Linux网络系统的攻击与防范

罗明英,秦 光

(西昌学院 信息技术系,四川 西昌 615022)

【摘 要】本文就Linux平台下的计算机网络攻击的防范进行了分析和研究,指出如何从系统、数据、网络、服务、应用程序和日常维护方面采取防范措施,以保证Linux网络系统的安全,对于架构Linux网络和Linux网络管理有着十分重要的意义。

【关键词】Linux系统;网络安全;网络攻击;防火墙;安全策略

【中图分类号】TP393.08 【文献标识码】A 【文章编号】1673-1891(2006)03-0071-04

1 引言

Linux的Open Source策略使它成为网络中常用的一种服务器操作系统,尽管Linux系统是稳健的,但并不说明它是绝对安全的,因此要保Linux网络系统的安全就要采用一定的防范攻击的措施。Linux网络系统中被攻击的方式主要有拒绝服务、中间人、IP欺骗和缓冲区溢出攻击等。拒绝服务的攻击方式是企图使网络过载,当攻击成功时,可能会导致整个系统瘫痪,这种攻击方式经常同时采用IP欺骗方式,以隐蔽攻击为特点。中间人攻击是通过路由器来完成,先控制一台路由器,再窃取IP包,将其解开后,重定向或替换。对付这种攻击的办法是利用数据加密和采用IPV6协议。IP欺骗是利用TCP/IP协议中不检查返回地址的这个安全漏洞,来达到攻击网络的目的。攻击者利用这一点能够改变IP地址来掩盖发出攻击的地址。缓冲区溢出攻击的原理是向一个有限空间的缓冲区拷贝过长的字符串,覆盖相邻的存储单元,以引起程序运行的失败。由于自动变量保存在堆栈中,当发生缓冲区溢出时,存储在堆栈中的函数返回地址也会被覆盖。这时,发生溢出的函数就无法正常返回。这种情况下,系统一般报告:"coredump"或"segmentfault"。严重的是如果覆盖缓冲区是一段精心设计的机器指令序列,它可能通过溢出,改变返回地址,将其指向自己的指令序列,从而改变该程序的正常流程。这段精心设计的指令一般指向"/bin/sh",所以这段代码有时被称为"shell code"。通过这样的溢出可以得到一个shell,但是如果被溢出的是一个suid root,得到的将是一个root shello这样机器的控制权就会易手,此后系统就有可能受到恶意的攻击。根据Linux网络系统中受到攻击的目标和范围,可以从系统、数据、网络、服务、应用程序和日常维护等方面采取相应的防范措施。

2 加强linux网络系统安全性的防范措施

2.1 系统安全防范

2.1.1 用户与口令安全

身份验证是Linux系统做主要的用户安全技术,Linux为合法用户提供账户,用户登录时必须输入合法的账户和口令,经系统对账户和口令验证合法后才能进入,连续多次登录失败将禁止再次登录,要避免使用脆弱口令。

2.1.2 对象访问的安全性

Linux系统对文件、目录和进程等对象的访问采用强制访问控制(MAC)来实现,不同的用户只能访问到与其有关的、指定范围的对象信息。用户不同,对这些对象的授权也应不同。对于本地或远程关机、网络访问、文件目录的读、写、备份、设备驱动程序的装卸、进程优先级变更、用户或计算机能否被信赖的权限设置以及域中工作站的增删、服务增删等应严格区分用户的不同而给予适当的权限。

收稿日期:2006-08-21

作者简介:罗明英(1964-),女,副教授,在读软件工程硕士,主要从事计算机教学工作。

2.1.3 系统配置的安全性

(1)设置 BIOS 密码。

(2) 配置系统在启动 LILO 时就要求密码验证可以防止破坏者启动系统。

(3) Linux 系统采用 EXT2 文件系统或扩展 .EXT2 文件系统，数据分区存储，设置分区属性和文件的只添加或不可变属性来提高文件的安全性。实际工作中，将不同的应用程序安装在不同的主分区并设置关键的分区为只读，将系统目录设置为 711 模式，仅将少量的目录设置为读写模式以保护系统目录。只要可能，就将磁盘设置为只读，对重要文件(女 I:ILOG 文件)设置为只添加或不可变属性，这将让入侵者无法清除或变更重要的系统文件

