计算机网络中的攻击检测与防御技术研究

李 聪
天津渤海职业技术学院 天津 300402

摘 要：随着计算机网络的广泛应用和高度依赖，网络攻击事件频发，给个人、企业和国家的信息安全带来了巨大威胁。本文旨在探讨计算机网络中的攻击检测与防御技术，分析当前常见的网络攻击手段，并介绍相应的检测与防御策略。通过综合研究现有技术，本文为提升网络安全防护能力提供了理论参考和实践指导。

关键词：计算机网络；攻击检测；防御技术；网络安全

引言

计算机网络作为现代社会的重要基础设施，承载着大量的数据传输和信息交换任务。然而，随着网络技术的不断发展，网络攻击手段也日益复杂和多样化。为了保障网络系统的安全性，研究有效的攻击检测与防御技术显得尤为重要。本文将从网络攻击的常见手段出发，探讨攻击检测与防御技术的发展现状和未来趋势。

1 网络攻击的常见手段及特征

一是拒绝服务攻击（DoS 和 DDoS）：拒绝服务攻击通过向目标服务器发送大量无效请求，导致服务器资源耗尽，无法为正常用户提供服务。分布式拒绝服务攻击（DDoS）则利用多个被控制的计算机同时发起攻击，进一步增强了攻击的破坏力和隐蔽性。二是网络钓鱼攻击：网络钓鱼攻击通过伪造合法网站或发送欺诈性电子邮件，诱骗用户提供敏感信息，如用户名、密码、银行卡号等。这类攻击往往利用社会工程学手段，具有较高的欺骗性和成功率[1]。三是嗅探攻击：嗅探攻击通过截获网络传输的数据包，获取其中的敏感信息。攻击者可以使用网络嗅探工具来监视网络流量，进而提取目标信息。四是僵尸网络攻击：僵尸网络是由大量被恶意软件感染的计算机组成的网络。攻击者可以远程控制这些计算机，发起DDoS攻击、传播恶意软件等。僵尸网络具有隐蔽性强、破坏力大的特点。

2 计算机网络中的攻击检测技术

2.1 基于签名的检测

在计算机网络中，基于签名的检测技术是一种高效识别已知攻击行为的方法。该技术依赖于一个预定义的攻击特征库，该库包含各种恶意行为的独特标识，即“签名”。这些签名通常基于恶意软件样本的特征信息，如文件名、内容字符串或字节等。当网络流量通过检测系统时，系统会对流量内容进行扫描，提取其特征信息，并与特征库中的签名进行比对。如果匹配成功，即流量中的内容与某个恶意行为签名相符，系统会立即识别出该攻击行为，并采取相应的防御措施。这种方法的优点在于其高准确性，因为签名是基于已知恶意行为的精确特征生成的，因此能够迅速且准确地识别出这些已知攻击。然而，基于签名的检测技术也存在一定的局限性。首先，它只能识别已知的攻击行为，对于新型或变种的恶意软件，如果其特征尚未被纳入特征库，则可能无法被检测出来。其次，随着恶意软件的不断演化和变异，特征库需要不断更新以保持其有效性，这无疑增加了维护成本和工作量。为了应对这些挑战，研究人员和安全机构正在不断探索和改进基于签名的检测技术。例如，通过引入机器学习算法，系统能够自动分析网络流量，发现潜在的未知攻击模式，并生成新的签名以更新特征库。此外，一些先进的入侵检测系统还结合了基于异常的检测技术，通过监控网络流量的正常行为模式，来检测偏离基线的异常行为，从而进一步提高检测的全面性和准确性。

2.2 基于行为的检测

行为分析检测，作为攻击检测领域中的一项重要技术，其核心在于通过对网络环境中各类动态信息的深度剖析，来识别并响应潜在的安全威胁。该技术不依赖于预先定义的攻击特征库，而是侧重于分析网络流量模式、设备性能参数变化、系统日志记录等多维度数据，以期在海量信息中捕捉到异常行为或事件的蛛丝马迹。具体而言，行为分析检测首先会收集一段时间内的网络活动数据，这些数据涵盖了从网络层到应用层的广泛信息，如数据包大小、传输频率、访问模式、资源使用状况等。随后，利用统计学方法、机器学习算法或深度学习模型，对这些数据进行深度挖掘和模式识别。通过分析正常网络行为与异常行为之间的差异，系统能够建立起一套动态的行为基准线，并据此判断新出现的活动是否偏离了正常范围。该技术的一大显著优势在于其对未

