针对Linux系统主机谈--防范黑客经验 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/145/2021_2022__E9_92_88_E5_AF_B9Linu_c103_145218.htm 文章主要是针对LINUX主机谈的。 一、堡垒往往是从内部被攻破的，小心你身边的人。 经验表明，绝大多数的网络攻击，来自同事、网友和主机用户。这些人能直接或者间接地进入你的主机系统，甚至有可能知道你的密码。小小的疏漏，都会造成致命的错误。我曾经给我同事演示盗取他论坛密码，方法很简单，INCLUDE，然后ECHO，变量值就显示出来了，变量值里就存有密码，只有几行代码。我告诉他把密码直接写到论坛源码里去，这样就没事了。换个角度，你不是网管，只是主机上的用户，网管一个小小的失误，很可能会毁掉你的网站。 二、经常翻看服务器日志。 日志里有各种访问信息，通过分析日志文件，你很容易发现试图进入你管理后台或者试图探测主机的人。11月初的时候，以为学校的小路由器总断线，我改用服务器代理上网，用的是红帽子9。服务器运行不到一个月，我翻看了一下日志，发现至少有五个国家和地区的IP试图探测我的系统，有美国、韩国、日本、台湾、印度。于是我做了IPTABLES，对那几个IP网段做了屏蔽，倒是安静了一些日子，服务器上只产生了很少的日志信息。后来我发现，试图探测系统的IP有不少是国内的，屏蔽IP显然不是什么好办法，好好做做IPTABLES比什么都强。举个例子，我服务器上的SSH和WEBMIN服务限定为只有葫芦岛铁通的IP才可以访问，这样很容易查到试图入侵系统的黑客。说到翻看日志，我居然发现有网络监控部门的访问记录，劝大家以后开网站

小心点，别以为别人不知道你做了啥~ 三、别相信法律武器 如果你是政府网站的网管，你大可不必担心别人黑你，一般人他不敢。多数情况下，别人黑了你，你都没有办法。就算你有足够证据，也未必会得到法律的有效保护，更何况你的网站没有注册登记，被人黑了也就黑了，真是没处告去。所以安全防护还要靠你自己。 四、我的网站安全策略。 现在大部分的网站，尤其是单位和个人网站，都是用CMS做的。CMS一般都有漏洞，包括论坛在内，这是不可避免的，脚本对数据过滤不严就会产生SQL注入漏洞，你的数据库内容很可能被篡改。我是这么做的。 1、禁止FTP登陆主机。 这么做很不方便，因为FTP空间经常使用。 2、把CMS源码文件OWNER设成ROOT，其实很简单，登陆超级用户后，拷贝一下目录就可以了。 3、改源码。因为CMS不会反复打开后台数据库，打开数据库的指令通常只有几条（多数时候是两条，前台源码里一条，后台源码里一条），过滤一下，很容易找到相应的脚本行。 4、ZEND优化。ZEND优化类似编译，实际上它还有源码加密的功效，这样隐藏在源码里的数据库密码就不会露出来了。 5、双用户。一个数据库用两个用户名打开。MYSQL的权限管理可以到字段。添在你源码里的打开数据库的那个用户，权限尽可能降低，而另一个管理用的用户名，则拥有对数据库的全部权限。权限设好了，就算把管理密码贴到大街上，别人也奈何不了你。 6、该数据库原始文件权限，SU后拷贝一下目录，这样即使是数据库管理员，也黑不了你的网站~一般来说是不用这么做的。 7、物理上的安全措施。媒体资料、数据库、网站前台、后台分别放在不同服务器上。这么做有点BT了，不过安全没的说，除非

关键系统，否则没必要搞这么严格。什么是关键系统呢？不只是国防、经济建设、金融等等系统才是重要系统，有一定规模的网站都属于关键系统，安全漏洞可能使数年心血毁于一旦。