面向网络欺骗防御的攻击诱捕技术研究

高雅卓,刘亚群,邢长友,张国敏,王秀磊
(陆军工程大学 指挥控制工程学院,江苏 南京 210007)

摘 要:作为一种主动对抗攻击者的手段,网络欺骗防御技术得到了学术界和产业界的广泛关注,其中攻击诱捕技术是网络欺骗防御的核心所在。其基本理念是通过建立虚假的网络和业务系统环境,引诱攻击者对诱捕系统发起攻击而达到监控分析攻击行为的目的。着眼于面向攻击诱捕的网络欺骗防御技术研究,讨论了攻击诱捕技术的基本概念及典型架构,并从决策控制和欺骗环境构建两个方面对攻击诱捕机制的实现机理进行了探讨。总结了攻击诱捕技术在欺骗防御场景中的作用,在此基础上从传统诱捕机制、虚拟化诱捕机制以及智能诱捕决策等方面分析了攻击诱捕技术的研究现状及关键技术,为欺骗诱捕系统的设计提供了一定的思路,总结分析了现有研究存在的问题,并展望了未来的发展方向和面临的挑战。

关键词:欺骗防御;攻击诱捕;蜜罐;虚拟化;博弈论
中图分类号:TP393.0 **文献标识码**:A **文章编号**:1673-629X(2022)03-0114-06
doi:10.3969/j.issn.1673-629X.2022.03.019

Research on Network Deception Defense Oriented Attack Trapping Technology

GAO Ya-zhuo,LIU Ya-qun,XING Chang-you,ZHANG Guo-min,WANG Xiu-lei
(School of Command and Control Engineering,Army Engineering University of PLA,Nanjing 210007,China)

Abstract:As a means to actively counter attackers,cyber deception defense technology has received extensive attention from academia and industry,among which how to capture attacker is the core of cyber deception defense. The basic idea is to achieve the purpose of monitoring and analyzing attacks by establishing a false network and trapping environment to lure attackers. Focusing on the research of network deception defense technology for attack trapping,the design ideas of attack trapping system are investigated,the typical architecture of attack trapping technology is analyzed,and the design of trapping system is divided into two parts:decision-making control and deception environment. Discussed the three major modules of deception environment design,and divided the development of attack trapping technology into three stages:traditional trapping,complex trapping and intelligent trapping. Combined with the development of attack trapping technology,the key technologies for the design of each module of the deception environment are discussed. Based on the existing problems in the design of trapping systems,the future development trend of attack trapping technology is analyzed.

Key words:deception defense;attack trapping;honeypot;virtualization;game theory

0 引 言

随着互联网技术的蓬勃发展,网络安全问题已经受到了业内的广泛关注。传统的防御手段如防火墙、IDS 和 IPS 等只能被动地对攻击者进行检测阻断,而攻防双方信息的不对称性使得这些被动防御技术很难应对如今复杂多样的网络攻击手段。

为了解决这种攻防不对称的现象,基于欺骗的网络主动防御思想应运而生。欺骗防御的主要思想是“通过干扰攻击者的认知以促使攻击者采取有利于防御方的行动[1]”。典型的欺骗防御技术[2]包括特征混淆技术、指纹隐藏技术以及攻击诱捕技术等。其中特征混淆主要是产生虚假的网络特征来欺骗攻击者的认知,如产生虚假网络拓扑结构[3]、虚假通信关系[4]等。指纹隐藏技术[5]主要是避免暴露网络实体的真实指纹信息,包括协议指纹、操作系统指纹、应用指纹等。攻击诱捕[6]则主要通过构建虚假的网络实体,诱使攻击者对这些虚假网络实体进行攻击,从而达到暴露攻击行为、消耗攻击资源的目的。

收稿日期:2021-03-29 **修回日期**:2021-07-29
基金项目:国家自然科学基金项目(61379149,61772271);国家博士后科学基金项目(2017M610296)
作者简介:高雅卓(1998-),女,硕士,研究方向为网络空间安全;邢长友,硕导,副教授,研究方向为网络空间安全;张国敏,硕导,副教授,研究方向为网络空间安全和网络管理。

