基于 LAMP 的 WEB 安全模型

张艳萍，高忠新
(1. 牡丹江师范学院 网络信息中心，黑龙江 牡丹江 157012)

摘　要：从 Linux 平台安全、Apache 安全、MySQL 数据库安全及 PHP 开发技术等几个方面探讨了如何架设一个安全高效的 WEB 网站技术，并给出了一个可行的安全模型。

关键词：LAMP；网络安全；WEB 网站
中图分类号：TP393.0　　**文献标识码**：A

A WEB security model based on LAMP

ZHANG Yan Ping, GAO Zhong Xin
(Network Information Center, Mudanjiang Normal College, Mudanjiang 157012, China)

Abstract: This text discusses how to design a safe and efficient WEB from Linux terrace safety, Apache safety, MySQL safety and PHP developing technology, and gives a viable safe model.

Key words: LAMP; the network safety; website of WEB

1998 年，Michael Kunze 为德国计算机杂志 c't 写作一篇关于 Free 软件如何成为商业软件替代品的文章，创建了 LAMP 这个名词，是由 Linux 操作系统、Apache 网络服务器、MySQL 数据库和 PHP(Perl 或 Python)脚本语言组合而成的，随之 LAMP 技术成为 WEB 服务器的事实标准。

美国互联网市场调研机构 NetCraft 2006 年统计数据表明，互联网发展在全球继续呈现快速增长趋势。在过去三年中，全球网站数量已经翻了一倍。统计还显示，WEB 服务器市场中，基于 Linux 的 Apache 依然是网站的第一选择。目前，Linux 及 Apache 在网站操作系统及 WEB 服务器软件市场的份额为 62.7%，大型社区平台因安全性和交互性考虑，采用 Windows 软件平台的越来越少，正在逐步转向 LAMP 平台。

然而，在 Internet/Intranet 的大量应用中，网络本身的安全面临着重大的挑战，随之而来的信息安全问题也日益突出。在网络安全问题泛滥的今天，其安全性问题同样面临着考验。

根据网络安全的木桶理论，网络的安全性取决于各个网络组件的安全，因此本文从 Linux 安全、Apache 安全、MySQL 数据库安全、PHP 开发技术、防火墙及入侵检测技术等几个方面探讨了如何架设一个安全高效的 WEB 网站。

1 WEB 平台的安全模型

1.1 层次模型设计

图 1 给出了 WEB 平台的安全模型。

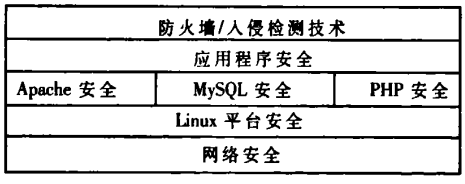

图 1 WEB 平台的安全模型

WEB 安全是一个综合系统问题，笔者将其划分为几个层次，根据网络安全的木桶理论，只有将模型中的各项安全尽可能考虑周全并切实实施安全规程，才能保证整个系统的安全性。由于篇幅有限，本文没有讨论网络框架的安全性问题。

1.2 Linux 平台安全

操作系统作为安全的最底层至关重要，没有操作系统平台的安全就没有任何安全可言，有些技术人员往往只对平台进行了简单的安全设置，而完全依赖于防火墙的做法是造成站点安全的最大隐患。因此，Linux 平台安全应考虑到安装系统、增强 Linux 安全配置因素。

1.2.1 安装系统

在进行系统安装时，如果没有进行规划，将会造成

安全漏洞。目录划分不正确会造成访问的安全隐患以及管理维护的复杂，甚至系统崩溃；无用的软件包安装也会导致出现安全漏洞。因此 Linux 平台安全应首先从规划安装开始。

(1)安装系统时应考虑磁盘分区的安全性

根目录(/)、用户目录(/home)、临时目录(/tmp)和/var目录应分开到不同的磁盘分区，避免访问的安全隐患，也便于系统维护；以上各目录所在分区的磁盘空间大小应充分考虑，避免因某些原因造成分区空间用完而导致系统崩溃；对于/tmp 和/var 目录所在分区，大多数情况下不需要有 suid 属性的程序，所以应为这些分区添加 nosuid 属性。

