关于 ILAS Ⅱ网上业务系统平台安全构建的思考

邓伟富

(广州少年儿童图书馆, 广东 广州 510300)

〔摘 要〕图书馆开展网上业务, 给读者带来方便的同时, 也给图书馆的应用服务器带来了安全隐患。针对这一情况, 文章根据 ILASⅡ的特点和服务器系统 SCO UNIX 的安全机制, 为 ILASⅡ的网上业务构建出安全可靠的网络系统平台。

〔关键词〕ILASⅡ; 网上业务; 系统安全

〔中图分类号〕G250 7 〔文献标识码〕A 〔文章编号〕1002- 1167 (2010) 01- 0051- 03

ILAS (Integrated Library of Automation System) 是由深圳图书馆承担并组织开发出来的一套能适应国内外不同层次、多种规模、各种类型图书馆使用的图书馆自动化集成系统, ILASⅡ是第二代产品。ILASⅡ于 1998 年通过文化部主持的专家技术鉴定, 与会专家一致认为“系统的各项技术指标均处于国内领先地位, 达到国际先进水平”。全国现有 1700 多家图书馆使用该系统, 其市场占有率位居第一。

ILASⅡ不仅保留了 ILAS 早期系统的全部功能, 而且引入了许多新的服务思想, 特别是结合图书馆业务的发展需要, 增加了一系列网上服务功能, 如: 网上书目查询、读者借阅情况查询, 网上预借、预约、续借等网上业务。这些功能给读者带来很大的方便, 通过互联网, 在家就可以享受上述网上服务功能。

图书馆开展这些网上业务, 给读者带来方便的同时, 也给图书馆的应用服务器带来了安全隐患。读者能通过互联网访问服务器上的数据库, 意味着要将服务器连接到存在黑客、病毒、恶意代码等众多不安全因素的互联网上。

本文针对服务器安全隐患这一情况, 根据 ILASⅡ的特点和服务器系统 SCO UNIX 的安全机制, 为 ILASⅡ网上业务构建出安全可靠的网络系统平台。

1 ILASⅡ服务器安全隐患分析

1.1 不安全的互联网

2008 年 11 月 18 日, 国内最大的信息安全企业瑞星公司发布了《2008 年中国大陆地区电脑病毒疫情 & 互联网安全报告》, 报告指出, 2008 年 1 月至 10 月, 全国约有 8100 多万台电脑 (包含企业用户) 曾经被病毒感染, 其中通过网页挂马方式被感染的超过 90%。2008 年 10 月份, 瑞星对 1 万台上网电脑的抽样调查表明, 这些电脑每天遇到的挂马网站, 高峰期达到 8428 个, 最低也有 1689 个, 去除单台电脑访问多个挂马网站的情况, 每天平均有 30% 的网民访问过挂马网站, 中国大陆地区已经成为全球盗号木马最猖獗的地区之一。

瑞星公司的统计、研究表明, 目前的互联网非常脆弱, 各种基础网络应用、电脑系统漏洞、Web 程序的漏洞层出不穷, 这些都为黑客、病毒制造者提供了入侵系统和破坏系统的机会。

电脑病毒、黑客攻击和流氓软件给服务器带来的危害如下: 篡改、更换网站信息或者删除该网站的全部内容; 通过在网络上设置陷阱或事先在生产或网络维护软件内置入逻辑炸弹或后门程序, 在特定的时间或特定条件下, 根据需要干扰网络正常运行或致使生产线或者网络完全陷入瘫痪状态; 通过窃取管理员用户名和密码, 进入系统破坏性删除重要业务数据文件。

1.2 ILASⅡ服务器的安全隐患

由于 ILASⅡ服务器连接在不安全的互联网上提供远程服务, 使服务器成为黑客、电脑病毒攻击的一个对象, 而服务器操作系统——SCO UNIX 由于自身的系统漏洞和系统管理员的管理不善, 往往更容易被入侵。

1.2.1 系统存在没有利用到的服务和端口

SCO UNIX 系统的完整安装包括 1000 个以上应用程序和库软件包。不过, 多数服务器管理员没有安装发行版本中的每个软件包, 而倾向于进行基本安装, 其中包括几个服务器程序的安装。

