基于Snort的军卫一号网络入侵检测和控制系统

No.1 Military Medical Network Intrusion Detection and Control System Based on Snort

王晔，沙琨，王士勇，雷长海
(第二军医大学 网络信息中心，上海 200433)

WANG Ye, SHA Kun,WANG Shi-yong,LEI Chang-hai
(Network Information Center,Second Military Medical University,Shanghai 200433,China)

[摘 要] 本文实现了一种基于开源软件Snort的入侵检测和控制系统，基于安全引擎BASE提供的入侵事件的详细报表，并通过与网络防火墙和核心交换机联动实现实时控制，可以方便医院网络管理者对于军卫一号网络提供完整、方便和自动化的全面防网络入侵控制和保护。

[关键词] 军卫一号；计算机网络安全； 网络防火墙；入侵检测系统
[中图分类号] TP393.08 [文献标志码] B
[文章编号] 1674-1633(2010)08-0042-02

Abstract: This paper presents a network intrusion detection and controlling system which is based on Snort. The system can also provide a detailed graph report about the intrusion events. Cooperating with the network Firewalls and Switches, this system can automatically and instantly control the illegal usage of network.

Key words: No.1 military;computer network safety;network fire wall;intrusion detection system

随着现代社会向信息化、网络化方向快速发展，军卫一号计算机网络安全的日常管理与维护工作已成为当今军队医疗工作一个突出的问题。在传统的安全模型中，网络防火墙作为计算机网络安全的一种防护手段得到了广泛的应用，但随着攻击技术的发展，这种单一的防护手段已经不能确保网络的安全，防火墙对于防范黑客产生了明显的局限性，主要表现为：防火墙无法阻止内部人员所做的攻击 对信息流的控制缺乏灵活性在攻击发生后，利用防火墙保存的信息难以调查和取证。为了确保计算机网络安全，不断有新的安全技术被提出。入侵检测系统IDS(Intrusion Detection Systems)[2]能够帮助网络系统快速发现入侵攻击，并作出响应，扩展了系统管理员的安全管理能力，从而得到快速发展和广泛应用。

入侵检测系统就是依照一定的安全策略，对网络、系统的运行状况进行监视，尽可能发现各种攻击企图、攻击行为或者攻击结果，以保证网络系统资源的机密性、完整性和可用性。它可以通过计算机网络或计算机系统中的若干关键点收集信息并对其进行分析，从中发现网络或系统中是否有违反安全策略的行为和遭到攻击的迹象，同时作出响应。入侵检测作为一种积极主动的安全防护技术，能很好地弥补防火墙的不足。它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、进攻识别和响应），提高了信息安全基础结构的完整性。

收稿日期：2009-05-20
通讯作者：雷长海，副教授，第二军医大学网络信息中心主任。
作者邮箱：wangyee@fudan.edu.cn

1 系统拓扑结构

根据医院军卫一号网络的特点，我们在网络出口处配置入侵监测系统 IDS，对来自外部网和医院局域网内部的各种行为进行实时检测，及时发现各种可能的攻击企图，并采取相应的措施。它的主要作用是：

(1) 监视、分析用户及系统活动；

(2) 审计系统构造和弱点。识别反映已知进攻的活动模式并向相关人士报警；

(3) 统计分析异常行为模式；

(4) 评估重要系统和数据文件的完整性。审计跟踪管理操作系统，并识别用户违反安全策略的行为。

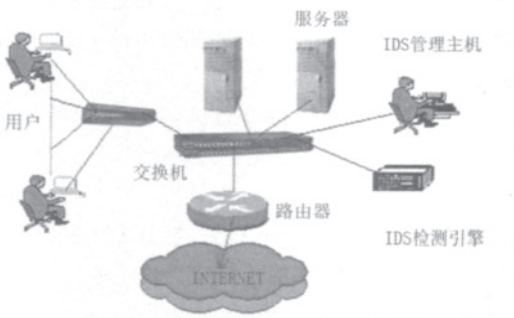

图 1 网络入侵检测系统拓扑结构

入侵检测系统集入侵检测、网络管理和网络监视功能于一身，能实时捕获内外网之间传输的所有数据，利用内置的攻击特征库，使用模式匹配和智能分析的方法，检测网络上发生的入侵行为和异常现象，并在数据库中记录有关事件，

作为网络管理员事后分析的依据；如果情况严重入侵监测系统可以发出实时报警并和核心交换与防火墙系统联动，使得医院网络管理人员能够及时采取应对措施。系统的拓扑结构如图 1 所示：