在上述技术中,特征混淆和指纹隐藏都是通过更改或隐藏原本真实资源的特征,以达到预防延缓攻击的目的。而攻击诱捕则是伪造了一个能够与攻击者交互的欺骗环境,通过诱导攻击者发起错误攻击,达到检测并分析攻击者行为特征的目的。相对于其他技术而言,面向攻击诱捕的欺骗防御技术更具有主动性,也更能打破攻防不对称的局面。

面向攻击诱捕的网络欺骗防御思想最早可以追溯到 1989 年[7],传统的攻击诱捕技术通常是使用模拟程序部署的低交互蜜罐或使用普通虚拟机实现的简单高交互蜜罐,虽然具备一定的诱捕能力,但是总体而言部署功能单一、结构僵化、灵活性也较差[8],很难适应当今复杂多变的 APT 攻击和零日漏洞攻击。为了更好地与攻击者进行交互,一些新的攻击诱捕机制在设计思路上通常与博弈论、机器学习等思想相结合以提供更加逼真的诱捕链,在实现上则利用容器、SDN 等技术以平衡成本与性能的冲突,从而建立智能灵活的攻击诱捕场景。

该文后面部分安排如下:第一节介绍了面向攻击诱捕的网络欺骗防御基本架构,并分析了利用传统蜜罐技术构建攻击诱捕环境的方法;第二节介绍了基于虚拟化的新型诱捕模型,重点从与虚拟化技术结合以及攻击状态迁移两个角度进行了讨论分析;第三节介绍了当前智能诱捕阶段的决策机制,主要从博弈对抗和智能优化模型两个方面进行介绍。

1　攻击诱捕概念及典型架构分析

1.1　网络攻击诱捕的基本概念与架构

攻击诱捕系统主要分为决策控制模块和欺骗环境两大模块(见图 1)。决策控制模块主要是分析当前收集到的信息,并对欺骗环境的设计进行决策;欺骗环境主要负责引诱攻击、与攻击者交互并监控攻击行为信息。

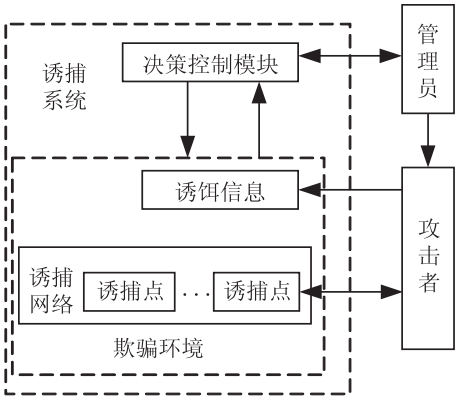

图 1　攻击诱捕系统结构

在引诱攻击方面,主要有间接引诱和直接引诱两种方式,直接引诱是指攻击者直接进入诱捕系统中[9],间接引诱是指攻击者由于非法使用诱饵信息或出现其他攻击行为被管理员发现后迁移至诱捕系统中[10]。

诱捕系统的欺骗交互主要体现在诱捕网络中,诱捕网络的设计主要包括两个方面:一是网络内部各个诱捕点的诱捕机制设计,单个攻击者与诱捕网络的交互实际上是与某个特定诱捕点的交互;二是诱捕网络架构的场景构建,由于单个诱捕点的欺骗能力受限,大型的诱捕系统通常会将多个诱捕点组合起来形成诱捕网络以提供更加逼真全面的诱捕。

由此根据欺骗环境的三个模块可以将诱捕系统设计的关键要素分为:诱饵信息、诱捕点和诱捕网络,根据三个模块的自身特性,可以将其关键技术分别分为诱饵信息生成技术、诱捕机制设计技术和诱捕场景构建技术。在以后的诱捕系统设计中,主要都是针对这三个关键技术进行研究设计。