通常, 系统管理员安装了操作系统却不关注那些被安装了的程序。因为不需要的服务可能会被安装, 并使用默认设置配置, 而且可能还被默认启用。这就会导致不需要的服务, 如 Telnet、FTP、DHCP、或 DNS 在服务器上运行, 而管理员对此却一无所知。由此而带来的是存在进入到该服务器的不必要的通道, 给黑客制造了一条潜在的入侵路径。

1.2.2 系统没有及时升级, 存在系统漏洞

多数包括在默认安装中的服务器程序是稳定的、被全面测试过的软件。在生产环境中使用了多年后, 这些软件的源码已经被全面精化, 许多软件中存在的错误已被发现并修正。

然而, 世界上并不存在完美无缺的软件, 万事都有提高的余地。除此之外, 由于更新的软件在生产环境中的使用时间不长, 或者因为它没有其它服务器软件那么流行,

它可能没有像人们所期待的一样被全面测试过。

开发者和系统管理员经常会在服务器程序中发现可被当作漏洞而利用的程序错误，并在错误跟踪和安全相关的网站或计算机紧急响应组的网站上公开这些信息。虽然这些机制是向网络社区发出安全弱点警告的有效方法，但它却要依靠管理员来及时地给各自的系统升级（打补丁）。如果黑客也能够获得同样的弱点跟踪服务，他们一有机会就会使用这些信息来攻击未加补丁的系统。

1.2.3 系统管理员的工作疏忽

据系统管理网络和安全学院（System Administration Network and Security Institute, SANS）调查，导致计算机安全弱点的主要原因是“指派未经培训的人员来维护安全，并且不提供使其能够胜任的培训和时间”。这不仅是指那些没有经验的管理员，也指那些过分自信或自以为是的管理员。

一些管理员忘记给服务器升级（打补丁），而另一些则忘记查看来自系统内核或网络交通的日志消息。一个常见错误是不改变服务的默认口令或密码，或设置的密码过于简单，容易被黑客译破。例如，某些数据库有默认的管理口令，因为数据库开发者假定系统管理员在安装后会立即改变这些口令。如果某个数据库管理员忘记改变口令，一个毫无经验的黑客也能够使用众所周知的默认口令来获得数据库的管理特权。这些都会导致服务器弱化。

1.2.4 系统带有固有的不安全因素的服务

如果所选的网络服务带有固有的不安全因素，即便是警惕性最高的组织也可能成为受害者。例如，许多服务是在用于可信任网络的假定条件下被开发的；然而，一旦这些服务可通过互联网被使用，这个假定条件就不适用了。互联网本身就带有固有的不可信任性。

还有一类不安全网络服务是那些需要用户名和口令来验证的服务。Telnet 和 FTP 就属于这类服务。如果分组嗅探软件正在监视远程用户和这类服务器间的连接，口令就能够被轻而易举地窃取。

以上提及的服务还会轻易地遭到安全行业称之为“中间人”（man-in-the-middle）的攻击。在这类攻击中，黑客会设计让网络上的一个已攻破的名称服务器指向自己的机器而不是实际的目标服务器来重新导向网络交通。一旦某人打开了一个到该服务器的远程会话，黑客的机器就会充当一个隐型导管，悄悄地坐在远程服务和毫无疑心的用户间截取信息。黑客可以用这种方法来收集管理性口令和原始数据，服务器和用户对此却一无所知。

另一类不安全服务是网络文件系统和信息服务，如 NFS 或 NIS。它们仅仅是为 LAN 而开发的，但是不幸的是，后来又被扩展到 WAN 以方便于远程用户。按照默认设置，NFS 没有配置任何验证或安全机制来防止黑客挂载 NFS 共享以便存取其中的数据。NIS 也有网络上的每个计算机都必须知道的重要信息，包括口令和文件权限。它们都存在于一个纯文本的 ACSII 或 DBM（由 ASCII 推导出的）数据库中。能够进入这个数据库的黑客就能够进入网络上的每个用户帐号，包括管理员的帐号。

