一台服务器开着FTP、SMTP、SSH等服务，那么新建一个用户默认就享有对以上的服务的操作权限，那么如果一个用户的帐号密码泄露会涉及到多个服务。因此，不管是PC还是服务器在类Linux系统中部署PAM认证是非常必要的。通过新型的认证模块PAM就能解决认证方面的不足，加强Linux系统安全。 2.PAM认证的方式 PAM认证一般遵循这样的顺序：Service(服务)→PAM(配置文件)→pam_*.so。PAM认证首先要确定那一项服务，然后加载相应的PAM的配置文件(位于/etc/pam.d下)，最后调用认证文件(位于/lib/security下)进行安全认证。通常情况下，在Linux系统安装完成后会在/etc/pam.d路径下为我们提供了一些默认的配置文件。另外，大家要知道/lib /security目录是认证文件的默认存放位置。/etc/pam.d路径下的默认配置文件是我们进行PAM配置的模板，通常情况下我们根据安全需要对于进行修改或

者添加相应的项即可。 3.PAM认证的构成 客观地说PAM认证还是比较复杂的，简单地讲它包括四种常见认证类型(module type)：即auth认证管理、account用户管理、password密码认证管理、session会话管理。以/etc/pam.d/login 为例，我们可以看到它的配置文件，区域1中的auth、account、password、session等都是认证类型。区域2中的required、 requisite、sufficient 、optional是认证的流程控制。最后面的区域3就是认证的PAM文件了。来源：考试大的美女编辑们 4.PAM认证的流程 为了便于大家深入了解PAM认证的流程，我们以验证用户登录的PAM-login为例进行说明。PAM认证流程是从行首验证到行尾，逐条认证。比如用户登录服务器，共有十条auth类型认证，假设第一条认证失败，一般情况后九条也必须要认证。为什么就一般情况呢?其实还有非一般情况。那么这个用户动作成功与否是要看auth认证后面的区域2是怎么处理的。看到处理字段有required和optional，其中required代表认证必须通过，也就是说，无论成功多少条语句，只要失败一条，那么认证就失败。看到的区域3就是认证的模块了，第二行中的“ pam_securetty.so ”就是这个文件。在RHEL中，认证多是用相对路径。来源：考试大 5.PAM认证测试 pam_securetty.so是一个认证模块文件，该认证模块只对root用户有效，当root登录系统时，会查看有没有安全终端，安全终端就是 /etc/securetty文件里的东西，比如你运行“ W ”命令看到TTY下面的东西就是安全终端。如果有安全终端就通过认证，否则失败。有些管理员为了安全，不让root用户直接登录，他会把/etc/securetty文件清代空，这就保证了在有root密码时，也不能够在本地登录。 为了以下的实验方便，能看

出效果来，我们把“ auth required pam_securetty.so ”这条认证加入SSH服务的PAM模块谁文件里(/etc/pam.d/sshd)的第一行，目的就是让SSH服务应用这条认证。大家可在控制台窗口中执行“ vi etc/pam.d/sshd ”然后添加这条认证语句。同样的道理，如果把这条语句加到login文件(默认这条认证是被注销掉的，我们取消前面的#就可以了)，控制的是从本地控制台登录，同样的话如果把这条语句加入到sshd文件内，那么它将控制的是从远程登录服务器22端口的过程。来源：考试大的美女编辑们 下面我们试着SSH登录系统看看效果，在控制台中执行命令“ ssh -l root localhost ”，可以看到无论我们的root用户的密码正确与否都无法通过SSH远程登录到系统，可见上面的认证已经生效。在一般情况下，为了服务器的安全，大家通过PAM认证拒绝root远程登录系统。 6.PAM认证的处理方式 了解了认证类型的工作方式，我们还应该深入的理解认证的处理方式，它的认证处理方式是required，表示这一模块的认证是必须成功的，但如果失败，认证过程不会即刻终止，PAM将继续下一个同类型认证。上面“ pam_securetty.so ”认证失败了，但认证并没有结束，认证的“ 指针 ”还在向下走。在root用户SSH登录认证失败的前提下还提示用户输入密码，虽然认证不可能成功。来源：www.100test.com 处理过程中除了required，还有requisite、sufficient和optional，我们再来看看requisite的效果。还用SSH 服务为例，把/etc/pam.d/sshd文件第一行中的“ auth required pam_securetty.so ”改成“ auth requisite pam_securetty.so ”。再次尝试登录，也是输入3次密码后被拒绝了。但是细心的读者如果一边看文章一边尝试着实验的话，你会发现当你

在输入密码时，用required反应的速度要慢一些，并且在系统日志中是没有记录的，认证同样是失败的。这说明required和requisite类似的地方是认证必须通过，而不同的是如果失败，认证过程将立即终止，不会去认证下面的条目。 7.限制root登录控制台 我们修改用/etc/pam.d/login来限制root登录控制台，打开login文件删除第二行中的#，取消对“ auth required pam_securetty.so ”的注销。然后我们本地登录服务器，通过测试我们发现当用required时，你在输入root及密码后，你得到了一个拒绝信息，用requisite时，当你输入root回车时同样会得到拒绝信息登录失败，这是由刚才的认证方式触发的。来源：www.examda.com 8.PAM认证可选模块 在PAM认证中，sufficient表示如果认证成功，那么对这一类型的模块认证是充足的了，其他的同类模块将不会再检验，当认证失败，它会进行下一条认证，如果下面同类型的认证成功，结果依然成功。optional表示这一模块认证是可选的，也不会对认证成功或失败产生影响，这个就比较危险了。比如我们在/etc/pam.d/sshd文件内加入“ auth required/lib/security/pam_listfile.so item=user sense=allow file=/etc/sshusers onerr=succeed ”其含义是只允许出现在/etc/sshuser文件内的用户远程登录。然后我们执行命令“ ssh -l root localhost ”，当sshusers文件没有root用户时候，登录失败，很明显他被PAM模块拒绝了。那么我们改一下认证文件，将 required改成sufficient，尝试再次登录，结果成功登录。 总结：PAM认证是Linux服务器系统最主要的安全认证模式，掌握PAM认证对于加强系统安全非常重要。本文结合理论与实践对PAM认证做了一定的分析，实际上关于PAM认证

是一个大课题，希望以后有机会和大家进一步分享基于PAM认证的Linux系统安全技巧和经验。 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