FreeBSD下构建安全的Web服务器 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/240/2021_2022_FreeBSD_E4_B8_8B_c103_240645.htm 序言 在我们跑Web服务器的时候，大家可能都会一致认为使用Linux＋Mysql＋Apache＋PHP整个开源的系统是比较好的选择，但是我个人认为这是不合理的，首先要根据你的应用来觉得你使用什么服务。假如你需要跑Oracle等大型应用的话，而且Oracle在Linux下是支持的比较好的，那么使用Linux是个好的选择，因为在FreeBSD下安装Oracle是个非常麻烦的事情。那么如果是跑普通的网站应用的话，我觉得使用FreeBSD＋ Mysql＋Apache＋PHP是个好的选择，因为对于一个网站来讲，稳定安全是第一位的，否则你的网站什么时候被人修改了都不知道怎么回事，或者被黑客入侵，把数据修改或者删除，那就糟糕了，毕竟现在什么红客、黑客的一堆，不能不防。当然，不是说Linux不安全，但是在Linux下集成了很多不安全的程序，导致了它的不安全，但如果设置的好，Linux一样可以很安全。在中国网络应急响应中心（http://www.cert.org.cn）这几个月的数据来看，每个月被入侵成功最高的是Linux系统，占百分之六十多，然后过来是Windows系统，占百分之三十多，而FreeBSD的入侵比例是百分之几。 任何系统都可以很安全，也可以很不安全，关键是管理员怎么做的，世界上没有最安全的系统，只有更安全的系统。下面的文章就是在FreeBSD平台上构建一个比较安全的Web服务器，希望对网管和网络安全爱好者能有一些启发，权当抛砖引玉，希望能够有更好阐述的文章。 一、系统和服务程序的安装 1. 系统安装 为了保证系统的安全，我们

系统准备采用最新的FreeBSD版本，首先是安全，系统兼容性也比较好，这个主要是个人习惯和需求，为了简单起见，这里我们选用了最新的FreeBSd5.3版本进行安装。整个安装过程我就不讲了，如果不清楚的朋友可以参考FreeBSD中文手册（http://www.freebsd.org.cn），整个过程不是很复杂，虽然没有Windows/Linux的系统安全简单，但是比起有些Unix的安装来讲是人性许多的。安装中必须把基本包和内核源代码都装上，为了以后编译内核方便，如果另外，如果喜欢使用ports安装软件的话，还要把ports装上，但是尽量一些没有必要的程序不要装。如果要安装 Webmin等，还要把perl等包装上。系统文件拷贝完以后，会要求配置一些设置，比如把IP地址、名字服务器等设好，不要打开IPv6，不需要 DHCP等服务，不要系统默认的FTP服务，配置 /etc/inetd.conf 时把SSH服务打开，方便我们进行远程管理，如果不想使用inetd这个超级服务来管理的话，可以关闭它，在/etc/rc.conf中添加inetd_enable="NO"，然后设置sshd_enable="YES"一样可以打开SSH服务，后面我们会详细谈到SSH的设置。 系统装完后，在 /etc/inetd.conf 中把除了ssh之外的服务全部关闭，特别是telnet和rlogin等服务，一定要慎重，否则很可能每几天系统就被入侵了。安装完系统后，建议对系统进行升级，比如使用 make world 或 cvsup 把系统内核和ports进行升级。这个步骤和Windows装完后打补丁差不多。 2. 服务程序安装 系统装完以后，就开始安装我们的应用软件，我们的方针还是最新的软件是最安全的，比如能够防止一些老版本中的溢出等等。我们基本就是要让我们的系统有数据库，同时能够处理Web服务，同时能够远程对网站进行文件管理的FTP服务。

我们基本选择的程序都是比较通常的程序。另外，为了有个可视化的管理工具，我们同时也可以安装一个基于浏览器的管理工具Webmin，方便没有ssh客户端等等的时候进行管理。首先我们选用的Web服务是Apache httpd 2.0.53，这是目前的最新版本，当然你也可以考虑1.3的版本，主要是看个人习惯。我们网站是PHP程序编写，所以要安装PHP，版本是 4.3.11，也是最新的版本，如果你的网站程序需要PHP5的支持，那么可以下载php5.0.4.数据库还是最快速的Mysql，选择的版本是最新的 4.0.23，如果你需要外键、事务、子查询、存储过程等的支持，那么你可以考虑4.1和5.0的版本。最后我们的FTP选择最安全的vsFTPd，因为它是最安全快速的，我在局域网中测试它的最高创数速率能够达到10MB/S，proFTPd只有8MB/S，vsFTPd针对小型FTP服务器支持非常好，毕竟我用户不多，几个更新网站而已，当然，如果你喜欢简单方便，也可以考虑使用FreeBSD自带的FTPd，功能和易用性也是不错的。如果你用户比较多，并且功能要求比较高，建议使用proFTPd、pure-FTPd、wu-FTPd等，但有些FTPd不是非常安全，选择时候一定要慎重考虑。 服务器程序列表： Apache 2.0.53 下载地址：http://httpd.apache.org PHP 4.3.11 下载地址：http://www.php.net Mysql 4.0.23 下载地址：http://dev.mysql.com vsFTPd 2.0.2 下载地址：http://vsftpd.beasts.org 反正最少的服务 最少的端口 安全的设置 = 最大的安全，尽量能够不需要使用的服务就不要安装，比如telnetd、rlogind等，那么相反会对服务器安全构成威胁。安装以上程序你可以采用手工编译安装，也可以采用FreeBSD的ports 来进行安装，这看个人爱好，我个人比较喜欢使用手

