基于欺骗防御技术的网络安全攻击检测与技术实现

Network Security Attack Detection and Technical Realization Based on Deception Defense Technology

黄 健(中国联通湖北分公司,湖北 武汉 430000)
Huang Jian(China Unicom Hubei Branch,Wuhan 430000,China)

摘 要:
介绍了基于欺骗防御技术的网络安全攻击检测和技术实现方法,并与传统方案进行对比,结果表明,欺骗防御技术可以更有效地识别并防御恶意攻击。提出的仿真能力、欺骗环境构建、威胁识别分析等技术实现方式很好地展现了欺骗防御技术的主动防御能力,为网络安全攻击检测和响应优化提供了新的思路和方法,对提高网络安全防御能力具有重要意义。

关键词:
欺骗防御技术;网络安全;攻击检测;威胁识别
doi:10.12045/j.issn.1007-3043.2023.08.014
文章编号:1007-3043(2023)08-0062-05
中图分类号:TN915.08
文献标识码:A
开放科学(资源服务)标识码(OSID):

Abstract:
It introduces a network security attack detection and implementation method based on deception defense technology, and compares it with traditional solutions. The results show that the method based on deception defense technology can more effectively identify and defend against malicious attacks. The simulation capability, deception environment construction, threat identification and analysis and other technical implementation methods proposed well demonstrate the active defense capability of deception defense technology, it provides new ideas and methods for network security attack detection and response optimization, which is of great significance for improving network security defense capabilities.

Keywords:
Deception defense technology;Network security;Attack detection;Threat identification

引用格式:黄健. 基于欺骗防御技术的网络安全攻击检测与技术实现[J]. 邮电设计技术,2023(8):62-66.

1 概述

随着网络技术的快速发展和互联网的普及,网络安全已成为世界范围内的一个热点话题[1]。网络安全攻击的形式和威胁日益复杂和严重,传统安全防御技术已经无法满足对新型威胁的检测和响应要求。攻击者可以利用各种漏洞和技术手段,以各种形式发起攻击,例如网络钓鱼、DDoS攻击、勒索软件攻击、社交工程等,这些攻击方式对于个人和组织的财产和安全都造成了极大的威胁[2-3]。为了有效地防御这些攻击,安全防御技术也在不断地发展和完善。在传统的安全防御中,常见防御技术包括入侵检测系统(IDS)、入侵防御系统(IPS)、反病毒软件、网络防火墙、网关等[4]。然而,随着攻击技术的不断发展和演变,这些传统的安全防御技术也越来越难以满足新的安全防御需求。攻击者可以使用各种技术绕过传统的安全防御措施,例如使用新型漏洞、恶意软件等手段[5]。

欺骗防御技术作为一种新兴的安全防御技术,具有一定的创新性。它不同于传统的防御方法,是一种主动的安全防御技术,通过欺骗攻击者的方式,提高

收稿日期:2023-06-17

网络安全的防御水平[6]。欺骗防御技术可以通过欺骗攻击者或篡改攻击者获取的信息，从而防止攻击者进一步实施攻击，其本质是通过与攻击者进行信息互通，让攻击者认为攻击已经成功实施，从而降低攻击者的兴趣和能动性，提高安全防御的效率和效果[7-8]。另外，欺骗防御技术可以在传统的安全防御技术的基础上，增加一层主动的防御机制，提高安全防御的能力。使用欺骗防御技术可以有效地识别和防止高级威胁和内部攻击，提高网络安全的防御水平[9]。因此，探索基于欺骗防御技术的网络安全攻击检测和技术实现方法，对于提高网络安全防御能力、网络安全响应效率和准确性具有重要意义。

2 基于欺骗防御技术的网络安全攻击检测方法

传统的网络安全攻击检测方法，如基于规则的检测方法、基于统计分析的检测方法和基于行为分析的检测方法等，存在诸多局限性，无法满足网络安全的全面防御需求[10]。因此，基于欺骗防御技术的网络安全攻击检测方法逐渐引起了人们的重视。本章主要介绍基于欺骗防御技术的网络安全攻击检测的4种主要方法，包括入侵检测系统欺骗技术、蜜罐技术、虚假数据技术和欺骗攻击者，如图1所示。