(2)软件包与服务安装

对于主机，不应安装过多的软件包。这样可以降低因软件包而导致出现安全漏洞的可能性。在选择主机启动服务时不应选择非必需的服务。

1.2.2 增强 Linux 安全配置

系统安装完成后，应增强 Linux 的安全配置，将漏洞和访问的安全隐患消灭在萌芽中。

(1)升级：每一次升级都可以看作是对软件缺陷的弥补，可以有效地填补漏洞并增强软件的功能。Linux 系统安全上的升级包括：

·内核升级。

·GNU libc 共享库升级。

(2)启动和登录安全性：为防止非授权用户获得权限和本地用户非法登录管理终端，必须对系统启动和登录进行设置，以保证系统不被非法访问，具体设置如下：

·设置 BIOS 密码且修改引导次序禁止从软盘启动系统。

·设置用户口令，限制口令长度及复杂性。

·禁止所有默认的被操作系统本身启动的并且不必要的账号。

·更改口令文件属性，从而防止非授权用户获得权限。

·修改“/etc/lilo.conf”增加参数 restricted 和 password，使系统在启动 lilo 时就要求密码验证。

·修改/etc/inittab 文件，禁止 Ctrl+Alt+Delete 重新启动机器命令。

·编辑/etc/pam.d/su 文件，限制 su 命令。

·编辑/etc/rc.d/rc.local 将泄漏系统信息的行注释掉，然后清空/etc/issue、/etc/issue.net 文件内容。

(3)限制网络访问：通过限制网络访问可以有效避免来自网络的攻击和非法访问。

·Inetd 设置 。确认/etc/inetd.conf 的所有者是 root，编辑/etc/inetd.conf 禁止以下服务：telnet shell login exec talk ntalk imap pop-2 finger auth。或使用/etc/hosts.deny 和/etc/hosts.allow 来增加访问限制。

·登录终端设置。编辑/etc/securetty，使 root 仅可在 tty1 终端登录。

· 改变/etc/inetd.conf 文件，避免显示系统和版本信息。

·设置文件的访问权限来实现远程访问控制。

·合理设置 POP-3 和 Sendmail 等电子邮件服务，安装支持加密传送密码的 POP-3 服务器。

·小心配置 FTP 服务。通过对/etc/ftpusers 文件的配置，禁止 root、bin、daemon、adm 等特殊用户对 FTP 服务器进行远程访问。除非特别需要，一般应禁止匿名 FTP 服务。

(4)防止攻击：黑客的攻击无处不在，通过对平台的安全设置可以有效减少和防止攻击。

·阻止 ping 攻击：在/etc/rc.d/rc.local 文件中增加如下一行：---- echo 1 > /proc/sys/net/ipv4/icmp_echo_ignore_all，阻止 ping。

·IP 欺骗攻击：在 host.conf 文件中增加 order bind，hosts；multi off；nospoof on 三行内容来防止 IP 欺骗攻击。

·DoS 类型攻击：修改/etc/security/limits.conf，对系统所有的用户设置资源限制防止 DoS 类型攻击。

(5)备份：在完成 Linux 系统的安装以后应该对整个系统进行备份，以后可以根据这个备份来验证系统的完整性，这样就可以发现系统文件是否被非法篡改过。如果发生系统文件已经被破坏的情况，也可以使用系统备份来恢复到正常的状态。

1.3 Apache 安全

Apache 作为站点搭建软件其安全设置关系到整个站点的安全性能。其密码被窃、非法访问、CGI 脚本等安全问题都会导致站点出现安全漏洞和隐患，因此安装完 Apache 后需通过如下措施来增强其安全性。

