一种基于 SNORT 的入侵防御系统

Introduction of An IPS based on SNORT

潘 玲 黄云森 张 凡 （深圳大学现代教育技术与信息中心 518060）

摘要：网络安全无疑是目前网络研究的热点，本文阐述了在安全领域单纯的防火墙和入侵检测系统存在的缺陷，指出了入侵检测系统的发展方向，并介绍了一种将防火墙技术和入侵检测系统相结合的防御系统，该系统对于主机和网络的安全能有效的防护。

关键词：入侵检测系统 入侵防御系统防火墙 CIDF 模型

1 IDS 系统研究

随着网络应用的不断普及和网络技术的不断发展，网络安全故障不断出现，使得网络安全越来越受到网络管理人员和广大用户的重视，随之而来的是安全技术和安全产品的不断发展，包括防火墙、入侵检测系统等等。所谓入侵检测是对入侵行为的发现，包括主机入侵检测（HIDS）和网络入侵检测（NIDS）。它通过对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被攻击的迹象。与其他安全产品不同的是，入侵检测系统需要更多的智能，它必须可以将得到的数据进行分析，并得出有用的结果。入侵检测系统是对传统安全产品的合理补充，它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。

目前的入侵检测系统大部分是基于各自的需求和设计独立开发的，不同系统之间缺乏互操作性和互用性，这对入侵检测系统的发展造成了障碍，因此美国国防部高级研究计划局（DARPA）在 1997 年 3 月开始着手公共入侵检测框架 CIDF（Common Intrusion Detection Framework）标准的制定[1]。

CIDF 阐述了一个入侵检测系统的通用模型，是当前 IDS 的典型结构。它将入侵检测系统分为 4 个组件，如图 1 所示：事件产生器（Event generators）、事件分析器（Event analyzers）、响应单元（Response units）、事件数据库（Event databases）。事件产生器的目的是从整个计算环境中获得事件，并向系统的其他部分提供此事件。事件分析器分析所得到的数据，并产生分析结果。响应单元则是对分析结果做出响应的功能单元，它可以做出切断连接、改变文件属性等强烈反应，也可以只是简单报警或日志记录。事件数据库是存放各种中间和最终数据的地方的统称，它可以是复杂的数据库，也可以是简单的文本文件。各组件之间的通信格式为 CISL（Common Intrusion Specifation Language）。

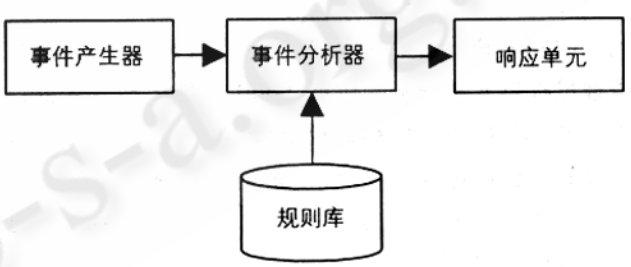

图 1 CIDF 模型

入侵检测系统能实时检测到网络上的入侵行为，并能实时记录该行为，但作为一个网络安全产品，其缺陷也是显而易见的：它只能被动地检测网络遭到了何种攻击，并以日志形式记录下来供管理人员分析，而它的阻断攻击能力非常有限，不能及时的发现攻击并阻断攻击，所以对网络的防御保护有限，只能给管理员提供事后的分析。而防火墙作为访问控制产品，它可以基于 IP 地址或端口号对进出网络的数据包过滤，从而对内部网络提供一定的保护，而且目前的防火墙可以提供网络地址转换、服务代理、流量统计等功能，甚至

有的防火墙还能提供 VPN 功能。但防火墙的访问控制粒度比较粗,它主要基于 TCP/IP 协议的过滤方面表现出色,对于应用级攻击不具备阻止能力。从功能上看,单纯的 IDS 系统和单纯的防火墙系统都不能对日益严峻的网络攻击及时有效的做出反映、保护网络和系统的正常运行。应用需要一种有效的能防御攻击的系统,能够主动的、积极的抵御入侵:当它检测到攻击对网络或系统的攻击企图后,它会自动地将攻击包丢掉或采取措施将攻击源阻断。这正是日益复杂的网络和主机系统在安全方面所亟需的功能。

