文章编号:1000 - 582X(2002)06 - 0152 - 03

网络安全监测*

张 亮
(江苏警官学院,南京 210012)

摘 要:"网络安全监测"通过实时分析网上数据流来监测非法入侵活动,并根据监测结果实时报警、响应,达到主动发现入侵活动、确保网络安全目的。系统由嗅探器、监测中心、远程管理服务器等构成,采用基于模式、基于统计 2 种方法发现入侵。方案技术的关键是入侵识别,解决的主要难点是数据流实时性与查询速度矛盾、入侵模式动态添加等问题,具有漏洞自检、智能分析、双向监测等功能。它是传统网络安全产品的强有力助手、是对付越演越烈的网络入侵的重要工具。

关键词:嗅探器; 入侵识别; 监测报警; 网络安全
中图分类号:TP393.08 **文献标识码**:A

网络安全的实质是信息安全[1]。凡涉及网上信息保密性、完整性、可用性、真实性、可控性的技术和理论都是网络安全研究领域,而网络入侵监测是其中主要方面。"网络安全监测"通过实时跟踪网上数据来监测非法入侵活动,并根据监测结果实时报警、响应,达到主动发现入侵活动的目的。它是对付网络入侵的重要工具、是传统网络安全产品的强有力助手。

1 现状分析

1.1 入侵手段简介

网络入侵是指以各种手段破坏数据保密性、完整性,或进行未经授权的访问、使用。分为理论入侵和技术入侵两个层面[2]。前者是密码学意义上的入侵,专注于其入侵概念或入侵过程、算法,而不考虑具体实现,包括对加密算法的入侵、对签名算法的入侵、对密钥交换和认证协议的入侵等;后者与特定的网络协议、操作系统及应用程序有关,有明确的入侵步骤,入侵者可借助一定的分析手段与入侵工具达到特定入侵目的。一般而言,理论入侵是技术入侵的基础,几乎每种技术入侵最终都可归结为某类理论入侵,但理论入侵却未必是现实可行的技术入侵。根据入侵的逻辑实质和入侵针对的安全弱点位置,网络入侵手段主要有:

1)网络监听。大部分传输介质如 FDDI、Ethernet、Token - ring、无线接入网等都可实施网络监听。

2)对加密算法的入侵。即对密码进行惟密文入侵、已知密文入侵、选择密文入侵、选择明文入侵及穷举入侵等,通常,只有相当实力的组织才拥有破译特定密码的人力、物力、财力。

3)对软件设计的入侵。计算机软件日益复杂的直接后果就是安全隐患剧增,特别是当软件的运行效率与产品实用性、安全性发生冲突时,大部分软件开发人员选择牺牲软件自身的安全。

4)对系统配置的入侵。由于现代计算机系统庞大芜杂,管理人员通常只使用系统默认配置或对更改配置后的安全后果不了解,导致入侵行为的发生。它往往和对软件设计的入侵相结合。

5)对网络协议的入侵。Internet 作为 TCP/IP 的第 5 层结构,从数据链路层到应用协议层在设计上都存在不同程度的安全弱点,如入侵者修改数据包改变其流向、伪造 IP 地址进行 IP Spoofing 入侵、借助海量数据包耗尽主机 TCP 连接资源、对用户服务器进行电子轰炸、绕过防火墙侵入用户系统等。

除上述几种入侵外,还有权限让渡、由社会工程引起的密钥泄露、恶意程序入侵(如病毒、特洛伊木马)、物理入侵(如偷窃加密机、盗取用户身份标识、强劫数据中心或密钥存储中心)等。

1.2 安全策略现状

网络安全核心是如何在网络环境下保证信息本身保密性、完整性与操作的正确性、合法性、不可否认性[3]。目前主要的网络安全策略有:

1)操作系统安全。采用物理上、时间上、逻辑上、密码技术上隔离等措施,保证系统安全性。

2)保密网关。进入网关的所有访问都受到过滤、认证、授权等,所有出关信息亦受相应检查,从而保护

* 收稿日期:2002 - 03 - 01
作者简介:张亮(1966 -),男,江苏南京人,助理研究员,硕士。研究方向:警用电子装备。

内部网的信息安全。

3)加解密技术。目前各种加解密技术、身份认证与数字签名、访问控制等已较成熟,应用亦较广泛。采用可信赖第三方服务器进行密钥分发、身份确认的 Kerberos 公钥加密系统就是其中的杰出代表。由于一些加解密技术需用户介入,系统认证作用有所削弱。

