netfilter技术分析及在入侵响应中的应用

甘迎辉[1]，刘 勇[2]，秦志光[2]

(1. 成都三零盛安信息系统有限公司 成都 610041; 2. 电子科技大学计算机科学与工程学院 成都 610054)

【摘要】从netfilter总体结构入手，分析了netfilter的连线跟踪、包过滤、地址转换、包处理等关键技术。在此基础上，研究了入侵响应策略，提出了基于netfilter的主动响应模型。经测试证明，这种主动响应模型灵活高效，可以极大地增强系统对入侵行为的防御能力。

关 键 词 连线跟踪; 入侵响应; 主动响应; 入侵行为重定向

中图分类号 TP309 文献标识码 A

An Analysis of Netfilter and Its Implementation in Active Response

GAN Ying-hui[1]，LIU Yong[2]，QIN Zhi-guang[2]

(1. 30 SAN Information System Co., Ltd. Chengdu 610041; 2. School of Computer Science and Engineering, UEST of China Chengdu 610054)

Abstract Netfilter is the framework inside the Linux 2.4.x kernel which enables packet filtering, network address translation (NAT) and other packet mangling. This paper begins with introduction to the framework of netfilter, and some key technology, such as the connection tracking, packet filtering, network address translation, and packet mangling are analyzes in detail. In addition, the strategy of response to intrusion is researched in this paper, and an active response model based on netfilter is given. Through the test proofed, the model could efficiently strengthen the system security.

Key words connection tracking; response to intrusion; active response; intrusion redirect

当前，网络攻击技术和攻击工具表现出攻击速度加快和攻击工具自动化的新趋势，工具越来越复杂，系统脆弱性探测速度加快，对防火墙的渗透显著增多，针对网络基础设施的攻击不断增加。针对攻击，要求动态地调整安全策略，自动做出反应。netfilter是Linux内核中用于扩展各种网络服务的结构化底层框架，新的响应特性加入到内核中并不需要重新启动内核。netfilter模块的易扩性，为实现动态安全策略提供了很好的基础。

1 netfilter技术分析

netfilter是由Rusty Russell提出的Linux 2.4内核防火墙框架，该框架既简洁又灵活，可实现安全策略应用中的许多功能，如数据包过滤、数据包处理、地址伪装、透明代理、动态网络地址转换(Network Address Translation，NAT)，以及基于用户及媒体访问控制(Media Access Control，MAC)地址的过滤和基于状态的过滤、包速率限制等。

1.1 netfilter框架

netfilter提供了一个抽象、通用化的框架[1]，作为中间件，为每种网络协议(IPv4、IPv6等)定义一套钩子函数。Ipv4定义了5个钩子函数，这些钩子函数在数据报流过协议栈的5个关键点被调用，也就是说，IPv4

收稿日期：2003 – 02 – 28
基金项目：国家863计划资助项目(2002AA142040)
作者简介：甘迎辉(1971 –)，男，硕士，主要从事网络安全方面的研究.

协议栈上定义了5个“允许垂钓点”。在每一个“垂钓点”，都可以让netfilter放置一个“鱼钩”，把经过的网络包(Packet)钓上来，与相应的规则链进行比较，并根据审查的结果，决定包的下一步命运，即是被原封不动地放回IPv4协议栈，继续向上层递交；还是经过一些修改，再放回网络；或者干脆丢弃掉。

