ISSN:2705-0971(Print); 2705-0947(Online)
Pisco Med Publishing

计算机网络入侵检测技术研究

纪阳阳

西安外事学院 陕西省西安市 719000

摘要：现如今，网络技术发展的越来越快，全球信息化的进程也在逐步剧增，网络信息系统的影响力也日益扩大，小到单位，大到国计民生都离不开这个基础设施。所以，在整个国防安全当中，网络安全也是一个非常关键的组成部分。在我们所熟知的防火墙等安全措施推行之后又出现了一道更为安全的闸门，那就是入侵检测技术，该项技术属于动态防护，其能够迅速在众多网络数据当中检测出哪些是正常的通讯，而哪些又是非正常的入侵。这样一来，既能够缓解人工分析以及解码所产生的庞大工作量，还能够使入侵检测系统的适应性得到提升。以此作为基础，本文具体的论述了计算机网络入侵检测技术。

关键词：计算机；网络入侵；检测技术

1 引言

自本世纪开始，信息和网络技术都走上了高速发展的道路，由于互联网规模的日益扩张，其所带来的影响也在整个社会中不断蔓延开来。受到多方面的驱动，例如政治、军事或者是经济等，黑客们对计算机以及网络基础设施，尤其是那些隶属于某个官方机构的网站，发起了强烈的攻势。结合强有力的入侵检测，能够在最快的时间内对网络流量当中的异常入侵行为进行有效的辨识。基于此，或许会触发自动响应步骤，又或许会对系统管理员进行快速提醒，让他们采取有效措施快速解决问题，使恶意行为中断，以防更多的损失出现。因此，对于如今的社会来说，入侵检测技术意义重大。

2 入侵检测技术概述

2.1 入侵检测简介

作为自发安全防护技术，入侵检测提供了三项实时保护：第一项是针对内部攻击；第二项是针对外部攻击；第三项是针对用户误操作，在网络或者是系统被侵害以前及时进行拦截。所以，入侵检测又被大家称为是站在防火墙身后的双层保护门，可以在对网络性能不造成任何影响的前提下检测网络及系统。实现入侵检测，通常都会执行下列任务：第一，对用户以及系统活动进行实时的监视，并进行深入的分析；第二，审计系统的整体构造，并发现弱点；第三，对已经知悉的进攻活动模式进行有效的识别，并及时向有关人士报警；第四，对非正常行为模式做出全面的分析；第五，对重要的系统及数据文件是否完整进行评估；第六，对操作系统进行审计，并且要进行跟踪式管理。对于防火墙来说，入侵检测是一项非常合理的补充，既能够帮助操作系统及时应对来自于外部的网络攻击，又能够对操作系统管理人员的安全管理水平进行不断的强化，从而使信息安全基础结构变得更加完整。

2.2 入侵检测系统的架构

通常来说，入侵检测系统的分类是基于两种标准之下的：第一种分类是根据系统所处理的数据来源；第二种是根据检测非法事件的方式。由于处理的数据来源有所差异，入侵检测系统能够被划分为两种：第一种是基于主机的 (HIDS)；第二种是基于网络的 (NIDS)。通过图 2-1 我们能够看出，NIDS 借助监控网络流量来对入侵行为进行检测。通常来看，其是对流经网络上的一些关键设备进行快速的抓取和分析，例如路由器或者是交换机等，以此来实现网络行为的监控。

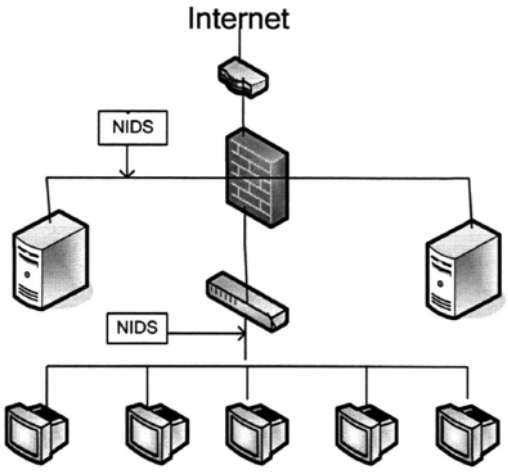

图 2-1 NIDS 示意图

ISSN:2705-0971(Print); 2705-0947(Online)