2.1 入侵检测系统欺骗技术

入侵检测系统的主要思想是在入侵检测系统中加入虚假信息，以达到欺骗攻击者的目的[11]。该技术包括入侵检测系统欺骗攻击者和欺骗检测器2种类型。入侵检测系统欺骗技术的优点在于能够有效地欺骗攻击者，从而降低攻击的成功率，同时又能够保持入侵检测系统的正常运行，不影响网络的正常使用。此外，该技术还可以通过收集攻击者的信息和行为数据，提高对攻击行为的了解和分析能力，为进一步加强网络安全防御提供有价值的数据支持。

2.2 蜜罐技术

蜜罐技术的主要思想是通过在网络中布置虚假系统或服务，吸引攻击者攻击蜜罐，从而收集攻击者的信息和行为数据，以提高网络安全防御的能力[12]。

蜜罐技术包括低交互蜜罐和高交互蜜罐2种类型。低交互蜜罐提供基本的服务，并通过重定向攻击者到虚假系统或服务来降低攻击成功率，但无法提供详细的攻击行为信息。高交互蜜罐可以模拟真实系统的环境和行为，记录攻击者的所有行为，提供有价值的数据支持，但需要投入大量的资源来维护和管理。蜜罐技术的优点在于可以有效提高网络安全防御能力并降低攻击者的成功率，但其局限性在于需要与其他防御措施相结合才能更好地应对不同类型的攻击行为。

2.3 虚假数据技术

虚假数据技术的主要思想是通过制造虚假数据来引诱攻击者以识别并阻止攻击行为。虚假数据技术可以分为主动型虚假数据技术和被动型虚假数据

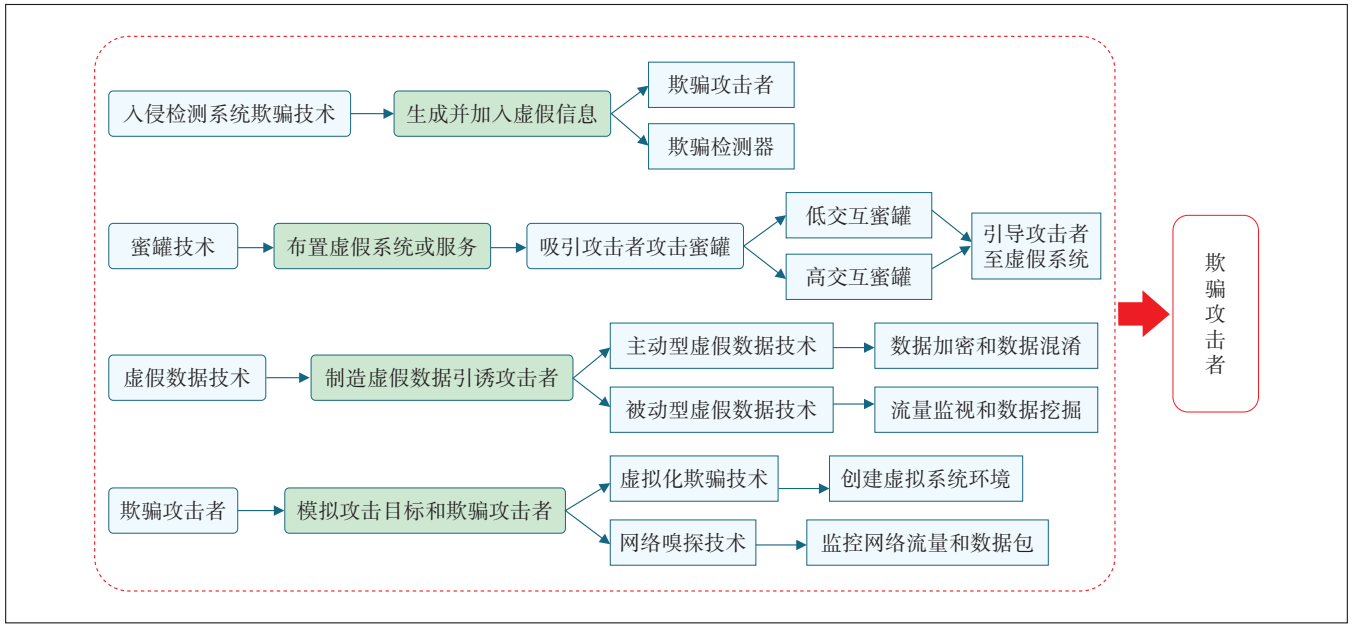

图1　基于欺骗防御技术的网络安全攻击检测方法

技术2种类型。主动型虚假数据技术是将虚假数据注入真实数据中来干扰攻击者的攻击行为，但会对真实数据的可靠性产生影响。被动型虚假数据技术是在真实数据流中添加虚假数据来诱骗攻击者进行攻击，但需要更复杂的算法来识别攻击者的行为。

