网络入侵检测系统安全性能检测研究*)

Research on Test Methodology for Network Intrusion Detection System Security

吕志军　黄　皓　曾庆凯　陈道蓄　谢　立
(南京大学计算机软件新技术国家重点实验室　南京210093)
(南京大学计算机科学与技术系　南京210093)

Abstract　Network Intrusion Detection System(NIDS) is a key component of network security system, whose effect is dependent on its own security. Whether the NIDS security is considered in the design phase, NIDS must be tested to ensure its reliability. Firstly, in this paper, the vulnerability of NIDS is analyzed, the basic security of NIDS is studied; finally, the test methodology for NIDS is studied.

Keywords　NIDS, Overburden, Invalidation, Subterfuge, Test

1. 引言

随着计算机和网络技术在社会生活各方面应用的深入发展，计算机网络系统安全已成为计算机科学当前的研究热点之一。但随着网络技术在应用中的发展及攻击者技术的日益提高，单纯的防火墙已经不能满足安全需求，因为它无法控制内部网络用户和透过防火墙的入侵者的行为、无法处理合法用户的非法行为问题，需要采用多方位、多样的手段来保证网络安全。目前计算机网络系统安全在技术上包括访问控制、防火墙、审计、防病毒、加密和入侵检测系统等等；其中NIDS作为入侵检测系统(Intrusion Detection System，IDS)的一种，正成为网络安全解决方案中的一个重要组成部分，发挥着越来越大的作用，它通过检查所有网络用户的行为，从中识别出是否有非法行为，但NIDS本身是一个软件，也有可能受到攻击，因此，无论NIDS在设计时是否考虑过本身的安全性能，都必须对它进行检测，以保证它的可靠性。在本文中，首先分析了NIDS的各个部件可能存在的弱点，针对这些弱点，指出NIDS应具有的基本安全性能，最后给出了几种检测这些安全性能的方法。

2. 入侵检测系统

2.1　定义

入侵检测在文[1]中被定义为"标识出个体非授权使用计算机系统或越权使用系统资源的行为"。我们在这里给出一些补充定义：任何试图非授权或越权访问计算机系统资源，或破坏资源的完整性、可信性的行为，无论其成功与否，都认为是入侵，对这些入侵行为的识别就是入侵检测。

IDS就是完成上述入侵检测任务的计算机软件和硬件系统。很多IDS是实时检测入侵行为，但也有一些系统是非实时的，对收集的数据和日志进行事后分析。

2.2　IDS分类

一般来说，可以根据检测的数据来源和检测所依据的原则，对IDS系统进行分类。根据检测的数据来源，入侵检测可分为基于主机(Host-Based)的入侵检测系统和基于网络(Network-Based)的入侵检测系统。

基于主机的入侵检测系统往往以系统日志、应用程序日志等作为数据源，当然也可以通过其他手段(如监督系统调用)从所在的主机收集信息进行分析。主机型入侵检测系统保护的一般是所在的系统。目前很多UNIX类型的操作系统都有产生详细审计记录的功能模块，例如SunOS的C2级基础安全模块(C2 Basic Security Module of SunOS)。有了详尽的审计记录做数据源，基于主机的入侵检测系统能对计算机系统做全面的监控、对用户行为的分析粒度可以细到系统调用级。但不同系统产生的审计记录格式不同，这种类型的入侵检测系统存在移植性的问题。为了解决这个问题，

*)本课题得到国家科技攻关项目基金的资助。吕志军　硕士研究生、主要研究方向为计算机网络安全。黄　皓　副教授、主要研究方向为计算机网络安全、分布式计算。曾庆凯　教授、主要研究方向为计算机网络安全、分布式计算。陈道蓄　教授，博士生导师，主要研究方向为计算机网络安全、分布式计算、并行处理。谢　立　副校长，教授，博士生导师，主要研究方向为计算机网络安全、分布式计算、并行处理。

