基于 Linux 系统的 DoS 攻击检测和审计系统①

黄 月，刘卫国

(中南大学 信息科学与工程学院，长沙 410083)

摘 要：在分析传统入侵检测系统不足的基础上，提出了基于 Linux 操作系统的 DoS 攻击检测和审计系统。网络安全检测模块通过统计的方法检测内网发起的 DoS 攻击行为，网络行为规范模块过滤用户对非法网站的访问，网络行为审计模块则记录内网用户的非法行为。实验证明，相比传统的入侵检测系统，该系统能够有效地检测出 DoS 攻击，并能规范网络用户行为和有效审计非法网络行为。

关键词：Linux 系统；入侵检测；拒绝服务攻击；网络行为审计

DoS Attack Testing and Auditing System Based on Linux

HUANG Yue, LIU Wei-Guo

(School of Information Science and Engineering, Central South University, Changsha 410083, China)

Abstract: With analysing the weakness of traditional intrusion detection system, a Linux-based DoS attack testing and auditing system is proposed. The network security detection module is used to detect the DoS attack from intranet, the network behavior regulation module is used to filter the behavior when users access to the illegal websites and the network behavior audit module is used to record the illegal behaviors of intranet users. Experiments show that the system has good performance in detecting DoS attacks, and the system can also regulate and audit illegal behaviors of the network users by contrast with the traditional intrusion detection system.

Key words: Linux system; intrusion detection; DoS attack; network behavior audit

1 引言

伴随网络技术的飞速发展，网络安全问题也日益凸显出来，为越来越多的人所关注。DoS 攻击具有很大的隐蔽性和渗透性，实施简单，攻击成功率高，因此对它的防范具有很大难度[1]；而对于规范内网用户的行为，减少内网用户对网络的不恰当使用，并且对用户在使用网络过程中产生的法律风险可以做到有据可查等等的需求，使得网络行为审计变得越来越重要。

入侵检测系统作为一种积极主动的安全防护技术，由于其可以提供对内部攻击、外部攻击和误操作的实时保护，成为当前研究的热点[2]。但是，传统入侵检测系统也存在以下不足:

(1) 传统的入侵检测系统只是监视系统，告知当前网络的安全状态，起到预警的作用，并不能有效的阻止针对网络的攻击[3]。

(2) DoS 攻击使用的是伪造的源 IP 地址，而传统入侵检测系统只能识别 IP 地址，无法定位 IP 地址，不能识别数据的来源，所以无法有效应对 DoS 攻击。

(3) 传统入侵检测系统一般通过第三方的抓包库将网络数据抓到应用层，然后进行规则匹配。从内核到应用层数据的拷贝增加了系统的负担，在高速网络环境下容易成为系统的瓶颈。

(4) 传统入侵检测系统不能审计被保护网络内部用户的行为，比如防范内网用户的网络攻击行为、禁止用户访问非法网站，在发生类似对网络不恰当使用的网络行为时网络管理人员不能进行有效追查。

为此，本文提出一种基于 Linux 系统、核心工作在内核态、融合了网络安全检测和审计的系统。该系

① 基金项目:国家自然科学基金(61073187)
收稿时间:2010-10-17;收到修改稿时间:2010-11-30

统不仅可以检测 DoS 攻击，而且可以检测内网用户的安全行为和审计内网用户的网络行为。

2　系统结构模型

2.1 模型背景

Linux 内核虽然是一个单片集成内核，但它提供了动态可加载内核模块的接口，通过 insmod 命令可以在内核启动后将用户的功能模块加载到内核空间运行，并且一旦 Linux 功能模块被加载，那么它和普通核心代码都成为内核的一部分，具有和核心代码相同的权限和职责[4]。为此，本文将安全检测功能和网络行为规范功能以 Linux 内核模块的形式来实现，并分别将其命名为网络安全检测模块和网络行为规范模块。

此外，Linux 内核提供了通用可扩展的 netfilter 架构，该架构为每种网络协议（网桥、IPv4 等）定义了一套钩子函数，这些钩子函数在数据包流经协议栈的几个关键点时被调用[5]。其中，基于网桥的 netfilter 架构如图 1 所示。

