分布式网络入侵检测系统 NetNumen 的设计与实现*

李 旺[1], 吴礼发[2], 胡谷雨[2]

[1](解放军理工大学 通信工程学院 电信工程系,江苏 南京 210016);
[2](解放军理工大学 指挥自动化学院 计算机教研室,江苏 南京 210016)
E-mail: wang_wang_li@sina.com; wulifa@sina.com

摘要: 详细介绍了在 Linux 环境下基于规则的分布式网络入侵检测系统 NetNumen.同现有的网络入侵检测系统相比,NetNumen 将异常检测(检测包到达频度的异常)和特征检测(检测特定攻击和攻击工具的固有特征)有机地结合起来,对 DoS(denial of service),DdoS(distributed denial of service)攻击的检测效果较现有方法有明显的改善.

关 键 词: 入侵检测;入侵检测系统;网络安全;DoS(denial of service);DdoS(distributed denial of service)
中图法分类号: TP393 文献标识码: A

近年来,随着 Internet 的迅速发展,网络攻击事件时有报道,网络安全问题显得日益重要.作为网络安全防护工具"防火墙"的一种重要的补充措施,入侵检测系统(intrusion detection system,简称 IDS)得到了迅猛的发展.入侵检测系统通过从计算机网络中的若干关键点收集信息并加以分析,检查网络中是否有违反安全策略的行为和遭到袭击的迹象,从而提供对内部攻击、外部攻击和误操作的实时保护.有两类主要的 IDS:基于主机的 IDS 和基于网络的 IDS.基于网络的 IDS 主要是从网络中的关键网段收集网络分组信息,从而发现入侵证据.它能在不影响网络性能的情况下对网络进行监测,发现入侵事件并作出响应.

本文详细介绍了基于规则的分布式网络入侵检测系统 NetNumen 的设计与实现.与现有的同类基于网络的入侵检测系统相比,NetNumen 将异常检测和特征检测有机地结合起来,对 DoS(denial of service),DdoS (distributed denial of service)攻击的检测效果较现有方法有明显的改善.

1 背 景[1]

基于网络的入侵检测实际上也是一种信息识别与检测技术.网络入侵活动的实际体现就是数据包,它作为信息输入到检测系统之中.检测系统对其进行分析和处理之后,得到的就是网络入侵的判断.因此,传统的信息识别技术也可以用到入侵检测中来.

在基于网络的入侵检测中,不但数据包的先后次序十分重要,数据包产生的时间也要作为一个重要的变量输入到识别系统之中.如,DoS 攻击,完全是依靠短时间内大量网络活动来耗尽系统资源的.此外,入侵检测比一般的信息识别有更强的上下文和环境相关性.在不同的环境下,有完全不同的结果.

1.1 入侵检测方法

现存入侵检测系统的入侵检测方法主要有两类:基于异常(anomaly-based)的入侵检测和基于特征(signature-based)的入侵检测.

异常入侵检测系统记录用户在系统上的活动,并且根据这些记录创建活动的统计报告.如果报告表明它与

* 收稿日期: 2001-02-12; 修改日期: 2001-06-07
基金项目: 国家 863 高科技发展计划资助项目(863-306-ZD08-01-2)
作者简介: 李旺(1975－),男,湖南湘潭人,讲师,主要研究领域为网络管理,通信系统工程;吴礼发(1968－),男,湖北蕲春人,博士,副教授,主要研究领域为网络管理与网络安全;胡谷雨(1963－),男,浙江东阳人,博士,教授,博士生导师,主要研究领域为计算机网络与网络管理,军事通信网.

正常用户的行为有明显的不同,那么检测系统就会将这种活动视为入侵.特征入侵检测是事先对已知的入侵方式进行定义(即定义入侵方式的特征),并且将这些方式写进系统中,将网络上检测到的攻击与系统定义的已知入侵方式进行对比,如果两者相同,则认为发生了入侵.

