一种校园网的网络安全策略

方贤进,李敬兆,姚亚锋,陈代梅
(安徽理工大学 计算机科学与技术系,安徽 淮南 232001)

摘 要:随着网络攻击者知识的成熟以及攻击工具与手法的复杂多样,网络安全问题也日益突出起来,单纯的防火墙策略已无法满足网络安全的需要。为了更进一步提高网络安全,必须采用防火墙与入侵检测系统相结合的网络安全技术。另一方面,校园网网络服务平台一般是基于开放源代码软件的,故文中提出了采用 Linux 系统下 IPtables 包过滤 + Squid&Socks 代理服务器的防火墙体系和网络入侵检测系统 Snort 相结合的网络安全策略来增强校园网的安全,并详细地阐述了在校园网环境下如何实现该策略以及相关的关键技术。

关键词:网络安全;防火墙;入侵检测系统
中图分类号:TP393.08 **文献标识码**:A **文章编号**:1673-629X(2006)05-0121-04

A Network Security Strategy for Campus Network

FANG Xian-jin, LI Jing-zhao, YAO Ya-feng, CHEN Dai-mei
(Computer Department of Anhui University of Science and Technology, Huainan 232001, China)

Abstract: With the increase of attackers' knowledge and all kinds of attack tools and methods, network security becomes a more and more important issue. Simple firewall strategy is insufficient for network security requirement. In order to further enhance network security, firewall technology and intrusion detection system must be used together. On the other hand, campus network's service platform is based on open source code software generally, so this paper presents a network security strategy to enhance campus network security, which is founded on integration of IPtables-based packet filter firewall, Squid&Socks-based proxy server and network intrusion detection system Snort on Linux OS. Finally, the method of implementing this strategy and the related key technique are discussed in detail on campus network environment.

Key words: network security; firewall; intrusion detection system

0 引 言

根据调查,中国很多高校校园网的网络服务平台都是基于 Linux 开放源代码软件,其体系结构一般具有以下特点:

* 校园网用户访问校外 CERnet/Internet 资源都是通过 Linux 系统下的 Squid Web 缓存代理和 Sock5 代理进行的。

* 对校园网用户的收费通常按照网络流量收费。

* 为了对校园网用户进行收费,使用 Squid 提供代理认证服务。

* 校园网采用 100M/1000M 以太网技术,利用高端具有第三层交换功能的中心交换机连接校园中各建筑物内的子网。

由于学校是一个非赢利性的机构,使用 Linux 操作系统下开放源代码的自由软件作为防火墙是一种普遍采用的网络安全策略[1,2]。

a. 包过滤防火墙软件采用 Linux 操作系统下的 IPtables。

IPtables 是一个功能强大的软件,有可能会成为防火墙的标准,它工作在 OSI 参考模型的网络层和传输层,在新的版本中还提供了日志功能,IPtables 的增强功能还包括增加了二个表 Nat 和 Mangle 及其相应的默认链。

b. 代理服务器使用性能卓越的 Squid 代理 + Socks 代理。

Squid Web 缓存代理的性能几乎是所有代理服务器软件中最好的,它工作在 OSI 参考模型的应用层。但 Squid 只支持下列协议的代理:HTTP, FTP, Secure Sockets Layer(安全套接层,SSL), Wide Area Information Server(广域网信息服务器,WAIS), Gopher。

Squid 不支持使用 UDP 协议的客户端程序,不能用于支持视频会议、新闻组、RealAudio 或视频游戏(如 Quake)的协议,因此为了使校园网用户能使用 Internet 中的 UDP 协议的服务如 QQ、IRC 聊天服务、在线视频服务,需要安装 Socks 代理。

基于 Linux 开放源代码软件的校园网网络架构以及

收稿日期:2005-12-06
基金项目:安徽省高校自然科学基金重点资助项目(2003kj020zd)
作者简介:方贤进(1970-),男,安徽舒城人,讲师,硕士研究生,研究方向为计算机网络、信息安全。

