基于网络的入侵检测系统的研究及实现

肖竟华，卢 娜
（武汉科技大学 计算机科学与技术学院，湖北 武汉 430081）

摘 要：随着网络技术的发展，保护信息以及网络的安全变得越来越重要。文中归纳了入侵检测系统的结构和类别，并提出了一个基于网络的入侵检测系统的设计思想。该系统在 Linux 操作系统下以 Snort 为内核，MySQL 作为后台数据库，用 PHP 开发实现。最后分析了该系统的可以改进的方面以及网络入侵检测目前面临的问题。

关键词：入侵检测系统；Snort；MySQL
中图分类号：TP393.08 **文献标识码**：A **文章编号**：1673－629X(2007)02－0242－03

The Study and Implementation of NIDS

XIAO Jing-hua，LU Na
（Computer School，Wuhan University of Science and Technology，Wuhan 430081，China）

Abstract：With the development of network technology，to protect the security of the information and network become more and more important. In this paper，conclude the architecture and classifications of IDS. Then proposed an implementation of a NIDS which is developed on the base of Linux operating system. Use Snort as kernel，MySQL as database，and PHP as program language. At the end of the paper，analyze defects and the possible improvement of the NIDS，also the problems that NIDS is now being facing with.

Key words：intrusion detection system；Snort；MySQL

0 引 言

最初，入侵检测的概念是由 Anderson 于 1980 年提出的。入侵检测是通过从计算机网络或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入侵的迹象的一种安全技术[1]。将入侵检测的软硬件组合起来便是入侵检测系统（Intrusion Detection System，IDS）。它包含了 3 个功能部件：

1）信息收集；

2）信息分析；

3）结果处理。

入侵检测的第一步是信息收集，收集内容包括系统、网络、数据及用户活动的状态和行为。它需要在计算机网络系统中的若干不同关键点（不同网段和不同主机）收集信息。第二步是信息分析，又可分为模式匹配、统计分析、完整性分析，其中完整性分析往往用于事后分析。最后进行结果处理。

对于入侵检测系统分类，从数据分析手段看，通常可以分为两类：滥用（Misuse）入侵检测和异常（Anomaly）入侵检测。前者主要利用特征集合或者对应的规则集合进行特征匹配或者规则匹配，如果发现满足条件匹配，则指示发生了一次攻击行为，是基于知识的检测。后者通常会建立一个关于系统正常活动的状态模型并不断进行更新，如果发现超过设定阈值的差异程度，则指示发现了非法攻击行为，是基于行为的检测。

从数据来源来看，入侵检测目前可以分为 3 类：基于主机的入侵检测（HIDS）、基于网络的入侵检测（NIDS）和分布式入侵检测（NDIS）。

基于网络的入侵检测系统是由遍及网络的传感器（Sensor）组成，传感器使用原始的网络分组数据包进行攻击分析，并能够自动向中央控制台报告。其优势在于：

（1）成本低，不占用主机资源；

（2）攻击者转移证据很困难；

（3）能够检测未成功的攻击企图；

（4）实时检测，一旦发现恶意访问或攻击可以随时发现；

（5）独立于主机的操作系统类型，一般没有移植性问题。

基于网络入侵检测有实时检测的要求，算法应拥

收稿日期：2006－05－23
作者简介：肖竟华（1955－），女，湖北武汉人，副教授，硕士生导师，研究方向为系统软件开发、操作系统、信息安全。

有高效、易于扩充的特点[2]。文中在 Linux 操作系统下以 Snort 为内核,MySQL[3]作为后台数据库,用 PHP 开发出一套基于网络的入侵检测系统。

1　基于网络的入侵检测系统的实现

1.1　系统结构设计

由于目前该入侵检测系统偏重于检测分析功能,即着重为网络管理员提供用于分析统计检测到的网络攻击相关信息并提取相应结果进行电子取证,因此分为两个模块:入侵检测模块和查询管理模块。在这里,需要说明由于把 Snort 作为 NIDS 使用,在硬件要求方面需要两块网卡,一块用于正常的网络通信,另一块用于监听(通常成为探测器)。另外,对于磁盘空间的要求和 CPU 速度较高[4]。其系统结构图如图 1 所示。