(4)用户登录时系统提示信息可能暴露系统，应尽可能隐蔽系统信息。

(5)限制系统管理员允许登录的控制台设备，取消普通用户的 shutdown、reboot 和 halt 等控制台访问权限。

(6)设置无操作时间超越限制时，账户被强制注销以防用户离开时忘记注销。

(7) 系统管理员应强制所有用户在注销时删除运行过的命令历史记录，不同用户也可修改自己的 profile 文件来消除运行过的历史命令。这能防止他人窥探用户历史命令，对 root 用户尤其重要。

(8)暂存文件和目录的安全。Linux 系统中暂存目录为/tmp 和/usr/tmp，如果对这些目录存放暂存文件，别的用户可能会破坏这些文件，因此，使用暂存文件最后将文件屏蔽值定义为 0070 最保险的办法是建立自己的暂存文件和目录$Home/mytemp，并且不要将重要文件存放于公共的暂存目录。

(9) suid/sgid 的安全。尽量不写 suid/sgid 程序，in 为现有文件建立一个链，即建立一个引用同一文件的新名字。如果目录已经存在，该文件被删除而代之以新的链，或存在的目录的文件不允许用户写，则请求用户确认是否删除该文件，因为只允许在同一文件系统内建链。若要删除一个 suid 文件，就要确定文件的链接数，只有一个链时才能确保该文件被删除。若 suid 文件已有多个链，一种方法是改变其存取方式，这将同时修改所有链的存取许可，也可用 Chmod000 文件名命令取消文件的 suid 和 sgid 许可，同时也取消文件的全部链。

2.1.4 慎重使用某些命令

有些命令在使用时存在安全隐患，如 cp\mv 和 cpio 等，使用时要特别小心。

2.1.5 启用安全审计技术

启用系统审计功能以便记录系统发生的安全事件，对各种系统日志文件，包括一般信息日志、网络连接日志、文件传输日志及用户登录日志等进行审核，可发现各种潜在的安全问题。

2.2 数据安全防范

数据传输时可能被攻击者非法截获或监听，存储的数据也可能被攻击者获得，为了提高数据的安全性，往往对网络上传输和存储数据按照一定的加密算法进行加密处理。数据安全可以采用以下方式实现。

(1) 采用加密文件系统。Linux 提供多种加密文件系统，比较有代表性的是 TCFS(Transparent Cryptographic File System)。另外用 crypt 命令也可给用户文件加密，它使用一个关键词将标准输入的信息编码变成不可读的杂乱字符串，送到标准输出设备。再次使用该命令，用同一关键词作用于加密文件后，可恢复文件内容。一般来说，文件加密后应删除原始文件，只留下加密后的版本，且不能忘记加密关键词。VI命令一般都有加密功能，用 Vi—x 命令可编辑加密后的文件。加密关键词的选取规则和口令的选取规则相同。由于 crypt 程序可能被做成特洛伊木马，故不宜用口令作为关键词。最好在加密前用 pack 或 compress 命令对文件进行压缩，然后再加密。

(2)对用户的密码的传输和存储进行加密。可以对用户密码文件 password 进行加密处理，也可要求用户采用安全 shell(ssh) 以实现对用户账户号和口令的加密传输。

(3)在数据敏感的环境中，禁止用户使用让数据在网络中明文传输的命令，如 ping 命令等。

2.3 网络安全防范

2.3.1 保证主机安全

使用 TCPWrappers 可以阻止和限制入侵者从特定的机器入侵系统。TCPWrappers 是一个介于外来服务请求和系统服务回应的中间处理软件。它提高系统安全性主要体现在，一个是获取访问权限前的控制，一个是获取访问后的处理。TCP Wrappers 需要 xinetd 来作用。Xinetd 是 Linux 的超级守护进程，它提供访问控制、请求记录、地址绑定、重定向和资源利用等服务。在 ReadHat 7.2 以上版本中可以默认安装，如果自己安装，可先从 http://www.xinetd.org/xinetd-2.3.5.tar.gz 中获取 xinetd