所采用网络安全技术的原理如图 1 所示。

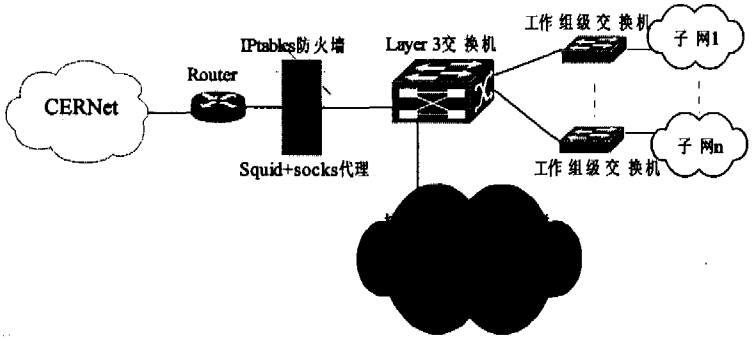

图 1 当前校园网网络架构及网络安全技术原理

校园网系统中,基于 IPtables + Squid + Socks 代理的网络安全策略具有下面的缺点和不足:

(1)防火墙提供了处理进出通信的集中点,因此防火墙无法防御校园网内部用户对 Web,FTP,DNS,MAIL 等服务器发起的攻击,因为按照图 1 中的原理,校园网内部的网络流量并没有经过防火墙。

(2)灵活性和功能性较差。Web 服务器、FTP 服务器、DNS 服务器、MAIL 服务器安装在防火墙后面时必须使用 IPtables 的端口转发或者反向的 NAT 服务。

(3)由于 TCP/IP 的实现,数据包可能会在人们注意不到的地方穿过,而过分严格的过滤策略又会影响校园网用户的正常使用。

(4)虽然 IPtables 防火墙有日志功能,但是系统管理员可能不知道黑客已经攻击了网络,除非仔细监视防火墙日志,但这种方法费时又乏力,而且要借助于第三方程序。

(5)探测和测试防火墙的配置时有很大的困难。利用 IPtables 实现防火墙时需要反复测试 IPtables 规则,另外 IPtables 也不能探测和阻碍黑客的端口扫描行为。

随着攻击者知识的日趋成熟,攻击工具与手法的日趋复杂多样,单纯的防火墙策略已经无法满足网络安全的需要,网络的防卫必须采用一种纵深的、多样的手段。同时,当今的网络环境也变得越来越复杂,各式各样的复杂的设备,需要不断升级、补漏,使得网络管理员的工作不断加重,不经意的疏忽有可能造成重大的安全隐患,在这种情况下,进一步研究校园网的网络安全策略已经非常必要。

1 防火墙 + 入侵检测系统的网络安全策略

1.1 什么是入侵检测系统

入侵检测系统(Intrusion Detection System, IDS)指的是任何有能力检测系统或网络状态改变的系统或系统的集合[3]。IDS 随后能发送警报或采取预先设置好的行动来帮助保护你的网络。

具体说来,入侵检测系统的主要功能有:

(1)监测并分析用户和系统的活动;

(2)核查系统配置和漏洞;

(3)评估系统关键资源和数据文件的完整性;

(4)识别已知的攻击行为;

(5)统计分析异常行为;

(6)操作系统日志管理,并识别违反安全策略的用户活动。

从 IDS 的结构上来看,IDS 可分为基于主机的 IDS(HIDS)和基于网络的 IDS(NIDS)。HIDS 往往以系统日志、应用程序日志等作为数据源,从所在的主机收集信息进行分析,并作为监控程序运行。主机型入侵检测系统保护的一般是自身所在的系统。有名的基于主机的 IDS 是 PortSentry 软件。NIDS 的数据源则是网络上的数据包并加以分析,它工作 OSI - RM 的网络层。在部署 NIDS 时,往往将一台主机的网卡设于混杂模式(promiscuous mode),监听所有本网段内的数据包并进行分析。Linux 操作系统下的 Snort 就是最有名的基于开放源代码的 NIDS。NIDS 的结构一般包括传感器、监视和存储主机、分析器或控制站。

1.2 防火墙与 IDS 的关系

防火墙是保证安全的最基本方式,防火墙可以按照需要来阻断或允许网络通信。IDS 不能充当防火墙的替代品,只能是防火墙的重要补充,其基本功能是监视内部网络的流量,并对识别到的重要攻击特征进行报警。

防火墙是减少扫描威胁的最有效的方式。IDS 可以帮助探测和阻碍主机扫描。但是 IDS 主要是监控内部网络传输,而不能作为防火墙来保护网络。这是因为防火墙作为集中点,能够拦截或允许进出通信。

1.3 采用防火墙 + IDS 的校园网网络安全策略

尽管入侵检测系统没有得到足够的重视和应用,但为了保证校园网的安全,采用防火墙 + IDS 的网络安全技术是最好的策略,因为它不仅可以保护校园免受外界攻击,也可以对校园网内部的网络通信进行检测,并发出警报或采取相应的主动行为。