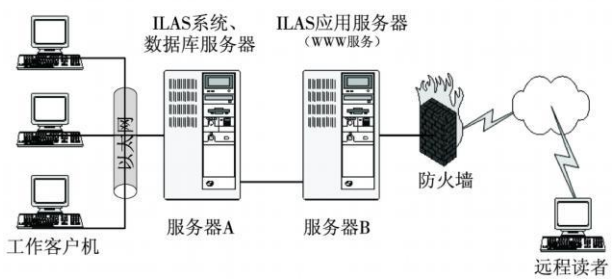
2 ILASⅡ服务器的安全配置

由于 ILASⅡ服务器是基于 SCO UNIX 操作系统的，在这个系统平台上运行 ILASⅡ图书馆业务应用系统，所以，安全配置应在这两个系统上进行操作。

2.1 ILASⅡ应用系统的配置措施

对于 ILASⅡ系统，根据其作用严格地讲，可分为系统服务器、数据库服务器、应用服务器。工作用户首先登入系统服务器，取得系统的运行环境，包括操作权限、所用子系统、所用数据库、有关业务管理的参数、系统功能菜单、应用程序屏幕文件、应用程序输出格式文件等等。一旦进入系统，每个子系统所用数据库由网络服务程序按照参数自动寻找。数据库所在服务器称为数据库服务器。应用服务器主要指用于提供 WWW 服务等。服务器均以 UNIX 为操作平台。物理上系统服务器、数据库服务器、应用服务器可以是同一台服务器。

根据以上特点，在安装服务器时，将 ILAS 的系统服务程序和数据库配置在同一台服务器上（下称服务器 A），而将应用服务（主要指 WWW 服务）程序配置在另一台服务器上（下称服务器 B）。如下图：



在单位局域网内，工作人员的客户机直接登陆服务器 A，而网上读者则登陆访问服务器 B，服务器 B 根据读者的数据请求，从服务器 A 提取业务数据，再返回给读者。服务器 B 通过外网卡的公有 IP 与互联网连接，而通过内网卡的私有 IP 与局域网内服务器 A 连接，避免了图书馆业务数据直接与互联网相连接，加强了数据的安全性。

（1）设置服务器 B，使得网上的数据请求都从服务器 A 的数据库中提取。配置文件 ILASⅡ.ini 为服务器程序运行的首要参数，固定放在 /ilas/ 下，因为应用服务器（服务器 B）上的 UNIX 应用程序（包括 CGI）是按照 ILASⅡ.ini 中的 IP 和 ILASPATH 寻找系统服务器（服务器 A），并从中提取数据。所以 ILASⅡ.ini 的内容要设置为：

IP= 系统服务器 IP 地址（即服务器 A 的 IP）

PORT= 端口号（与以本服务器为系统服务器的工作站端口号相同）

ILASPATH= 系统服务器 ILASⅡ安装路径（一般为/u/ILASⅡ_GB）

LOCALPATH= 本服务器 ILASⅡ安装路径 (一般为/u/ILASⅡ_GB)

(2) 将服务器 B 伪装成数据库服务器, 即使有黑客入侵, 破坏的也只是服务器 B 的数据。如果仅作为提供 WWW 服务的服务器 B, 其主要运行的程序包括: 数据库服务程序 ldbms_server 和网络服务程序 ILASⅡ_netserver。而目录与文件也仅需以下几个:

目录	文件
/u/ILASⅡ_GB/bin	ldb_* 、ILASⅡ_netserver、ldbms_server
/u/ILASⅡ_GB/lib	三个以 AB 字母开头的系统授权文件
/u/ILASⅡ_GB/webpac	CGI 服务程序和 HTML 文本

现在, 从服务器 A 中复制一份完整的目录/u/ILASⅡ_GB, 放在服务器 B 中的相同位置。这样, 服务器 B 既有上述必要的程序文件, 又包含了 database、log 等伪装的重要业务数据。

2.2 SCO UNIX 操作系统的安全配置措施

SCO UNIX 作为一个技术成熟的商用网络操作系统, 广泛地应用在金融、保险、邮电等行业, 其自身内建了丰富的网络功能, 具有良好的稳定性和安全性。但是, 如果用户没有对 UNIX 系统进行正确的设置, 就会给入侵者以可乘之机。因此在网络安全管理上, 不仅要采用必要的网络安全设备 (如防火墙等) 还要及时给系统升级 (打补丁), 并且在操作系统的层面上进行合理规划、配置, 避免因操作系统的漏洞而给应用系统造成风险。

