MTD增强的网络欺骗防御系统

高春刚[1,2],王永杰[1,2],熊鑫立[1,2]
1.国防科技大学 电子对抗学院,合肥 230037
2.安徽省网络安全态势感知与评估重点实验室,合肥 230037

摘 要:计算机网络正在飞速发展,但随之而来的系统破坏、信息泄露等网络安全问题也日益突出。攻击者在正式攻击前通常进行大量的网络侦查,以发现目标网络和系统上的可利用漏洞,而传统网络系统中的静态配置为攻击者发现网络目标和发起攻击提供了极大的优势。为了减轻攻击者持续性网络侦查攻击的有效性,基于软件定义网络开发了移动目标防御(moving target defense,MTD)增强的网络欺骗防御系统。该系统采用网络欺骗技术,混淆攻击者收集到的目标网络和系统信息,延长攻击者扫描到网络内真实脆弱性主机的时间,提高其时间成本;并在此基础上融合移动目标防御技术,动态随机地变换网络内节点的IP地址,增强网络欺骗系统的防御效能。实现了系统原型并对其进行评估,在虚拟网络拓扑规模为3个网段且地址变换周期为30 s的配置下,该系统将攻击者发现脆弱性主机的时间平均延迟7倍,将攻击者成功攻击脆弱性主机的概率降低83%,同时系统额外开销平均在8%以内。

关键词:网络侦查攻击;网络欺骗;移动目标防御;软件定义网络
文献标志码:A **中图分类号:**TP393 doi:10.3778/j.issn.1002-8331.2105-0169

MTD Enhanced Cyber Deception Defense System

GAO Chungang[1,2], WANG Yongjie[1,2], XIONG Xinli[1,2]
1.College of Electronic Engineering, National University of Defense Technology, Hefei 230037, China
2.Anhui Key Laboratory of Cyberspace Security Situation Awareness and Evaluation, Hefei 230037, China

Abstract: Computer networks are developing rapidly, but network security such as system damage and information leakage are also becoming increasingly prominent. Attackers usually conduct a large number of network reconnaissance before a formal attack to discover exploitable vulnerabilities in the target network and system. The static configuration in traditional network systems provides a great advantage for adversaries to find network targets and launch attacks. To reduce the effectiveness of adversaries' continuous reconnaissance attacks, this paper develops a moving target defense enhanced cyber deception defense system based on software-defined networks. The system uses cyber deception technology to confuse the target network and system information collected by the attacker, extends the time for the attacker to scan the real vulnerable hosts in the network, and increases the attacker's time cost. Besides, this paper integrates IP address randomization technology on the cyber deception, dynamically and randomly changes the IP addresses of nodes in the network to enhance the defensive effectiveness of the network deception system. Finally, the system prototype is implemented and evaluated. In a configuration where the virtual network topology scale is three network segments, and the address conversion cycle is 30 seconds, this system delays the adversaries' discovery of vulnerable hosts by an average of seven times, reducing the probability of adversaries successfully attacking vulnerable hosts by 83%. At the same time, the system overhead is less than 8% on average.

Key words: network reconnaissance attack; cyber deception; moving target defense; software defined network

互联网在给人们带来高效和便利的同时,网络安全问题也日趋严重,已经成为政府和企业最迫切需要解决的问题之一。企业和政府通过门户网站将各种信息系统、数据资源和互联网资源集成到一个信息管理平台上,并建立对外部客户和内部人员的信息通道,从而能够释放存储在内部和外部的各种信息。而对于攻击者来说,这些门户网站则成为他们进入内网的入口[1]。传统的网络防御技术大都是通过入侵检测、防火墙等技术

作者简介:高春刚(1996—),男,硕士研究生,研究方向为网络安全、主动防御,E-mail:gangchungaog9432@nudt.edu.cn;王永杰(1974—),男,博士,教授,研究方向为网络安全、主动防御;熊鑫立(1991—),男,博士,讲师,研究方向为动态防御。

收稿日期:2021-05-13 **修回日期:**2021-07-26 **文章编号:**1002-8331(2022)15-0124-09

来保护网络及系统安全，但这些技术都是静态化的，高级持续性威胁（advanced persistent threat，APT）[2]攻击者可长期对目标的固有脆弱性进行反复的漏洞分析和渗透，直到达到最终目标[3]。因此安全人员开始将目光聚焦于主动防御技术，网络欺骗[4]作为其中之一被提出。网络欺骗是根据蜜罐的思想演进而来的一种防御机制，通过在己方网络信息系统中布设骗局，干扰攻击者对己方网络信息系统的感知与判断，从而达到发现、延迟或阻断攻击者活动的目的[5]。然而，目前以蜜罐、蜜网为主的网络欺骗防御系统都存在诱骗性不足、静态性、部署复杂以及维护困难等缺陷。APT攻击者经过精心的探测分析仍然可以绕过防御机制，而蜜罐一旦失效，不仅不能保护网络系统，甚至会被攻击者当做跳板去攻击其他资源[6]。