工安装，如果不明白具体安装的朋友可以参考我的Blog上关于安装Apache PHP Mysql的方法。 二、系统安全设置 1. 用户控制 尽量少的用户，我们的FTP帐户是和系统帐户绑定在一起的，所以我们添加用户的时候先建立一个目录，然后把新建的用户主目录指向到该目录下。假设我需要一个用户能够管理我的网站，而我网站的目录是在 /usr/www 目录下，那么我们新建立的用户 www_user 的主目录就指向 /usr/www 目录，同时它的shell是没有的：/usr/sbin/nologin，主要是为了防止它通过ssh登陆到系统。同时FTP的密码也要设置的非常复杂，防止黑客通过暴力破解获得FTP权限。另外还要说道我们的root用户的密码，我想最少应该不要少于10位的数字＋字母＋字符的密码（我的密码是18位），否则是非常不安全的，如果密码简单，那么黑客通过短时间的暴力破解 SSH中的root帐户，不用几天，系统就可能被攻破了，同时也建议最少一个月更改一次root用户的密码。（强烈建议一般帐户不要有登陆系统的权限，就是把shell设为/usr/sbin/nologin）一般如果要使用root权限建议建立一个属于wheel组的小用户，然后登陆后通过su命令提升为root用户进行管理，如果黑客通过破解了我们普通用户的权限后登陆系统，也不能直接通过root权限进行管理，这是一种安全防范的简单方法。 2. 文件访问控制 有时候被黑客入侵后拿到了小权限用户，比如传了一个WebShell到系统中，那么对方很可能会把 /etc/passwd 等内容直接读取出来，同时查看/etc/master.passwd中对加密后的root用户的密码hash进行破解，最后拿到密码进行登陆系统。那么我们就要控制部分文件只有root能够访问，其他用户无权访问。比如uname，gcc等，如果黑客拿到小权限用户后

就会查看系统版本，然后找到该版本系统对应的溢出程序，使用gcc来进行编译，如果我们能够限制黑客访问uname和gcc等程序，能在一定程度上减缓黑客入侵的脚步。 使用chmod来改变某个文件的权限信息，比如我要 /etc/passwd 和 /etc/master.passwd 文件只能允许root访问： 使用八进制数字来设置 # chmod 700 /etc/passwd # chmod 700 /etc/master.passwd 使用字符标记来进行设置 # chmod u w r x，go-w-r-x /etc/passwd # chmod u w r x，go-w-r-x /etc/master.passwd 系统中有多个重要文件需要设置控制访问权限，一定要控制好，否则将会构成重要威胁。 3. 系统服务和端口控制 端口开的越多就越给黑客多一个入侵的机会，服务越多，危险越大，因为你不知道那些服务是不是有潜在的漏洞或者又发现了新的漏洞，所以尽量少的服务，比如sendmail默认是打开的，那么些建议你把sendmail关闭， 关闭防范是在 /etc/rc.conf中加上： sendmail_enable = "NONE"，如果设为"NO"那么只能够关闭掉pop3服务，不能关闭smtp的服务，所以要设置为"NONE". 系统中最好除了我们能够看到的Apache、Mysql、vsFTPd、SSH之外不要打开其他任何端口和服务。基本的方式是使用netstat -a 查看打开的端口，然后从对应的端口来找相关的服务，比如我们这里应该只允许开的端口有 21， 22， 80，3306等，如果有其他端口，那么一定要仔细检查，很可能是黑客的后门或者是会对系统安全构成威胁的服务。同时有些服务不需要监听网络连接的话，只是需要本地的连接，比如Mysql，那么就可以关闭Socket监听，这个将在Mysql安全设置中讲解，另外，可以通过防火墙来控制部分端口访问和连接状况，比如Mysql的3306端口只允许192.168.0.1访问，那么

我们就在ipfw里添加规则： ipfw add 10001 allow tcp from 192.168.0.1 to 10.10.10.1 80 in 这样就能够防止黑客来访问服务器上的Mysql服务。具体防火墙的设置将在下面“ 防火墙设置 ”中详细讲解。 4. 日志管理和控制 （略） 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