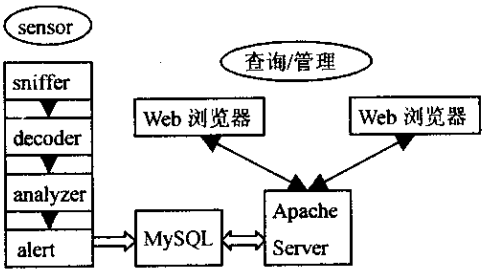

图 1　系统结构

其中入侵检测模块通过将探测器设置为混杂模式并利用 Libpcap 监听主干网,并将捕获的入侵事件写入 MySQL 数据库,主要功能为提供分析统计数据,并为计算机取证提供原始证据。

查询管理模块主要是对以上数据库中数据进行处理并为管理员提供图形化界面操作,它由 Apache 和 Web 浏览器组成。用户可以通过局域网查询、分析、统计 MySQL 数据库中的数据。

1.2　系统结构设计

1.2.1　入侵检测模块

该模块分为 4 个组件:

1) 包捕获/解码引擎;

2) 预处理插件;

3) 检测引擎;

4) 输出报警。

其工作流程如下:第一步是捕包装置,在包被以原始状态捕获后,送给包解码器。包解码器将特殊协议翻译为内部数据结构。在最初的捕包和解码完成后,由预处理程序处理流量。许多插入式预处理程序对包进行检测或操作后将它们交给下一个组件:检测引擎。检测引擎对每个包的一个方面进行简单的检测以检测入侵。最后一个组件是输出组件,它对可疑行为产生警报。

包捕获和解码的功能为捕获网络的传输数据并按照 TCP/IP 协议的不同层次将报文进行解析。Snort 利用一个外部捕包程序库 Libpcap 抓包。该库函数可以为应用程序提供直接从链路层捕获报文的接口函数,并可以设置报文的过滤器捕获指定的数据。具体来说包捕获和解码过程为:首先 Libpcap 捕获数据帧,然后根据预先定义的过滤规则从网络上获取监听子网上的报文,进行 TCP/IP 栈由下至上的处理过程,主要进行 IP 重组和 TCP/UDP 协议层分层协议处理,最后进行应用层协议分析。

检测引擎是整个模块的关键部分,主要是将数据包和组织好的检测规则进行比较。它可以分为两个部分:

(1) 规则建立/翻译;

(2) 基于规则的检测引擎。

规则由规则头和规则体组成。其中规则头包括规则动作选项(本系统只采用 Alert 选项)、协议、IP 源/目的地址和源/目的端口等信息。而规则体则由分析数据包内容(Content)选项、TCP/ICMP/IP 选项集合以及规则识别选项集合等组成。举一个归属于 Attack-R 的实例:alert tcp $HTTP_SERVERS $HTTP_PORTS→ $EXTERNAL_NET any(msg:"ATTACK RESPONSES http dir listing";content:"Volume Serial Number";flow:from_server,established;classtype:bad-unknown;sid:1292;rev:4;)。该规则表达意义是对 $HTTP_SERVERS $HTTP_PORTS 到 $EXTERNAL_NET 任意端口,从服务器返回的已建立的 TCP 连接或会话中的包进行报警,检测引擎应该匹配含有 Volume Serial Number 的包,报警显示有人正在使用 http 浏览服务器的磁盘目录信息,攻击类型为畸形流量,Snort ID=1292,版本号 4。在处理这些规则文件时,采用一个二维链表来存储它们以便和后面将要到来的数据包进行匹配。链表头(Chain Heads)包含源/目的 IP 地址以及端口这些普通信息,链表选项(chain options)定义更为详细的信息,如 TCP 标志、ICMP 代码类型、特定的内容类型、负载容量等。检测引擎对进来的包依次分析,与数据包中数据匹配的第一条规则触发在规则定义中指定的动作。凡是与规则不匹配的数据包都被丢弃。检测引擎中关键部分是 plugin 插件,如端口扫描等。

1.2.2　查询管理模块

该模块提供 Web 浏览器和存储数据的数据库之间的接口,用于数据浏览和分析。主要功能如下:

1) 用于数据库搜索和查询接口。用户可以通过网络特定的参数,如时间、日期等进行数据库搜索。

2) 数据包浏览器,能够从日志的数据包解码并显示第三层和第四层的信息。

3) 根据指定的参数生成饼图和条状图,并统计数据。

在这一模块中涉及大量的数据库操作。概括起来有以下 3 个主要部分:

