2025 年 第 25 卷 第 7 期
2025, 25(7):02654-10
科 学 技 术 与 工 程
Science Technology and Engineering
ISSN 1671—1815
CN 11—4688/T

DOI:10.12404/j.issn.1671-1815.2402609
引用格式:杨宇, 陈一丁, 赵荣, 等. 网络安全主动防御研究综述[J]. 科学技术与工程, 2025, 25(7): 2654-2663.
Yang Yu, Chen Yiding, Zhao Rong, et al. Review of research on active defence for network security[J]. Science Technology and Engineering, 2025, 25(7): 2654-2663.

自动化技术、计算机技术

网络安全主动防御研究综述

杨宇[1], 陈一丁[2], 赵荣[1], 陈明媚[3], 闫钰[2]
(1. 武警工程大学信息工程学院, 西安 710086; 2. 武警工程大学研究生大队, 西安 710086; 3. 武警工程大学基础部,西安 710086)

摘 要 随着现代网络信息技术的不断发展,作为传统被动的网络安全防御手段已经无法有效应对不断变化的新型网络威胁,不能满足当前网络安全的需求。作为现如今主要网络防御手段,主动防御克服传统防御的诸多缺陷,能够有效应对未知网络活动,展现出很强的优势。从主动防御的发展过程出发,对网络安全主动防御目前存在的主要技术进行了梳理,总结分析了网络安全入侵防护、网络安全入侵检测、网络安全入侵预测、网络安全入侵响应 4 个层面的主要技术优缺点,并对其未来发展方向进行了分析与展望。

关键词 网络安全主动防御; 入侵防护; 入侵检测; 入侵预测; 入侵响应
中图法分类号 TP393; **文献标志码** A

Review of Research on Active Defence for Network Security

YANG Yu[1], CHEN Yi-ding[2], ZHAO Rong[1], CHEN Ming-mei[3], YAN Yu[2]
(1. College of Information, Engineering University of People Armed Police, Xi'an 710086, China;
2. College of Graduate Brigade, Engineering University of People Armed Police, Xi'an 710086, China;
3. College of Ministry of Basic Education, Engineering University of People Armed Police, Xi'an 710086, China)

[**Abstract**] With the continuous development of modern network information technology, the traditional passive network security defences are static defences that can not effectively respond to new types of network threats and can no longer meet the needs of network security. As the main network defence mean, active defence overcomes the many defects of traditional defence, can effectively respond to unknown network activities, showing strong advantages. Starting from the development process of active defense, the main technologies currently existing in network security active defense were sorted out, and the advantages and disadvantages of the main technologies at four levels, namely, network security intrusion defence, network security intrusion detection, network security intrusion prediction, and network security intrusion response, were summarised and analyzed, as well as the analysis and outlook of its future development direction.
[**Keywords**] active defence for network security; intrusion prevention; intrusion detection; intrusion prediction; intrusion response

随着互联网的快速发展,万物进入互联时代。日新月异的网络技术更加全面、深刻地进入寻常百姓家。人们的生活因为网络的迅速发展而变得丰富多彩,但也因为网络的不断变化而面临多种多样的网络风险挑战[1]。近年来,中国网络安全环境遭受各种网络安全事件的冲击,境内外敌对势力对中国政治、经济、军事等各个领域数据进行信息窃取和破坏愈演愈烈,各种网络安全事件不断发生[2],如 WannaCry[3]、Conficker[4]、eBay[5] 等网络攻击事件的发生,一再表明网络安全一直面临着严峻挑战[6]。以防火墙、入侵检测、安全扫描、口令验证等技术构成的传统网络安全防御是一种被动等待式防御手段[7],已经难以有效应对现如今不断演进的新型网络攻击[8]。因此,突破传统网络安全防御的局限性,研究与发展能够动态、实时保护的网络安全主动防御技术迫在眉睫。

1 网络安全主动防御概况

1.1 主动防御

防御指为了抵御某种攻击、威胁或者危害而采

收稿日期: 2024-04-10 修订日期:2024-10-14
基金项目: 全军军事理论项目;大学基础创新研究项目(WJY202306)
第一作者: 杨宇(1981—),男,汉族,内蒙古赤峰人,博士,副教授,硕士研究生导师。研究方向:网络安全。E-mail:631672442@qq.com。

取一系列对策。防御的形式多种多样,可以是军事上的防御,也可以是社会治安上的防御,还可以是个人防御,无论哪一种形式的防御,其目的都是减少和避免不必要的损失。防御的概念最早在作战领域中被提出,防御方通常在形式上是被动的,然而,防御方通过提前准确了解攻击方的动向,积极调整防御部署,及时填补漏洞,构建合理防线,必要时主动出击消灭敌人[9]。

1.2　网络安全主动防御

主动防御一词最初由英文"proactive defence"翻译而来,它的确切含义是指带有提前预谋的主动防御,指通过某些机制阻止攻击者对目标发起攻击[10]。美国国家安全机构2011年首次提出了网络安全主动防御战略[11],该战略提出了将被动防御与主动防御同步,对可能存在的网络威胁进行实时检测、分析和跟踪并对其进行迁移和消灭。由于现在并未有人对网络安全主动防御给出明确的定义,致使该领域的概念尚未统一。基于这种状况,许多中外专家进行了大量的研究工作。美国国际互联网安全系统公司(International Internet Security Systems,ISS)提出了网络安全主动防御防护检测响应模型(protection detetion response model,PDR)如图1所示。

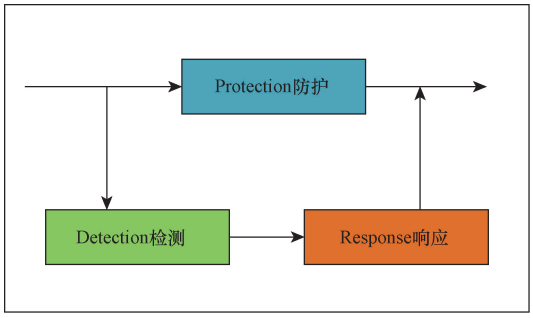

图1　PDR模型[12]

Fig. 1　Model of PDR[12]