的最新源代码包，然后编译安装，假设安装目录是/home/src，安装步骤如下：

```
cd/home/src
tarxvzfxinetd*
cdxinetd*
./configure - prefix = /etc - with - libwrap - with - loadavg - with - inet6
make
makeinstall
cpxinetd/sample. comf/etc/xinetd. conf
```

其中，参数 prefix 是指定安装目录，with - libwrap 是加载 libwrap. a 库，使之可以使用 TCPWrapper 功能。with - loadavg 使之具有限定连接数的功能，避免 DOS 攻击。with - inet6 使之支持 ipv6。

完成后，可用 vi xinetd. conf 对其中的各种服务参数作相应的修改，例如设 user = root，表明用户只能是 root。

2.3.2 设置防火墙

防火墙的作用是阻止非授权用户进入、离开和穿过网络或主机系统一种部件或一系列部件，可以采用系统附带的工具和专用防火墙来实现主机系统或网络的安全。在 Linux 2.0 版内核中防火墙被称为 ipforward，在 2.2 版内核为 ipchains，而在 2.4 版内核中则是 netfiltero 以 ipchains 为例，它先禁止所有包，再根据所需要的服务允许特定的包通过防火墙，从而实现 Linux 网络系统过滤型防火墙。每一种服务都有自己特定的端口，具体可参阅 /etc/services · 或 RFCl700。实现步骤如下：

(1) 在/etc/rc. d/目录下用 touch 命令建 firewall 文件，执行 chmodu + xfirewall 以更改文件属性，编辑/etc/rc. d/rc. 10cal 文件，在末尾加 i/etc/rc. d/firewall 以确保开机时能自动执行该脚本并刷新所有的 ipchains。

(2)设置包过滤，如设置 icmp 包过滤，由于 icmp 包通常用于网络测试等，故允许所有的 icmp 包通过。

```
#defineicmppackets
/sbin/ipchains - Ainput - picmp - J  ACCEPT
```

(3) 设置缺省包过滤规则：除允许通过的包以外，禁止其他包通过。

```
#deflneallmleSOninUtChain
/sbin/ipchains - Ainput - j  DENY—1
```

通过以上步骤，就建立了一个相对完整的防火墙。

2.3.3 采用端口入侵检测

任何网络连接都是通过开放的应用端口来实现的。如果尽可能少地开放端口，就大大减少了攻击者成功的机会。应采用端口检测程序或专门的入侵检测系统来检测扫描并阻止入侵者，关闭那些无用的端口。

2.3.4 禁止设置缺省路由

在主机中，应该严格禁止设置缺省路由，即 default routeo 为每一个子网或网段设置一个路由，否则其它机器就可能通过一定的方式访问该主机。

2.4 服务安全防范

对不同的服务采用不同的安全认证。具体做法如下：

(1)有效使用 Linux 系统的安全认证方法。这主要通过可插式认证模块 PAM(Pluggable Authentication Modules) 来实现。它通过提供一些动态链接库和一套统一的 API，将系统提供的服务和该服务的认证方式分开，使得系统管理员可以灵活地根据需要给不同的服务配置不同的认证方式而无需更改服务程序，同时也便于向系统中添加新的认证手段。系统管理员通过 PAM 配置文件指定什么服务需要采用何种认证方法。