校园网环境中采用防火墙 + 入侵检测系统的网络安全架构的原理如图 2 所示。

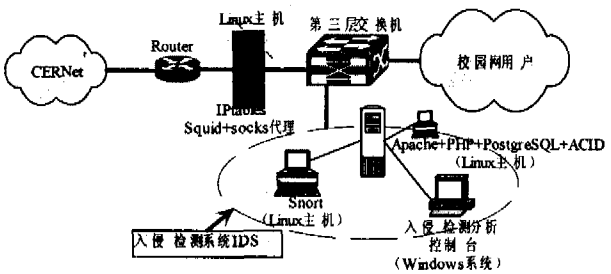

图 2 采用防火墙 + 入侵检测系统的网络安全架构原理

2 防火墙 + IDS 网络安全策略的实现

2.1 文中的模拟实验环境

为了模拟校园网环境中部署防火墙 + IDS 的网络安全策略,建立如图 3 所示的实验环境。

其中主机 A 为 Linux 操作系统,安装入侵检测系统 Snort 及相关的附件,例如 Snort 日志数据到 PostgreSQL

数据库管理系统、入侵检测分析控制台所需的组件 Apache + PHP Web 服务器、入侵检测分析控制台软件 ACID（采用 PHP 技术开发）、PHP 用于连接各种 Web 数据库的库 ADODB Library for PHP4 等。

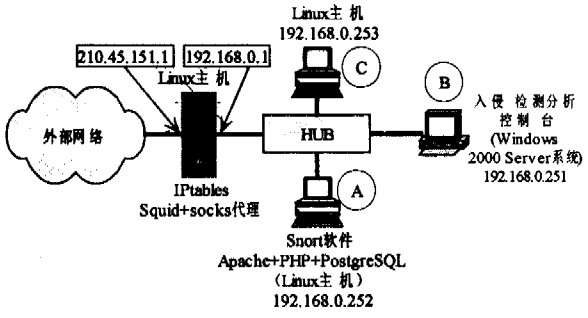

图 3　模拟实验环境

主机 C 是一个完全安装的 Linux 操作系统，不仅安装了各种 Internet 服务器软件，如 FTP，WWW，TELNET，SENDMAIL，DNS Server，X Window，用于模拟被攻击主机，而且还安装了各种 Unix 系统的测试或攻击工具，如端口扫描器 Nmap、包嗅探器 ethereal、攻击工具 Tribe Flood Network 2000、扫描工具 netcat、防火墙探测工具 SendIP、ARP 地址欺骗工具 arpsproof 等，用于模拟攻击主机。

主机 B 安装 Windows 2000 Server 操作系统，并配置 IIS Web Server 用于测试 Unicode 漏洞攻击和缓冲区溢出攻击，并安装了用于测试的黑客程序 IIS5hack.exe。

配备防火墙是为了让 IDS 测试防火墙里面的主机对防火墙的扫描和攻击，例如 SCAN SOCKS Proxy attempt，SCAN Squid Proxy attempt，SCAN Proxy Port 8080 attempt 等。

2.2　防火墙的部署

包过滤和代理服务器防火墙都是采用基于 Linux 操作系统下的开放源代码软件，Linux 主机上应至少安装两块网卡。

(1)安装 IPtables 软件，实现包过滤防火墙的安全策略，建立相应的规则集。IPtables 的安装非常简单，在 RedHat Linux 下既可以采用 RPM 包安装方式，也可以采用编译安装方式。

下面主要介绍如何用 IPtables 工具进行防火墙配置。

＊ 清除所有规则：

```
iptables -F
iptables -t nat -F 清除 NAT 表中的所有规则
```

＊ 重置所有链的默认设置，让所有的链默认都是允许的：

```
iptables -P INPUT ACCEPT
iptables -P OUTPUT ACCEPT
iptables -P FORWARD ACCEPT
iptables -t nat -P PREROUTING ACCEPT
iptables -t nat -P POSTROUTING ACCEPT
```

＊ 校园网内主机的 IP 地址如果不是合法的就应该利用地址伪装成合法的地址。

```
iptables -t nat -A POSTROUTING -j SNAT --to-source 192.168.0.251
```