在PDR模型中,网络安全入侵防护、网络安全入侵检测和网络安全入侵响应三部分作为网络安全主动防御模型的重要组成部分[12]。苏杰等[13]认为网络安全主动防御通过对网络内部可能存在的攻击、外部的网络入侵和内部操作的失误提供全时防护,主动防御手段与传统防火墙等被动防御手段相结合可以为网络安全构建一条实时防护体系。黄健明等[14]认为将攻防博弈过程与网络安全态势动态演化角度相结合,可以为网络安全主动防御提供精准决策。罗璎珞等[15]从主动防御的由来与发展的角度分析网络安全攻击趋势以及相应的安全需求,确定主动防御的核心技术框架为认证与授权、加密与完整性校验和对抗与相应三部分。向林泓[16]从基于主机的防御系统出发,介绍分析了基于行为的主动防御系统的技术和实现细节,并从入侵防护、入侵检测、入侵预测和入侵响应4个层面提出了网络安全主动防御模型,如图2所示。

罗跃斌[17]从动目标防御(moving target defense,MTD)出发,在四层网络安全主动防御模型基础上提出了在本攻击面上进行主动变换,以此来迷惑入侵者,进而提升自身网络安全的可靠性,用动态、多样、实时的主动防御技术防护未知的漏洞和后门被网络攻击者利用。

现详细阐述基于网络安全入侵防护、入侵检测、入侵预测和入侵响应4个方面的网络安全主动防御系统,分析各组成的主要技术手段和工作原理,并对未来网络安全发展趋势进行预测。

2　网络安全入侵防护

入侵防护系统(intrusion prevention system,IPS)是一种主动、智能的入侵防御系统,在网络安全受到入侵和攻击之前,便将攻击包丢掉或采取措施将攻击源阻断,如图3所示[18]。IPS与传统网络安全

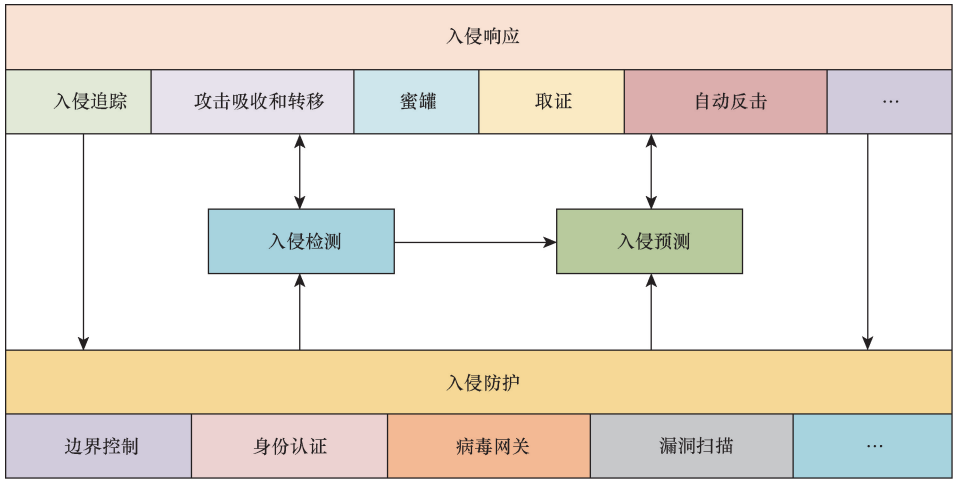

图2　网络安全主动防御模型[16]

Fig. 2　Network security active defence model[16]

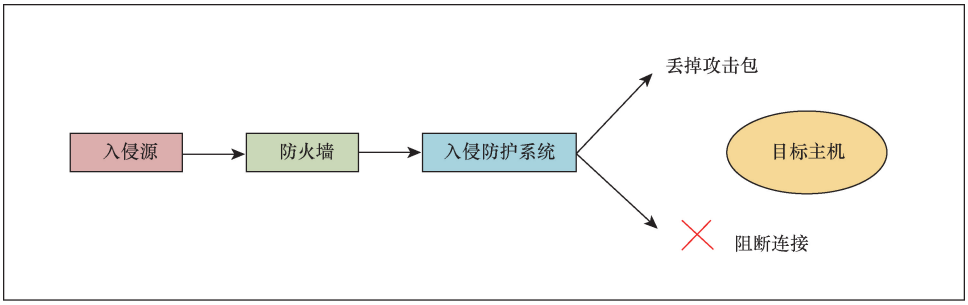

图 3 入侵防护系统模型[18]

Fig. 3 Intrusion prevention system model[18]

防护系统相比主要具有两个关键区别:自动拦截和在线运行[19]。入侵防护工具(软件与硬件方案)必须设置好相应策略,当攻击来临时做出自动拦截响应,而不是当网络遭受恶意攻击是才做出反映;当系统要实现自动响应必须做到在线运行,当攻击者与目标服务器建立会话时,所有的数据都会经过位于活动路径中的 IPS 传感器,传感器检测到相应的恶意代码,经过与相应策略比对,在恶意代码未转发到服务器之前,将含有恶意代码的数据包进行拦截,从而有效阻止网络系统遭受攻击。

2.1 入侵防护系统的分类

入侵防护系统主要根据 IPS 设备部署的方式进行分类,一般可分为基于网络的入侵防护系统基于网络的入侵防护系统(network-based intrusion prevention system,NIPS)、基于主机的入侵防护系统基于主机的入侵防护系统(host-based intrusion prevention system,HIPS)和应用型入侵防护系统应用入侵防护系统(application intrusion prevention system,AIPS)3 种。

基于网络的入侵防护系统 NIPS,如图 4 所示[20],是指采用线上工作方式,实时对流经的网络流量进行检测,一旦检测到入侵行为,立即进行响应。基于主机的入侵防护系统 HIPS,如图 5 所示[21],是指通过检查主机、网络服务或网络服务客户