1.2　基于传统蜜罐的攻击诱捕机制

基于欺骗的防御思想最初仅被网络管理员作为一种主动防御的新思路而使用[7]。直到 20 世纪末期,以 Honeyd[11] 为代表的一批低交互蜜网成为了主流,这一时期蜜网项目组提出了许多蜜网的概念,如 2003 年的“分布式蜜网[12]”,2004 年的“蜜场[13]”等,并且都根据这些概念进行了项目的开发[14];在这一时期,国内也有多个团队开始对蜜罐技术进行关注,如诸葛建伟等人加入了蜜网项目组[15],并成为其在中国的分支团队;同时也有学者在蜜罐技术的基础上提出了新的欺骗诱捕技术。

然而,这一时期的欺骗诱捕技术处于传统诱捕阶段,大多数为简单的诱捕系统,对攻击者的捕获能力并不全面,主要停留在网络服务和应用程序的层面,并没有针对操作系统级别进行重点防护。

这一阶段的诱捕系统大多为简单的蜜罐系统,虽然在应用技术和机制设计上都不够成熟,但是已经逐渐形成了攻击诱捕机构的雏形,以后的攻击诱捕系统基本都是按照这一时期的架构进行改进。

2　虚拟化网络攻击诱捕机制

随着攻击技术的发展,传统诱捕机制的灵活性不足、难以快速构建高逼真的诱捕场景等问题越来越突出。随着 SDN[16]、轻量级的虚拟化技术 LXC[17] 以及 Docker[18] 等技术的发展,许多团队开始将新型网络和虚拟化技术与诱捕系统的设计思想相结合,提出了结合 SDN 的诱捕系统结构[19]、结合容器的主动防御[20]等思想,更好地平衡了交互能力高低和系统规模大小的冲突。

这一阶段的欺骗诱捕技术开始进入复杂诱捕阶段,主要是通过将欺骗诱捕的思想与新兴技术进行结

合,实现在低成本大规模部署的基础上,提高系统交互的能力,重点转向虚拟化的诱捕架构设计和诱捕过程中攻击状态的迁移机制。

2.1 虚拟化诱捕架构

在复杂诱捕阶段,传统的攻击诱捕架构开始与新型的虚拟化技术结合,形成了基于虚拟化技术的新式诱捕架构,其中较为主流的两种虚拟化技术分别是虚拟机技术和轻量级虚拟化技术。

2.1.1 基于虚拟机的诱捕环境生成机制

虚拟机在很长一段时间都是诱捕机制设计过程中最常用的技术。Argos[21]对 Qemu 进行扩展,使用动态污点分析跟踪整个运行过程中收到的网络数据;为了更好地提升蜜罐的真实性,Biederman 等人[22]提出了一种部分克隆生产系统内部虚拟机快照的诱捕系统框架,由于基本镜像仍然是源虚拟机的快照,所以蜜罐环境与生产环境基本一致,隐蔽性更好。

为了更好地对虚拟机进行监控,诱捕机制通常会结合虚拟机自省技术进行设计,虚拟机自省主要是一种从虚拟机外部监控虚拟机内部运行状态的方法,Stewart 等人[23]对多种诱捕机制的实现方法进行比对,发现 VMI 技术在应用上通用性更强,安全性更高,并且不会受到攻击者的影响。

VMI 技术在诱捕机制中应用的重点在于对虚拟机内部行为的监控功能,SPEMS[24]系统集成并改进了多个开源软件工具,利用 VMI 技术在外部监视虚拟机内部程序的执行情况;Urias 等[6]设计了一个能够配置并控制虚拟机的自省程序 KVMi,用于承担虚拟机监视器的角色,能够在不添加任何构件的情况下实时监测虚拟机状态。