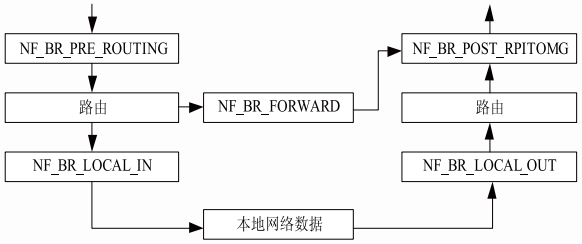

图 1　网桥钩子点描述

网桥 netfileter 架构为用户提供了 NF_BR_PRE_ROUTI- NG 、 NF_BR_LOCAL_IN 、 NF_BR_FO- RWARD、NF_BR_LO- CAL_OUT、NF_BR_POST_ ROUTING 五个钩子点。考虑本文要实现对数据包的透明转发，并不涉及对到达网桥本身数据的操作，网络安全检测模块和网络行为规范模块可以挂在 NF_BR_PRE_ROUTING 、 NF_BR_FORWARD 和 NF_BR_P- OST_ROUTING 三个钩子点之一，本文选择将其挂在 NF_BR_FORWARD 钩子点，即在对网络数据进行转发的过程中进行网络安全检测和网络行为规范。

综合以上 Linux 特性和本文要实现的功能，本文提出的系统结构模型如图 2 所示。

模型由网络安全检测模块、网络行为规范模块、网络行为审计模块和 Web UI 管理模块构成。其中网络安全检测模块检查内网向外网发起的 DoS 攻击，网络行为规范模块检查是否内网用户访问了非法的网站，网络行为审计模块负责将网络安全检测模块和网络行为规范模块产生的安全事件记录到数据库，而网络管理人员则可通过 Web UI 管理模块查询用户产生的安全事件。

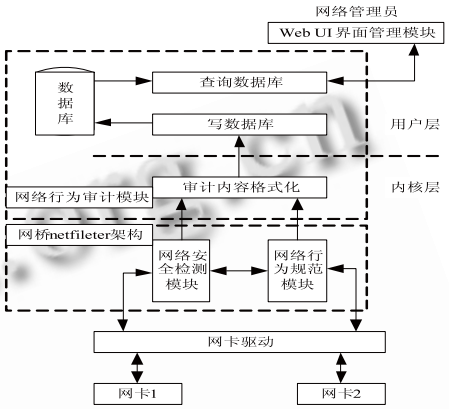

图 2　安全检测和审计模型

为描述模型的工作过程，本文做如下假定：假设网桥设备部署在被管理网络的出口，其中网卡 1 连接内网，网卡 2 连接外网，网卡 1 和网卡 2 构成一组网桥。即从网卡 1 收到的数据将转发给网卡 2，从网卡 2 收到的数据将转发给网卡 1。

由于网卡之间对数据分析处理的流程类似，本文只以网卡 1 向网卡 2 转发数据为例进行阐述。当从网卡 1 收到一数据包时，网卡驱动将数据包交给内核，内核在 netif_receive_skb 函数中将数据交给网桥，网桥通过检查数据的目的 MAC 地址来判定该数据包是需要转发的数据还是到网桥本身的数据，或者是一个多播的数据。文中以转发数据来分析数据的处理流程。转发数据最终会跑到网桥的 NF_BR_FORWARD 钩子点，在该钩子点挂载了网络安全检测模块和网络行为规范模块。对流经的数据包首先会进行安全检测，如果安全检测模块检测到某个安全事件而丢弃该数据包，那么安全检测模块会生成一条拒绝记录并将其交给应用层的写数据库后台程序，由数据库后台程序完成拒绝记录的写操作。如果经过网络安全检测模块没有产生数据丢包，那么该数据会继续网络行为规范模块的过滤。同样，如果该数据违反了网络行为规范模块的某个规则，那么模块会丢弃该数据包并产生丢包记录交给应用层的数据库后台程序。如果经过这两个

模块的检查，数据包都没有被丢弃，那么该数据包将被成功转发给网卡 2。

2.2 网络安全检测模块

本模块主要用来检测从内网向外网发起的 DoS 攻击，其中包括 TCP、UDP、ICMP 小包攻击和 SYN 泛洪。DoS 攻击的特点是攻击主机通过在短时间内和被攻击主机建立大量连接、或者攻击主机通过向被攻击主机发送大量攻击包，从而使得被攻击主机资源耗尽或者使得访问被攻击主机的带宽资源耗尽而造成拒绝服务。根据以上特点，本文通过统计单个主机在单位时间内发送 TCP、UDP、ICMP 数据包的个数以及单个主机单位时间内可以和目标主机特定端口建立的最大 TCP 连接数来检测 DoS 攻击。