从检测所依赖的知识基础来看,基于特征的入侵检测必须了解所有攻击的攻击特征,而基于异常的入侵检测则必须了解系统期望的所有正常的使用行为.在现实中,这两者都是很难做到的.因为这两种方法所依赖的知识基础的不完整性,都可能产生大量的误报和漏报事件.比较而言,异常入侵检测可以检测到一些新的、特征入侵检测检测不到的攻击.

上述两种方法中的每一种都不能保证能够准确地检测出变化无穷的入侵行为.因此,在网络安全防护中要充分衡量各种方法的利弊,综合运用这些方法才能有效地检测出入侵者的非法行为.NetNumen 正是基于这一思想而设计的.

此外,还有一些新的技术、理论被应用在入侵检测上,例如:基于神经网络的入侵检测方法、基于模型推理的入侵检测技术,还有利用移动代理进行网络入侵检测等等.但这些方法普遍处在研究阶段,目前还没有出现较为完善的产品.

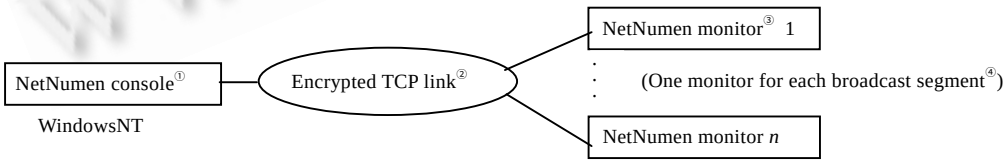
1.2 入侵检测系统现状

目前,国内外一些研究机构和企业已研究或开发出了多种类型的入侵检测系统.其中有主要用来验证一些概念和算法的研究用的系统,较为知名的有:加州大学圣巴巴拉分校开发的 NetStat,它采用的技术是基于状态转换的入侵检测;美国 Lawrence Livermore 国家实验室开发的 Bro,开发它的主要目的是研究入侵检测系统的健壮性,即研究采用何种措施可以防止入侵检测系统本身被攻击.

还有一些流行的商用入侵检测系统,如:由科学应用国际公司(Science Applications Internatinal Corporation)开发的基于主机的入侵检测系 CMDS;由 Axent 公司开发的基于网络的入侵检测系统 NetProwler,它通过匹配已知的入侵模式来检测入侵,还支持用户定义入侵模式;另一个著名的系统是 ISS(Internet Security Systems)公司的 RealSecure,它由 3 部分组成:基于网络的识别引擎、基于主机的识别引擎和管理员模块,它支持基于主机的入侵检测和基于网络的入侵检测.Cisco 的 NetRanger 可检测 3 种攻击:已知的攻击、已知攻击的变种、复杂的组合攻击.除了提供大量的已知攻击模式定义外,它还支持用户定义入侵模式.中科网威信息技术有限公司的“天眼”入侵检测系统、启明星辰公司的黑客入侵检测与预警系统 SkyBell(天阗),集成了网络监听、实时协议分析、入侵行为分析及详细日志审计跟踪等功能.

2 NetNumen 系统的结构及实现

NetNumen 由控制台(console)和监控器(monitor)组成,如图 1 所示.根据被监视的网络的大小可以有一个或多个 NetNumen 监控器分布在网络的各个广播域.NetNumen 控制台给网络管理员提供配置和浏览检测结果的可视化用户接口.它是一个基于 Windows 平台的软件,采用 TCP 协议与 NetNumen 监控器交互,传输的数据进行了加密.NetNumen 控制台根据用户的设置自动更新被管理的 NetNumen 监控器的系统配置,如攻击特征表、告警信息过滤表等,同时也可以接收 NetNumen 监控器所发送的告警信息.