虚拟机自省技术主要应用于虚拟机中,对部署成本有一定的要求,近年来成本更低的轻量级虚拟化技术也越来越受到研究人员的关注。

2.1.2 基于轻量级虚拟化的诱捕环境生成机制

虚拟机虽然能在一定程度上平衡部署成本和交互程度的冲突,但是在一台资源有限的服务器上能建立的虚拟机数量仍然有限,难以实现大规模的诱捕网络部署,此外,现有的虚拟机检测技术等使得攻击者很容易发现自身处于一个危险的环境中而提高警惕,而 Alexander[25]根据研究发现容器技术可以很好地规避这一缺陷。目前常用的容器技术主要有 LXC[17]和 Docker[18]。

Honeypatches[10]将使用 LXC 作为诱捕点,将触碰了诱饵补丁的攻击会话转移到特定的诱捕点内进行攻击诱捕;容器的自身特性使其可以作为嵌入式的诱捕点直接部署在真实系统内部,AHEAD[20]提出可以将主动防御工具封装在 Docker 内部直接安装到真实系统中,迫使攻击者在攻击的过程中必须筛选真实服务和虚假服务,延缓了攻击者的攻击时间,但是由于此架构的安全性仅通过 Docker 自身的隔离性保证,一旦攻击者通过容器逃逸进入主机中时,生产系统仍然面临较大威胁。

2.2 攻击状态迁移机制

在攻击诱捕系统中除了初始的架构设计,还需要考虑在与攻击者交互过程中的攻击状态迁移机制。攻击状态迁移指的是在攻击诱捕过程中对攻击流量的重定向传输,通常发生在诱捕系统与生产系统之间,或者诱捕系统内部不同的诱捕点之间。

2.2.1 诱捕系统与生产系统之间迁移

诱捕网络与生产网络之间的攻击状态迁移一般发生在合作部署的诱捕系统中,此类诱捕系统主要针对内部攻击,在迁移过程中,为了保证会话状态的连续性,往往需要将生产环境中的源服务进行同步迁移。

初始状态下攻击者与生产网络进行交互,在生产网络内部因为执行非法动作被发现后,攻击会话将迁至诱捕网络内部,此后攻击者只与诱捕网络进行交互。

此类诱捕系统较为经典的架构 HADES[26]提出当攻击者的流量在生产网络中被发现时,就通过一系列操作将攻击流量引至一个高逼真的诱捕环境中。

近年来,为了实现流量透明迁移,同时保证源主机的正常会话状态,攻击迁移通常会与 SDN 技术相结合,INTERCEPT+[19]通过更改虚拟机迁移代码,使得迁移以后源虚拟机仍保持运行,这样可以保证与源虚拟机通信的正常用户可以继续交互,同时使用 SDN 交换机隔离诱捕网络和真实系统;此外,Sandnet[27]还将攻击迁移的思想应用于微服务背景,使用容器代替了虚拟机,并且考虑了迁移之前生产网络内部容器之间的通信问题,将与被怀疑容器交互的相关容器同时进行迁移,同样用 SDN 技术进行流量控制。

2.2.2 诱捕系统内部迁移

诱捕系统内部的攻击状态迁移主要发生在不同类型的诱捕点之间,一般是在决策控制器发现攻击的状态发生变化后,将攻击会话从原来的诱捕点迁移至另一类诱捕点中。

这种状态迁移最常发生在混合蜜网中高交互蜜罐与低交互蜜罐之间,对大量的低交互蜜罐捕获的流量进行分析,然后把需要重点分析的流量导入高交互蜜罐中,这种混合蜜网的主要目的是结合高交互蜜罐和低交互蜜罐的优点。

为了进一步降低被攻击者发现的几率,HoneyDOC[28-29]提出了一种与 SDN 技术结合的 TCP 重放机制,可以将攻击者流量进行无缝迁移,迁移之后无需重新建立连接。