知攻击和变体攻击的高度敏感性。由于不依赖于特定的攻击签名，行为分析能够捕捉到那些利用新型漏洞、变形攻击手段或零日攻击试图绕过传统防御措施的攻击行为[2]。然而，这一优势也伴随着挑战：高误报率。复杂多变的网络环境、正常的业务波动、以及用户行为的多样性，都可能被误识别为潜在的攻击迹象，导致大量无关紧要的警报产生，增加了安全管理人员的工作负担，并可能影响他们对真正威胁的响应效率。因此，优化行为分析检测的关键在于提高算法的精确度和智能化水平，减少误报的同时保持对真正威胁的高检出率。这要求不断优化分析模型，融入更多上下文信息，以及采用更为先进的机器学习和人工智能技术，以实现更精准的行为识别和威胁判定。

3 计算机网络中的攻击防御技术

3.1 防火墙技术

防火墙，作为计算机网络安全架构中的基石，扮演着守护者的角色，严格把控着网络边界的进出流量。它不仅是一道物理或逻辑的屏障，更是网络安全策略的具体执行者，通过一系列精细设计的规则，对往来于内部网络与外部网络之间的数据包进行严格的筛选与监控。现代防火墙技术已远超传统意义上的端口过滤，发展出了深度包检测（DPI）和应用层过滤等高级功能，极大地增强了其防护能力。深度包检测技术，顾名思义，能够深入到数据包的内容层面，对载荷数据进行细致分析，而不仅仅局限于检查数据包的头部信息。这一特性使得防火墙能够识别并阻止隐藏在看似正常流量中的恶意内容，如嵌入在HTTP请求中的恶意脚本或隐藏在加密通信中的攻击指令。应用层过滤，则是针对特定应用程序或服务的流量进行专项管理。随着网络应用的多样化，许多攻击开始利用高层协议（如HTTP、FTP、SMTP等）的复杂性进行隐蔽操作。应用层过滤技术通过理解这些协议的工作机制，能够识别并拦截那些试图利用协议漏洞或进行未授权操作的流量，有效防止了诸如SQL注入、跨站脚本（XSS）等应用层攻击。此外，现代防火墙还融入了状态检测、入侵防御系统（IPS）以及虚拟专用网（VPN）集成等功能，进一步提升了其安全防护的全面性和灵活性。状态检测技术通过维护网络会话的状态信息，能够更准确地判断数据包的合法性，防止了诸如TCP拆分攻击等基于会话的攻击方式。而IPS功能则让防火墙具备了主动防御的能力，能够在检测到攻击行为时立即采取措施，如阻断连接、发送警报等。

3.2 入侵检测系统（IDS）与入侵防御系统（IPS）

入侵检测系统（IDS）与入侵防御系统（IPS）是网络安全领域中两个紧密相连且功能互补的技术，共同构成了强大的入侵防御体系。IDS，作为网络的“耳目”，其核心任务是通过持续监控网络流量、系统日志以及关键文件的变化，来识别任何可能表明攻击活动的异常模式或行为。它运用多种分析手段，包括签名识别、异常检测、行为分析等，对收集到的数据进行深度剖析。一旦检测到潜在的威胁，IDS会立即触发警报，通知安全团队进行调查和响应。这种被动防御机制，虽然不直接干预网络流量，但为及时发现和应对安全事件提供了宝贵的时间窗口。相比之下，IPS则更加积极主动。它在检测到攻击行为后，不仅能发出警报，还能根据预设的安全策略，直接对攻击流量采取阻断、重定向或修改等防御措施。IPS通常集成于网络的关键节点，如防火墙之后，能够实时分析并处理流经的数据包，有效阻止诸如DDoS攻击、恶意软件传播、网络钓鱼等威胁的进一步扩散。这种主动防御策略，显著缩短了从检测到响应的时间，降低了攻击造成的潜在损失[3]。IDS与IPS的结合使用，形成了一种层次分明、相辅相成的防御机制。IDS负责广泛监控，提供早期预警；IPS则负责快速响应，直接阻断威胁。这种综合防御体系不仅提高了网络安全事件的检测率，还大大增强了网络的自我防护能力，是现代网络安全策略中不可或缺的一部分。通过不断优化两者的协同工作，可以更有效地抵御日益复杂的网络攻击，保护网络环境的稳定与安全。