＊ 如果将 DNS，WEB，MAIL，FTP 等服务器放在防火墙里面，可以利用端口转发机制实现外部网络访问这些服务，其它的服务禁止，如 TELNET。端口转发在网络中的应用也是非常经典的。比如当服务器接收到 80 端口请求以后，将其转到内网 192.168.0.252:80 上，192.168.0.252 再将数据返回给请求连接。

```
iptables -t nat -A PREROUTING -p tcp -m tcp --dport 53 -j DNAT --to-destination 192.168.0.253:53
iptables -t nat -A PREROUTING -p tcp -m tcp --dport 80 -j DNAT --to-destination 192.168.0.252:80
iptables -t nat -A PREROUTING -p tcp -m tcp -dport 21 -j DNAT --to-destination 192.168.0.253:21
```

＊ 如果默认的 INPUT 链是 DROP 就要进行如下设置：

```
iptables -A INPUT -p tcp -dport 53 -i eth0 -j ACCEPT
iptables -A INPUT -p tcp -dport 80 -i eth0 -j ACCEPT
iptables -A INPUT -p tcp -dport 21 -i eth0 -j ACCEPT
```

＊ 对来自外部网络的主机不能访问 1023 以下的内部端口。

```
iptables -A INPUT -i eth0 -p tcp -m tcp --dport 0:1023 -j DROP
iptables -A INPUT -i eth0 -p udp -m tcp --dport 0:1023 -j DROP
```

＊ 拒绝从防火墙的 Internet 接口（eth0）进行的欺骗攻击，并进行日志记录。

```
iptables -A INPUT -i eth0 -s 210.45.151.1 -j LOG
iptables -A INPUT -i eth0 -s 210.45.151.1 -j DROP
```

＊ 拒绝全部从 eth0 进入的 ICMP 通信，即不想防火墙外面的用户能够 ping 到我。

```
iptables -A INPUT -i eth0 -p icmp -j DROP
```

＊ 拒绝从 eth0 进入的 TELNET 登录。

```
iptables -A INPUT -i eth0 -p tcp -dport 23 -j DROP
```

(2)安装 squid Web 代理服务器。

Squid 可以通过 IP 地址、主机名、MAC 地址、用户/密码认证等识别用户，也可以通过域名、域后缀、文件类型、IP 地址、端口、URL 匹配等控制用户的访问，还可以使用时间区间对用户进行管理，所以访问控制是 Squid 配置中的重点[4]。Squid 用 ACL（Access Control List，访问控制列表）对访问类型进行划分，用 http_access deny 或 allow 进行控制。用户/密码认证为 Squid 管理提供了更多便利，最常用的认证方式是 NCSA，该模块需要另外编译安装。

可以采用两种方式安装 Squid Web 缓存代理，但注意的是 Squid 服务器进程使用大于 1023 端口，所以不能以 root 身份运行服务器进程，而应该创建一个普通的用户如 Squid，然后以 Squid 用户运行该服务器进程。对 Squid 进行配置主要是通过配置文件/etc/squid/squid.conf，读者可参阅有关 Squid.conf 的详细的文档。

(3)安装 Socks5 代理服务器。

在 Linux 的发行版当中一般都没有 Socks5 代理服务器软件,所以必须下载最新版的 Socks5 源文件 socks5 - v1.0r11. tgz 进行安装,之后建立配置文件/etc/socks5. conf[4]。

permit——允许任何人使用 socks5 代理,不需要验证;

permit - 192. 168. 0.——限制只让某个 IP 段如 192.168.0.0/24 使用 Socks5 代理;

permit - 192.168.0.10——允许某个 IP 使用 Socks5 代理;

Socks5 还可以使用用户验证机制,需要建立一个/etc/socks5. passwd 文件,读者可查看相关的帮助文档进行设置。

配置好 socks5. conf 文件以后,使用命令 socks5 -t 启动 Socks5 服务器,然后可通过 QQ 或其他软件进行测试。

2.3 Linux 操作系统下 Snort NIDS 的部署

可按照下面的步骤对入侵检测系统 Snort 进行部署[5]。

(1)下载安装 snort - 2.1.3. tar. gz 的编译安装包,通过指定编译时的选项来获得对某一种数据库支持。安装 Snort 的先决条件:

a. 安装库 Libpcap。这是负责捕获网络数据包的库。

b. 安装库 libpcre。pcre(Perl - compatible regular expressions) library 提供了一组函数就像 Perl 那样来实现正则表达式的模式匹配。

c. 一个数据库管理系统。文章中实验环境选用 PostgreSQL- 7.2 版本。为了使 Snort 日志到数据库,安装 PostgreSQL 之后,需要建立 PostgreSQL 数据库用户 Snort。通过执行 create_ postgresql 脚本创建 PostgreSQL 数据库 Snort database。