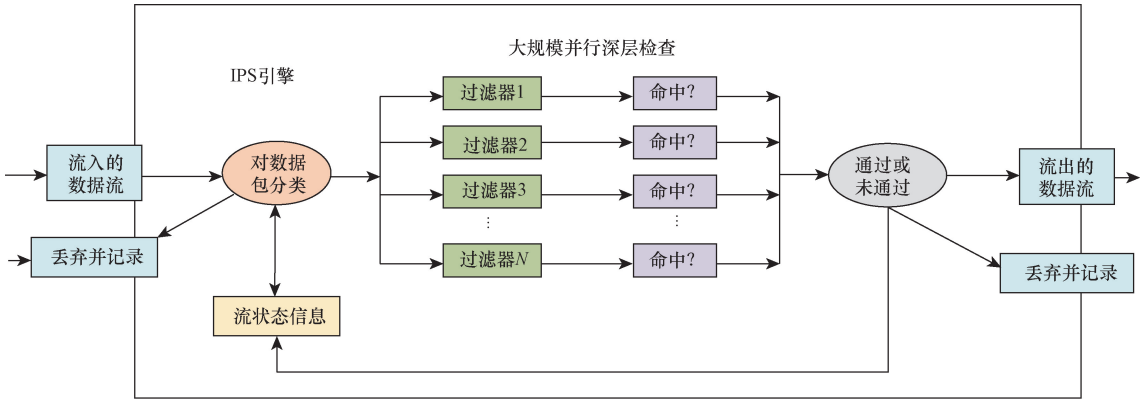

图 4 NIPS 工作原理图[20]

Fig. 4 Working principle diagram of NIPS[20]

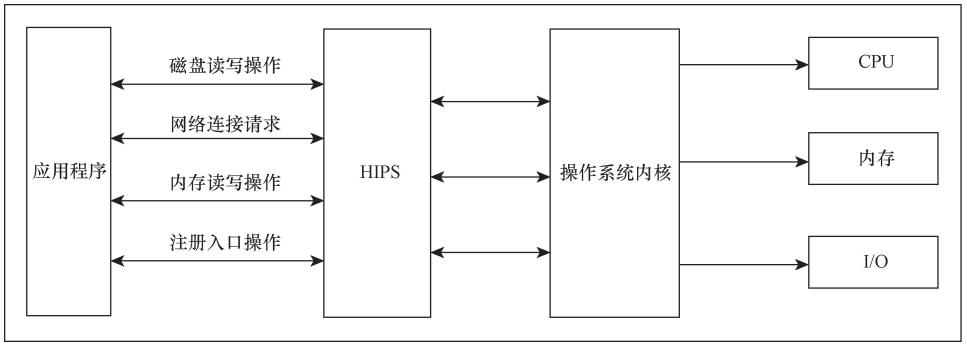

图 5 HIPS 工作原理图[21]

Fig. 5 Working principle diagram of HIPS[21]

端是否违反了相应安全策略进行及时响应,基于主机的入侵防护系统在主机或者服务器上部署软件代理程序,以此保护应用程序和操作系统免受网络安全攻击[22]。而 AIPS 是 NIPS 的一个特例,它与 NIPS 不同的地方是它被配置在应用服务器之前的网络链路上。

2.2　入侵防护系统关键技术

入侵防护系统关键技术主要有四点:

(1)嵌入式运行方式。通过采用嵌入式运行模式的 IPS 设备才能够实现实时安全防护,根据安全策略对数据包进行检查核对与处理。

(2)策略与分析。为保护网络环境的安全可靠,IPS 必须能够对网络行为进行细致的分析和具有全面可靠的安全策略,并根据入侵行为的种类和方式方法进行有针对性的响应[22]。

(3)全面的入侵特征库。随着信息安全的种类在不断增加,IPS 必须具备完善的入侵数据库[23],并升级到各 IPS 传感器上。

(4)高效处理数据包的能力。IPS 高速处理数据包[24]的能力对所要保障的网络系统尤为重要,在防护网络安全的同时也要维持保障正常的数据包通过。

2.3　入侵防护系统发展方向

根据入侵防护系统的工作方式、工作原理和关键技术特征,IPS 代表网络防御已从被动式防御转变为主动防御,弥补了防火墙等传统防御手段的局限性,可以实时、主动对网络线路中存在的恶意攻击和异常数据包进行响应,也可预防已知与未知的网络攻击。IPS 顺应时代的发展,是新时代网络安全防御的重要组成部分,必将会在网络安全防御体系中起到更加重要的作用。

3　网络安全入侵检测系统

入侵检测系统(intrusion detection system,IDS)是一种对网络流量即时监控,对不可靠的传输行为进行报警或对其采取相应防御手段,以此来保护网络安全的系统[25]。Aderson[26]早在 1980 年时使用了“威胁”一词对入侵进行了定义,入侵指在没有得到网络所属人同意的情况下擅自对网络及相关信息进行登录访问及更改,造成网络相关问题的出现。Denning[27]在 1987 年提出最早的 IDS 模型,如图 6 所示,此后的 IDS 模型均是以此模型为基础进行发展与研究。1988 年发生了 Morris Internet 蠕虫事件[28],许多中外研究开始对网络安全入侵检测系统 IDS 进行不间断研究。Heberlein 等[29]发现基于网络的入侵检测在局域网中可以检测流量信息,进而追踪可疑行为。这时网络入侵检测已经进入到了局域网中。Mukherjee 等[30]分析了网络安全入侵检测的发展,并对 IDS 系统相关原型进行了梳理归纳。Lee 等[31]从 IDS 系统的自适应性和学习性出发,提出了基于神经网络的网络安全入侵检测模型。目前,IDS 已经发展出许多不同种类、不同类型。

3.1　入侵检测系统的分类

目前,入侵检测系统主要从采用的分析方法和数据的来源两个方面进行分类。

根据 IDS 采用的分析方法分为:异常检测[32]和误用检测[33]。异常检测是先建立一个标准值,以此来评定网络行为是否正常。该方法的要点是标准值的确定。该方法可以及时检测出未知的网络入侵行为,但也比较容易产生错误报警[34]。误用检测是指将入侵行为放入已知入侵行为库中,进行对比确定该行为的入侵种类。该方法能够对已有的入侵行为进行检测,但对未知入侵行为无法进行判断,该方法误报率低,准确率高,但容易产生漏报。

根据 IDS 采用的数据来源分为:主机式入侵检测、网络式入侵检测和混合式入侵检测[35]。主机式 IDS 是指通过分析主机上的日志和数据来判断是否发生入侵行为[36]。该方法具有一定的局限性,更适合网络安全威胁种类少、攻击频率低的情况,已不适