(1)利用.htaccess 文件实现的密码保护

·建立.htpasswd 文件。

·用.htaccess 文件实现保护(require valid-user)。

·增加新的许可用户。

·建立允许访问的组。设置方法是建立一个名为 .htgroup 的文本文件。

·在.htaccess 文件中加入 deny from all 禁止读取安全相关文件。

(2)关注 CGI 脚本

CGI 脚本是可执行程序，一般存放在 WEB 服务器的 CGI-BIN 目录下面，在配置 WEB 服务器时，要保证 CGI 可执行脚本只存放于 CGI-BIN 目录中，这样可以保证脚本的安全，且不会影响到其他目录的安全。

(3)升级 Apache 软件通过升级 Apache

增强软件功能并弥补软件缺陷，消除安全隐患。

1.4 MySQL 数据库安全

站点数据库具有容易受到黑客攻击、非法访问、数据丢失等安全问题，因此对 MySQL 数据库设置相应的

安全防范措施以保证其安全、可靠、不间断运行是安全模型的重要内容之一。具体设置如下：

(1)安装 MySQL 数据库后，初始化并设置 root/usr/local/mysql/；mysql/usr/local/mysql/var；mysql/usr/local/mysql/三个 MySQL 数据库目录权限为只读，以防止非法访问。

(2)修改 MySQL 的 root 密码，以防止管理员密码被窃取。

(3)删除所有用户名为空的用户，增加系统安全性。

(4)备份数据库，防止数据丢失。最好能实现双机热备份。

(5)尽可能使用 SSL 与数据库连接以增强数据库访问的安全性，防止信息泄漏。

(6)升级 MySQL 软件，增强软件功能并弥补软件缺陷，消除安全隐患。

1.5 PHP 编程安全

程序设计中往往由于程序员的疏忽致使应用程序存在安全漏洞或隐患，因此对编程中存在的几个问题提出如下解决方案：

(1)欺骗 SQL 语句：有些程序员习惯用逻辑与来提取和验证数据库中用户名和密码，这样只要在用户框和密码框输入"1' or 1='1"就可通过验证了，从而给攻击者提供了非常简单的登录数据库的手段，改进的方法是不要用逻辑与，将用户的提取及验证与密码的提取、验证分开用两个 SELECT 语句完成。这样虽然麻烦却消除了 SQL 语句被欺骗的安全问题。

(2)PHP 手册里有几个例子存在安全问题，实际使用时不要照搬。要真正明白语句的用法并在程序编写完成后进行严格的安全测试。

(3)不要以环境变量、Cookie 变量、session 变量等作为关系生死的判断条件。因为这些变量太容易被伪造。

(4)利用 PHP 可以与 SSH 连接的特性以及执行远程命令的能力，加强安全性。

①安装 ssh2.so。

②将 libssh 和 PHPr 链接起来。有一个 PECL 模块可以完成这个功能。可以使用 PEAR 安装它(pear install-f ssh2)。

③确保这个新的 SSH2.SO 模块被 PHP 加载。编辑 php.ini 文件(对于 CLI 实用程序：/etc/php5/cli/php.ini，对于 Apache 实用程序：/etc/php5/apache2/php.ini；增加一行：extension=ssh2.so)。

(5)升级 PHP 软件，增强软件功能并弥补软件缺陷，消除安全隐患。

1.6 防火墙及入侵检测技术

1.6.1 防火墙

作为系统的第一道防线，其主要作用是监控可信任网络和不可信任网络之间的访问通道，可在内部与外部网络之间形成一道防护屏障，拦截来自外部的非法访问并阻止内部信息的外泄，但它无法阻拦来自网络内部的非法操作。它根据事先设定的规则来确定是否拦截信息流的进出，但无法动态识别或自适应地调整规则，因而其智能化程度很有限。防火墙技术主要有 3 种：数据包过滤器(packet filter)、代理(proxy)和状态分析(stateful inspection)。现代防火墙产品通常混合使用这几种技术。

用 Linux+iptables 做防火墙具有很高的灵活性和稳定性，但安装和设定起来比较麻烦，容易出错。设置防火墙关键是设置一个好的安全规则并严格实施，如何配置和使用已经有很多文章论述过，读者可以自行查阅。

1.6.2 入侵检测(IDS—Instrusion Detection System)