4)防火墙。这是目前应用最广泛、最行之有效的网络安全技术。其基本结构分为包过滤和应用代理,前者关注网络层、传输层保护;后者注重应用层的保护。防火墙通过监视、限制、更改数据流,对外屏蔽内部网拓扑结构、对内屏蔽外部危险站点,达到防范非法访问目的。当前,一些高性能的防火墙也具有网络安全监测能力,但由于性能的限制,通常不具备实时入侵监测能力,而主要是事后分析,没有实时性。作为具有强大控制功能的网络数据的唯一通道,防火墙一旦被入侵成功,将造成巨大灾难。

这些手段各有优缺点,但都是被动防御,存在一定局限性。因此,开发"网络安全监测"系统,配合现有网络安全手段,对网上信息进行监测,主动发现非法入侵活动,确保网络安全,显得尤为重要。

2　网络安全监测

2.1　方案设计

"网络安全监测"系统由嗅探器、安全监测中心、远程管理服务器组成,采用的技术手段主要有基于主机的入侵监测和基于网络的入侵监测两种。前者通过分析主机的事件来判断是否存在入侵,监测软件通常安装在主机上,准确性、安全性较好;后者通过分析网上数据包来监测是否发生入侵行为,可保护某一网络,但不如前者准确。这里主要讨论基于网络的入侵监测。

它通过对网上数据流实时跟踪、分析,捕捉可疑的入侵活动,发现存在的安全问题,并根据监测结果实时响应、报警,同时提供详尽的网络安全审计报告。这样变以往被动防守为主动监测,不但具有网络管理、漏洞自检、智能分析功能,而且对输入、输出信息提供同样的监测,有效防止网络外部、内部入侵。由于系统本身不作为主机,不能对其实施入侵,确保了自身的安全。其工作流程:假设网上数据包都具有潜在敌意,这些数据包被抓包模块捕获后,包模块对数据包分拆、组合、分析,确认其有效性、合理性,对无效、泄密、入侵的数据包,系统实时报警并详细记录入侵事件,以备今后查询、取证[4]。

2.2　嗅探器

嗅探器按用户定义的安全模式实时监测网上数据,识别正在发生的入侵。若发现入侵行为,即按照安全策略实时响应,并向监测中心报警。同时作相应记录,以便今后审计分析。显然,嗅探器要监测、识别各种入侵,首先要捕获网上传输的所有数据包。因此,需将网络适配器设置在全收模式下,这样网上数据包才能传输至嗅探器进行入侵分析。为有效监测,嗅探器应安置在网络敏感部位,如防火墙或路由器之后、内部网入口处、重要服务器的周围等,其强大的监测功能为用户提供全面、有效的入侵监测能力。

除实时报警、响应,嗅探器还能通过检查数据包内容获得入侵证据,以备今后查询、取证。此外,还需遵守网络管理相关标准。它识别的入侵方式主要有:网络协议标记入侵,如 IP 地址假冒、猜测序列号、IP 欺骗入侵、会话劫持入侵等;应用型入侵和易受到入侵的弱点如 CGI、NFS、FTP、Sendmail 等的缺陷、指针和 DNS 中缓冲区溢出;非法字符串,如"Secret"、"Aggress"等,并设置关键字表供程序寻找匹配。考虑到包分析的速度,当关键字表过长时会影响系统性能,需进行相应处理,将在下面详细介绍。

2.3　入侵识别

入侵识别的方法有模式匹配、统计分析、完整性分析 3 种[5],前两种为实时入侵监测,第 3 种为事后分析。这里主要介绍模式匹配、统计分析两种,它们是对网上数据流实时进行入侵监测,系统根据用户历史行为模型、神经网络模型、存储在计算机中的专家知识等对数据流进行分析,如发现入侵行为即断开其与主机的连接,并收集证据、恢复相关数据,这个过程循环进行,从而完成对网络入侵的实时监测。

嗅探器主要采用基于模式、基于统计两种方法的结合发现入侵。前者采用人工智能方法,将已知攻击手段抽象并形成入侵模式库。网上信息与入侵模式库相比较即可发现入侵行为。该过程可以很简单(如非法字符串的匹配),也可能较复杂(如利用数学表达式表示安全状态的变化)。其优点是系统负担小、监测准确率高、技术相当成熟、只需收集相关数据的集合即可。但入侵模式库必须事先定义好,因此只能对已知的攻击手段进行监测,而不能监测从未出现过的入侵手段。由于入侵模式库可随时更新,因而可通过及时添加新出现入侵的方法对其升级,以反映新的入侵类型;后者首先给系统对象,如用户、文件、目录、设备等创建一个统计描述,统计正常使用时的属性参数,如监测出网络属性参数在正常范围外,即认为发生入侵行为。该方法主要用在:DOS 攻击监测、基于统计用户身份智能识别、基于统计的协议自动识别等。其优点是可监测未知的或更为复杂的入侵,但很多攻击手段并没有相应的统计特征,因此能监测的入侵手段有限。且误报、漏报率较高,不适应用户正常行为的突然改变。