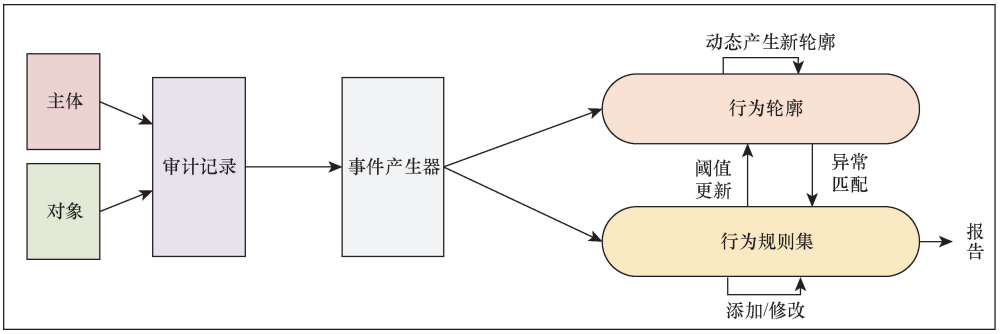

图 6　IDS 模型[27]

Fig. 6　Model of IDS[27]

合现在网络安全威胁种类多、攻击频率大的情况。网络式 IDS 是指将网络型 IDS 部署在网络上,实时分析检查特定网段、关键点上的数据流,及时发现入侵行为并做出响应。但该方法对加密了的数据包无法做出判断。混合式 IDS 是指结合了前面两种 IDS 的优点[37]。既能对主机上的数据信息进行检查,也能对特定网段和关键点上的数据流进行检查。

3.2 入侵检测系统关键技术

入侵检测系统的关键环节主要有 3 个,首先对数据的进行采集及预处理,然后对信号进行分类,最后对入侵行为进行响应预测以确保网络安全 3 个重要环节,如图 7 所示[38]。每个关键环节都有各自的关键技术:①在数据采集及处理阶段所用到的关键技术是数据的采集[39],数据采集有两种,分别为公开数据采集(主要对经典、应用广泛的数据和非常用数据进行采集)和人工数据采集(主要是将传感器等部署在若干关键点上对网络环境中的数据进行采集)。数据预处理阶段所用到的关键技术有数据归一化(因采集的数据来源各不相同,归一后便于数据的进一步检测)、数据数值化(将数据按照一定规则、策略映射到数值域中)、数据平衡(将 IDS 检测的数据流的攻击分布进行平衡);②在信号分类阶段所用到的关键技术主要有基于机器学习的 IDS(首先通过机器对大量数据进行分析和总结,直至找到相应规律,然后对相应的参数进行调节,最后再对数据测试训练,以此往复积累经验改进相应性能[40])和基于深度学习的 IDS[41]。

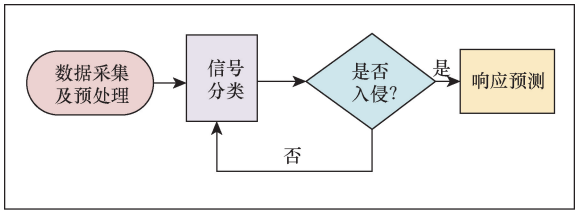

图 7 IDS 流程图[38]

Fig. 7 Flowchart of IDS[38]

3.3 入侵检测系统发展方向

根据 IDS 的工作方式、工作原理和关键技术等特点,IDS 的作用在于识别入侵行为、检测监视网络环境中的运行数据流量、及时提供入侵行为信息保护网络安全,面对越来越复杂的网络环境和不断变化的网络威胁,虽然存在与其他安全技术手段融合等问题,IDS 依然会起到至关重要的作用。

4 网络安全入侵预测系统

入侵预测是指通过对网络流量、用户数据等信息进行监测与分析,提前发现与确定网络中潜在的安全隐患,并采取相应防御措施保护网络系统安全。入侵预测系统(intrusion prediction system,IPS)是一种不仅可以检测攻击,还可以感知和预测未来可能发生攻击的系统[42]。IPS 比 IDS 更加能帮助我们保护我们的网络,通过警告安全管理员未来攻击的有效措施保护网络安全。任伟等[43]提出基于神经网络的网络安全态势预测的办法,但因参数设置复杂极易出现预测缺陷[44]。文献[45]提出了将自回归移动平均模型(autoregressive moving average model,ARMA)与隐马尔科夫模型(hidden Markov model,HMM)相结合的网络安全预测方法,但因其建模时间长,并不能实时地对网络安全态势进行反映。许多专家学者不断在网络安全入侵预测领域展开研究,通过不断地研究实验,入侵预测主要包括数据收集、数据预处理、特征提取、构建模型、预测报警四部分组成,如图 8 所示。首先对网络流量数据、系统日志文件等相关数据进行收集,并对收集到的数据进行预处理,去除相应异常值干扰;从预处理后的数据中提取有价值的数据特征;再利用机器学习、深度学习等方法进行入侵预测模型构建,并对构建后的模型进行测试;对新流入的网络流量进行分析评估,对于网络安全威胁进行报警响应,防止网络遭到攻击损害,对于正常安全的网络流量进行数据流出操作[46]。

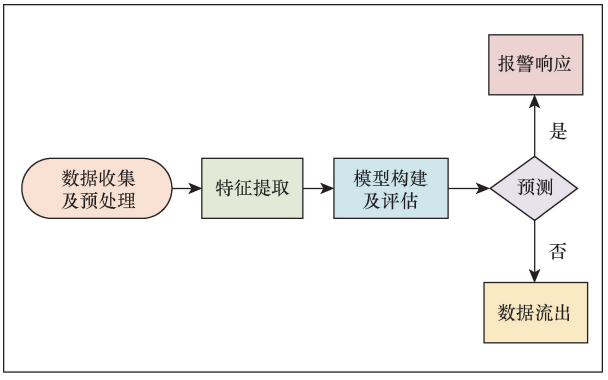

图 8 入侵预测流程图

Fig. 8 Flowchart of intrusion prediction

4.1 入侵预测系统的分类

目前,随着网络的快速发展,作为网络安全态势评估技术一部分的入侵预测系统的种类也在随着入侵态势感知的变化而不断变化。目前,入侵预测系统有基于灰色理论的入侵预测系统[47]、基于神经网络的入侵预测系统[48]、基于时间序列的入侵预测系统等。基于目前对于网络安全入侵预测系统的学习研究,还没有得出一致的预测模型相应的预测适用范围,主要对基于灰色理论和神经网络两类

系统进行学习研究。

基于灰色理论的网络安全入侵预测系统是指利用灰色系统理论模型对网络安全数据进行分析,对可能发生的网络安全风险进行预测,较适用对较少数据的中长期预测;基于神经网络的网络安全入侵预测系统是指利用神经网络技术对网络安全数据进行分析对可能发生的网络安全风险进行预测,基于神经网络的入侵预测系统具有自主学习能力,通过不断地学习、测试使自身检测能力不断提升,进一步提高应对不断变化的网络安全风险的能力。