综合采用了统计技术、规则方法、网络通信技术、人工智能、密码学、推理等技术和方法，其作用是监控网络和计算机系统是否出现被入侵或滥用的征兆。经过不断发展和完善，作为监控和识别攻击的标准解决方案，IDS 系统已经成为安全防御系统的重要组成部分。以下是几款 Linux 平台下的工具软件，综合应用它们以建立自己的 IDS 系统。

(1)Psad 是端口扫描攻击检测程序的简称，它作为一个新工具，可以与 iptables 和 Snort 等紧密合作，展示所有试图进入网络的恶意企图。这是首选的 Linux 入侵检测系统。它使用了许多 Snort 工具，可以与 fwsnort 和 iptables 的日志结合使用，这意味着可以深入到应用层并执行一些内容分析。它可以像 Nmap 一样执行数据包头部的分析，向用户发出警告，甚至可以对其进行配置以便自动阻止可疑的 IP 地址。

(2)Snort 是一款轻量级且易于使用的工具，可以独立运行，也可以与 psad 和 iptables 一起使用。从 Linux 的发行版本的程序库中可以找到并安装它，这比起过去的源代码安装是一个很大的进步。至于保持其规则的更新问题，也是同样的简单，因为作为 Snort 的规则更新程序和管理程序，oinkmaster 也在 Linux 发行版本的程序库中。

(3)系统日志。网络管理人员要始终提高警惕，随时注意各种可疑状况，并且按时检查各种系统日志文件，包括一般信息日志、网络连接日志、文件传输日志以及用户登录日志等。在检查这些日志时，要注意是否有不合常理的时间记载。

2 结束语

任何一种单一的安全措施其防范能力都是有限的，一个安全的系统必须采取多层次、多种安全措施、多管齐下才能更好地保证系统安全。本文根据网络安全的木桶理论提出了一种安全模型，并对其中涉及的技术进行了阐述，由于篇幅和水平，本文只能是抛砖引玉。假如一个站点采取了以上模型并实施了各种安全措施，则入侵者要想侵入你的系统而又不被发现几乎是不可能的。

(下转第 119 页)

(1)将整个网络分成50×50的方格,只有处于同一个方格内的节点才能进行正常通信。

(2)每个节点都拥有与"ferry"进行长距离通信的能力,不过由于长距离通信消耗的能量比正常通信消耗的能量大得多,节点只会在网络初始化时期通过该长距离通信向"ferry"通知自己的坐标数据以及从"ferry"处获取初始化信息。

(3)在模型中,ferry每一个系统时间前进一个单位格,即ferry在当前的方格只停留一个单位时间,普通节点只有与ferry处于同一方格内才能进行普通数据传输。

(4)每个节点的移动速度是每个单位时间可以前进一个单位格,包括斜对角方向的单元格。

为了比较网络中节点数目导致的NIMF和CB-NIMF两种算法节点移动时间的差异,当网络中节点数目分别为10、25、50、75、100、125、150、175、200时,分别仿真了两种算法下节点的移动时间,结果如图5所示:当网络中节点数目较少时,CB-NIMF和NIMF两种方式中的总节点移动时间相差不多,但是随着网络中节点数目增加,CB-NIMF方式下总节点移动时间将会比NIMF方式下总节点移动时间越来越少,也就是说,当节点数目比较大的时候,CB-NIMF比NIFM具有明显的优势。这也与前面的分析一致,当节点的数目增多,簇内节点的数目相应增多,高层次的节点将会增加,而层次越高的节点,其非正常工作时间与"ferry"路由周期T的关系就越小,甚至可以说只与节点间的距离有关。而在一个基于NIMF的DTN网络中,每个节点的非正常工作时间都与"ferry"路由周期T密切相关,导致网络中所有节点的非正常工作时间总和与节点数目以及T成正比。