2.4　解决难点[6]

1)由于网上数据极其庞大,需要有效的海量数据

库来处理如此大的数据流量,但是会给查询带来很大的不便。要从网上传输的海量数据中查询符合某条件的字符,如遍历整个数据库,速度必然缓慢。本方案采取给源地址、目标地址等加索引的方法提高查询速度。该方法需大量内存,且时间上有延迟,可能出现新的数据包无法及时插入问题,不仅影响实时性,还会因堵塞的数据包较多导致系统崩溃。为解决实时性与查询速度矛盾,可对加索引的字段进行处理,如取源地址字符串的前几位组成新的字段,并对新的字段加索引。这样,既保证实时性,查询速度也大大提高。

2)系统设计重点是包模块分析,因为模块中包含监测网络黑客入侵的模式库,且入侵模式库是按优先级高低安排的,优先级的高低是由黑客入侵行为所造成的危害程度来定义,通常按由高到低顺序分析数据包。为实现对入侵模式的动态添加,而不更改模块其它部分的代码,把类型相似的入侵放在预留出许多空的虚函数的同一模块,每个虚函数代表一种入侵,其返回值为"1"。要添加新入侵,只要在空的虚函数中添加相应代码,此虚函数返回值也为"1"。函数中还要保存入侵者各种信息,以便产生入侵报告记录。数据包通过时,嗅探器立即调用入侵模式模块,依次检查各函数,若其返回值为"0",则此数据包满足入侵模式,系统立即报警、响应。当然,嗅探器要继续检查后面各函数,直到结束为止。考虑到优先级问题,需把代表优先级高的函数放在入侵模式库的前面。

3 结 语

"网络安全监测"是防火墙等传统网络安全产品的强有力助手,是对付越演越烈的网络入侵的有效手段。作为监测网络安全的重要工具,它适用于所有 TCP/IP 网络,能对网络入侵进行全方位监测、准确判断入侵方式、及时报警或阻断,具有网络监测、实时协议分析、入侵行为分析、详细日志审计跟踪等功能。和任何软件产品一样,本方案也存在一定局限性,主要表现为加密可能使监测功能削弱。可以相信,在网络安全监测市场上将不断推出功能更完备、性能更优异、安全性更强的产品,满足人们日益提高的要求。

参考文献:

[1] 张亮.指纹识别式鼠标[J].重庆大学学报(自然科学版),2002,25(2):139-142.
[2] 黄旸,胡伟栋,陈克非.网络入侵与安全防护的分类研究[J].计算机工程,2001,27(5):131-133.
[3] 张亮.动态身份认证[J].网络安全技术与应用,2001,1(11):26-28.
[4] 孙静,曾红卫.网络安全检测与预警[J].计算机工程,2001,27(7):109-110.
[5] 闵君,龚晶莹.入侵检测技术的研究[J].计算机应用研究,2002,19(2):1-4.
[6] 张志吉,唐毅.网络入侵与预警系统[J].上海大学学报,1999,5(12):126-127.

Network Security Monitor

ZHANG Liang
(Jiangsu Police College, Jiangsu Province, Nanjing 210012, China)

Abstract: Illegal traffics on network can be actively detected by network security monitor. An advanced system is given which can capture network data stream and intercept malicious attack, so as to alarm or take response action in real-time. The system is composed by sniffer, monitor control center, remote management unit, etc. Attack activities under surveillance can be distinguished by two methods, which are rule based method and statistics based method. Intrusion recognition by sniffer is the key technology of the system. In addition, dilemma between real-time data stream and high inquiry speed, as well as dynamic addition of attack rules contributes to the main concern of system design. Backdoor of The system can be self detected, while intelligent analysis and bi-directional surveillance ability has also been implemented. With all these advance features, the system is presented not only as a strong assistant to traditional network security products, but also an important tool for counter-fighting with rampant network intrusion nowadays.

Key words: sniffer; intrusion recognition; monitor alarm; network security

(责任编辑 吕赛英)