2 Snort部署

入侵检测系统基本可以分为两大类：基于特征的入侵检测系统和异常行为检测系统。入侵者常具有用软件可以检测到的特征，如病毒。入侵检测系统将检测包含已知入侵行为特征或者异常于 IP 协议的数据包。基于一系列的特征及规则，入侵检测系统能够发现并记录可疑行为并产生报警。基于异常的入侵检测系统通常是分析数据包中协议头部的异常，在某些情况下这种方式要比基于特征的入侵检测系统更好一些。通常情况下，入侵检测系统在网络上捕获数据包与规则比对或者检测其中的异常。我们使用的 Snort[1] 是一个开放源码的网络入侵检测系统（NIDS），用于分析 IP 数据包登录(packet logging),可以免费得到。NIDS 是用来检测网络上的信息流的入侵检测系统。Snort 上是一个基于规则的 IDS，但是 Input 插件可以分析协议头部异常 [3]。Snort 除了能够进行协议分析、内容搜索和包含其它许多预处理程序，还可以检测上千种蠕虫病毒、漏洞、端口扫描以及其它可疑行为检测。Snort 使用一种简单的基于规则的语言来描述网络通讯，判断对于网络数据是放行还是拦截，其检测引擎是模块化的。

Snort 在逻辑上可以分成多个部件，这些部件共同工作，来检测特定的功绩，并产生符合特定要求的输出格式。一个基于 Snort 的 IDS 包含下面的主要部件：包解码器、预处理器、探测引擎、日志和告警系统、输出模块。

我们在军卫一号网络出口交换机的端口上配置了端口镜像用于监控所有外部网络数据流，然后在双网卡的 Windows2003 服务器上安装了 Snort 系统，将服务器的一张网卡设置成混合模式，用于接收镜像端口的数据流。此外我们在服务器上安装了 MySql Server 存储 Snort 抓取的数据，用于后期的入侵报表和分析。

3 入侵事件报表

结合基本分析和安全引擎（BASE）Web GUI，Snort 可以生成图形界面的入侵事件详细报表。Snort 经过配置、登录到 MySQL 后，BASE 就能获取警报触发器的报告，并且根据源地或目的地 IP 地址、TCP 或 UDP 端口号以及警报类型，显示流量的异常情况。另外，如果在网络上多个部位布有多个 Snort 探测器，那么它们都能登录到同一个数据库，BASE 就能综合任何一个或所有这些探测器的监测结果来生成报告。

4 网络系统联动

用 Snort 和 Base 我们可以采集并查看网络中的异常入侵事件，但是网络中入侵事件发生非常频繁，全部由医院信息系统管理员人工察看很难做到即时反应，将网络危险及时化解。因此设计一个与网络防火墙和交换机联动 [4-6] 的入侵控制系统是非常必要的。

我们设计了一个 Windows Service 手动定时启动 Snort 抓包模块，定时分析产生的日志信息，对于在一定时间段内反复出现的网络入侵事件，我们将记录源地址和目的地址。同时我们基于 TcpClient 实现了一个自动 Telnet 登录网络防火墙和三层主交换机的模块，发生入侵事件时我们的入侵控制系统将自动登录防火墙和主交换机，采用 ACL（访问控制列表）的方式屏蔽源地址和目的地址对于该网络端口的通信，从而达到实时对入侵事件做出反应的要求。

此外，我们设置了黑名单的机制，如果某些 IP 频繁发起网络入侵事件而被系统屏蔽，那么系统将自动将这些 IP 加入黑名单，在网络防火墙和三层交换机上使用 ACL 屏蔽所有这些黑名单 IP 的通信。

由于 Snort 对邮件病毒也会产生报警，会导致系统将很多邮件服务器的 IP 加入黑名单，从而导致邮件无法正常接受，一般而言我们将邮件病毒过滤的工作交给邮件过滤网关，因此我们设立了白名单机制，将一些已知的邮件服务器 IP 加入白名单，确保不被系统屏蔽。

图 2 是我们系统对于当前自动屏蔽 IP 的报表，并列出了详细的屏蔽原因。

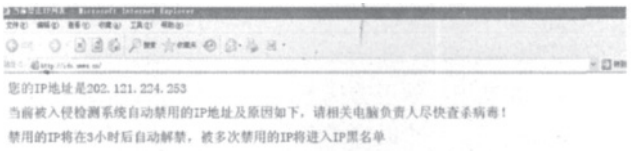

图 2 与防火墙联动自动屏蔽的IP列表

5 结论

本文实现了一种基于开源软件 Snort 的入侵检测系统，基于 BASE 提供了入侵事件的详细报表，并通过与网络防火墙和核心交换机联动实现实时控制，可以方便医院网络管理者对于军卫一号网络提供完整、方便和自动化的全面防网络入侵控制和保护。

[参考文献]

[1] 孙振龙,等.基于数据挖掘技术的Snort入侵检测系统的研究[J].微计算机信息,2006(33): 212-214.

[2] 陈汝伟,等.融合多种技术的网络入侵检测系统[J].网络安全技术与应用,2008(11):27-29.

[3] 赵旭,王长山.Snort入侵检测系统的改进[J].西安工程科技学院学报,2007,21(6):859-863.

[4] 章胜南.医院计算机网络系统的安全与维护[J].中国医疗设备,2008(5):34-35.

[5] 张蔚.联动式网络入侵防御系统的研究[J].通信管理与技术,2008(3):43-46.

[6] 张中辉,等.基于联动机制的入侵防御系统[J].计算机时代,2006(7):28-30.