(2)配置 snort. conf 文件。

* 设置内部网络的网络变量,其值是遵从 RFC 1918 的 IP 地址空间,例如:

```
var HOME_NET [210.45.144.0/24,210.45.145.0/24]
```

或者设置内部网络的 IP 地址空间为任意的。

```
var HOME_NET any
```

* 配置内部网络的服务器列表,这样 Snort 就只检查针对某一种正在运行的服务的攻击。配置方案类似上面的变量 $ HOME_ NET。

```
var DNS_SERVERS $HOME_NET
var SMTP_SERVERS $HOME_NET
var HTTP_SERVERS $HOME_NET
var SQ_SERVERS $HOME_NET
var TELNET_SERVERS $HOME_NET
```

* 配置输出选项,在此说明如何配置使 Snort 输出警报到 PostgreSQL 数据库中。

```
output database: alert, postgresql, user = snort dbname = snort
```

(3)安装和配置入侵检测控制台 ACID。

入侵检测分析控制台(Analysis Console Intrusion Detection, ACID)是一个基于 PHP 技术的分析引擎,用于搜索和处理由各种 IDS、Firewall、网络监视工具生成的存储在数据库中的安全事件,例如它可以搜索和处理 Snort IDS 生成的存储在 PostgreSQL 数据库中安全事件。使用和安装 ACID 的先决条件:

* 一个数据库管理系统用于存储网络事件,目前支持的数据库系统有 MySQL, PostgreSQL, Microsoft SQL Server。文章中实验环境使用的是 PostgreSQL 数据库管理系统。

* Web 脚本语言 PHP4.0.4 或更高版本,这是开发 ACID 的语言。

* 一个支持 PHP 的 Web 服务器,如 Apache、Netscape、IIS。

* 支持 PHP4 的 ADODB 库。由于 PHP 对数据库的访问功能不是很标准,因此建立一个数据库类库来隐藏对不同数据库的访问,使编写的代码可以实现对不同数据库的访问。文中实验环境中使用的是 ADODB Library 4.55 版本。

* 需要入侵检测控制台软件 ACID - 0.9.6b21. tar. gz。

ACID 的主要配置文件是 acid_ conf. php,主要配置参数[1,6]如下:

```
/* 设置 ADODB Library 文件的路径 */
$DBlib_path = "/www/html/acid/adodb";
/* 设置警报数据库的类型 */
$DBtype = "postgres";
/* 设置警报数据库的连接参数
* - $alert_dbname :snort 警报数据库名字
* - $alert_host:数据库存储的主机
* - $alert_port:访问数据库的端口
* - $alert_user:数据库用户名
* - $alert_password:数据库用户的 password
*/ $alert_dbname = "snort";
$alert_host = "localhost";
$alert_port = "5432";
$alert_user = "snort";
$alert_password = "snort";
```

3 结论与展望

防火墙与入侵检测技术的结合是一种应对复杂网络环境下的网络安全策略。IDS 是一种主动保护免受攻击的一种网络安全技术,它作为防火墙的合理补充,入侵检测技术能够帮助系统对付网络攻击,扩展了系统管理员的安全管理能力(包括安全审计、监视、攻击识别和响应),提高了信息安全基础结构的完整性。

但防火墙与入侵检测技术结合的网络安全策略面临很多挑战[3],例如入侵检测系统如何与防火墙很好地交

(下转第 210 页)

这些服务的调用均要首先在注册中心搜索以决定调用的端口和方式。基础架构服务提供支持以上各层功能的消息服务和集成基础设施，主要包括：消息队列、消息转换、消息路由、负载均衡、事件服务、会话服务、名称管理、事务管理、安全管理、日志管理和应用程序接口(API)[5]。元数据存储库存放企业应用集成所涉及到的所有数据元模型、规则等，它是一个存储规则和模式的数据仓库。

3.3 企业应用层

企业应用层是在企业集成层基础之上的各种企业应用，它利用企业集成层所提供的服务接口、通信协议和一些基础架构服务实现了企业各种应用的开发、再利用和重新整合。该层主要包括了现有的一些典型 Web 应用、电子商务应用和企业 Portal 门户等。

