网络服务器的通用及专用的保护方法 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/287/2021_2022__E7_BD_91_E7_BB_9C_E6_9C_8D_E5_c101_287457.htm 针对黑客威胁，网络安全管理员采取各种手段增强服务器的安全，确保WWW服务的正常运行。象在Internet上的Email、ftp等服务器一样，可以用如下的方法来对WWW服务器进行保护： 安全配置 关闭不必要的服务，最好是只提供WWW服务，安装操作系统的最新补丁，将WWW服务升级到最新版本并安装所有补丁，对根据WWW服务提供者的安全建议进行配置等，这些措施将极大提供WWW服务器本身的安全。 防火墙 安装必要的防火墙，阻止各种扫描工具的试探和信息收集，甚至可以根据一些安全报告来阻止来自某些特定IP地址范围的机器连接，给WWW服务器增加一个防护层，同时需要对防火墙内的网络环境进行调整，消除内部网络的安全隐患。 漏洞扫描 使用商用或免费的漏洞扫描和风险评估工具定期对服务器进行扫描，来发现潜在的安全问题，并确保由于升级或修改配置等正常的维护工作不会带来安全问题。 入侵检测系统 利用入侵检测系统（IDS）的实时监控能力，发现正在进行的攻击行为及攻击前的试探行为，记录黑客的来源及攻击步骤和方法。 这些安全措施都将极大提供WWW服务器的安全，减少被攻击的可能性。 二：网站的专用保护方法 尽管采用的各种安全措施能防止很多黑客的攻击，然而由于各种操作系统和服务器软件漏洞的不断发现，攻击方法层出不穷，技术高明的黑客还是能突破层层保护，获得系统的控制权限，从而达到破坏主页的目的。这种情况下，一些网络安全公司推出了专

门针对网站的保护软件，只保护网站最重要的内容--网页。一旦检测到被保护的文件发生了{非正常的}改变，就进行恢复。一般情况下，系统首先需要对正常的页面文件进行备份，然后启动检测机制，检查文件是否被修改，如果被修改就需要进行恢复。我们对以下几个方面的技术进行分析比较：监测方式 本地和远程：检测可以是在本地运行一个监测端，也可以在网络上的另一台主机。如果是本地的话，监测端进程需要足够的权限读取被保护目录或文件。监测端如果在远端的话，WWW服务器需要开放一些服务并给监测端相应的权限，较常见的方式是直接利用服务器的开放的WWW服务，使用HTTP协议来监测被保护的文件和目录。也可利用其它常用协议来检测保护文件和目录，如FTP等。采用本地方式检测的优点是效率高，而远程方式则具有平台无关性，但会增加网络流量等负担。 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