除了诱捕点交互程度的不同,诱捕系统还会根据攻击者的可信性和攻击阶段为其提供不同级别的诱捕点进行交互,HoneyV[9]通过 IDS 判断所有入站流量的可信级别,并根据结果将不同级别的攻击者放入四个不同监视级别的蜜罐中进行分析;还可以根据攻击者攻击阶段的不同进行分级,Honeyproxy[30]根据攻击的阶段不同设置了三种代理模式,有效地防止了蜜罐追踪,但是一个代理仅能管理一个攻击者,所以需要为每个监控的端口都部署一个代理。

3　智能诱捕决策机制

除了先进的虚拟化技术和网络技术,强化学习的思想也对网络安全领域产生了一定影响,目前已有团队开始将强化学习与攻击诱捕的思想相结合[31],以期实现智能化的诱捕系统,此前也已经有不少学者将博弈论[32]的思想应用于攻击诱捕技术当中,并且取得了较大的进展。

当前阶段可以称为智能诱捕阶段,主要是将攻击诱捕的思想与其他领域的思想进行交叉,通过与博弈论和机器学习等方向的结合,进一步提高系统智能交互的能力,注重具体的诱捕流程设计。

3.1　攻击诱捕中的博弈对抗

博弈论的思想常常应用于诱捕机制的设计。Walter 等人[33]在诱捕机制中引入了超博弈的思想,防御方通过改变参数,欺骗攻击者的视图,使得攻击者误认为自己拥有完全信息,以此最大化防御方优势;王娟等人[34]提出了一种基于多阶段攻击的 SDN 动态蜜罐 SDHG,使用不完全信息动态博弈对不同阶段的攻防策略进行建模,并证明了模型的可行性,最后使用 Docker 容器对原型系统进行了实现,并在与其他策略的对比中体现了该方法的优越性;姜伟等人[35]对攻防博弈模型和马尔可夫决策进行了扩展,提出了一种随机博弈的模型,更加贴合攻防博弈的现实情况。

博弈论除了可以针对单个诱捕点内部的诱捕机制进行建模,在诱捕点的分配决策中也可以起到较大的作用。Aliou[36]利用博弈论对蜜罐的分配进行决策,减少攻击者发现蜜罐的概率;Attiah[37]将攻防双方进行了多层次的策略建模,双方都根据策略的成本、潜在的攻击收益或损害以及预测对手策略的有效性来调整自己的策略,并最终得到了混合策略纳什均衡。

除了单独使用博弈论,Ahmed 等人[38]还将博弈论与攻击图相结合,判断在已知当前攻击者位置的情况下接下来多跳诱捕点的分配策略。

3.2　智能优化模型

机器学习主要是研究如何让计算机能够模拟人类的学习行为,从而自主提高自身性能的学科。由于机器学习思想自身的特性,其在攻击诱捕系统中的应用场景更为广泛。

传统生成诱饵信息的方法大多是根据真实数据集特征生成的,这类诱饵信息中保留了部分源数据的信息,仍存在被攻击者窃取隐私的风险。DPSYN[39]提出一种将深度学习与差分隐私相结合自动生成诱饵数据库的方法,这种方法不仅可以根据原有数据集的特征生成相似度较高的数据,也能有效防止在诱饵数据中暴露源数据的隐私信息,更加安全。

除了生成诱饵信息,机器学习还可以与诱捕机制设计相结合,用于进行攻击识别和智能诱捕。在攻击检测识别方面,Nadiya[40]提出了一种基于机器学习聚类思想的算法,用于在诱捕点中辨认攻击者,并将结果用于后期的防御策略的配置;另一种更加常见的方法是使用强化学习的思想进行智能诱捕,这种将强化学习加入诱捕系统的思想最早来自于 2011 年的 Heliza[41],Pauna 等人[31]使用类似的建模方法针对该思想进行了改进,之后又将 Cowrie 蜜罐与 DQN 思想[42]相结合,实现了一种自适应的智能 SSH 蜜罐。

除了 Heliza 的建模方法之外,SMDP[43]提出将马尔可夫决策过程的方法应用于攻击诱捕中,把连续时间过程转化为等效的离散决策模型,并使用强化学习对该模型进行了训练,最后得到了规避风险、成本效益和时间效益的最优策略。