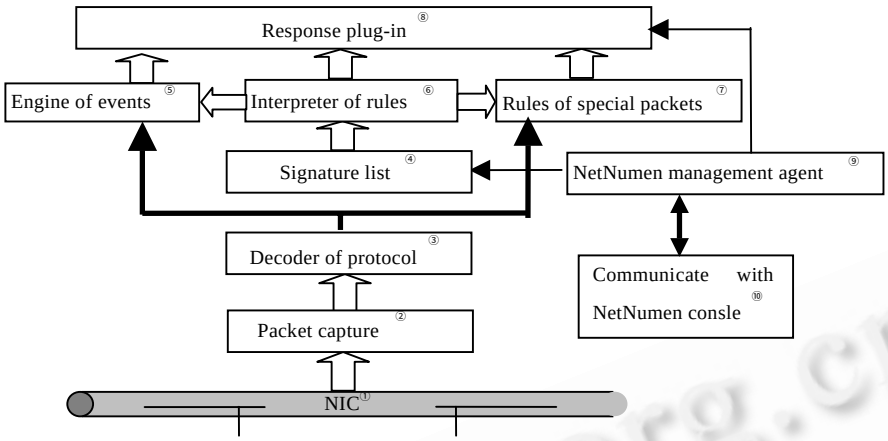


①NetNumen 控制器,②加密的 TCP 连接,③NetNumen 监控器,④每一个需要监控的广播域放置一个监控器.

Fig.1 The structure of NetNumen

图 1 NetNumen 系统结构

监控器是 NetNumen 的核心,本文着重讨论它的结构和实现.如图 2 所示,监控器主要由 6 个部分组成,每一部分的功能与实现如图 2 所示.



①网络接口卡,②分组捕获器,③协议解码器,④攻击事件特征规则,⑤事件判决引擎,⑥规则解释器,⑦特征包到达速度判决器,⑧响应插件,⑨NetNumen 管理代理,⑩与 NetNumen 控制台交互.

Fig.2 The structure of NetNumen monitor

图 2 NetNumen 监控器结构

2.1 分组捕获器

分组捕获器通过入侵检测系统所属的宿主操作系统内核中所提供的分组捕捉机制,为入侵检测系统提供从物理网络(网络接口卡)直接收集数据链路层网络原始信息的能力.这部分对于保证整个入侵检测系统的效率和可移植性至关重要.即:在该层必须屏蔽掉不同系统中不同数据链路设备的差异,同时,这部分必须要有很高的网络数据捕捉性能.

在 NetNumen 系统中,采用了 libpcap(lib for packet capture):一个与具体实现无关的访问操作系统所提供的分组捕获机制的分组捕获函数库[2].它同时支持源自 Berkeley 内核下的 BPF,SOLARIS 2.x 下的 DLPI,SunOS 4.1 下的 NIT,Linux 下的 SOCKET_PACKET 套接口以及其他若干操作系统.

2.2 网络协议解码器

网络协议解码器相当于一个网络协议分析仪,实现相当于计算机系统中网络协议栈的功能.它将“分组捕获器”获得的数据链路层的信息(数据包),根据不同的网络协议解码相应的分组数据结构,并将此已解码的协议分组信息提交“判决引擎”.该部分决定了入侵检测系统可以处理的网络协议数量,并且直接影响到系统自身的安全性.

通过对常见攻击手段的分析,我们发现绝大多数的攻击手段集中于 TCP/IP 协议族的 TCP,ICMP 和 UDP 这 3 种协议之中,其中以 TCP 协议为最多.所以 NetNumen 的网络协议解码器最先对 TCP 协议进行了比较细致的分析,兼顾 ICMP 和 UDP 协议,而对于其他网络协议暂时没有进行解析.

2.3 规则描述语言语法解释器

语法解释器是用来解释由自定义的规则描述语法所描述的攻击事件的特征和相应的响应规则,用来对“事件判决引擎”进行控制,使其能根据所描述的攻击事件模式特征来识别攻击事件,并控制“响应子系统”的相应动作.

