入侵检测系统简介

1.网络安全现状

1.1 我国网络安全现状

近年来，随着互联网在中国的迅速发展，政府、经济、军事、社会、文化和人们生活等各方面都越来越依赖于网络。网络经济的兴起和发展，极大地改变了人们的生活、工作和思维方式，促进了经济的发展。尤其是从 1999 年开始，在世界信息化大潮的影响和政府的大力推动下，国内逐渐兴起了一股政府上网、企业上网和家庭上网的热潮，眼下“数字中国”正大踏步向我们走来，大量建设的各种信息化系统已经成为国家关键基础设施，其中许多业务要与国际接轨，诸如电信、电子商务、金融网络等。但在这个发展潮流中，网络安全隐患始终难以解决，应该说国内网络安全是当今网络应用中最敏感的问题，是影响国家大局和长远利益的重大关键问题。黑客入侵给这个产业造成的负面影响是显而易见的。然而，由于网络安全的脆弱性，黑客在网上的攻击活动每年都以几何级数的速度在增长。尽管目前世界上已经有许多防火墙产品，但由于防火墙技术本身的局限性，无法彻底地防护智能化侵袭者如黑客对系统的攻击。

1.2 网络面临的威胁

（1）黑客的攻击

据统计，几乎每 20 秒全球就有一起黑客事件发生，仅美国每年所造成的经济损失就超过 100 亿美元。他们利用网络的各种漏洞和缺陷，或者修改网页进行恶作剧；或者非法进入主机破坏程序；或者闯入银行网络转移资金；或者窃取网上信息兴风作浪；或者进行电子邮件骚扰；或者施放病毒使网络陷于瘫痪等等。

政府、军事、邮电、金融和商业运营网络更是他们攻击的主要目标。新千年伊始，黑客便大肆攻击全球知名网站，一度使著名的“CNN”、“yahoo”、“Amazon”、国内的“新浪网”等陷入几个小时的瘫痪，2001 年“国际劳动节”期间，更是中美黑客组织的短兵相接，.CN 的网站或者被修改首页、或者被攻瘫痪达一千多个。

（2）管理的缺陷

网络系统的严格管理是企业、机构及用户免受攻击的重要措施。事实上，很多企业、机构及用户的网站或系统都疏于管理。据 IT 界企业团体的调查，美国 90%的 IT 企业对黑客攻击准备不足.目前，美国 75% - 85%的网站都抵挡不住黑客的攻击，约有 75%的企业网上信息失窃，其中 25%的企业损失在 25 万美元以上。我国的 ISP、证券公司及银行也多次被国内外黑客攻击。但是仍然有许多单位对自己网络的安全问题毫无认识，甚至遭到了黑客攻击都毫不知晓。

（3）软硬件的不足

国外先进国家对信息技术尤其是网络技术实行垄断，目前国内网络建设不论是网络硬件（如路由器、交换机、服务器等），还是系统软件基本上是采用拿来主义，这种将本国的信息系统完全建立在别国产品基础上的国家信息安全是非常危险的，这就对网络安全提出了更深层次的需求。同时，网络技术和软件技术本身就存在着大量漏洞和 Bug，缺乏相应的安全机制。

1.3 防火墙的缺陷

（1）防火墙难于防内

人们普遍认为：只要设置防火墙守住网络的门户不让黑客进入就万事大吉了。的确，设置防火墙对保证网络门户的安全很重要，但它并非无坚不摧。防火墙无

法防止来自网络内部的攻击，这几年的统计表明，大约 75%-80%的蓄意攻击由企业内部工作人员发起，因为他们知道企业的安全策略。

（2）防火墙难于管理和配置，易造成安全漏洞

防火墙的管理及配置相当复杂，要想成功的维护防火墙，要求防火墙管理员对网络安全攻击的手段及其与系统配置的关系有相当深刻的了解。防火墙的安全策略无法集中管理。一般来说，由多个系统（路由器、过滤器、代理服务器、网关、堡垒主机）组成的防火墙，管理上有所疏忽是在所难免的。目前国内使用的许多硬件防火墙是国外产品，其复杂界面和英文说明，使许多管理员望而却步。

（3）防火墙的安全控制主要是基于 IP 地址的，难于为用户在防火墙内外提供一致的安全策略。许多防火墙对用户的安全控制主要是基于用户所用机器的 IP 地址而不是用户身份，这样就很难为同一用户在防火墙内外提供一致的安全策略，限制了企业网的物理范围。