虚假数据技术的优点在于能够干扰攻击者的攻击行为，降低攻击成功率，提高网络安全防御能力，但局限性在于需要投入大量的资源来维护和管理虚假数据，也需要与其他防御措施相结合才能更好地应对不同类型的攻击行为。虚假数据技术的发展趋势是通过机器学习等技术来提高虚假数据技术的可靠性和智能化程度，以更好地应对网络安全攻击。

2.4 欺骗攻击者

欺骗攻击者是一种基于欺骗防御技术的网络安全攻击检测方法，其具体方法包括虚拟化欺骗技术和网络嗅探技术。虚拟化欺骗技术通过欺骗攻击者的目标系统，将其注意力转移到虚拟环境中，以达到降低攻击成功率的目的。网络嗅探技术指通过监控网络流量和数据包，识别和拦截攻击行为，对新型攻击行为进行检测。然而，欺骗攻击者方法也存在一些局限性和挑战，需要在实践中加以应用和完善。

3 基于欺骗防御技术的实现方式

欺骗防御技术是防守者得以观察攻击者行为的网络防御战术，通过诱骗使攻击者暴露自身，目前主流的基于欺骗防御技术的实现方式有多种，包括仿真能力、欺骗环境构建、威胁识别、攻击者画像等，本章主要对以上几种实现方式进行详细介绍。

3.1 仿真能力

基于欺骗防御技术的仿真能力通常有多种类型，包含应用服务类、漏洞类、操作系统类、工控类以及定制仿真。

3.1.1 应用服务仿真

a）Web类：仿真类型包括Weblogic/tomcat/thinkphp/wordpress/wiki/wildfly/wordpress/Jenkins/beescms等。

b）数据库类：仿真类型包括MySql/phpmyadmin/DB2/Redis/PostgreSQL等。

c）通用服务类：仿真类型包括SSH/Telnet/FTP/Extmail等。

3.1.2 漏洞仿真

通常系统会带有高甜度的漏洞，例如Log4j2、Shiro、Struts2等，为保障高仿真度和诱捕能力，甚至可定制热点漏洞的仿真。

3.1.3 操作系统仿真

欺骗防御技术通常可支持Windows、Linux等常见系列操作系统仿真能力，可构建办公环境、业务环境、生产环境等高仿真业务环境。

3.1.4 工业控制仿真

欺骗防御技术为满足工业应用环境，通常也具备工业控制仿真能力，可支持IEC104/IEC61850/S7/Modbus/工业OMS系统的高仿真能力，可进行工控系统的蜜网布设。

3.1.5 定制仿真

欺骗防御技术为满足特殊业务应用需求，通常内置Web框架，通过上传标签主题、标签页icon、页面logo、背景图等信息，可快速生产成Web蜜网，具备溯源社交账号等能力。

3.2 欺骗环境构建

欺骗防御技术可通过漏洞设计、诱饵投放、仿真系统设置等构建高仿真欺骗诱捕环境，它不参与真实网络业务交互，对实际业务环境无任何影响。欺骗防御技术可基于用户网络的环境，通过占用空余IP/网段、采用诱捕探针部署在已有的终端进行攻击导流来构建蜜网，攻击者一旦达到蜜网即可被吸引至仿真系统，由仿真系统完成交互，捕获攻击行为。诱饵投放主要以主机诱饵和互联网诱饵为主，互联网诱饵在公开的网站中设置虚假信息，在黑客收集信息阶段对其造成误导，使其攻击目标转向蜜网，间接保护其他资产。主机诱饵需要提前投放到真实环境中，如放置SSH连接蜜网过程中的公钥记录或在主机诱饵上开放有利用价值的端口，在攻击者做嗅探时，将攻击者的攻击视线转移到蜜网之中。