4　存在的问题及进一步研究方向分析

从蜜罐的思想提出开始算起,目前欺骗诱捕技术已经发展了近 30 年,虽然在学术领域已经得到了较广泛的认可,但仍然存在不少问题,下面将主要讨论这些关键性的问题并提出一些解决方法。

4.1　利用机器学习与博弈论构建智能化诱捕场景

目前的诱捕系统大多是根据预先设定的场景建立的,在与攻击者交互的过程中很少会根据攻击者攻击的变化动态地更改诱捕场景,导致诱捕场景的结构较为僵化,难以迷惑高级的攻击者。

因此可以考虑结合攻击链的概念,将诱捕技术与博弈论相结合,根据攻击者攻击手段的变化给出攻击者期望的响应,构建动态博弈的诱捕场景。

4.2　结合其他防御技术增强生产流量诱捕能力

由于诱捕系统只能捕获交互对象的数据,如果攻击者不与诱捕系统进行接触,诱捕系统就永远无法检测到攻击的存在。

因此可以考虑将攻击诱捕技术与其他的防御技术相结合,如 Takabi[44]提出了一种将欺骗防御与 MTD 相结合的防御思想,可以用于缓解内部攻击。

4.3 跨平台一体化数据收集分析机制

目前的诱捕系统大多是复杂的大型网络,这些网络中往往需要使用不同类型的诱捕软件,然而大多数软件并没有统一的数据收集格式,使得数据收集工作十分繁杂,另一方面,理解和利用这些收集到的原始数据对分析员的专业素养要求较高。

因此,统一数据收集格式至关重要,同时应该简化数据分析的过程,尽量实现自动化分析,提高分析结果的可读性。

5 结束语

欺骗诱捕技术自从 1989 年提出以来,在网络安全领域应用十分广泛。该文立足于诱捕系统欺骗环境设计的三大模块,根据诱捕系统的发展阶段对各个模块的设计进行讨论分析,主要目的在于为诱捕系统的设计者提供一个简单的参考,并在最后给出了当前诱捕系统具有的问题和未来发展的趋势。虽然目前诱捕系统仍然有许多难以解决的问题,但是仍符合网络安全未来趋势的发展。

参考文献:

[1] 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.

[2] HAN X,KHEIR N,BALZAROTTI D. Deception techniques in computer security[J]. ACM Computing Surveys,2018,51(4):1-36.

[3] MEIER R,TSANKOV P,LENDERS V,et al. Nethide:secure and practical network topology obfuscation[C]//Proceedings of the 27th USENIX security symposium. Baltimore,MD,USA:USENIX Association,2018:693-709.

[4] MEIER R,GUGELMANN D,VANBEVER L. Itap:in-network traffic analysis prevention using software-defined networks[C]//Proceedings of the symposium on SDN research. Santa Clara,CA,USA:Association for Computing Machinery,2017:102-114.

[5] ALBANESE M,BATTISTA E,JAJODIA S,et al. A deception based approach for defeating os and service fingerprinting[C]//2015 IEEE conference on communications and network security. Florence,Italy:IEEE,2015:317-325.

[6] STOUT W,URIAS V,LOVERRO C,et al. Now you see me now you don't:advancing network defense through network deception[R]. Albuquerque,NM (United States):Sandia National Lab (SNL-NM),2017.

[7] STOLL C. The cuckoo's egg:tracking a spy through the maze of computer espionage[M]. London:The Bodley Head Ltd,1989:1-3.

[8] 石乐义,李 阳,马猛飞. 蜜罐技术研究新进展[J]. 电子与信息学报,2019,41(2):498-508.

[9] RASHIDI B,FUNG C,HAMLEN K W,et al. Honeyv:a virtualized honeynet system based on network softwarization[C]//NOMS 2018 IEEE/IFIP network operations and management symposium. Budapest,Hungary:IEEE,2018:1-5.