3.3 数据加密技术

数据加密技术，作为信息安全领域的核心基石，是确保数据隐私与完整性的强有力手段。在数字时代，信息的高效流通与共享带来了前所未有的便利，但同时也让数据暴露在了各种潜在威胁之下。数据加密通过复杂的算法，将明文数据转换为难以解读的密文形式，从而在数据传输和存储过程中，为数据披上了一层坚实的“保护甲”。加密过程通常涉及两个关键要素：加密算法和密钥。加密算法是执行加密和解密操作的数学函数，其强度决定了加密的安全性。而密钥，则是加密和解密过程中不可或缺的秘密数字序列，只有掌握正确密钥的实体才能解读加密后的数据。根据密钥的使用方式，数据加密可分为对称加密和非对称加密两大类。对称加密，又称单密钥加密，使用相同的密钥进行加密和解密。这种方法速度快，适合大量数据的加密传输，但密钥的分发和管理成为了一个挑战。非对称加密，或称公钥加密，则使用一对密钥：公钥用于加密，私钥用于解密。这种机制解决了密钥分发的问题，因为公钥可以公开，而私钥保密，非常适合于安全通信和数字签名等

应用。数据加密技术的应用范围广泛，从网络通信中的SSL/TLS协议，保护网页浏览和数据传输的安全，到数据库加密，确保存储数据的隐私，再到云服务和物联网安全，数据加密都是不可或缺的一部分。它不仅能够有效防止数据在传输过程中被窃取或篡改，还能在数据静态存储时，提供持续的保护，确保即使数据落入不法之手，也无法被轻易解读。

3.4 身份认证与访问控制

身份认证与访问控制是网络安全体系中至关重要的两个环节，它们共同构成了保护系统资源免受未经授权访问的坚固防线。身份认证技术，是确认用户身份真实性的过程。它通过多种方式实现，包括但不限于密码验证、双因素认证、生物特征识别以及数字证书等。密码验证是最基础也是最常见的方式，用户需输入预设的密码来证明自己的身份。双因素认证则结合了两种或多种认证方式，如密码加手机验证码，提高了安全性。生物特征识别，如指纹识别、面部识别等，利用人体独有的生物特征进行认证，难以伪造，安全性更高。数字证书则是由可信第三方颁发的电子文档，用于证明用户身份和公钥的有效性。访问控制技术，则是在身份认证的基础上，根据用户的身份、角色、权限等因素，对系统资源进行细粒度的访问管理。它确保用户只能访问其被授权的资源，防止信息泄露和非法操作[4]。访问控制模型多样，包括自主访问控制（DAC）、强制访问控制（MAC）和基于角色的访问控制（RBAC）等。DAC允许用户自主决定谁可以访问其资源。MAC则根据资源的敏感程度和用户的权限等级进行访问控制。RBAC通过为用户分配角色，角色再关联权限，实现了更灵活、可扩展的访问管理。身份认证与访问控制的结合，不仅确保了只有合法用户才能访问系统，还根据用户的身份和权限，对访问行为进行了精细化的控制。这种双重保障机制，大大增强了系统的安全性，有效防止了未经授权的访问和潜在的安全威胁，是构建安全、可信网络环境的基石。

4 未来发展趋势

一是智能化与自动化：未来网络安全防御将更加注重智能化和自动化。通过引入机器学习和人工智能技术，可以实现对网络流量的实时监控和智能分析，提高检测的准确性和效率。同时，自动化防御措施将能够更快速地响应攻击事件，减少损失。二是协同防御与信息共享：随着网络攻击手段的不断演变，单一的安全防御措施已经难以应对复杂的网络威胁。未来网络安全防御将趋向于协同防御和信息共享。不同组织和企业之间将加强合作，共同应对网络攻击事件。同时，通过信息共享平台，及时分享安全威胁情报和防御经验，提高整体安全防护能力。三是新兴技术的应用：量子安全通信、区块链等新兴技术将为网络安全防御带来新的机遇和挑战。量子安全通信利用量子力学的原理实现无条件安全通信，可以有效抵御量子计算机的攻击。区块链技术则通过分布式账本和智能合约等技术手段，提高数据的安全性和可信度。

结语

计算机网络中的攻击检测与防御技术是保障信息安全的重要手段。通过综合应用多种技术和策略，可以有效提升网络安全防护能力。未来，随着技术的不断发展和创新，网络安全领域将迎来更多的机遇和挑战。我们需要不断加强技术研究和创新，提高网络安全的整体能力，为构建安全可靠的网络环境做出应有的贡献。

参考文献

[1]史明华,吴嘉玮.计算机网络攻击及防御技术研究[J].中国管理信息化,2020,23(22):198-199.

[2]张文川.计算机网络中的网络攻击与防御策略研究与应用[J].办公自动化,2023,28(23):62-64.

[3]陈伟峰.计算机网络攻击及防御技术分析[J].信息与电脑(理论版),2020,32(09):195-196.

[4]冯钶杰.对计算机网络攻击及防御技术的几点探讨[J].技术与市场,2019,26(09):133+135.