通过图 2–2 我们能够看出，HIDS 在主机上驻存，保障该台主机的安全是其主要的责任，其所监控的数据有以下几种：第一种是流经这台主机处于非混杂模式的网卡的一切数据包；第二种是该台主机的系统日志；第三种是系统调用等。需要注意的是凡是 HIDS 监控的网络数据包必然都是指向其所驻存的主机。

这两种 IDS 各有各的优点。相比较而言，HIDS 因为获取的数据更为详细，其检测率非常可观，误报率也很低。但是它也存在一定的缺陷，因为其只会对一台计算机的行为进行监控，对网络中其他计算机的存在视而不见，对威胁的反应会相对迟缓。当其在本机上察觉出入侵踪迹的时候，黑客的行动通常已经有所展开。除此以外，手段比较厉害的攻击者能够借助对本机日志文件加以修改等来避免检测。因此通常来讲，HIDS 都是网络纵深防御体系的最后防线。NIDS，可以说是站在防火墙后面的双层防线。NIDS 只会对网络数据包进行监控，相比较于 HIDS 来说，能够供其分析的数据非常稀缺，因此 NIDS 的检测率并不乐观，误报率也时常比较高。但是，其对入侵的整体状态极度敏感，可以在出现入侵的时候敏锐的做出反应。

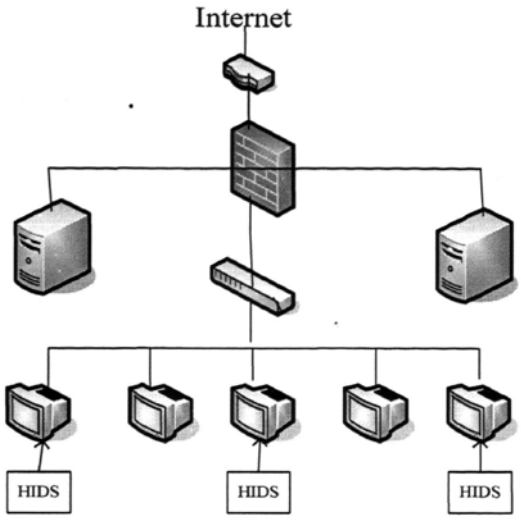

图 2-2 HIDS 位置示意图

3 入侵检测系统的局限性

3.1 入侵技术在不断发展

网络攻击技术研究是入侵检测技术的核心依托，借助跟踪入侵技术的发展，使得入侵检测水平不断强化。在网络平台上存在着非常密集的黑客站点，他们通常会将大量的系统漏洞资料发布出来，并讨论各式各样的攻击方法。让人不禁胆战心惊的是这些活动都是有组织性的，在国外，信息战手段已经和核生化武器被列入相同危险等级。破坏者的能力我们无法预测，入侵技术发展的越来越强，入侵检测的难度也就越来越大，对一切可能出现的入侵手段进行预测非常困难，所以有效的入侵检测系统，既要满足对已知入侵模式的识别，还要具备对未知入侵模式的应对能力。

3.2 入侵活动可以具有很大的时间跨度和空间跨度

有预先谋划好的入侵活动通常来说都会有一套非常周密的策划准备。一项入侵活动会分为多个环节，而每个环节都很有可能会在某一个时间段，或者某一个地点分别实现。这对预警来说，极大的增加了难度。所有的检测模型通常都会被有限的时间窗口所制约，这样就会导致滑出时间窗口的部分事实被忽略。而且，在空间范围比较广阔的情况下所出现的非正常现象，检测模型的综合以及联想水平也会受到局限。

3.3 非线性的特征还没有有效的识别模型

对于入侵检测技术而言，其难度一方面在于提取入侵模式，另一方面在于入侵模式的检测方式和算法。事实上，入侵模式可以说是一个静态事物，然而实际上的入侵活动并非静止，相反是灵活多变的。站在技术层面来说，入侵技术的发展已经上升到了一定的阶段，然而无论是站在理论上还是实践上，入侵检测技术都未得到真正的发展。所有出现在市场上的入侵检测系统，基本上也都是水平相当。对于如此复杂的网络入侵活动，在对网络入侵检测技术进行深入研究的时候，不只要关注入侵技术，还要对入侵检测策略以及模型的理论投入更多的重视。

4 入侵检测技术的发展方向

入侵检测技术正在持续的发展过程当中，然而入侵技术也并未停下脚步。现如今的高速网络，特别是不断发展起来的交换技术等，导致通过共享网段侦听的网络数据采集手段出现了一定的局限性。近年来，入侵检测技术的发展方向主要有以下几个：