3.3 威胁识别分析

欺骗防御技术基于行为识别能力，依靠高仿真业务在网络中布下层层陷阱，当攻击者访问时，可对攻击行为进行全程记录和报文捕获，对0day及APT等高级攻击与未知威胁进行有效发现，捕获攻击过程。技术上采用驱动层监控，早于入侵者入场，隐藏自身存在，具有先手优势，捕获关键恶意行为。对于攻击者的行为，从多维度的信息入手，根据攻击数据进行研判，识别已知攻击行为的攻击类型、攻击手段、攻击工具等，可对攻击详细数据和攻击报文进行进一步分析，发现未知威胁等。

3.4 攻击者画像

欺骗防御技术可通过记录攻击者的IP地址、所在区域、攻击时间、攻击手段等，进一步溯源并获取到攻击者的设备指纹和虚拟身份。根据攻击时间、攻击目标、攻击过程、设备指纹等进行汇聚处理、深度分析，溯源攻击者信息，以攻击者为单位展示攻击过程、攻击阶段、攻击路径和攻击手段。结合攻击行为和攻击者身份进行攻击者画像，展示攻击全过程。攻击者画像如图2所示。

4 欺骗防御技术价值体现

欺骗防御技术较传统安全防御技术，有着独特的价值体现，尤其在面对0day漏洞这种不可预知的安全威胁时，无有效手段提前判断形势，传统手段往往只能待事件发生后做应急响应，采取相应的措施以减轻或消除对系统的威胁[13]。这些往往都是被动响应，在网络安全事件发生后采取相应的措施，如隔离受感染的主机、清除恶意代码等[14-15]。而欺骗防御技术通过强大的业务高仿真和蜜网组建能力，在入侵者必经之路上构造陷阱，混淆攻击目标，吸引攻击者进入蜜网，拖住攻击者，延缓攻击，保护真实系统，可提前发现攻击者的行为，分析攻击目的和意图，制定防御方案，提前预警，为应急响应争取时间。

在HW场景中，传统安全防御技术，如防火墙、WAF、IPS等更偏向于防控，溯源取证能力不足。而通过多节点部署的基于欺骗防御技术的蜜罐产品，可全网覆盖，形成一张巨大密网，对红队攻击行为进行诱捕。通过IP溯源、设备指纹获取、社交信息溯源、深度溯源等多种技术方式，实现对攻击者的全面溯源。通过多种溯源信息的结合，可进行攻击者画像，进一步溯源到攻击者的真实信息，定位其地理位置、身份信息等，为蓝方提供防守得分的有效依据。图3给出了HW场景蜜罐部署示意。

5 结论与展望

本研究基于欺骗防御技术，探索了一种更有效的网络安全攻击检测和常见技术能力的实现方式。通过对比传统安全防御技术，突出了欺骗防御技术在面对0day威胁和HW场景中的技术优势。

首先，本研究详细介绍了基于欺骗防御技术的网络安全攻击检测方法，包括入侵检测系统欺骗技术、蜜罐技术、虚假数据技术和欺骗攻击者等4种方法，为网络安全攻击检测提供了新的思路和方法；其次，介绍了几种常见的基于欺骗防御技术的技术实现方式，包括仿真、欺骗环境构建、威胁识别分析和攻击者画像；最后，通过对比传统安全防御技术的2种应用场景，加深读者对欺骗防御技术的理解，进一步体现出