很多入侵检测系统将审计记录收集作为一个单独的底层模块，仅通过使用不同的底层模块就可使系统在多种平台上运行。

基于网络的入侵检测分析所需数据来源于在网络和操作系统协议栈中传输的数据包，其收集信息的方式类似于嗅探器(Sniffer)将一台机子的网卡设于混杂模式(promisc mode)，监听所有本网段内的数据包并进行判断。通过对包头和内容的分析，可以检测出一些已知的网络入侵；也可以使用异常检测的方法，监控整个网络上的数据包传输情况。一般网络型入侵检测系统担负着保护整个网段的任务。

根据检测所依据的原则，入侵检测可分为异常检测(Anomaly Detection)和误用检测(Misuse Detection)两大类。异常检测又称为基于行为(Behavior-Based)的入侵检测，它通过检测用户的异常行为来发现入侵事件，这种检测方法的原则是：任何与已知行为模型不符合的行为都认为是入侵行为。异常检测系统在学习阶段为用户正常情况下的行为建立行为模型(Profile)，以后系统将用户当前行为与原先的行为模型进行比较，如果发现有较大的偏差就产生告警。同样，异常检测系统也可为整个计算机系统和网络建立正常状态模型。它的优点是：可以发现未知的入侵行为，同时有一定的学习能力。它的缺点是：1)当用户合法地改变行为模式时(如使用新的应用程序)系统会误认为入侵发生；2)入侵者可通过对正常行为模式缓慢的偏离使系统逐渐适应；3)对于新用户，系统的学习阶段何时结束不易确定，同时在该阶段难以对用户进行正常的检测。

误用检测又称为基于知识(Knowledge-Based)的入侵检测，它首先对已知的入侵建立入侵特征(Signature)，然后根据当前的用户行为和系统状态对入侵进行匹配。这种检测方法的原则是：任何与已知行为模型符合的行为都是入侵行为。它的优点是：对入侵行为检测的准确性高。它的缺点是：只能发现已知的入侵行为。

2.3 NIDS 标准和模型

由于网络系统安全的需要，近几年 IDS 发展很快。许多研究机构和公司都对此进行了研究，如国内的南大苏富特公司、网威公司、启明星辰公司，国外的cisco、ISS 公司等都推出了自己的相应产品。

尽管现在有很多种 IDS 产品，但它们有各种各样的结构，还没有一个被广泛接受的统一标准。目前，有两个组织在进行 IDS 标准化工作，分别是美国国防部高级计划研究局的 CIDF(Common Intrusion Detection Framework working group)工作组和 Internet 工程任务组的 IDWG(Intrusion Detection Working Group)工作组。这里我们主要介绍 CIDF 的有关标准。CIDF 阐述了一个入侵检测系统(IDS)的通用模型。它将一个入侵检测系统分为以下部件：事件产生器；事件分析器；响应单元；事件数据库。

由于本文主要介绍对 NIDS 的技术检测，所以主要介绍 CIDF 对 NIDS 的规定。图1是 CIDF 规定的 NIDS 结构中各个部件之间的关系。

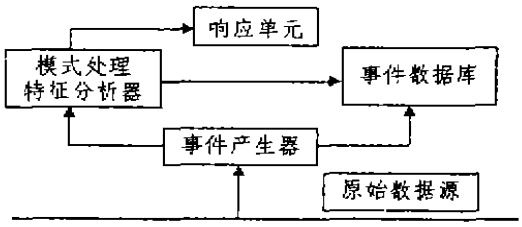

图1 NIDS 模型中各部件之间的关系

CIDF 将 NIDS 需要分析的数据统称为事件，它是网络中的数据包。

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。事件分析器分析得到的数据，并产生分析结果。响应单元则是对分析结果作出反应的功能单元，它可以作出切断连接、改变文件属性等强烈反应，也可以只是简单的报警。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。