2 基于 Snort 的入侵防御系统

Snort[2]是目前使用最广泛的开放源代码入侵检测系统,它可以实时记录 IP 包的内容并进行流量分析。其分析方式包括协议分析、内容查找及匹配,能用来探测多种攻击和嗅探(如缓冲区溢出、端口扫描、CGI 攻击、SMB 探测等等)。Snort 同样的也是遵循 CIDF 模型,它主要包括数据包捕获和解析子系统、入侵检测模块以及日志及报警子系统。其中数据包捕获子系统利用从 libpcap 库函数,从网络采集数据包,并按照 TCP/IP 协议的不同层次将数据包解析,以构成分析模块的数据基础;日志和报警子系统则是在检测到入侵行为的同时将其进行及时的日志记录及报警,从而为网络管理员提供入侵分析的依据,Snort 支持多种形式的日志记录,可以是文本、XML、libpcap 格式,也可以把信息记录到 syslog 或者数据库中;Snort 中的入侵检测模块则是整个系统的核心,它负责对网络数据进行分析,以发现入侵企图和行为。

从检测模式上来看,Snort 采用基于模式匹配的检测技术,即针对每一种入侵行为,都提炼出它的特征,并按照 Snort 的规则描述语言[3]写成规则,从而形成一个规则数据库。然后将捕获的数据包按照一定的算法和规则库中的规则进行匹配,若匹配成功,则认为该入侵行为成立,并进行相应的响应动作。由于其开发源代码,可以方便的对其进行修改和定制,使其能与 Linux 上原有的防火墙 iptables 系统联动,使得 Snort 在检测到网络攻击的情况下,可以对攻击包进行丢弃或拒绝等操作,而不是简单的报警或日志记录,从而可以对外界的随机进攻及时做出响应,保护系统的正常运行。

2.1 工作原理

整个系统由 iptables 和 snor_inline 两个模块构成,如图 2 所示,iptables 负责包过滤功能,snort_inline 则完成入侵检测功能。当 iptables 接收发送到系统的数据包后,不是将包与过滤规则相匹配,而是将数据包从系统数据区放到用户数据区,供 snort_inline 对包进行入侵检测分析,snort_inline 根据入侵规则库所描述的入侵行为,对数据包进行模式匹配,如果发现数据包与规则库中某种入侵行为匹配,则按照该规则选项定义的行为,返回 drop 或 reset 等处理结果给 iptables,并以日志的形式记录下入侵行为,iptables 接收到处理结果后,就能自动的丢弃该包;如该数据包未能与任何规则匹配上,则 snort_inline 返回 pass 结果给 iptables,iptables 就会允许该包的通过。

由于 snort 的轻量级、功能强大、能快速检测网络攻击等特征,而 iptables 能根据分析结果对包进行相应的过滤,使得该系统具备很强的入侵防御功能。同时 snort 的入侵规则定义语言简单、高效,能及时根据网络的需要和新入侵手段的变换来编写和调整规则库,使得系统具备很强的扩展行和入侵检测的及时有效性。

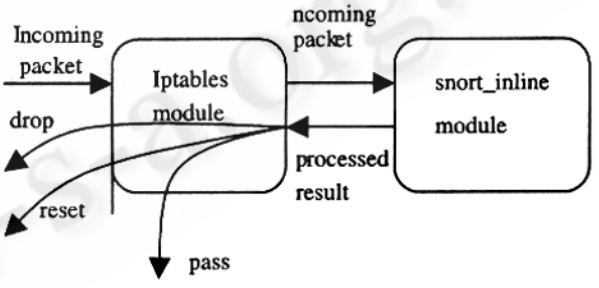

图 2　系统原理图

2.2 工作流程

由于要与防火墙 iptables 联动,Snort_inline 对数据包的采集不再使用 libcap 库函数,而是采用 libipq 库从系统核心队列中获得进出系统的数据包。该入侵防御系统具体的工作流程如图 3 所示。