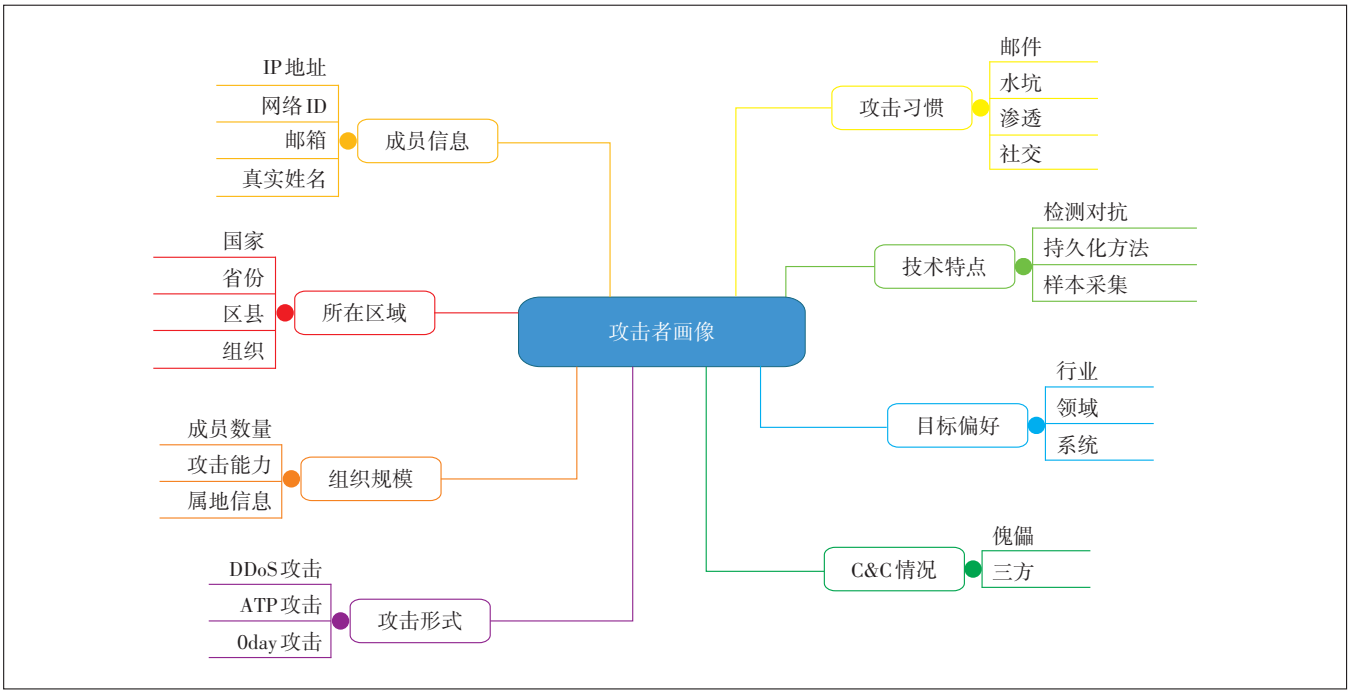

图2　攻击者画像

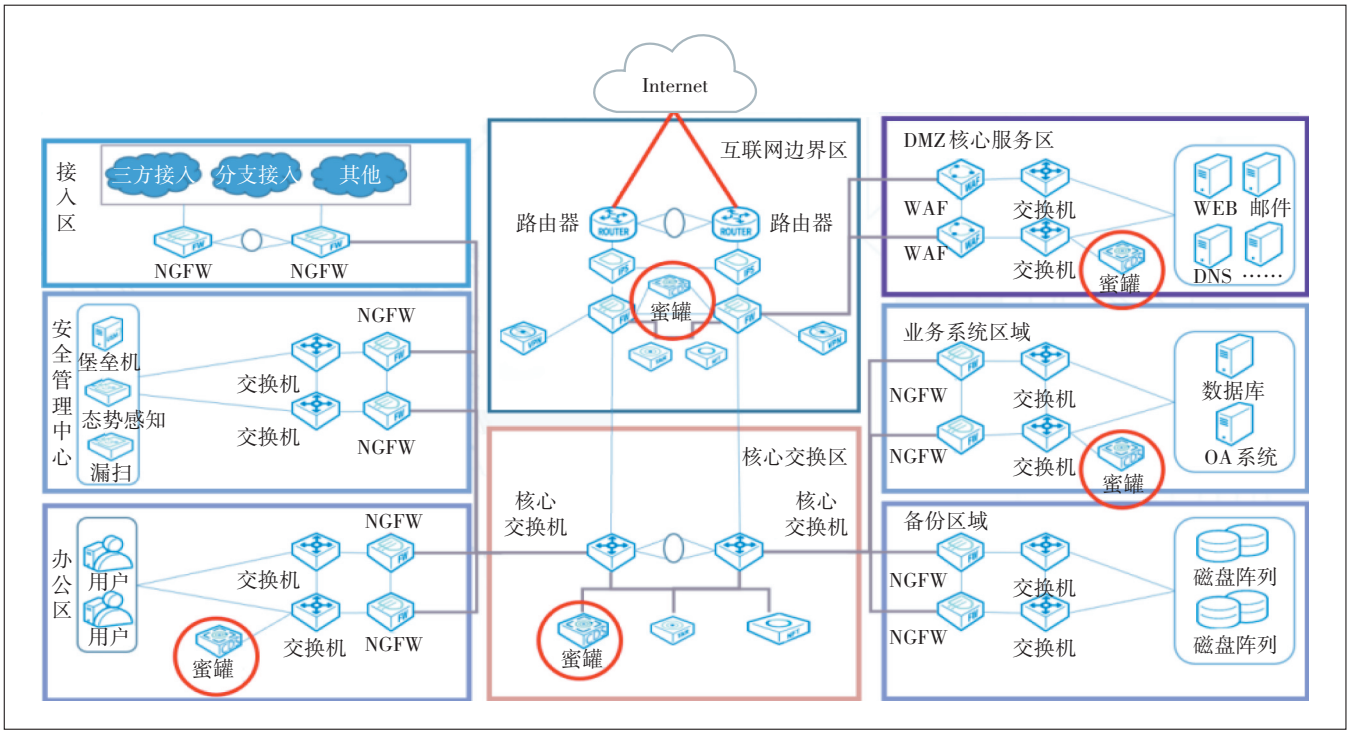

图3 HW场景蜜罐部署示意

欺骗防御技术的能力优势。

总之，本研究为网络安全攻击检测和响应优化提供了新的思路和方法，对于提高网络安全防御能力具有重要意义。后续研究还需要进一步深入探究和解决相关问题，以更好地应对不断变化的网络安全威胁。

参考文献：

[1] 周杨，黄媛媛. 新形势下网络安全企业业态浅析[J]. 信息通信技术与政策，2023，49(2)：30-34.

[2] 吴育辉，杨正泽，张蓉. 新形势下地方院校网络安全管理探讨[J]. 安顺学院学报，2023，25(1)：118-122.

[3] 白天毅. 计算机网络安全技术在网络安全维护中的应用探讨[J]. 长江信息通信，2023，36(2)：235-237.

[4] VANIN P，NEWE T，DHIRANI L L，et al. A study of network intrusion detection systems using artificial intelligence/machine learning [J]. Applied Sciences，2022，12(22)：11752.

[5] 罗婷婷. 面向防御的网络欺骗技术研究[J]. 信息与电脑(理论版)，2019，31(21)：186-187.

[6] 李文博，杜鹏昊. 基于下一代欺骗防御技术的网络安全能力建设[J]. 仪器仪表标准化与计量，2021(6)：22-25.