Ipv4中的一个数据包通过netfilter系统的过程如图1所示。

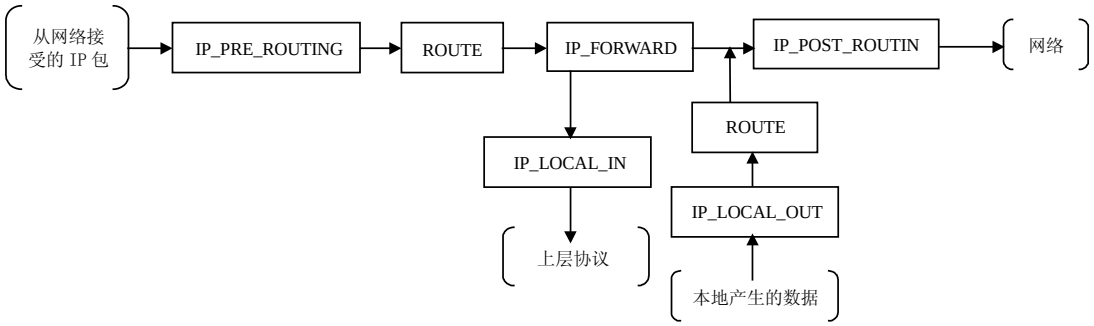

图1　Netfilter的功能框架

1.2　netfilter的关键技术

netfilter主要采用连线跟踪(Connection Tracking)、包过滤(Packet Filtering)、地址转换、包处理(Packet Mangling)4种关键技术。

1.2.1　连线跟踪

连线跟踪是包过滤、地址转换的基础，它作为一个独立的模块运行。采用连线跟踪技术在协议栈低层截取数据包，将当前数据包及其状态信息与历史数据包及其状态信息进行比较，从而得到当前数据包的控制信息，根据这些信息决定对网络数据包的操作，达到保护网络的目的。

当下层网络接收到初始化连接同步(Synchronize，SYN)包，将被netfilter规则库检查。该数据包将在规则链中依次序进行比较。如果该包应被丢弃，发送一个复位(Reset，RST)包到远端主机，否则连接接收。这次连接的信息将被保存在连线跟踪信息表中，并表明该数据包所应有的状态。这个连线跟踪信息表位于内核模式下，其后的网络包就将与此连线跟踪信息表中的内容进行比较，根据信息表中的信息来决定该数据包的操作。因为数据包首先是与连线跟踪信息表进行比较，只有SYN包才与规则库进行比较，数据包与连线跟踪信息表的比较都是在内核模式下进行的，所以速度很快。

1.2.2　包过滤

包过滤检查通过的每个数据包的头部，然后决定如何处置它们，可以选择丢弃，让包通过，或者更复杂的操作。

1.2.3　地址转换

网络地址转换源(NAT)分为(Source NAT，SNAT)和目的NAT(Destination NAT, DNAT)2种不同的类型。SNAT是指修改数据包的源地址(改变连接的源IP)。SNAT会在数据包送出之前的最后一刻做好转换工作。地址伪装(Masquerading)是SNAT的一种特殊形式。DNAT 是指修改数据包的目标地址(改变连接的目的IP)。DNAT 总是在数据包进入以后立即完成转换。端口转发、负载均衡和透明代理都属于DNAT。

1.2.4　包处理

利用包处理可以设置或改变数据包的服务类型(Type of Service, TOS)字段；改变包的生存期(Time to Live, TTL)字段；在包中设置标志值，利用该标志值可以进行带宽限制和分类查询。

2　基于netfilter的主动响应模型

2.1　入侵响应分析

入侵响应可以分为被动响应和主动响应两种类型[2~4]。在被动响应中，系统只报告和记录发生的事件；在主动响应中，系统阻断攻击过程或以其他方式影响攻击过程。

2.1.1　被动响应(Passive Response)

被动响应是指为用户提供信息，由用户决定接下来应该采取什么措施。有警报显示屏、电子邮件报警、

移动电话短信息报警等多种报警响应方式可供选择。被动响应很重要，应当根据危险程度高低的次序提交给用户。被动响应方式还可以利用网络管理基础设备，在网络管理控制台上发送和显示报警。

2.1.2 主动响应(Active Response)

主动响应措施可以归为针对入侵者采取措施、修正系统和收集更详细的信息3类。

网络反击是最极端的针对入侵者采取的措施。网络反击是指追踪至入侵者实施攻击的发起地，并采取措施以禁用入侵者的机器或网络连接。对入侵者采取断开网络会话，阻挡入侵IP地址的数据包是较为常用的形式。设陷追踪、自动发送邮件给系统管理员也是较有效的方法。