实现规则描述语言时必须找到一种方式,用尽可能少的要素,尽量简单的语法来描述最常见的攻击事件.这就需要对攻击手段进行细致的研究,抽象提取其中关键的特征要素,在理论与目前实现技术之间有效地加以折衷.

在 NetNumen 的实现中采用与 Snort(一种轻量级的网络入侵检测系统[3])中规则描述语言相同的语法.但 Snort 是一种单纯的基于特征的入侵检测系统,它的规则描述语言都是针对描述包自身的特征的,无法描述包到达的时间和频度.NetNumen 结合了异常检测的技术,对包到达的频度要进行检测,因此在 Netnumen 中对该语言

进行了语义上的扩充,增加了用来描述特征包到达速度的选项(arrive_speed),下面是一个简单的例子:

alert icmp any any–>12.18.1.1/24 any (arrive_speed:100/1000;msg:“大量 icmp 包”;)

在上述规则中,关键字“arrive_speed”表示包到达速率.上述规则的含义是:当从任意主机上的任意端口发往主机 12.18.1.1 上的任意端口的 ICMP 包的数量在 1 000 毫秒时间内超过了 100 个的时候就产生“大量 icmp 包”告警.

2.4 入侵事件“判决引擎”

判决引擎对已解码的网络协议数据进行分析,并从这些网络活动中寻找预先定义的攻击模式,一旦发现其中含有攻击事件的特征标志,即将此事件提交“响应子系统”.

事件判决引擎从攻击事件特征模式库中读入对每一种攻击事件的特征描述.每一个事件特征描述语句中第 1 个 alert,log 或 pass 表示将该攻击事件的特征放入哪一个特征集合中,这主要是为了提高 NetNumen 系统性能.NetNumen 系统目前在“事件判决引擎”中维持了 alert,log 和 pass 这 3 种不同的攻击模式集.“事件判决引擎”的工作步骤分为两步:

第 1 步.通过“规则语法解释器”从“攻击事件特征规则列表”文件中读取每一种攻击事件的特征,将其转化为对应于分组信息的数据结构,以链表的形式存储备用.

第 2 步.“事件判决引擎”接受从“网络协议解码器”中输出的、对应于每一个分组的特定数据结构.根据其中的内容遍历存储攻击事件特征标志信息的链表,一旦发现相应的攻击手段,根据“攻击事件特征模式库”文件中相应规则中所指定的响应种类作出相应的反应.

2.5 特征包到达速度判决器

在对攻击特征规则进行初始化存储的同时也根据配置初始化相应的计数器、定时器,用来记录特征包的到达.

特征包到达速度判决器对每一种要检测的包初始化一个“先进先出”(FIFO)队列,记录一定数量的包到达的时间戳,对符合条件的包的到达时间进行登记,并对一段时间内到达的包进行计数,一旦超出预先设置的门限值,即将此事件提交“响应子系统”.

2.6 响应子系统

根据事件“判决引擎”以及特征包到达速度判决器提交的事件种类,根据预先指定的响应行为来执行相应的反应动作.目前 NetNumen 监控器的响应部分较为简单,只提供文件记录、窗口出现告警信息两种响应方式.而今后的响应子系统可以根据用户需要进行扩展,比如增加动态防火墙配置功能等.目前在 NetNumen 监控器的实现中已经考虑到此类扩展的需求,并在系统结构中作了相应的考虑.

3 性能分析

本文对 NetNumen 系统进行了相关的测试.测试的硬件环境为 CPU:PII350,内存:128M,硬盘:6.4G,10M D-Link 网卡.软件环境为蓝点 Linux V2.0,内核版本 2.2.16.

测试方法:考虑到影响速度的因素主要是捕获到包后的判断、处理时间,因此,为了做到数据包连续不断地到达,本文测试时先用 tcpdump[2]捕获一定数量的数据包存于文件中(用 tcpdump 格式),然后用 NetNumen 进行处理,每种处理做 3 次取平均值.结论如下:

从处理速度方面来看(即单位时间能对多少数据包进行判断、处理),随着包数量的增长,处理时间基本呈线性增长.在上述测试平台的条件下,共有 818 条规则进行判断时(这 818 条规则基本涵盖了已发现的各类 backdoors,DoS,finger,FTP,缓冲区溢出,端口扫描等攻击),平均每秒约能处理 34 000 个数据包.