在这个模型中，前三者以程序的形式出现，而最后一个则往往是文件或数据流的形式。

2.4 NIDS 的特点

Crobbze 和 Spafford 在文[2]中，定义了一个 NIDS 系统应具有的特点：

·在人很少干预的情况下，能连续运行。

·在系统由于事故或恶意攻击，崩溃时，具有容错能力。当系统重新启动时，NIDS 能自动恢复自己的状态。

·它必须能抗攻击。NIDS 必须能监测自己的运行，检测自身是否被黑客修改。

·运行时，尽可能少地占用系统资源，以免于扰系统的正常运行。

·对被监控系统的安全策略，可以进行配置。

·必须能适应系统和用户行为的变化。如系统中增加了新的应用，或用户的应用改变。

当要监控的系统数目或攻击方法增多后，认为 NIDS 还要具有下列特点：

·当要实时监控大量主机时，系统应能扩展，

·当 NIDS 一些部件因为某些原因停止工作时，应尽量减少对系统其它部分的影响，

·系统应能允许动态配置。当系统管理员修改配置时，不需要重新启动配置

3. NIDS 的基本安全性能

3.1 NIDS 存在的弱点

在 CIDF 模型中定义的 NIDS 各个部件都存在被攻击的可能性。

"事件产生器"是 NIDS 系统中唯一的数据入口。对 NIDS 的事件产生器的攻击能使 NIDS 失去数据来源，不能检测所负责网络上发生的入侵事件，或者使其不能对获得的原始数据进行解码。

"模式处理特征分析器"的有效性也非常重要，因为整个 NIDS 依靠"模式处理特征分析器"来分析数据，产生安全信息。高水平的入侵者能找到很多办法来欺骗"模式处理特征分析器"，使其不能按照安全规则分析出入侵事件。如果一些"模式处理特征分析器"实现得比较简单，仅使用一些简单的特征匹配方法来检测入侵事件，则更可能被入侵者欺骗。

"事件数据库"中记录着系统检测到的各个入侵行为的数据。攻击者可以攻击"事件数据库"，使其不能正常地记录入侵行为，甚至可以篡改这些记录信息。

"响应单元"也是被攻击的对象之一。一方面，攻击者可以破坏"响应单元"，使其不能对攻击者的行为作出反应，如切断、阻隔攻击者的行为，甚至可以误导"响应单元"，使"响应单元"对系统内部正常的网络应用也作出反应，影响网络的正常运行。

3.2 NIDS 的基本安全性能

NIDS 作为一个安全产品，在系统中有重要的作用，它本身也成为被攻击目标。一个入侵者如果想攻击某个网络，他很可能要先攻击 NIDS，使其不能发挥作用或提供假信息。针对 3.1 节中列出的弱点，为了能正常发挥作用，有一定的抵御攻击能力，NIDS 至少应该具有以下基本安全性能。

(1)抗"过载"。"过载"是使 NIDS 因其处理能力限制，来不及处理接收到的数据，不能正确检测出"入侵"行为。

(2)抗"失效"。"失效"是使 NIDS 因耗尽资源或发生故障而不能工作。

(3)抗"欺骗"。"欺骗"是使 NIDS 错误理解它所接收到的数据。例如，检测方发给接收方一串字符"attack"，通过采用一些欺骗方法，使 NIDS 接收到的内容和接收方收到的信息不一致，如"atackt"。

要满足以上这些安全性能，在设计 NIDS 时，应充分考虑自己的处理能力，采用高性能机器，优化软件设计，提高软件处理能力，识别各种"欺骗"行为，减少"过载"、"失效"的发生。

4. NIDS 安全性能的检测

4.1 检测 NIDS 安全性能的重要性

因为 NIDS 是安全系统中的重要组成部分，系统的安全管理在很大程度上要依靠其提供的信息，一个有缺陷的 NIDS 系统，不但提供的安全信息少，还可能让该系统管理人员造成错觉，当发生入侵时，让系统不报警。