[10] ARAUJO F,HAMLEN K W,BIEDERMANN S,et al. From patches to honey-patches:lightweight attacker misdirection,deception,and disinformation[C]//Proceedings of the 2014 ACM SIGSAC conference on computer and communications security. Scottsdale,Arizona,USA:ACM,2014:942-953.

[11] PROVOS N. A virtual honeypot framework[C]//USENIX security symposium. CA,United States:USENIX Association,2004:1-14.

[12] WATSON D,RIDEN J. The honeynet project:data collection tools,infrastructure,archives and analysis[C]//Proceedings of the 2008 WOMBAT workshop on information security threats data collection and sharing. NW Washington,DC,United States:IEEE Computer Society Press,2008:24-30.

[13] SPITZNER L. Honeypot farms[EB/OL]. (2003-08-13). http://www.symantec.com/connect/articles/honeypot-farms.

[14] 陆腾飞,陈志杰,诸葛建伟,等. 面向蜜场环境的网络攻击流重定向机制的研究和实现[C]//第六届中国信息和通信安全学术会议(CCICS'2009). 南京,中国:东南大学,2009:14-20.

[15] 诸葛建伟,唐 勇,韩心慧,等. 蜜罐技术研究与应用进展[J]. 软件学报,2013,24(4):825-842.

[16] FEAMSTER N,REXFORD J,ZEGURA E. The road to SDN:an intellectual history of programmable networks[J]. Queue,2013,11(12):20-40.

[17] SOLTESZ S,PÖTZL H,FIUCZYNSKI M E,et al. Container-based operating system virtualization:a scalable,high-performance alternative to hypervisors[J]. ACM SIGOPS Operating Systems Review,2007,41(4):275-287.

[18] MERKEL D. Docker:lightweight linux containers for consistent development and deployment[EB/OL](2014-05-19). https://www.linuxjournal.com/content/docker-lightweight-linux-containers-consistent-development-and-deployment.

[19] HIRATA A,MIYAMOTO D,NAKAYAMA M,et al. Intercept+:Sdn support for live migration-based honeypots[C]//2015 4th international workshop on building analysis datasets and gathering experience returns for security (BADGERS). Kyoto,Japan:IEEE,2015:16-24.

[20] GASPARI F D,JAJODIA S,MANCINI L V,et al. Ahead:a new architecture for active defense[C]//ACM workshop on automated decision making for active cyber defense. NY,United States:Association for Computing Machinery,2016:11-16.

[21] PORTOKALIDIS G,SLOWINSKA A,BOS H. Argos:anemulator for fingerprinting zero-day attacks for advertised honeypots with automatic signature generation[J]. ACM SIGOPS Operating Systems Review,2006,40(4):15-27.

[22] BIEDERMANN S,MINK M,KATZENBEISSER S. Fast dy-

namic extracted honeypots in cloud computing[C]//Proceedings of the 2012 ACM workshop on cloud computing security workshop. Raleigh North Carolina, USA: ACM, 2012: 13-18.

[23] SENTANOE S, TAUBMANN B, REISER H P. Virtual machine introspection based SSH honeypot[C]//Workshop on security in highly connected it systems. Munich, Germany: Bavarian State Ministry for Education, 2017: 13-18.

[24] SHI J, YANG Y, LI C, et al. Spems: a stealthy and practical execution monitoring system based on VMI[C]//Cloud computing and security. Nanjing, China: Springer, 2015: 380-389.

[25] KEDROWITSCH A, YAO D, WANG G, et al. A first look: using linux containers for deceptive honeypots[C]//Proceedings of the 2017 workshop on automated decision making for active cyber defense - SafeConfig '17. NY, United States: Association for Computing Machinery, 2017: 15-22.

[26] STOUT W, URIAS V. Hades: high-fidelity adaptive deception & emulation system[R]. Albuquerque, NM (United States): Sandia National Lab, 2018.