(2) 取消目前不使用的服务并限制一般用户添加或删除服务。

(3) 对安全性低的服务进行重点监控。Linux 提供了多种服务供网络用户使用，其中的一些服务安全性很低，如 telnet、rlogin 和 rcp 等远程登录服务。当用户用 telnet 或 r 命令(rlogin 和 rcp 等)来远程访问本系统时，系统首先检查 .rhosts 文件(.rhosts 文件中存储的是可直接远程访问本系统的主机及用户名)中是否存有客户的主机名和用户名，一旦找到，它将允许客户直接访问它，而不需要输入口令。当黑客攻破系统后，就有可能在系统中留下一个“后门”，从而带来隐患。

2.5 应用程序安全防范

通过专业程序来防范系统的安全，目前最典型的方法为设置陷阱和设置蜜罐两种方法。陷阱是指激活时能够触发报警事件的软件，而蜜罐(honeypot)程序是指用来引诱企图入侵者，使其触发专门的报警程序。在 Linux 网络中，可以设计专门的陷阱程序，常用的有两种陷阱程序：一种是只发现入侵者而不对其采取报复行动；另一种是同时采取报复行

动。设置蜜罐的常用方法是故意声称 Linux 系统使用了具有许多脆弱性的 IMAP 服务器版本。当入侵者对这些 IMAP 服务器进行大量端口扫描时，就会落入陷阱并且激发系统报警。 phf 就是一个有名的蜜罐陷阱实例，它是一个非常脆弱的 Webcgi－bin 脚本。另外一类蜜罐陷阱程序可以通过在防火墙中将入侵者的 IP 地址设置为黑名单来立即拒绝入侵者继续进行访问。Linux 内核中的防火墙代码非常适合这样做。

2.6 日常维护安全防范

2.6.1 对系统及时备份

为了防止系统在使用的过程中发生意外情况而难以正常运行，应该对 Linux 完好的系统进行备份，良好的备份策略可以在系统文件已经被破坏的情况下，用系统备份来恢复到正常的状态。定期将系统与备份内容进行比较也可以验证系统的完整性是否遭到破坏。

2.6.2 及时使用安全补丁

系统的安全补丁是对系统中的一些不完善的地方和存在的安全隐患进行修补，及时使用补丁程序，可以减少系统的安全威胁，提高系统的安全性。

2.6.3 发现入侵及时处理

一旦发现了一个用户正从未知的机器登录，且该用户在系统没有相应的账号，表明此时系统正在受到攻击。为了防止系统的安全性进一步受到破坏，应该马上锁定该机器，如果攻击者已经登录到系统，应该马上断开主机与网络的物理连接。如果可能，进一步查看此用户的历史记录，再仔细查看其他用户是否也已经被假冒，攻击者是否拥有有限权限，最后应该杀掉此用户的所有进程，并把主机的 IP 地址加入到文件 hosts. deny 中 .

2.6.4 预防病毒

目前，受益于 Linux 的 Opensource 策略，在 Linux 上并未出现广泛传播的病毒，但作为 Linux 的系统管理员应及时了解新的技术和发展，以防在系统受到病毒侵害时能及时保护。

3 结束语

对于系统和网络攻击的防范，任何一种单一的安全措施其防范能力都是有限的。为了保证 Liunx 网络系统的安全性必须采取多种安全措施，多管齐下。一个优秀的系统管理员还要不断学习新的管理工具软件，不断了解 Linux 的最新动态信息，在实践中提高自己防范网络攻击的技术水平。假如一个 Linux 网络系统采取了以上各种安全措施，那么要想侵入这样的系统，攻击者不得不绕过防火墙，避开入侵检测系统，跳过陷阱程序，通过系统过滤，跳过日志检测器，修改文件系统属性和破坏安全登录服务器等等，才能达到最终目的。由于其中任何一个环节都可能激发报警，因此入侵者要想侵入这样的系统而又不被发现几乎是不可能的。本文所采用的各种安全防范措施在 Linux 的网络系统中得到运用，并且具有良好的实际效果。

参考文献：

[1]Haisen. [美]Linux 安全基础[M]. 北京：人民邮电出版社，2002.

[2]胡振昌 . 面向 21 世纪网络安全与防护[M]. 北京：希望电子出版社，1999.