NIDS 本身安全性能的设计或实现是否有缺陷，这些设计是否有效，都必须通过检测来检验。

NIDS 是否具有 3.2 节中的基本安全性能，是 NIDS 能否正常发挥作用的关键，因此，需要检测 NIDS 的安全性能。

4.2 检测 NIDS 安全性能的方法

4.2.1 "正常"检测　是根据 NIDS 的功能说明，模拟各种"入侵"行为，检验 NIDS 各个功能是否工作正常。

4.2.2 "过载"检测　其目的是通过发送大量数据，使 NIDS 因其处理能力限制，来不及处理接收到的数据，不能正确检测出"入侵"行为的方法，来检测 NIDS 是否具有抗"过载"能力。

检测过程分为两步，第一步，检测人员大量地发送数据给 NIDS，使其检测器过载；第二步，模拟进行网络攻击，检测 NIDS 能否正常工作。在正常情况下，NIDS 能检测出这些网络攻击，而在过载情况下，NIDS 因收集不到足够的数据，不能检测出发生的攻击。如果 NIDS 实现得比较好，它就不会被完全过载，还能正常工作。

4.2.3 "失效"检测　其目的是通过发送大量精心设计的数据，使 NIDS 因耗尽资源或发生故障而不能工作的方法，来检测 NIDS 是否具有"抗失效"能力，这种检测方法比"过载"检测难于实施。

经过精心设置，向 NIDS 发出一系列数据包，使 NIDS 因为本身的设计错误，在处理这些数据时，发生故障，不能继续工作。很多 NIDS 在设计时，使用模式匹配检测网络入侵，需要在内存或硬盘保存"入侵行为"的状态，才能正确检测。基于这个原理，发送可以产生大量状态的数据流，使 NIDS 保存大量的状态，耗尽内存和硬盘资源，无法保存后续"入侵行为"的状态，不能继续检测。

4.2.4 "欺骗"检测　其目的是通过改变所发送数据的属性，使 NIDS 错误理解它所接收到的数据，不能检测出入侵行为的方法，来检测 NIDS 是否具有抗"欺骗"能力，例如，将一个 IP 包分片，将要检测的内容分布在几个 IP 包分片中，当 NIDS 不能正确地重组 IP

包分片时，就可能检测不出检测的内容。

"欺骗"检测的原则是使 NIDS 截获到的信息与接收方正常收到的信息不一致。

很多欺骗方法是和具体的应用层数据内容有关，通过发送假数据，使 NIDS 不能正确识别出检测方的真实数据。NIDS 的检测原理是分析各个应用的数据，看其是否符合入侵特征。例如，提供 TELNET 服务的主机，限制"root"用户远程访问，当 NIDS 检测到"root"用户试图远程访问时，就认定为"入侵"。针对这个检测功能，可以通过下面的方法进行"欺骗"检测。

假设 IP 包从检测点到接收方的生存期(Time To Live，TTL)为20，从检测点到 NIDS 的 TTL 为10。第一步，检测点先发送一个 IP 包 A 给接收方，TTL 等于21，序列号为100～103，数据内容是"USER"，NIDS、接收方都接收到该包。第二步，检测点再发送一个 IP 包 B 给接收方，TTL 等于15，序列号等于104～107，数据内容为"HACK"，该包可以到达 NIDS 所在的网络，被 NIDS 截获到，但不能到达接收方所在网络。第三步，检测点再发送一个 IP 包 C 给接收方，该包的 TTL 等于21，序列号同 IP 包 B，为104～107，数据内容为"root"，接收方和 NIDS 都能接收到这个包。最后，接收方收到的信息是"USER root"，NIDS 收到信息"USER hack"或"USER root"。如果 NIDS 接受 IP 包 B，忽略 IP 包 C，则收到信息"USER hack"；如果用 IP 包 C 覆盖 IP 包 B，则收到信息"USER root"。通过改变 IP 包 B 和 IP 包 C 的发送顺序，可以使 NIDS 只得到数据"USER hack"，成功欺骗 NIDS。

在"欺骗"检测中，除通过生存期来检测外，还可以通过改变 IP 包的校验值或利用网络的 MTU(maximum transmission unit)等方法来实现"欺骗"检测。