[27] OSMAN A, BRUCKNER P, SALAH H, et al. Sandnet: towards high quality of deception in container-based microservice architectures[C]//2019 IEEE international conference on communications (ICC). Shanghai, China: IEEE, 2019: 1-7.

[28] FAN W, DU Z, SMITH-CREASEY M, et al. Honeydoc: an efficient honeypot architecture enabling all-round design[J]. IEEE Journal on Selected Areas in Communications, 2019, 37(3): 683-697.

[29] FAN W, FERNáNDEZ D. A novel SDN based stealthy TCP connection handover mechanism for hybrid honeypot systems[C]//2017 IEEE conference on network softwarization (NetSoft). Italy: IEEE, 2017: 1-9.

[30] KYUNG S, HAN W, TIWARI N, et al. Honeyproxy: design and implementation of next-generation honeynet via SDN[C]//2017 IEEE conference on communications and network security (CNS). NV, USA: IEEE, 2017: 1-9.

[31] PAUNA A, BICA I. Rassh - reinforced adaptive SSH honeypot[C]//2014 10th international conference on communications. Bucharest, Romania: IEEE, 2014: 1-6.

[32] BOUMKHELD N, PANDA S, RASS S, et al. Honeypot type selection games for smart grid networks[C]//Conference on decision & game theory for security. Vienna, Austria: Springer International Publishing, 2019: 85-96.

[33] FERGUSON-WALTER K, FUGATE S, MAUGER J, et al. Game theory for adaptive defensive cyber deception[C]//Proceedings of the 6th annual symposium on hot topics in the science of security. Nashville, Tennessee, USA: Association for Computing Machinery, 2019.

[34] 王　鹃,杨泓远,樊成阳. 一种基于多阶段攻击响应的 SDN 动态蜜罐[J]. 信息网络安全,2021,21(1):27-40.

[35] 姜　伟,方滨兴,田志宏,等. 基于攻防随机博弈模型的防御策略选取研究[J]. 计算机研究与发展,2010,47(10):1714-1723.

[36] SARR A B, ANWAR A H, KAMHOUA C, et al. Software diversity for cyber deception[C]//IEEE global communications conference. Taiwan: IEEE, 2020: 1-6.

[37] ATTIAH A, CHATTERJEE M, ZOU C C. A game theoretic approach to model cyber attack and defense strategies[C]//2018 IEEE international conference on communications (ICC). Kansas City, MO: IEEE, 2018: 1-7.

[38] ANWAR A H, KAMHOUA C A, LESLIE N. Honeypot allocation over attack graphs in cyber deception games[C]//2020 international conference on computing, networking and communications (ICNC). USA: IEEE, 2020: 502-506.

[39] ABAY N C, AKCORA C G, ZHOU Y, et al. Using deep learning to generate relational honeydata[M]//Autonomous cyber deception. Shanghai, China: Springer, 2019: 3-19.

[40] EL KAMEL N, EDDABBAH M, LMOUMEN Y, et al. A smart agent design for cyber security based on honeypot and machine learning[J]. Security and Communication Networks, 2020(8): 9.

[41] WAGENER G, STATE R, DULAUNOY A, et al. Heliza: talking dirty to the attackers[J]. Journal in Computer Virology, 2011, 7(5): 221-232.

[42] PAUNA A, IACOB A C, BICA I. Qrassh - a self-adaptive ssh honeypot driven by q-learning[C]//2018 international conference on communications (COMM). Bucharest: IEEE, 2018: 441-446.

[43] HUANG L, ZHU Q. Adaptive honeypot engagement through reinforcement learning of semi-markov decision processes[C]//International conference on decision and game theory for security. USA: Springer, 2019: 196-216.

[44] TAKABI H, JAFARIAN J H. Insider threat mitigation using moving target defense and deception[C]//Proceedings of the 2017 international workshop on managing insider security threats. Texas, USA: Association for Computing Machinery, 2017: 93-96.