4.1 分布式入侵检测

该种形式的入侵检测主要有两层含义：第一层含义是针对分布式网络攻击；第二层含义是借助分布式方法对入侵攻击进行有效的检测，其核心技术主要是检测信息的协同处理以及有效提取入侵攻击全局信息。以往所使用的 IDS 通常只能响应于单一的主机或者是网络架构，然而对于异构系统以及规模比较庞大的网络检测来说比较吃力，此外，IDS 系统的不同也没有办法实现协同工作，为了化解该问题，就需要采取该种入侵检测以及通用入侵检测技术构架。

4.2 智能化入侵检测

该种入侵检测实际上就是通过智能化的手段来实施

ISSN:2705-0971(Print); 2705-0947(Online)

入侵检测。在对入侵检测系统进行构建的时候，采用专家系统思想也是极其常见的一种方式，其能够使知识库更新扩展的越来越多，使入侵检测系统的防范水平日益强化。虽然在整个入侵检测技术领域已经开始应用了诸如智能体以及神经网络等，然而这些研究工作都还处于尝试阶段，对于智能化的 IDS 来说，仍然需要得到更深的研究。

4.3 全面的安全防御方案

该种防御方案实际上就是借助安全工程风险管理的思想等对网络安全问题加以处理。其在处理的过程中将网络安全视为一个整体性的工程，站在多个角度，如管理以及防火墙等来系统的评估所关注的网络，之后再提出有执行价值的解决方案。

4.4 应用层入侵检测技术

大量的入侵语义只有处于应用层的时候才能够被完好理解，然而当前的 IDS 只能够对 Web 等通用协议进行检测，没有办法对数据库系统等进行有效的处理。很多以客户、服务器结构等大型应用作为基础的，在对入侵检测技术进行保护的时候都需要介入到应用层。

5 结论

对于计算机网络安全领域来说，入侵检测技术自始至终都是热点与难点。现如今，接入网络的计算机数目越来越多，无论是政治领域，还是军事、民生等都受到了网络的影响。然而，有很多黑客因为受到了经济或者政治方面的驱动，做出了大量对社会不利的行为，使得经济损失惨重，人心惶惶。通过什么样的方式在最快的时间内从海量网络流量里精确检测出非正常流量，在萌芽阶段就对网络威胁控制进行扼杀，是入侵检测技术最为核心的目标。网络本身就具有一定的复杂性，而当前花样百出的攻击手段更是给入侵检测技术增加了难度，传统单一的入侵检测技术已经无法有效的对非正常行为做出识别。本文对入侵检测技术的原理以及众多基本问题等进行了深入的分析，并对国内外研究成果做出了全面的总结，简要地阐述了其优缺点。

参考文献：

[1] 谢潇雨 . 基于卷积神经网络的入侵检测模型研究 [D]. 南京：南京邮电大学 ,2019.
[2] 叶青 . 基于数据挖掘的网络安全态势感知研究 [D]. 南京：南京邮电大学 ,2019.
[3] 刘玉标 . 计算机网络入侵检测中人工智能技术的应用 [J]. 科技风 ,2019(32):94+97.
[4] 苏醒 . 基于网络行为的计算机网络安全预警与响应系统研究 [J]. 电子测量技术 ,2019,42(21):123-126.
[5] 张恒 , 康建明 , 张国海 , 杜洪恩 , 蒋平 , 彭强吉 . 基于改进 FMECA 方法气吸鸭嘴滚筒式排种器的可靠性分析 [J]. 石河子大学学报 (自然科学版),2019,37(05):543-548.
[6] 李妍 . 计算机网络入侵检测系统的研究 [J]. 科技风 ,2019(25):105-106.
[7] 王立纲 , 韩瑞美 .PA44-180 飞机起落架收放系统常见故障分析 [J]. 航空维修与工程 ,2019(06):84-86.
[8] 侯方正 . 基于贝叶斯网络模型的车载 ATP 故障预测研究 [D]. 成都：西南交通大学 ,2019.
[9] 孙少武 . 基于深度学习的液压泵健康状态监测方法研究 [D]. 秦皇岛：燕山大学 ,2019.
[10] 闫明辉 . 计算机网络入侵检测系统匹配算法的研究 [J]. 电子设计工程 ,2019,27(08):34-37+43.