（4）防火墙只实现了粗粒度的访问控制

防火墙只实现了粗粒度的访问控制，且不能与企业内部使用的其它安全机制（如访问控制）集成使用，这样，企业必须为内部的身份验证和访问控制管理维护单独的数据库。

1.4 入侵检测（IDS）的必要性

目前，有多种方法可以检测到网络入侵行为，但是几乎所有这些方法都要使用日志文件或跟踪文件。但是，这些文件记录的绝大多数数据是在系统正常运行时产生的。如果没有第三方工具把正常情形与异常情形时的记录内容区分开来，则入侵行为很难检测。目前，针对大多数企业网络存在外部入侵、恶意攻击、信息泄漏、资源滥用等现状，入侵检测技术是防火墙技术合理而有效的补充，可以

弥补防火墙的不足，它从计算机网络系统中的若干关键点收集信息，并分析这些信息，看看网络中是否有违反安全策略的行为和遭到袭击的迹象。为网络安全提供实时的入侵检测及采取相应的防护手段，如记录证据用于跟踪、恢复、断开网络连接等。入侵检测被认为是防火墙之后的第二道安全闸门，在不影响网络性能的情况下能对网络进行检测，从而提供对内部攻击、外部攻击和误操作的实时保护。

二、入侵检测系统的基本原理

2.1 入侵检测（IDS）的概念

入侵检测系统是一种主动的网络安全防护措施，它从系统内部和各种网络资源中主动采集信息，从中分析可能的网络入侵或攻击。对一个成功的入侵检测系统来讲，它不但可使系统管理员时刻了解网络系统（包括程序、文件和硬件设备等）的任何变更，还能给网络安全策略的制订提供指南。更为重要的一点是，它易管理、配置简单，从而使非专业人员非常容易地获得网络安全。而且，入侵检测的规模还应根据网络威胁、系统构造和安全需求的改变而改变。入侵检测系统在发现入侵后，会及时作出响应，包括切断网络连接、记录事件和报警等。

入侵检测的第一步是信息收集，采集内容和对象为系统、网络、数据及用户活动的状态和行为。采集信息时需要在计算机网络系统中的不同网段和不同主机采集。

IDS 主要执行如下任务：

1. 监视、分析用户及系统活动。
2. 系统构造和弱点的审计。
3. 识别反映已知进攻的活动模式并向相关人士报警。

4． 异常行为模式的统计分析。

5． 评估重要系统和数据文件的完整性。

6． 操作系统的审计跟踪管理，并识别用户违反安全策略的行为。

2.2 入侵检测（IDS）的分类

入侵检测通过对入侵行为的过程与特征进行研究，使安全系统对入侵事件和入侵过程作出实时响应，可按照其采用的技术及系统所检测的对象进行分类。

一般来讲，入侵检测系统采用如下两项技术：

一、异常检测技术。假定所有入侵行为都是与正常行为不同的。如果建立系统正常行为的轨迹，那么理论上可以把所有与正常轨迹不同的系统状态视为可疑企图。对于异常阀值与特征的选择是异常发现技术的关键。比如，通过流量统计分析将异常时间的异常网络流量视为可疑。异常发现技术的局限是并非所有的入侵都表现为异常，而且系统的轨迹难于计算和更新。

二、模式检测技术。假定所有入侵行为和手段（及其变种）都能够表达为一种模式或特征，那么所有已知的入侵方法都可以用匹配的方法发现。模式发现的关键是如何表达入侵的模式，把真正的入侵与正常行为区分开来。模式发现的优点是误报少，局限是它只能发现已知的攻击，对未知的攻击无能为力。

入侵检测系统按其输入数据的来源来看，可以分为 3 类：

1、基于主机的入侵检测系统：其输入数据来源于系统的审计日志，一般只能检测该主机上发生的入侵。

2、基于网络的入侵检测系统：其输入数据来源于网络的信息流，能够检测该网段上发生的网络入侵。

3、采用上述两种数据来源的分布式入侵检测系统; 能够同时分析来自主机

系统审计日志和网络数据流的入侵检测系统，一般为分布式结构，由多个部件组成。

前两类入侵检测系统虽然能够在某些方面有很好的效果，但从总体来看都各有不足，孤立地去评估都是不可取的。分布式入侵检测系统则同时具有这两方面的技术，可以互相补充不足，达到真正全面检测和防护的作用。黑盾 - 网络入侵检测系统（HD-NIDS）正是这样一种分布式入侵检测系统。