2.2.1 小包攻击检测

网络安全检测模块通过建立一个哈希表来统计单个主机在前 1 秒内发送 TCP、UDP 和 ICMP 数据包的个数。对于一个从内网发起的连接，如果它是 TCP、UDP 或者 ICMP 数据，以源 IP 作为散列关键字在哈希表中查找统计该 IP 发送数据包数目的统计结点。统计之前判断当前时间和结点中记录的时间是否超过 1 秒。如果没有超过 1 秒则增加该 IP 的发包计数，如果超过 1 秒则将该 IP 的发包统计计数置为 1，并且将统计时间记录为当前时间。如果在收到某一数据包后该 IP 的发包统计计数达到一定阈值，比如 1024，那么将该结点表示的 IP 标记为 DoS 攻击结点，以后该 IP 发送的数据将被丢弃，丢包记录将交给审计模块进行审计。

2.2.2 SYN 泛洪检测

检测单个主机对某目标主机特定端口 SYN 攻击的方法与小包攻击检测类似，同样采用统计的方法。所不同的是它针对 SYN 包进行检测，在进行散列时使用源 IP、目的 IP 和目的端口。当收到一个从内网发送的 SYN 数据包时，在散列的哈希表中查找与当前数据具有相同源 IP、目的 IP 和目的端口的结点，然后进行计数。如果在过去 1 秒内该主机和该目的主机特定端口建立的 SYN 连接数达到某个阈值，则 SYN 泛洪检测将该结点标记为 DoS 攻击结点，该结点后续的发包将被丢弃并进行审计。

2.3 网络行为规范模块

为规范内网用户的行为，网络行为规范模块通过建立一个禁止用户访问网站的黑名单来过滤用户可以访问的网站。

用户在访问网站之前都需要进行 DNS 解析，从 DNS 解析当中可以准确获取用户将要访问的网站。在本模块中维护了一个禁止用户访问网站的集合，比如反政府类型的网站或者其他不允许用户访问的网站。为加速判断该网站是否在当前的黑名单当中，首先计算每个黑名单 URL 的 MD5 值，然后将所有这些 MD5 值维护在一个递增数组当中。这样，当用户进行 DNS 解析时，可以先计算该 URL 的 MD5 值，再用该值在黑名单数组中进行二分查找。如果某个 DNS 请求中的 URL 匹配了 URL 黑名单，该数据将被丢包。对于被丢弃的数据，同样本模块会交给审计模块进行审计。

2.4 网络行为审计模块

当网络安全检测模块或者网络行为规范模块有内容需要记录时，它会将需要记录的数据进行格式化，其中可以包括源 IP、目的 IP、被丢包的原因等。整个网络行为审计模块的审计过程如图 3 所示。

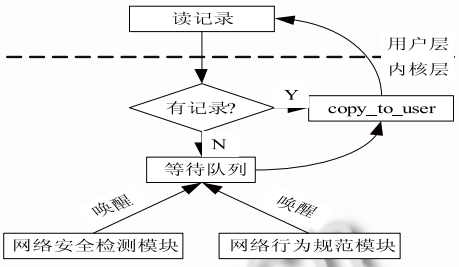

图 3 审计过程

审计工作过程描述如下：应用层的写数据库后台程序通过 ioctl 和内核模块进行通信，当内核模块有数据需要记录时，内核通过 copy_to_user 将数据发送给应用层，由应用层完成数据库的写操作。如果内核没有数据可以提供给应用程序，该应用程序将睡眠在一个等待队列上，一旦网络安全检测模块或者网络行为审计模块有数据需要记录时，它将唤醒该等待队列，然后通过 copy_to_user 将数据交给应用层来完成审计。

2.5 Web UI 管理模块

Web UI 管理模块主要是对数据库中的数据进行处理并为管理员提供图形化的操作界面，它由 Apache 服务器和 Web 浏览器组成。网络管理员可以利用局域网通过 Apache 查询、分析、统计数据库中的数据。比如，网络管理员可以通过浏览器来查询某个用户发起攻击以及访问非法网站的情况。