结论 目前，国内对 NIDS 的研究主要集中在实现 NIDS 的功能和提高性能上，对 NIDS 本身的安全性能研究较少，NIDS 在安全系统中的重要程度还取决于其本身的安全性能，因此有必要对其进行检测，来验证它的安全性、可靠性。本文仅对检测 NIDS 本身的安全性能提供了几种方法，还有待进一步研究。针对具体的 NIDS 产品来说，还需要从功能、价格等方面考虑，按照2.4节中列出的特点进行检测，如从检测类型设置、系统配置、报警、日志、结构、价格等因素来考虑。

参 考 文 献

1 Mukherjee B, Heberlein T L, Levitt K N. Network intrusion detection. IEEE Network, 1994, 8(3): 26～41

2 Crosbie M, Spafford G. Active defense of a computer system using autonomous agents [Technical Report 95-008]. COAST Group, Department of Computer Sciences, Purdue University, West Lafayette, IN 47907-1398, Feb. 1995

3 Stanford-Chen S. Common Intrusion Detection Framework. http://seclab.cs.ucdavis.edu/cidf/

4 Stanford-Chen S, et al. GrIDS-A Graph-Based Intrusion Detection System for Large Networks. In: The 19th National Information Systems Security Conf. 1996

5 Fox K L, et al. A Neural Network Approach towards Intrusion Detection. In: Proc. of the 13th National Computer Security Conf. Oct. 1990

6 Pukerza N F, et al. A Methodology for Testing Intrusion Detection Systems. IEEE Transactions on Software Engineering, 1996, 22: 719～729

7 StJohns M. Authentication Server. RFC 931, TPSC, Jan. 1985

8 Stevens W R. TCP/IP Illustrated, Vol 1. Addison-Wesley, Reading, MA, 1994

9 Postel J. Internet Protocol-DARPA Internet Program Protocol Specification. RFC 791, USC/Information Sciences Institute, Sep. 1981

10 Postel J. Internet Protocol-DARPA Internet Program Protocol Specification. RFC 791, USC/Information Sciences Institute, Section 3.2, line 1099, Sep. 1981

11 Atkinson R. Security Architecture for the Internet Protocol. RFC 1825, Naval Research Laboratory, Aug. 1995

12 Postel J. Transmission Control Protocol-DARPA Internet Prgram Pro-tocol Specification. RFC 793, USC/Information Sciences Institute, Sep. 1981

13 Jacobson V, Braden R, Borman D. TCP Extensions for High Performance. RFC 1323, LBL, ISI, Cray Research, May 1992

14 Joncheray L. A Simple Attack Against TCP. In: 5th USENIX UNIX Security Symposium, June 1995. ICSA lab

15 Paxson V. Bro, A System for Detecting Network Intruders in Real-Time. In: 7th Annual USENIX Security Symposium, Jan. 1998

16 Paxson V. End-to-End Internet Packet Dynamics. In: ACM SIGCOMM'97, Cannes, France, Sep. 1997

(上接第129页)

致谢：感谢国防科技大学软件教研室主任王戟博士提供了有关资料。

参 考 文 献

1 Computing Sciences Accreditation Board. Criteria for accrediting programs in computer science in the United States. Technical report in preparation for June 2000. Version 1.0, January 2000. http://www.csab.org/criteria2k/v10.html

2 Denning P J, Comer D E, et al. Computing as a discipline. Communications of the ACM, 1989, 32(1): 9～23

3. Denning P J. Our seed corn is growing in the commons. Information Impacts Magazine, March 1999. http://www.cisp.org/imp/march99/denning/03-99denning.htm

4 Lidtke D K, Stokes G E, et al. ISCC'99: An information systems-centric curriculum'99, July 1999. http://www.iscc.unomaha.edu.

5 Tucker A B, Barnes B H, et al. Computing Curricula'91. Association for Computing Machinery and the Computer Society of the Institute of Electrical and Electronics Engineers, 1991