4.2　入侵预测系统关键技术

入侵预测系统的关键技术有:①数据采集和处理:通过对需要检测的网络数据进行实时采集与处理,构建入侵预测的数据集[49];②特征选择与提取:通过对大量数据进行特征选择与提取,构建接下来识别是否为入侵行为的标准;③构建模型:通过基于神经网络等算法构建预测模型,并通过对大量历史数据进行学习测试,使模型掌握入侵行为的标准;④实时监测与响应。建立实时监测系统和预警机制,确保发现入侵行为即报警。网络安全入侵预测系统还存在许多的方式方法,今后的研究学习对入侵预测系统的准确性(自学习性)、实时性要加以研究。

4.3　入侵预测系统发展方向

随着网络环境的日益复杂,入侵预测系统所面对的安全隐患也越来越多样化,更加应该注意深度学习技术的应用,以此来提高应对未来复杂的网络安全空间;提高实时响应能力,以此来降低入侵威胁对网络环境的危害;增强智能化研究,将人工智能等高科技手段融入入侵预测系统中,构建更加智能化和自适应的安全防护体系。

5　网络安全入侵响应系统

入侵响应(intrusion response,IR)[50]是指对检测系统检测出来的入侵行为所采取的相应措施与行动,以达到阻止入侵行为进一步攻击网络系统,确保在发生网络入侵行为时能够最大程度保护网络系统的安全,对入侵行为所采取的响应包括报警、记录、追踪、阻断、取证、反击、恢复等[51]。入侵响应往往是网络安全主动防御系统中最后一个环节,是面对各种复杂网络环境和入侵行为的保护网络安全最后一道屏障。图9是《网络世界》[52]杂志曾对网络用户进行的一次调查结果占比图,结果显示,主动阻断攻击、与安全设备的联动、按紧急程度不同发出警报等都占据了较大比例,与入侵响应有关的研究领域已是网络用户心中比较关心的方面。以上这些因素促使了网络安全入侵响应的快速发展。

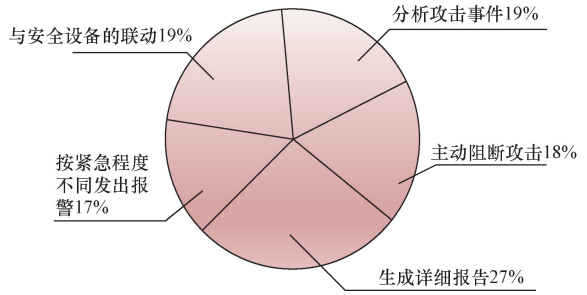

图9　网络用户调查结果占比图[52]

Fig. 9　Chart of web user survey results by percentage[52]

5.1　入侵响应系统的分类

入侵响应系统一般按照响应地点、响应范围和响应自动化程度进行分类[53],如图10所示。

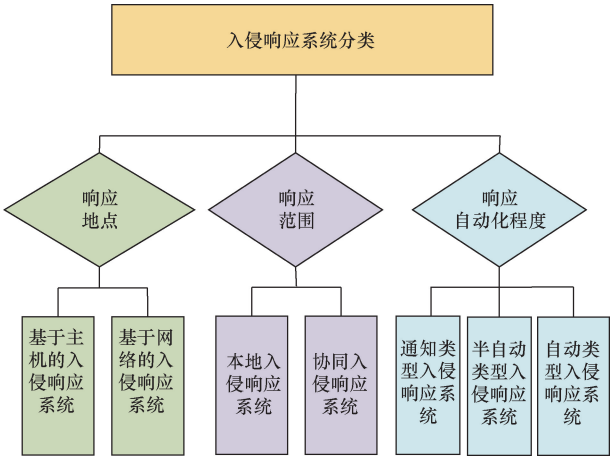

图10　入侵响应系统分类图[53]

Fig. 10　Classification chart of intrusion response system[53]

入侵响应系统根据响应的地点进行分类,可以分为基于主机和基于网络的入侵响应系统[54]。基于主机的入侵响应系统主要是用于保护主机,其响应地点为目标主机,相应的应对措施包括事件告警、事件记录、限制用户权限、暂停用户进程和备份数据等。基于网络的入侵响应系统的响应地点是相应网络节点上,包如交换机和路由器等,其响应包括对网络活动进行记录、对入侵者网络进行阻隔、对网络设备接口进行封闭、对网络攻击行为进行跟踪记录并对攻击者进行反击等[55]。

入侵响应系统按照响应范围进行分类,可以分为本地与协同入侵响应系统[56]。本地入侵响应系统主要是依靠本地安全事件的信息来保护本地主机或网络,而协同响应主要应用对象为大规模的网络环境,通过在多个响应系统之间共享信息,共同保护网络安全[57]。

入侵响应系统按照响应的自动化程度进行分类,可以分为通知类型入侵响应系统、半自动类型入侵响应系统(手工型响应系统)和自动类型入侵响

应系统[58]。通知类型入侵响应系统是通过将入侵检测系统检测出的入侵行为告知网络管理员,对于如何处理入侵行为则由管理人员负责。半自动类型入侵响应系统是在通知类型的基础上,在响应系统中事先增加了相应的响应程序供网络管理人员根据入侵类型进行相应选择,但选择的过程依然是管理人员进行。自动类型入侵响应系统在 IDS 检测到入侵行为后,直接对入侵行为进行分析、处理,不需要人为干扰。

5.2 入侵响应系统关键技术

入侵响应系统的关键环节是响应决策与响应执行,以自动类型的入侵响应系统为例进行相关介绍,如图 11 所示为自动入侵响应系统的结构模型[59],入侵响应系统响应决策模块对 IDS 检测出的网络入侵行为进行分析,再将相应的响应策略传递给响应执行模块,响应执行模块再根据响应工具库中的工具进行相应措施执行。这其中的关键技术主要有及时性的调整和响应策略的合理性。①及时性:入侵响应系统的作用是及时有效地对入侵做出响应,并消除其带来的不利影响。为实现这一目标,必须尽量缩短从检测到入侵到执行响应之间的时间,这就需要把响应决策与响应执行的相应执行算法的时间复杂程度不能太高。②选择响应策略的合理性[60]:响应策略的选择应在技术可以支持的前提下进行,制定可行适当的策略是重中之重,在进行响应时,若采取的措施带来的后果大于入侵带来的损失,那么响应就没有必要了,必须以最小的代价换取最大的安全。③丰富的相应策略知识库及工具库[61]:必须不间断地完成知识库、工具库的更新,建立完善的响应决策、执行方案,确定能够有效应对入侵行为的影响。