2.2.1 合理设置用户

由于 ILASⅡ的工作用户是由本身系统创建生成, 不依赖 UNIX 系统, 所以不要随意在 UNIX 系统创建用户, 因为用户名和密码管理永远是系统安全管理中最重要的环节之一。对网络的任何攻击, 都不可能没有合法的用户名和密码 (后台网络应用程序开后门例外)。但目前绝大部分系统管理员只注重对特权用户的管理, 而忽视对普通用户的管理, 为非法用户窃取信息和破坏系统留下了空隙。

有必要建立用户时, 一定要考虑该用户属于哪一组, 不能随便选用系统缺省的 group 组。要限制用户不成功登录的次数, 避免入侵者用猜测用户口令的方法尝试登录。为账户设置登录限制的步骤是: Scoadmin→ Account Manager→ 选账户→ User→ Login Controls→ 添入新的不成功登录的次数。

2.2.2 口令保护的设置

口令一般不要少于 8 个字符, 口令的组成应以无规则的大小写字母、数字和符号相结合, 绝对避免用英语单词或词组等设置口令, 而且应该养成定期更换各用户口令的习惯。口令的保护还涉及到对/etc/passwd 和/etc/shadow 文件的保护, 必须做到只有系统管理员才能访问这两个文件。

2.2.3 合理设置等价主机

设置等价主机可以方便用户操作, 但要严防未经授权非法进入系统。所以必须要管理/etc/hosts.equiv、.rhosts 和.netrc 这 3 个文件。其中, /etc/hosts.equiv 列出了允许执行 rsh、rcp 等远程命令的主机名字; .rhosts 在用户目录内指定了远程用户的名字, 其远程用户使用本地用户账户执行 rcp、rlogin 和 rsh 等命令时不必提供口令; .netrc 提供了 ftp 和 rexec 命令所需的信息, 可自动连接主机而不必提供口令, 该文件也放在用户本地目录中。由于这 3 个文件的设置都允许一些命令不必提供口令便可访问主机, 因此必须严格限制这 3 个文件的设置。在.rhosts 中尽量不用“+ +”, 因为它可以使任何主机的用户不必提供口令而直接执行 rcp、rlogin 和 rsh 等命令。

2.2.4 合理配置/etc/inetd.conf 文件

UNIX 系统启动时运行 inetd 进程, 对大部分网络连接进行监听, 并且根据不同的申请启动相应进程。其中 ftp、telnet、rcmd、rlogin 和 finger 等都由 inetd 来启动对应的服务进程。因此, 从系统安全角度出发, 我们应该合理地设置/etc/inetd.conf 文件, 将不必要的服务关闭。关闭的方法是在文件相应行首插入“#”字符。

2.2.5 合理设置/etc/ftpusers 文件

在/etc/ftpuser 文件里列出了不受欢迎的 ftp 用户表, 侵入者使用里面的用户名以 FTP 协议进行文件传输会被系统拒之门外。为了防止不信任用户传输敏感文件, 必须合理规划该文件。例如不允许 root 和 UUCP 用户进行 ftp 访问, 可将 root 和 UUCP 列入/etc/ftpusers 中。

2.2.6 删除不用的软件包及协议

在进行系统规划时, 总的原则是将不需要的功能一律去掉。如通过 scoadmin→ Soft Manager 去掉 X Window; 通过修改/etc/services 文件去掉 UUCP、SNMP、POP、POP2、POP3 等协议。

2.2.7 指定主控台及终端登录的限制

指定 root 用户只能在某一个终端 (或虚屏) 上登录, 这样可避免从网络远程攻击超级用户 root。对主控台进行指定, 设置方法是在/etc/default/login 文件增加一行: CONSOLE=/dev/tty01, 这样, 用户 root 只能在主机第一屏 tty01 上登录。

经过以上配置, 可将 ILASⅡ系统的灵活性配置和 SCO UNIX 系统平台的安全机制有效地结合起来, 构建出安全可靠的系统环境, 为图书馆开展网上业务提供保障。

〔参考文献〕

〔1〕ILASⅡ2.0 系统管理员手册〔Z〕. 深圳市深图朗思数字技术有限公司, 2000.

〔2〕曾巧红. 构筑图书馆网络安全的防护体系〔J〕. 图书馆论坛, 2004 (6).

〔3〕邓少雯. 网络环境下数字图书馆的安全与防范措施〔J〕. 图书馆论坛, 2004 (8).