从可伸缩性来看,测试表明,规则的增加并没有引起处理时间的线性增长.

4 相关工作比较

与一般的网络入侵检测系统相比,NetNumen 的独特之处在于增加了“特征包到达速度判决器”,从而将“异常检测”(统计包到达情况的异常)和“特征检测”(检测特定攻击和攻击工具的固有特征)有机地结合起来,对 DoS,DDoS 攻击的检测效果较现有方法有明显的改善.

拒绝服务攻击(denial of service)、分布式拒绝服务攻击(distributed denial of service)[4],主要依靠消耗网络带宽或系统资源,导致网络或系统不胜负荷以至于瘫痪而停止提供正常的网络服务,来达到攻击的目的.

现有大多数基于规则的 NIDS 对 DoS 和 DDoS 攻击的检测其主要技术是:使用特定端口、标志位、数据内容描述攻击特征.针对这类攻击的主要特点:攻击者使用的工具有明显的特征,的确能检测一些采用简单、著名工具的 DoS,DDoS 攻击.但是,如今的攻击工具其发展非常迅速,不但所使用的端口可以轻易地被用户改变,而且还出现了功能更强大、隐蔽性更强、关键字符串和控制命令口令使用更强壮的加密算法,甚至对自身进行数字签名等等这些技术,使得现有的这些检测技术不能有效地检测这类攻击.还有一类,纯粹野蛮地通过采用大量网络活动来消耗网络资源的方法实现 DoS 攻击的目的,例如,采用自编程序用多台机器同时对一攻击目标发送 ICMP 包,或同时打开许多 TCP 连接,这种攻击在发送的数据包上并没有什么异常,也可以说没有什么特别的特征,甚至它还可以很轻易地改变 IDS 所用来检测的特征.对这类的攻击,仅靠简单的规则匹配显然不能解决问题.

从上面提出的一些不易检测的 DoS,DDoS 攻击工具和方法来看,它们都有一个共同的特征:当这类攻击出现时,网络中会出现大量的某一类型的数据包.NetNumen 利用这一特征,采用异常检测的方法,通过统计某一类型的包在一段时间内到达网络的数量来作为衡量网络活动是否异常的标准.例如,在 2s 内如果有 100 个带有 SYN 标志的数据包到达,显然对于一个小规模的网络来说是不正常的.

因此,NetNumen 所采用的“异常检测”和“特征检测”相结合的方法,对 DoS,DDoS 攻击的检测效果较现有方法有明显的改善.大量的实验也证明这一方法是行之有效的.

5 结束语

NetNumen 入侵检测系统作为国家 863 高科技发展计划的重点项目:计算机网络管理与安全系统的一部分,已经进行了试用.实践表明,这种网络入侵实时检测系统是有效的,尤其在对 DoS,DDoS 攻击的检测效果上较同类系统有了明显改进.但是也还有一些问题可以做进一步的工作:(1) 进一步优化判决算法,考虑取得性能与功能上的平衡,为每一个数据包保存一段时间的各种信息,再用状态机来联系前后的数据包进行判断,这样可以进一步降低漏报率;(2) 在 NetNumen 系统自身的可靠性和安全性上还要进一步加强.

References:

[1] Allen, J., Christie, A., Fithen, W., *et al*. State of the practice of intrusion detection technologies. CMU/SEI-99-TR-028, 2000. http://www.sei.cmu.edu/publications/documents/99.reports/99tr028/99tr028abstract.html.

[2] Stevens, W.R. Unix Network Programming (Vol.1) Networking APIs: Sockets and XTI(2nd ed.). Prentice Hall PTR., 1998.