[3]曹元其 . Linux 安全综述 . http://www. yesky. com.

[4]DavidA. B 著 . 游华云译 . Linux 安全开发工具[M]. 北京：电子工业出版社，2000.

[5]陈旭，温阳东 . Linux 系统网络安全问题分析与对策[J]. 合肥工业大学学报，2002, 25(3):394－397.

[6]张文波，王成等 . 浅析 Linux 系统的网络安全策略和措施[J]. 吉林师范大学学报，2003,(2):63－65.

[7]www. tldp. org/HOWTO/IPCHAINS.

Attack and Prevention of Computer Network Based on Linux System

LUO Ming－ying, QIN Guang

(Department of Information technolgy, xichang College, Xichang sichuan 615022)

(下转85页)

一直是制约民营企业做大做强的“制度瓶颈”,随着上市“审批制”、“额度制”等由主管部门和地方政府逐个推荐和直接审批的作法的取消,今后要加大实施“核准制”的力度,让符合相关法规、政策的优质民营企业进入资本市场,这样不仅给资本市场的发展带来新鲜血液,更重要的是资本市场“公正、公平、公开”的原则得到体现。

第二、是积极为民营企业在二板市场上市创造条件。我国的二板市场尚在筹建之中,国内二板市场的建设,要根据国内大多数民营中小企业特点,确定设立模式及有关规章制度,对《证券法》和《公司法》中有关案例进行修订,如二板市场股票流通、员工持股计划、知识产权出资规定、保荐人制度和信息披露制度等。

第三、是通过吸纳风险投资、发展场外交易市场及发行债券等方式进行融资。在风险投资的主体中,除了政府风险投资机构及创业中心的风险投资外,还应当鼓励民营科技型企业吸纳外资及中外合资风险投资基金和风险投资等,适当时候,可使用社会保障基金等社会资金用于风险投资,同时,加大政府风险基金对民营企业“孵化器”支持力度;通过设立柜台交易市场,为民营企业股权流通及证券交易创造便利条件;让更多民营企业能顺利进入直接融资市场;让有条件的民营企业(股份公司)尝试发行债券、附新股认购权证的企业债券、浮动利率企业债券、企业的境外债券等品种,降低企业融资成本,改善资本结构。

参考文献:

[1]王光伟. 中国金融体制改革焦点问题研究[M]. 复旦大学出版社,2003,(1):121 -230.
[2]论民营企业的融资选择[M]. 中国海南改革发展研究院. 2005,3.
[3]浅议我国民营企业的融资环境[N]. 经济日报,2005,1,2.
[4]盛立军. 我国中小企业存在的融资障碍[J]. 经济导刊,2005,(4).
[5]民营企业如何与银行机构双赢[N]. 经济日报,2004,7,7.
[6]张玉利. 小企业成长管理障碍. 超星数字图书网,2003,5.

Factors Restraining Financing of Chinese Private Enterprises

GENG Xuan - zhen[1], DENG Jian - ping[1], YI Dong - ling[1], XIE Jian - bing[2]

(1. Xichang College, Xichang Sichuan 615013;
2. Xichang Power Liability Company. Ltd, Xichang Sichuan 615000)

Abstract: Private enterprises is the most dynamic part of China' s national economy. It not only created employment opportunities for the community, made our economy develop steadily, but also played a leading role in the local economic development. At the same time, every now and then, we noticed that Chinese private enterprises have great difficulties in financing. Therefore, this paper focuses on the possible causes of the financing difficulties.

Key words: Chinese private enterprises; Financing; Factors restraining financing

(责任编辑:张荣萍)

(上接 74 页)

Abstract: The paper analyses and researches the attack and prevention of computer network based on Linux system and points out how to take some measures to ensure the safety of Liunx network system from the following six aspects: system, data, network, service, application program and daily maintenance. It is very important for constructing and managing Linux network system.

Keywords: Linux system; Network security; Network attack; Firewalls; Security strategy

(责任编辑:张荣萍)