(1) 当系统接收到一个 IP 包后,且系统配置 iptables 以 QUEUE 方式工作,iptables 将该包从核心协议栈放到核心模块 ip_queue 的队列中,以供用户的应用来处理该包。

(2) 这时,等待数据的 Snort_inline 将通过 libiqp

的接口函数 ipq_read( ) 获取该 IP 包。

ables 和经典的入侵检测系统 Snort 相结合来实现的，

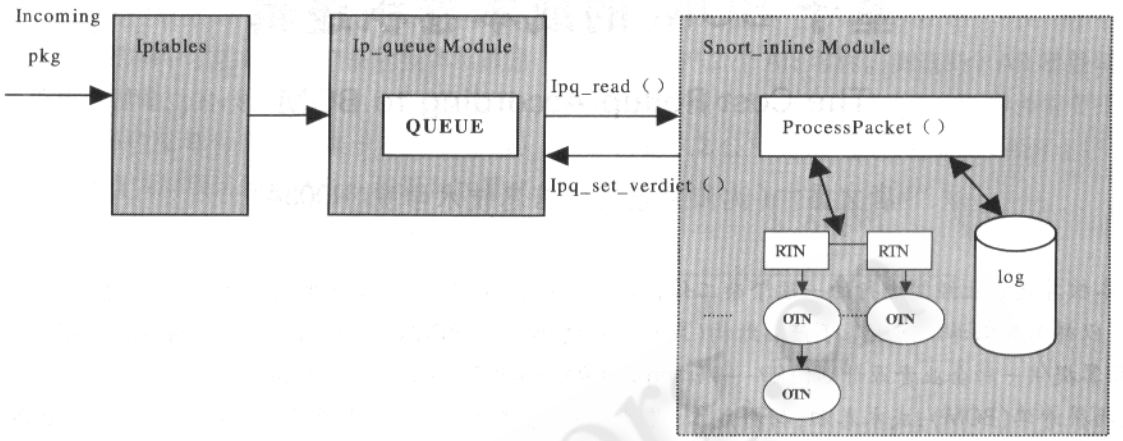

图 3　入侵防御系统工作示意图

(3) Snort_inline 包处理函数将对该数据包进行入侵检测：根据数据包的类型，查找遍历相应的规则树，对该包进行模式匹配，来确定该包是攻击包还是正常数据包，系统是该 pass 或 drop 或 sdrop 或是 reject 该包。并进行相应的日志记录。

(4) snort_inline 通过 Ipq_set_verdict( ) 调用将入侵检测的处理结果返回给 ip_queue。

(5) ip_queue 通知 iptables 对该包的处理结果。

(6) Iptables 通过该结果来过滤该包或者允许该包通过系统。

每个进入系统的数据包经过上述流程的处理，使得具备入侵企图或正在进行入侵行为的包被系统识别并且丢弃，而正常的数据包则得以通过系统到达目的地，从而使得系统具备主动的入侵防御能力，能及时处理攻击行为，从而保护系统或网络的正常运行。

这个 IPS 系统可直接安装配置在网络主机上，对主机进行安全防护；同时也可以应用在网关或网桥系统上，对进出网络的数据包进行监控，从而保护整个网络的安全。

3　结束语

本文分析了传统的防火墙和入侵检测系统在安全防护中存在的问题，提出了网络安全防护系统的趋势是联动的入侵防御系统，并介绍了一种代码简洁、高效的入侵防御系统，该系统是由成熟的包过滤防火墙 ipt-

因而同时具备了这两个系统的优点。

参考文献

1　杨沛、文贵华、丁月华，基于自治 Agent 的分布式入侵检测系统[J]，华南理工大学学报，2002，30(3)：1-4。

2　http://www.snort.org/[EB/OL]，2003-11.

3　Martin Roesch，Chris Green. Snort Users Manual. http://www.snort.org/docs/writing_rules/ [EB/OL].