修正系统弥补引起攻击的缺陷，类似生物体的免疫系统，辨认出问题所在并进行隔离。这类响应十分缓和，通常也是最佳的响应配置。

收集更详细信息在被保护系统关系重大，而且在当事人要求法律赔偿时，很有价值。典型应用是将攻击引导至诱骗系统。诱骗系统模拟其他系统特征，引诱攻击者进入，记录下攻击者的详细信息。这种方法收集信息对分析网络安全威胁趋势也很有作用。入侵追踪也是一个值得到关注的问题，由于网络协议的特点，追踪必须是分布式的，需要多节点有效协调。

2.2 基于netfilter的主动响应模型设计实现

为了实现针对入侵行为的主动响应，可以利用netfilter快速、高效的优点，构建以下基于netfilter的主动响应模型，如图2所示。

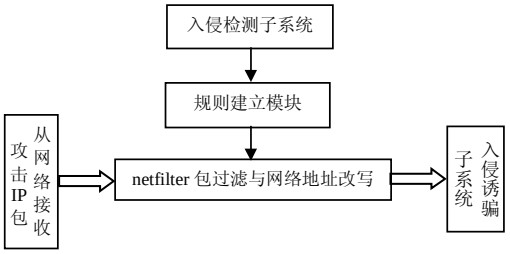

图2 基于netfilter的主动响应模型

基于netfilter的主动响应模型主要包括入侵检测子系统、规则建立模块和基于netfilter的包过滤与网络地址改写模块、入侵诱骗子系统等部分。

入侵检测是系统的一个重要构成部分，检测分析的正确性是正确响应的前提[5]。同时采用异常检测、误用检测。将误用检测用于网络数据包，异常检测用于系统日志。入侵检测子系统检测到入侵信息后，发送的报警信息(其中包含攻击源IP)触发规则建立模块。规则建立模块负责管理攻击源黑名单，并使用iptables建立包过滤规则，定义反击措施。针对不同的入侵方式反击措施可以选择断开联接、丢弃包或引导至诱骗子系统。一旦针对攻击源的规则建立，从网络接收的攻击IP包将被netfilter按规则进行处理，一部分攻击包将被重定向到入侵诱骗子系统。入侵诱骗子系统负责收集入侵信息，观察入侵者行为，记录其活动，以便分析入侵者的水平、目的、所用工具、入侵手段等。

3 总 结

基于netfilter的主动响应模型，针对当前攻击动态调整系统安全策略，阻止入侵行为，实现了对攻击行为的主动防御。系统接收的数据包通过内核进行处理，对应用程序和用户透明。正常数据流传输速率所受影响较小。转发攻击数据包的速度在微秒级(实际测试结果)，因而对攻击的反击隐蔽，黑客往往在毫无知觉的情况下被引导至诱骗系统。此外，该模型部署灵活，既可部署在网络边界设备上，也可部署在主机上，可以有效防御网络内部的攻击，弥补了防火墙的不足。

参 考 文 献

[1] Rusty R. Linux 2.4 packet filtering HOWTO[EB/OL]. http://www.netfilter.org/documentation/HOWTO/packet-filtering-HOWTO.html, 2002-01-24.

[2] 博嘉科技. Linux防火墙技术探秘[M]. 北京：国防工业出版社, 2002. 159-186

[3] 戴英侠, 连一峰, 王 航. 系统安全与入侵检测[M]. 北京：清华大学出版社, 2002. 138-148

[4] 姚晓宇, 顾冠群. 一种基于主动网的安全防御系统[J]. 计算机工程与应用, 2002, 38(6): 130-133

[5] Kemmerer R A, Vigna G. Intrusion detection: A brief history and overview[J]. Security & Privacy, IEEE Computer Magazine, 2002, 35(4): 27-30

编 辑 熊思亮