* 连接数据库。

```
$ db = mysql_ connect (" localhost "," root "," lusnort ") ;
mysql_ select_ db(" mydb ", $ db) ;
```

* 查询数据库。

```
$ temp_ sql =" SELECT DISTINCT layer4_ sport, COUNT(event. cid) ".
" FROM event ". $ criteria[0] .
" WHERE ". $ criteria [1] ." AND layer4_ sport is NOT NULL ".
" GROUP BY layer4_ sport ORDER BY layer4_ sport ";
$ result = mysql_ query( $ temp_ sql, $ db) ;
```

* 按照需要取回数据的两种方式。

```
a. $ myrow = mysql_ fetch_ row( $ result)) ;// * 结果按数组下标取回:$ myrow[i] ;
b. $ myrow = mysql_ fetch_ array( $ result) ;// * 结果按字段取回:$ myrow[" 字段名 "] ;
```

另外,在该模块中提供绘图功能,可以在网页中通过设定特定的参数,绘制统计图 style[pie | bar]。绘图步骤:

(1) 创建基本 PS 对象(假设为 $ image),填充背景,以后的全部 PS 操作都是基于这个背景图像的;

(2) 在 $ image 上作图;

(3) 输出这个图像。

以饼图为例,其设计思想是:首先以用 imagecreate()来生成一个空白图形,然后在空白图形中用 imagearc()圆弧函数先画圆弧,再画两条线连接圆心和圆弧端点,再用 imagefilltoborder 函数来填充扇形。

2 结束语

从网络安全多层次的防御的角度出发,入侵检测已经受到越来越多的关注,入侵检测技术也有了长足的发展。然而,入侵检测依然面临着许多问题:随着能力的提高,入侵者会研制更多的攻击工具,使用更为复杂精致的攻击手段;攻击者采用加密手段传输攻击信息;入侵检测系统自身的安全性也面临考验;过高的错报率和误报率;日益增长的网络流量导致检测分析难度加大,高速的网络环境导致很难对所有数据进行高效实时分析;响应单元的具体职能的定义和实现方法还不完善等[5]。

文中提出了一个以 Snort 为内核的轻量型入侵检测系统。Snort 采用 Libpcap 捕包,但这并不是最有效的方法。因为它一次只能处理一个包,成了制约入侵检测对高带宽(1 Gbit/s)网络进行监控的瓶颈。将来打算加载捕包模块到 Linux,使其内核本身进行捕包。同时,该系统没有提供网络设备联动,而仅仅是对入侵事件统计分析。这一方面也有待完善。

参考文献:

[1] 蒋国春,冯登国. 网络入侵检测原理与技术[M]. 北京:国防工业出版社,2001.

[2] 刘 武,段海新,杨 路,等. 基于 Web 的网络入侵检测取证系统的设计与实现[J]. 计算机应用,2003,23(5):50 - 52.

[3] DuBois P. MySQL 网络数据库指南[M]. 北京:机械工业出版社,2000.

[4] Koziol J. Snort 入侵检测实用解决方案[M]. 北京:机械工业出版社,2005.

[5] 俞晓雯,高 强,丁 杰. 一种入侵检测取证系统模型的设计[J]. 微机发展,2004,14(8):117 - 119.

(上接第 241 页)

择相应协议分析器和规则集,减少了需要匹配规则数。通过这些方法,拓宽了模式匹配模块的瓶颈,达到了提高检测效率和准确性的目的。

参考文献:

[1] 斯海飞,赵国庆. 入侵检测技术分析概述[J]. 电子对抗技术,2002,17(2):31 - 34.

[2] 宋劲松. 网络入侵检测——分析发现和报告攻击[M]. 北京:国防工业出版社,2004:77 - 94.

[3] Stevens W R. TCP/IP 详解(卷一:协议)[M]. 范建华等译. 北京:机械工业出版社,2002.

[4] 刘学波,孟丽荣. 高速网络环境下的网络入侵检测系统的研究[J]. 计算机工程与设计,2005,26(5):1236 - 1238.

[5] 侯方明,李大兴. 一种新的基于协议树的入侵检测系统的设计[J]. 计算机应用研究,2005,22(7):150 - 152.

[6] 罗桂琼. 基于协议分析的入侵检测系统[J]. 电脑与信息技术,2005,13(4):56 - 59.