Linux服务器策略Web站点的安全八要素 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/237/2021_2022_Linux_E6_9C_8D_E5_8A_c103_237551.htm 在政府和企业上网中，建立一个Web网站是不可缺少的重要内容之一，但是，通常他们面临着比其他网站更多的威胁，因此，建立一个安全的信息发布平台是至关重要的。这就要求这些用户必须对Web服务器的安全性有全面的认识。上海广电应确信有限公司(SVA Networks)全面分析了网络安全的各个方面，提出“ 内外兼修 ”的安全信息发布平台。从信息发布平台内部来看，应该做到： 1、增强服务器操作系统的安全，密切关注并及时安装系统及软件的最新补丁.建立良好的账号管理制度，使用足够安全的口令，并正确设置用户访问权限。 2、恰当地配置Web服务器，只保留必要的服务，删除和关闭无用的或不必要的服务。因为，启动不必要的服务可能使他人获得你的系统信息，甚至获取密码文件。 3、对服务器进行远程管理时，使用如SSL等安全协议，避免使用Telnet、FTP等程序，因为这些程序是以明文形式传输密码的，容易被监听.并严格控制远程root身份的使用，仅在绝对需要时，才允许使用具有高授权的操作。 4、禁止或限制cgi程序和asp、php脚本程序的使用。因为，这些程序会带来系统的安全隐患，而且，某些脚本程序本身就存在安全漏洞。 同时构建一个安全的服务器外部环境： 1、使用防火墙及壁垒主机，对数据包进行过滤，禁止某些地址对服务器的某些服务的访问，并在外部网络和Web服务器中建立双层防护。利用防火墙，将服务器中没有必要从防火墙外面访问的服务及端口阻隔，进一步增强开

放的服务的安全性。 2、使用入侵检测系统，监视系统、事件、安全记录和系统日志，以及网络中的数据包，对危险和恶意访问进行阻断、报警等响应。 3、使用漏洞扫描和安全评估软件，对整个网络进行全面的扫描、分析和评估，从用户账号约束、口令系统、访问控制、系统监测、数据完整、数据加密等多方面进行安全分析和审计。建立和提高用户的安全策略，及时发现并弥补安全漏洞。 4、在网关和服务器上使用多层次的防 病毒系统，尤其对于允许上传和交互信息发布的服务器来说，防止病毒及木马程序的侵入是保证服务器系统安全的一个关键。 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