(下转第 100 页)

实现“无处不在的图书馆”、“全天候的图书馆”的自助图书馆服务；如以大信息服务观为趋势的和以“便民服务”为内容所开展的服务，加大了网上信息导航服务内容等都是创新的成功案例。

五是服务的方式方法和手段的创新。服务理念决定服务方式方法，即有什么样的服务理念，就有什么样的服务。图书馆由传统理念上的“藏书楼”转变为“没有围墙的图书馆”，其服务的空间、领域得到前所未有的拓展，推动了服务方式方法的创新。如利用各种信息技术对分散化、多样性的信息资源进行有效整合和集成，使多种类型、多元化的信息资源形成一个有机整体，保障读者对信息资源的全方位、深层次的需求，为读者提供便利、高效的服务；如图书馆在现代技术条件下，开展“一站式”服务，帮助读者在短时间内全面获取所需信息的服务；如图书馆开展整体优化、馆际协作、联合互动、共建共享等集成化管理等，已成为现代图书馆服务的一种重要理论与方法。这一些都成为我们利用网络优势和现代化设施，组织、控制、创新、传播信息的新的方式方法和手段。

〔参考文献〕

〔1〕程亚男. 图书馆服务新论〔J〕. 图书馆，2000 (3).
〔2〕黄俊贵. 图书馆原理论略〔J〕. 中国图书馆学报，2001 (2).
〔3〕黄俊贵. 图书馆服务理念琐谈〔J〕. 图书馆，2001 (2).
〔4〕程亚男. 再论图书馆服务〔J〕. 中国图书馆学报，2002 (28).
〔5〕蒋永福，付军. 图书馆服务五原则〔J〕. 中国图书馆学报，2003 (3).
〔6〕刘亦平，高桂兰. 论图书馆服务职能的本位回归〔J〕. 图书馆，2004 (5).
〔7〕程亚男. 图书馆服务的人文分析与评判——三论图书馆服务〔J〕. 中国图书馆学报，2006 (3).
〔8〕程鹏. 2004—2005 年我国关于图书馆服务研究综述〔J〕. 图书馆论坛，2006 (6).
〔9〕程亚男. 公众的期待与期待的实现——四论图书馆服务〔J〕. 图书馆论坛，2007 (6).
〔10〕程亚男. 图书馆与互联网的博弈——五论图书馆服务〔J〕. 图书馆论坛，2008 (6).
〔11〕黄兴武. 图书馆服务：全民共享——覆盖全社会的图书馆服务体系的理论与实践〔J〕. 跨世纪，2008 (11).

Several Problems in Modern Library Service

YAN Yue-ying
(Guangzhou Party School, Guangzhou 510070, China)

Abstract: As a basic tenet, service is the master stroke that running through the development of library and the key value of library. In modern library service, readers need to be understood, studied and developed so as to improve the service level. New service ideas should be cultivated and the service mode should be conformed.

Keywords: library service; service idea; service mode

〔作者简介〕严跃英 (1959-)，女，副研究馆员，广州市委党校图书馆副馆长，已发表论文多篇。

〔收稿日期〕2009- 06- 04

(上接第 53 页)

〔4〕廖映虹. 如何提高网络安全防范意识〔J〕. 数字图书馆论坛，2005 (6).
〔5〕丁云. SCO UNIX 网络安全的技术措施〔J〕. 网络技术. 2004 (10).
〔6〕SCO UNIX 系统管理员宝典〔M〕. 北京：电子工业出版社，2000.
〔7〕SCO UNIX 网络安全管理〔EB/OL〕. http://www.chinaunix.net.
〔8〕2008 年中国大陆地区电脑病毒疫情 & 互联网安全报告〔EB/OL〕. http://it.rising.com.cn/new2008/News/NewsInfo/2008- 11- 18/1226970618d50435.shtml.

Thinking on the Safety Construction of the Platform of ILAS II Net- service System

DENG Wei-fu
(Guangzhou Children Library, Guangzhou 510000, China)

Abstract: The net-service of library makes it convenient for readers, but on the other hand brings forward safe challenges for library server. Based on the characteristics of ILAS II and the safety mechanism of server system SCO UNIX, the paper puts forward a safy and reliable platform of net system for ILAS II net-service.

Keywords: ILAS II; net-service; system safety

〔作者简介〕邓伟富，男，馆员，广州少年儿童图书馆采编部副主任。

〔收稿日期〕2009- 10- 19