[7] 裴辰晔. 网络欺骗防御技术在电厂网络安全中的应用[J]. 网络安全技术与应用，2022(10)：110-111.

[8] 顾煜. 多层次网络空间欺骗防御技术效能评估方法[D]. 南京：东南大学，2021.

[9] MAZHAR T，IRFAN H M，KHAN S，et al. Analysis of cyber security attacks and its solutions for the smart grid using machine learning and blockchain methods[J]. Future Internet，2023，15(2)：83.

[10] 贾召鹏. 面向防御的网络欺骗技术研究[D]. 北京：北京邮电大学，2018.

[11] 董志玮. 基于深度学习的无线通信网络入侵检测系统设计[J]. 长江信息通信，2023，36(2)：119-121，124.

[12] 康红莲. 基于蜜罐的欺骗防御系统的设计与实现[D]. 北京：北京邮电大学，2020.

[13] 贾召鹏，方滨兴，刘潮歌，等. 网络欺骗技术综述[J]. 通信学报，2017，38(12)：128-143.

[14] 王小英，刘庆杰，庞国莉. 恶意代码攻击下多业务通信网络安全响应仿真[J]. 计算机仿真，2020，37(10)：137-141.

[15] 厉莉. 分角色信誉模型与分级 Ad hoc 网络安全响应机制研究[D]. 沈阳：东北大学，2013.

作者简介：

黄健，高级工程师，，主要从事网络信息安全的规划、建设与运营工作。