为解决网络欺骗系统诱骗性不足的问题，通过数据包头重写技术生成与真实网络完全不同的虚拟网络拓扑，使攻击者更难发现网络中的真实脆弱性主机。移动目标防御[7]的思想是使系统动态化，通过增加系统的动态性、随机性和不确定性，增加攻击者的攻击难度和攻击成本，提高系统安全性[8]。其中IP地址随机化技术[9]以网络地址为移动参数，使网络地址随机且随时间变换，从而迷惑攻击者。因此，为解决网络欺骗系统静态性的问题，使用MTD中的IP地址随机化技术来增加网络欺骗系统的动态性，增强其防御效能。软件定义网络（software defined network，SDN）[10]为有效开发和管理网络系统提供了灵活的基础设施，并且操作开销小。因此，为解决网络欺骗系统部署复杂以及维护困难的问题，基于SDN构建网络欺骗防御系统。

因此，本文的目标是缓解高级持续性威胁攻击者对内网的入侵，方法是结合网络欺骗与移动目标防御建立一个MTD增强的网络欺骗防御系统。首先通过数据包头重写改变网络内主机的IP地址并生成大量的诱饵节点，构造虚拟网络拓扑，使攻击者在虚假的资源上花费更多的时间，增加攻击者的时间成本；但APT攻击者通常具备一定的蜜罐识别能力，可以根据与网络中节点交互后的响应来识别真实主机和诱饵节点。因此，本文在虚拟网络拓扑的基础上融合IP随机化技术，尽管攻击者可以在一段时间内收集到网络系统的部分信息，但部署IP随机化后这些信息将会失效，攻击者必须重新对网络进行侦查。通过将网络欺骗和移动目标防御相融合，可以完成它们不能单独实现的目标，有效地抵抗持续性的网络侦查攻击。

1　相关技术

为了阻止或减缓攻击者持续性网络侦查攻击，研究人员提出了许多主动防御方法，主要分为两类：网络欺骗防御和移动目标防御。

网络欺骗防御的核心是防御者利用欺骗和诱导手段有意地干扰攻击者的认知决策过程，从而使攻击者采取有利于防御者的行动。Akiyama等[11]提出基于蜜标的网络欺骗系统，通过在沙箱环境中设置用户名、口令、服务器地址等信息，当发现攻击时，这些蜜标就会被传送给攻击者，从而使其登录预先设置的蜜罐服务器。Achleitner等[12]假设攻击者已经成功进入内网，并且至少有一台主机已经感染了某种恶意软件，通过欺骗攻击者视图混淆攻击者获取的信息，从而延长攻击者识别真实主机的时间，但对主机之间的正常交互造成了较大的影响。Zhan等[13]探讨了如何提高网络欺骗的有效性来加固FTP（文件传输协议）服务来应对APT攻击，通过逻辑约束实例化一个新的FTP文件系统来确保欺骗的一致性，并通过图灵测试，发现参与者识别欺骗性环境的概率接近于随机猜测。Rrushi等[14]描述了在操作系统驻留的防御欺骗方法，核心思想是通过在计算机系统中展示虚假I/O设备，使感染目标主机的恶意软件无效。Rubio-Medrano等[15]提出了一个高交互、可扩展、高伪装的工控蜜罐来收集恶意数据样本以供将来分析时可以有效地欺骗攻击者，它被多种广泛使用的侦查工具识别为真实设备。

传统的网络欺骗系统存在很大的局限性，APT攻击者往往针对特定目标攻击，持续时间长且隐蔽性强，一旦攻击者检测到陷阱的存在并绕过，陷阱将失去意义，甚至沦为攻击者的入侵跳板。因此国内外相关学者针对网络欺骗技术的动态部署做了大量的研究，并取得了一定的成果。Zhe等[16]提出一种基于SDN的虚拟蜜网系统，结合SDN良好的可控性和可扩展性构建蜜网，解决了虚拟蜜罐动态部署复杂和蜜网流量控制困难的问题。Kong等[17]提出自动蜜网部署策略，能够自动生成、部署和调整蜜网部署策略，降低网络攻击的成功率，并从理论层面证明了策略的有效性。Niakanlahiji等[18]提出针对Web程序的个性化欺骗方法，通过与攻击者的交互动态描述每个攻击者的特征，并相应调整欺骗计划，实现个性化欺骗。