3　系统在实验室环境中的应用

本实验环境以当前实验室局域网络为基础而搭建，如图 4 所示。

在实验室内部构建 202.197.64.1 网段的局域网，局域网的计算机通过本文的系统跟 Internet 互联，即局域网内所有计算机的通信都透明的穿过本文的系统。实验分为 3 部分，包括小包攻击检测、SYN 泛洪攻击检测和网络行为规范检测以及相对应的结果查询。

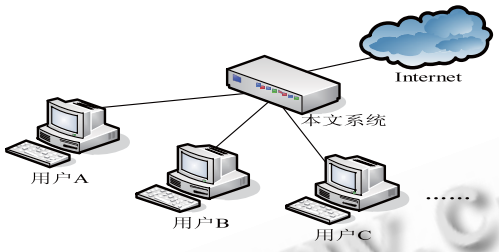

图 4　实验环境

(1) 小包攻击检测

在内网用户 A 使用 Iris 发包工具循环向目标主机 125.71.40.211 发送 TCP、UDP 和 ICMP 三类数据包，在重复发包 2 分钟后，让用户 A 访问任意网站，比如百度，发现访问不了，说明用户 A 访问网站的数据已经被丢弃。通过 Web UI 界面查询用户 A 这段时间的网络行为，如图 5 所示，首先有访问 DoS 而被拒绝的网络攻击行为，然后有访问百度而被拒绝的行为。

	源 IP	目的 IP	源端口	目标端口	拒绝原因	日期
1	192.168.1.12	125.71.40.211	3356	36479	用户因 DoS 攻击被拒绝	2010-11-25　10:56:15
2	192.168.1.12	220.181.6.19	6590	80	用户因 DoS 攻击被拒绝	2010-11-25　11:01:40

图 5　小包 DoS 攻击检测查询结果

(2) SYN 泛洪攻击检测

使用同样的 Iris 发包工在用户 B 上循环发送针对目标主机 125.71.40.211 的 SYN 包，重复连续发送 2 分钟后，通过 Web UI 管理界面查询用户 B 的网络行为，其中包括用户 B 对外网进行 SYN 泛洪攻击的行为，如图 6 所示。

	源 IP	目的 IP	源端口	目标端口	拒绝原因	日期
1	192.168.1.9	125.71.40.211	6341	80	用户因 DoS 攻击被拒绝	2010-11-25　11:18:40

图 6　SYN 泛洪 DoS 攻击检测查询结果

(3) 网络行为规范检测

网络行为规范模块加载时给其下发一个 URL 黑名单，其中包含测试 URL www.dj3344.com。然后在用户 C 主机上通过浏览器 firefox 访问网站 www.dj3344.com。发现访问不成功，再访问不在黑名单中的网站 www.biying.com.cn 则可以成功访问，通过 Web UI 管理界面查询用户 C 的网络访问情况如图 7 所示，从中可以看出包含用户访问 www.dj3344.com 而被拒绝的信息。

	源 IP	目的 IP	源端口	目标端口	拒绝原因	日期
1	192.168.1.19	202.197.38.34	6634	53	用户因 URL 过滤被拒绝	2010-11-25　11:25:15

图 7　URL 过滤查询结果

4　结语

通过实验证明，本文提出的系统不同于传统的入侵检测系统，它部署在被管理网络的出口，可以对违反网络行为的数据直接进行放行或丢弃，从而达到管理网络的目的。另一方面，网络行为审计模块可以对用户的上网行为进行准确记录，在用户产生非法网络行为时可以进行有效的追查。在用户业务逐步向网络转移的趋势下，网络安全检测和行为审计将起到越来越重要的作用。

本文的系统仅提供了对网络安全和行为审计的功能，考虑对内网用户行为的规范和管理，对网络数据的识别及内网用户流量的管理将是下一步需要研究的内容。对网络数据的识别将为用户行为的精细化管理和流量管控奠定坚实的基础。

参考文献

1 闫天杰,彭新光,王玲.DoS 渗透测试平台的设计与实现.太原理工大学学报,2007,38(4):290–293.

2 林果园,曹天杰.入侵检测系统研究综述.计算机应用与软件,2009,26(3):14–17.

3 崔捷.IDS 与 IPS 的分析与对比.网络安全技术与应用,2007,(12):84–85.

4 谢进忠,谢进益.Linux Kernel Module 及 TCP/IP 程序设计.北京:人民邮电出版社,2007.

5 许振文.Linux 下基于 Netfilter 的网络监听器的设计和实现.西安邮电学院学报,2009,14(1):134–136.