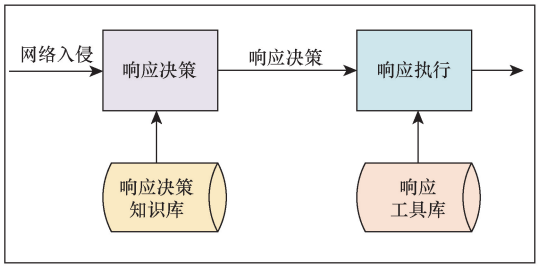

图 11 自动类型入侵响应系统体系结构图[59]

Fig. 11 Automatic type intrusion response system architecture diagram[59]

5.3 入侵响应系统发展方向

随着网络攻击越来越趋向于复杂化、自动化,入侵响应系统对于保护网络安全,减少网络入侵行为带来的破坏方面变得至关重要。目前,针对网络攻击行为作出快速反应方面,入侵响应系统仍需解决响应时间依然存在过长的问题,这将是今后入侵响应技术的主要发展方向,结合多个入侵检测系统与响应系统对网络系统进行联合保护,确保形成最优响应。

6 结论与展望

主动网络安全防护不是简单的技术措施,而是合理利用各组成部分并将其有机组合,形成主动网络安全防护系统,利用各种主动网络安全防护技术弥补各自的缺陷和不足,以各自的方式共同实现主动、完整的网络安全防护。首先介绍了网络安全主动防御在面对当前错综复杂的网络安全环境是如何发展起来的和当下网络安全主动防御的最终模型是如何构建起来的,然后从网络安全主动防御模型的 4 个组成部分出发,详细介绍了各部分的主要作用、系统分类、工作原理、关键技术手段和未来发展方向。在面对现如今网络空间环境日趋复杂,网络攻击手段日渐多样的今天,网络安全主动防御提供了高质量的解决办法。从网络安全主动防御 4 个组成部分的分类与其工作原理出发,介绍了各自适合的工作环境,在面对不同的网络安全环境时,可以根据需求的不同选择不同的防御系统,从而提高网络安全主动防御的最优性与可靠性。

网络安全主动防御是由多个组合部分互相配合而成的综合型防御系统,各部分之间的信息交互将有效提高网络安全主动防御的准确性与及时性,各部分对于入侵行为数据库的实时更新十分重要,可以实时辨别出各类网络入侵行为并及时采取适当的技术进行响应以达到网络安全主动防御的目的。总结了网络安全主动防御面临的关键问题并对未来研究方向进行了展望。

(1)复杂网络环境下的主动防御问题。网络系统越来越庞大且复杂,如何高效提取网络环境中的海量入侵行为特征数据并对其进行融合分析是当前网络安全主动防御领域研究的一个重点问题。对网络流量数据进行收集、预处理及特征提取十分必要,并将其进行数据归一化、数据数值化和数值平衡等操作可以极大地提高网络安全主动防御的防御效率。采用在线运行的入侵防护、基于深度学习的入侵检测、基于神经网络的入侵预测和自动类型的入侵响应相结合的主动防御系统在处理错综复杂的网络安全入侵行为问题上取得了较好的效果,但是在面对具体应用环境等方面仍然有待进一步的研究。

(2)最优算法问题。在网络安全主动防御的多个环节都会遇到算法问题,尤其是在入侵检测、预测和响应环节,基于机器学习与神经网络算法在网

络安全主动防御领域中已经取得了显著成效,利用机器学习与神经网络的主动防御在面对日益复杂的网络安全环境时显得更加游刃有余,更能高效、准确地在数以万计的网络行为中检测、预测出入侵行为并做到及时响应。目前存在的算法多种多样,在面对特定的应用环境时选择最适合的算法尤为重要,对提高网络安全主动防御系统性能具有重要意义。

(3)人机交互问题。随着技术的发展,人机交互在越来越多的领域被应用,无人化、智能化与网络安全主动防御体系的结合也越来越紧密。在入侵检测、入侵预测、入侵响应等关键环节中结合智能化手段,在极大程度上减少了人工资源的投入。面对复杂多变的网络安全环境,人机交互的应用让网络安全主动防御变得更加高效。在今后的网络安全主动防御方面,融入人工智能的网络安全主动防御技术的研究将成为重要研究方向。

(4)即刻响应问题。网络安全主动防御需要确保在网络安全事件发生时能够迅速做出响应,最大程度地减少网络入侵行为带来的损失并恢复正常运行。但目前仍然存在当防御系统检测出入侵行为时不能对入侵行为进行及时的响应问题,基于聚类的入侵响应决策系统和基于风险评估的入侵响应系统对于响应滞后问题取得了一定效果,但仍有不足。对于进一步简化响应决策与响应执行的相应执行算法复杂程度将成为接下来重点研究方向。

参 考 文 献

[1] 贾焰, 方滨兴, 李爱平, 等. 基于人工智能的网络空间安全防御战略研究[J]. 中国工程科学, 2021, 23(3): 98-105.
Jia Yan, Fang Binxing, Li Aiping, et al. Research on cyberspace security defence strategy based on artificial intelligence[J]. China Engineering Science, 2021, 23(3): 98-105.

[2] 方滨兴, 时金桥, 王忠儒, 等. 人工智能赋能网络攻击的安全威胁及应对策略 [J]. 中国工程科学, 2021, 23(3): 60-66.
Fang Binxing, Shi Jinqiao, Wang Zhongru, et al. AI-enabled cyberspace attacks: security risks and countermeasures [J]. Strategic Study of CAE, 2021, 23(3): 60-66.

[3] Akbanov M, Vassilakis V G, Logothetis M D. Ransomware detection and mitigation using software-defined networking: the case of WannaCry[J]. Computers & Electrical Engineering, 2019, 76: 111-121.

[4] Shin S, Gu G, Reddy N, et al. A large-scale empirical study of conficker[J]. IEEE Transactions on Information Forensics and Security, 2011, 7(2): 676-690.