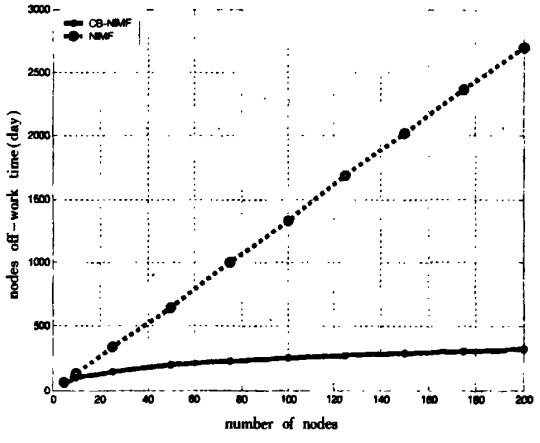

图5 CB-NIMF和NIMF仿真结果比较

当节点数目较少时,每次簇内的节点会比较少甚至可能只有1~2个节点存在。因为本算法规定每个簇内只有一个节点能与"ferry"节点进行直接通信,如果簇内节点很少时,采用CB-NIMF方式并不合适。不过,一般用于数据采集的传感器网络,其节点数目都比较多。而从前面的研究中看出,随着网络中节点数目的增加,CB-NIMF的优势也会逐渐增加。因此,CB-NIMF相比较于NIMF还是有巨大优势的。

本文针对用于数据采集且基于"ferry"的容迟网络中采用NIMF路由时节点移动时间过长的缺陷,根据网络中普通节点也可以进行数据路由以及网络分布的特点,提出新的基于簇的路由算法CB-NIMF,理论推导和仿真结果说明,CB-NIMF能有效地减少节点的移动时间,从而增加节点在固定时间内的数据采集量。

参考文献

[1] FALL K. A delay-tolerant network architecture for challenged internets. In Proc.SIGCOMM 2003,2003.

[2] ZHAO Wen Rui. Mostafa ammer ellen zegura. A message ferrying approach for data delivery in sparse mobile Ad Hoc networks. In ACM MobiHoc 2004,2004.

[3] GU Y, BOZDAG D, EKICI E, et al. Partitioning based mobile element scheduling in wireless sensor networks. In Proc.2nd Annual IEEE Conference on Sensor and Ad Hoc Communications and Networks,2005.

[4] ZHAO W, AMMAR M, ZEGURA E. Controlling the mobility of multiple data transport ferries in a delay-tolerant network. In Proc.INFOCOM 2005,2005.

[5] JEA D,SOMASUNDARA A, SRIVASTAVA M. Multiple controlled mobile elements(data mules) for data collection in sensor networks. In DCOSS 2005,2005.

[6] ZHANG Zhen, FEI Zong Ming. Route design for multiple ferries in delay tolerant networks. Wireless Communications and Networking Conference, 2007. WCNC IEEE, 2007.

(收稿日期:2008-10-13)

(上接第115页)

参考文献

[1] Understanding symantec's anti-virus strategy for internet Gateways. http://www.symantec.com/avcenter/reference/wpnavieg.pdf.

[2] ELLISON R J. Survivability: protecting your critical systems. IEEE Internet Computing ,December 1999.

[3] 中华人民共和国计算机信息系统安全保护条例. http://www.fosu.edu.cn/laws/law19.htm.

[4] MATHIAS H, DAVID G. SNMP versions 1&2 simple network management protocol theory and practice. International Thomson Computer Press,1995.

[5] STEVENS R W.TCP/IP Illustrated, Volume 1: The Protocols, Addison Wesley, 1994.

(收稿日期:2008-12-30)

基于LAMP的WEB安全模型

作者： 张艳萍， 高忠新， ZHANG Yan Ping， GAO Zhong Xin
作者单位： 牡丹江师范学院,网络信息中心,黑龙江,牡丹江,157012
刊名： 电子技术应用 ISTIC PKU
英文刊名： APPLICATION OF ELECTRONIC TECHNIQUE
年，卷(期)： 2009,35(4)

参考文献(5条)

1. STEVENS R W TCP//IP Illustrated 1994

2. MATHIAS H;DAVID G SNMP versions 1-2 simple network management protocol theory and practice 1995

3. 中华人民共和国计算机信息系统安全保护条例

4. ELLISON R J Survivability:protecting your critical systems[外文期刊] 1999(6)

5. Understanding symantec's anti-virus strategy for interact Gateways