3.4 客户访问层

客户访问层对企业应用来讲，其客户分成以下几类：Web 客户、一般服务请求者和动态商业伙伴。它们通过外部交互网关访问企业应用层的典型应用，充当了服务请求者的角色。它们可能会通过各种协议方式(如 HTTP，RMI－IIOP 等)访问企业应用层。基于 Web Services 的企业应用集成模型屏蔽了这些访问细节，在系统内部都是以 SOAP 方式访问调用各种企业服务。

图 1 是基于 Web 服务技术的企业应用集成模型。通过基于 Web 服务的标准服务接口和通用的通信协议(HTTP/SOAP/XML)，企业可以将各类应用封装成 Web 服务后发布到企业的 UDDI 注册中心。对这些服务的调用均要在注册中心搜索以决定调用的端口和方式。若注册中心是私有的，则集成的是企业内部的应用系统。如果注册到公有注册中心，则可以通过 Internet 跨企业间实现应用系统的集成。在图 1 中，应用系统既可以是已有的应用，也可以是新开发的 Web 服务应用。对于遗产系统，首先将它封装成 Web 服务组件，生成描述该系统功能和调用方法的 WSDL 文件，然后生成服务器端基于 SOAP 的服务调用框架，并在此基础上开发适用于已有系统的适配器，或者是通过网关连接这个应用系统，根据网关信息和该应用概要信息生成 WSDL 文件，最后将服务描述文件通过 UDDI API 发布到 UDDI 注册服务器中。

4 总 结

Web 服务技术由于是基于最广为接受的、开放的技术标准，支持服务接口描述和服务处理的分离、服务描述的集中化存储和发布、服务的自动查找和动态绑定以及服务的组合，成为新一代面向服务的应用系统的构建和应用系统集成的基础设施。采用基于 Web 服务的企业应用集成解决方案，能使企业内部的应用集成变得更加简单，同时又使企业间应用集成通过 Internet 实现自动化交互处理成为可能。与传统的企业应用集成方案相比较，它是一种松耦合的集成机制，它为解决企业的“数据孤岛”和“信息孤岛”现象提供了一种很好的解决方案。同时，Web 服务本身也处于发展和成长中，还有相当多的问题没有得到彻底解决，还需进一步的深入研究。

参考文献：

[1] 谢小轩，张 浩，夏敬华，等. 企业应用集成综述[J]. 计算机工程与应用，2002，38(22)：1－5.

[2] 黄双喜，范玉顺，赵大哲，等. 基于 Web 服务的企业应用集成[J]. 计算机集成制造系统－CIMS，2003，9(10)：864－867.

[3] Chung J Y，Lin K J，Mathieu R G. Web Services Computing：Advancing Software Interoperability[J]. IEEE Computer Society，2003，11：35－37.

[4] 柴晓路，梁宇奇. Web Services 技术、架构和应用[M]. 北京：电子工业出版社，2003.

[5] 程春玲，张登银. 基于 EAI 的多层分布式应用与实现[J]. 电子工程师，2004，30(9)：55－58.

(上接第 124 页)

互。文章中使用的 Snort 是一个基于模式串匹配的网络入侵检测系统，但随着校园网速度向 100Mbps 和 1000Mbps 的发展，如何提高 Snort 的性能和检测速度以跟上网络数据的传输速率是值得研究的一个课题。另外 Snort 是属于滥用检测(Misuse detection)的 IDS，滥用检测是基于已知的系统缺陷和入侵模式，故又称基于特征(Signature－Based)的检测。它能够准确地检测到已知特征的攻击，但却过度依赖事先定义好的安全策略，所以无法检测未知的新的攻击行为，从而产生漏报。如何通过其它途径研究入侵检测系统以减少其漏报和误报，提高其安全性和准确度也是值得研究的另一个课题。

参考文献：

[1] Stanger J，Lane P T. Linux 黑客防范开放源代码安全指南[M]. 钟日红，宋建才译. 北京：机械工业出版社，2002. 132－174.

[2] 黄 锋. 校园网防火墙的规划与实现[D]. 合肥：中国科学技术大学，2003.

[3] Northcutt S. 网络入侵检测分析员手册[M]. 余青霓，王晓程译. 北京：人民邮电出版社，2002.

[4] 王虹宇，张福利. Linux 服务器管理员教程[M]. 北京：国防工业出版社，2001. 215－248.

[5] Roesch M，Green C. The Snort Project. Snort™ 2. 1. 3 Users Manual[EB/OL]. http://www. snort. org/docs/snort-manual/2. 4/snort-manual. pdf，2004.

[6] Moulding P. PHP 技术内幕[M]. 北京：中国水利出版社，2003. 108－149.