[5] Bogenschneider B N, Lu L. Anatomy of an eBay fraud[J]. International Journal of Ethics and Systems, 2024, 40(4): 845-861.

[6] Liu Y, Peng W, Su J. A study of IP prefix hijacking in cloud computing networks[J]. Security and Communication Networks, 2014, 7(11): 2201-2210.

[7] MacFarland D C, Shue C A, The SDN shuffle: creating a moving-target defense using host-based software-defined networking[C]// Proceedings of the Second ACM Workshop on Moving Target Defense. New York: ACM, 2015: 37-41.

[8] Jartelius M. The 2020 data breach investigations report-a CSO's perspective[J]. Network Security, 2020(7): 9-12.

[9] 刘世文, 马多耀, 雷程, 等. 基于网络安全态势感知的主动防御技术研究[J]. 计算机工程与科学, 2018, 40(6): 1057.
Liu Shiwen, Ma Duoyao, Lei Cheng, et al. Research on active defence technology based on network security situational awareness [J]. Computer Engineering and Science, 2018, 40(6): 1057.

[10] 杨锐, 羊兴. 建立基于主动防御技术的网络安全体系[J]. 内江科技, 2008, 29(5): 138-138.
Yang Rui, Yang Xing. Establishment of network security system based on active defence technology [J]. Neijiang Science and Technology, 2008, 29(5): 138-138.

[11] Department of Defense of USA. Department of defense strategy for operating in cyberspace[R]. New York: Department of Defense of USA, 2011.

[12] Wu K, Zhang T, Chen F. Research on active controllable defense model based on zero-PDR model[C]//2010 Third International Symposium on Intelligent Information Technology and Security Informatics. New York: IEEE, 2010: 572-575.

[13] 苏杰, 葛勇. 主动防御技术及其在网络安全中的应用[J]. 中国科技信息, 2005 (6): 12-12.
Su Jie, Ge Yong. Active defence technology and its application in network security[J]. China Science and Technology Information, 2005 (6): 12-12.

[14] 黄健明, 张恒巍. 基于随机演化博弈模型的网络防御策略选取方法[J]. 电子学报, 2018, 46(9): 2222-2228.
Huang Jianming, Zhang Hengwei. A network defence strategy selection method based on stochastic evolutionary game model[J]. Journal of Electronics, 2018, 46(9): 2222-2228.

[15] 罗璎珞, 应向荣. 主动防御的由来与发展[J]. 计算机安全, 2003 (30): 27-29.
Luo Yingluo, Ying Xiangrong. The origin and development of active defence[J]. Computer Security, 2003 (30): 27-29.

[16] 向林泓. 主动防御技术的研究和实现[D]. 成都: 电子科技大学, 2011.
Xiang Linhong. Research and implementation of active defence technology [D]. Chengdu: University of Electronic Science and Technology, 2011.

[17] 罗跃斌. 网络主动防御关键技术研究[J]. 长沙: 国防科学技术大学, 2017.
Luo Yuebin. Research on key technologies of network active defence[J]. Changsha: National University of Defence Science and Technology, 2017.

[18] 胡征兵, 苏军. 入侵防护技术综述[J]. 微型电脑应用, 2005, 21(11): 56-58.
Hu Zhenbing, Su Jun. A review of intrusion prevention technologies[J]. Microcomputer Applications, 2005, 21(11): 56-58.

[19] Du Z. Network security model based on active and passive defense hybrid strategy[J]. Converter, 2021(12): 45-51.

[20] 黄金莲, 高会生. 入侵防护系统 IPS 探讨[J]. 网络安全技术与应用, 2005 (8): 35-37.
Huang Jinlian, Gao Huisheng. Exploration of IPS for intrusion

protection system[J]. Network Security Technology and Application, 2005 (8): 35-37.

[21] 聂林, 张玉清, 王闵. 入侵防御系统的研究与分析[J]. 计算机应用研究, 2005, 22(9): 131-133.
Nie Lin, Zhang Yuqing, Wang Min. Research and analysis of intrusion prevention system[J]. Computer Application Research, 2005, 22(9): 131-133.

[22] 胡晓江. 入侵防御系统的研究与应用[J]. 信息与电脑: 理论版, 2010 (5): 1-2.
Hu Xiaojiang. Research and application of intrusion prevention system[J]. Information and Computer: Theoretical Edition, 2010 (5): 1-2.

[23] 熊皓. 基于特征库的网络数据库安全的研究[J]. 科技视界, 2013 (23): 3-33.
Xiong Hao. Research on network database security based on feature library[J]. Science and Technology Perspectives, 2013 (23): 3-33.

[24] Jo W, Kim S, Lee C, et al. Packet preprocessing in CNN-based network intrusion detection system[J]. Electronics, 2020, 9(7): 1151.

[25] 牛颉. 基于人工智能的网络入侵检测技术研究[D]. 北京: 北京邮电大学, 2021.
Niu Jie. Research on network intrusion detection technology based on artificial intelligence [D]. Beijing: Beijing University of Posts and Telecommunications, 2021.

[26] Anderson J P. Computer security thread monitoring and surveillance[R]. Fort Washington, USA: James P Anderson Co, 1980.

[27] Denning D E. An intrusion-detection model[J]. IEEE Transactions on Software Engineering, 1987, 13(2): 222-232.

[28] Stephens P, Induruwa A. Cybercrime investigation training and specialist education for the European Union[C]//Second International Workshop on Digital Forensics and Incident Analysis (WDFIA 2007). New York: IEEE, 2007: 28-37.

[29] Heberlein L T, Dias G V, Levitt K N, et al. A network security monitor[R]. Livermore, CA (United States), Lawrence Livermore National Lab(LLNL); California University, Department of Electrical Engineering and Computer Science, 1989.

[30] Mukherjee B, Heberlein L T, Levitt K N. Network intrusion detection[J]. IEEE, 1994, 8(3): 26-41.

[31] Lee S C, Heinbuch D V. Training a neural-network based intrusion detector to recognize novel attacks[J]. IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans, 2001, 31(4): 294-299.

[32] 江涛. 计算机网络入侵检测技术研究[J]. 中国新技术新产品, 2023 (13): 143-145.
Jiang Tao. Research on computer network intrusion detection technology [J]. China New Technology and New Products, 2023 (13): 143-145.