[3] Roesch, M. Snort-Lightweight Intrusion Detection for Networks. In: Proceedings of the USENIX LISA’99 Conference. http://www.usenix.org/events/lisa99/full_papers/roesch/roesch.pdf

[4] Denial of Service Attacks. http://www.cert.org/tech_tips/denial_of_service.html.

Design and Implementation of Distributed Intrusion Detection System NetNumen*

LI Wang[1], WU Li-fa[2], HU Gu-yu[2]

[1](*Department of Telecommunications, Institute of Communications Engineering, PLA University of Sciences and Technology, Nanjing* 210016, *China*);

[2](*Teaching and Research Section of Computer, Institute of Command Automation, PLA University of Sciences and Technology, Nanjing* 210016, *China*)

E-mail: wang_wang_li@sina.com; wulifa@sina.com

Abstract: A rule-based distributed intrusion detection system NetNumen is presented in Linux in this paper. Compared with the existing network-based intrusion detection system, NetNumen combines anomaly detections (detecting the anomaly frequency of packets' arriving) with signature detections (detecting the immanent characters of specialized attack and attack instrument), which improves the detection effect of the attack of DoS (denial of service)and DdoS (distributed denial of service) dramatically.

Key words: intrusion detection; IDS (intrusion detection system), network security; DoS (denial of service); DdoS (distributed denial of service)

* Received February 12, 2001; accepted June 7, 2001
Supported by the National High Technology Development 863 Program of China under Grant No.863-306-ZD08-01-2

敬告作者

《软件学报》创刊以来,蒙国内外学术界厚爱,收到许多高质量的稿件,其中不少在发表后读者反映良好,认为本刊保持了较高的学术水平.但也有一些稿件因不符合本刊的要求而未能通过审稿.为了帮助广大作者尽快地把他们的优秀研究成果发表在我刊上,特此列举一些审稿过程中经常遇到的问题,请作者投稿时尽量予以避免,以利大作的发表.

1. 读书偶有所得,即匆忙成文,未曾注意该领域或该研究课题国内外近年来的发展情况,不引用和不比较最近文献中的同类结果,有的甚至完全不列参考文献.

2. 做了一个软件系统,详尽描述该系统的各个方面,如像工作报告,但采用的基本上是成熟技术,未与国内外同类系统比较,没有指出该系统在技术上哪几点比别人先进,为什么先进.一般来说,技术上没有创新的软件系统是没有发表价值的.

3. 提出一个新的算法,认为该算法优越,但既未从数学上证明比现有的其他算法好(例如降低复杂性),也没有用实验数据来进行对比,难以令人信服.

4. 提出一个大型软件系统的总体设想,但很粗糙,而且还没有(哪怕是部分的)实现,很难证明该设想是现实的、可行的、先进的.

5. 介绍一个现有的软件开发方法,或一个现有软件产品的结构(非作者本人开发,往往是引进的,或公司产品),甚至某一软件的使用方法.本刊不登载高级科普文章,不支持在论文中引进广告色彩.

6. 提出对软件开发或软件产业的某种观点,泛泛而论,技术含量少.本刊目前暂不开办软件论坛,只发表学术文章,但也欢迎材料丰富,反映现代软件理论或技术发展,并含有作者精辟见解的某一领域的综述文章.

7. 介绍作者做的把软件技术应用于某个领域的工作,但其中软件技术含量太少,甚至微不足道,大部分内容是其他专业领域的技术细节,这类文章宜改投其他专业刊物.

8. 其主要内容已经在其他正式学术刊物上或在正式出版物中发表过的文章,一稿多投的文章,经退稿后未作本质修改换名重投的文章.

本刊热情欢迎国内外科技界对《软件学报》踊跃投稿.为了和大家一起办好本刊,特提出以上各点敬告作者.并且欢迎广大作者和读者对本刊的各个方面,尤其是对论文的质量多多提出批评建议.