[33] 张博, 姚静, 梁旭辉. 入侵检测系统对计算机网络的安全维护[J]. 网络安全技术与应用, 2022(1): 17-19.
Zhang Bo, Yao Jing, Liang Xuhui. Security maintenance of computer network by intrusion detection system protection[J]. Network Security Technology and Application, 2022(1): 17-19.

[34] 杨智君, 田地, 马骏骁, 等. 入侵检测技术研究综述[J]. 计算机工程与设计, 2006, 27(12): 2119-2123.
Yang Zhijun, Tian Di, Ma Junxiao, et al. A review of intrusion detection techniques [J]. Computer Engineering and Design, 2006, 27(12): 2119-2123.

[35] Prasad S, Srinath M V, Basha M S. Intrusion detection systems, tools and techniques—an overview[J]. Indian Journal of Science and Technology, 2015, 8(35): 1-7.

[36] Jakić P. The overview of intrusion detection system methods and techniques[C]//Sinteza 2019-International Scientific Conference on Information Technology and Data Related Research. New York: IEEE, 2019: 155-161.

[37] Cahyo A N, Sari A K, Riasetiawan M. Comparison of hybrid intrusion detection system[C]//2020 12th International Conference on Information Technology and Electrical Engineering (ICITEE). New York: IEEE, 2020: 92-97.

[38] 张昊, 张小雨, 张振友, 等. 基于深度学习的入侵检测模型综述[J]. 计算机工程与应用, 2022, 58(6): 17-28.
Zhang Hao, Zhang Xiaoyu, Zhang Zhenyou, et al. A review of deep learning-based intrusion detection models[J]. Computer Engineering and Applications, 2022, 58(6): 17-28.

[39] Sulaiman N S, Nasir A, Othman W R W, et al. Intrusion detection system techniques: a review[C]//Journal of Physics: Conference Series. IOP Publishing, 2021, 1874(1): 012042.

[40] 杨艳艳, 李雷孝, 林浩, 等. 参数并行: 一种基于群启发式算法的机器学习参数寻优方法[J]. 科学技术与工程, 2022, 22(5): 1972-1980.
Yang Yanyan, Li Leixiao, Lin Hao, et al. Parameter parallelism: a parameter optimization method for machine learning based on group heuristic algorithm[J]. Science Technology and Engineering, 2022, 22(5): 1972-1980.

[41] Wang Z. Deep learning-based intrusion detection with adversaries [J]. IEEE Access, 2018, 6: 38367-38384.

[42] Abdlhamed M, Kifayat K, Shi Q, et al. Intrusion prediction systems[J]. Information Fusion for Cyber-security Analytics, 2017 (10): 155-174.

[43] 张峰, 秦志光, 刘锦德. 基于入侵事件预测的网络安全预警方法[J]. 计算机科学, 2004, 31(11): 77-79.
Zhang Feng, Qin Zhiguang, Liu Jinde. A network security early warning method based on intrusion event prediction[J]. Computer Science, 2004, 31(11): 77-79.

[44] 任伟, 蒋兴浩, 孙锬锋. 基于 RBF 神经网络的网络安全态势预测方法[J]. 计算机工程与应用, 2006(31): 136-138.
Ren Wei, Jiang Xinghao, Sun Tanfeng. A network security posture prediction method based on RBF neural network [J]. Computer Engineering and Application, 2006(31): 136-138.

[45] Man D, Wang Y, Yang W, et al. A combined prediction method for network security situation[C]//2010 International Conference on Computational Intelligence and Software Engineering. New York: IEEE, 2010: 1-4.

[46] Abdlhamed M, Kifayat K, Shi Q, et al. Intrusion prediction systems[J]. Information, 2017, 691: 155-174.

[47] Shi Y Q, Li T, Chen W, et al. A quantitative model for network security situation awareness based on immunity and grey theory [J]. Control and Man Agement(CCCM), 2009, 8: 14-18.

[48] Tang C H, Yu S Z. Method of network security situation prediction based on likelihood BP[J]. Computer Science, 2009, 36 (19): 97-100, 168.

[49] Yu Z, Tsai J J P, Weigert T. An automatically tuning intrusion

detection system[J]. IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics), 2007, 37(2): 373-384.

[50] Inayat Z, Gani A, Anuar N B, et al. Intrusion response systems: Foundations, design, and challenges[J]. Journal of Network and Computer Applications, 2016, 62: 53-74.

[51] 晏丰. 基于风险的入侵响应决策技术研究[D]. 北京: 北京交通大学, 2006.
Yan Feng. Research on risk-based decision-making technology for intrusion response[D]. Beijing: Beijing Jiaotong University, 2006.

[52] 宋丽娜. 从被动应战到主动防御[N]. 网络世界, 2004-09-20(21).
Song Lina. From passive response to active defence[N]. Network World, 2004-09-20(21).

[53] Foo B, Glause M W, Howard G M, et al. Intrusion response systems: a survey[J]. Information Assurance: Dependability and Security in Networked Systems, 2008, 2008: 377-416.

[54] Efe A, Abacı İ N. Comparison of the host based intrusion detection systems and network based intrusion detection systems[J]. Celal Bayar University Journal of Science, 2022, 18(1): 23-32.

[55] Kumar S, Gupta S, Arora S. Research trends in network-based intrusion detection systems: a review[J]. IEEE Access, 2021, 9: 157761-157779.

[56] Forrest S, Hofmeyr S A, Somayaji A. Computer immunology[J]. Communications of the ACM, 1997, 40(10): 88-96.

[57] Stakhanova N, Basu S, Wong J. A taxonomy of intrusion response systems[J]. International Journal of Information and Computer Security, 2007, 1(1/2): 169-184.

[58] Anwar S, Mohamad Z J, Zolkipli M F, et al. From intrusion detection to an intrusion response system: fundamentals, requirements, and future directions[J]. Algorithms, 2017, 10(2): 39.

[59] Kourki N S, Kabiri P. An adaptive and cost-based intrusion response system[J]. Cybernetics and Systems, 2017, 48(6/7): 495-509.

[60] Shameli-Sendi A, Louafi H, He W, et al. Dynamic optimal countermeasure selection for intrusion response system[J]. IEEE Transactions on Dependable and Secure Computing, 2016, 15(5): 755-770.

[61] Rezapour A, GhasemiGol M, Takabi D. A systematic mapping study on intrusion response systems[J]. IEEE Access, 2024, (12): 46524-46550.