现有网络欺骗技术的动态部署方法都是根据当前的网络环境动态调整蜜网网络结构和蜜罐类型，十分依赖恶意流量检测技术，且具有被动性，仍然无法有效防御具备反蜜罐能力的攻击者。

移动目标防御技术通过多样化、动态化和随机化的方法改变IP地址、端口等网络要素，增加攻击者进行网络探测、网络窃听和拒绝服务攻击的难度[19]。目前网络层移动目标防御系统框架大都是基于SDN实现，基于SDN的网络层移动目标防御利用SDN的特点来优化移动目标防御技术，高度可编程的SDN可以有效地增加攻击的不确定性、复杂性和成本[20]。AEH-MTD[21]采用跳频同步策略，客户端和控制器通过同步模块对本地时

钟进行校准,采用源地址熵和流量法检测网络状态,根据检测结果,采用时间自适应和空间自适应的方法对端点信息进行调整,相比于之前的方法具有更大的动态性和灵活性。Narantuya 等[22]为解决单个 SDN 控制器的 MTD 系统的单点失效问题,提出基于多个 SDN 控制器的 MTD 架构,保证了大规模网络中 MTD 系统的性能和安全性。Wang 等[23]提出基于双层 IP 地址调频的移动目标防御方法,设置独立间隔和规则,根据网络安全状况和要求跳变设备 IP 地址和虚拟 IP 地址,防止网络入侵和网络窃听。

MTD 可以不依赖恶意流量检测技术,通过动态变换网络信息干扰攻击者对网络系统的认知,但频繁的变换带来巨大的性能损耗;网络欺骗防御部署后不会对系统性能造成太大影响,但无法有效应对长期潜伏收集信息的 APT 攻击者。因此如何将 MTD 和网络欺骗技术融合来更大程度地发挥防御的有效性是一个非常重要的研究。

2　威胁模型

企业和政府通过门户网站将各种信息系统、数据资源和互联网资源集成到一个信息管理平台上,方便了与外部和内部人员的交互,但门户网站也成为了攻击者进入内网的入口,攻击者一旦拿下网站所在主机的权限,就可以以此为跳板进一步入侵内网。

如图 1 所示,门户网站部署在 DMZ[24]的服务器上,外网人员和内网人员均可以访问门户网站,但外网人员不可以直接访问内网。攻击者已经利用网站上存在的漏洞获取网站所在服务器的管理员权限,并以此为跳板探测内网,准备进一步地入侵。

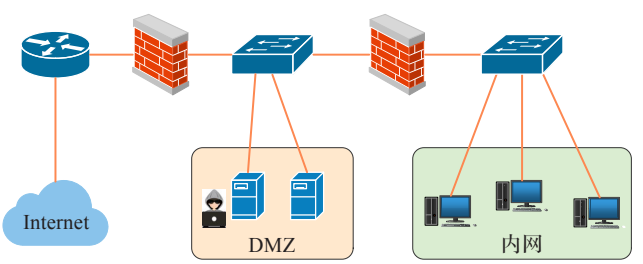

图 1　威胁模型

Fig.1　Threat model

攻击者进行网络侦查时会采取最高效的策略,通常先进行全网段扫描,扫描出网络中所有存活主机,再对存活主机进行进一步探测,分析其可能存在的漏洞,最后攻击存在漏洞的主机。但这种策略不适用于部署了地址变换的网络系统,因为当攻击者扫描出网络中所有存活主机后,准备对存活主机进行进一步探测和漏洞利用时,其虚拟 IP 地址很可能已经过时。所以对于部署了地址变换的网络系统,攻击者只能探测到一个存活主机后立即进行漏洞分析和利用。

对威胁模型提出几点假设:

(1)攻击者的目标为内网中的主机,且攻击者具有足够的耐心来入侵内网。

(2)攻击者具有很强的漏洞分析和漏洞利用能力,对于发现的每一个漏洞都能成功利用。

(3)攻击者意识到 IP 随机化机制已被部署时,会随机探测 IP 地址,发现漏洞后立即攻击。

(4)攻击者在系统进行 IP 地址变换后仍然执行攻击步骤。

3　系统设计

本文基于 SDN 实现网络欺骗系统。图 2 显示了网络欺骗系统的系统架构,它由三个主要组件组成,包括虚拟网络拓扑模块、IP 随机化模块和欺骗服务器,其中虚拟网络拓扑模块和 IP 随机化模块都在 SDN 控制器中实现。

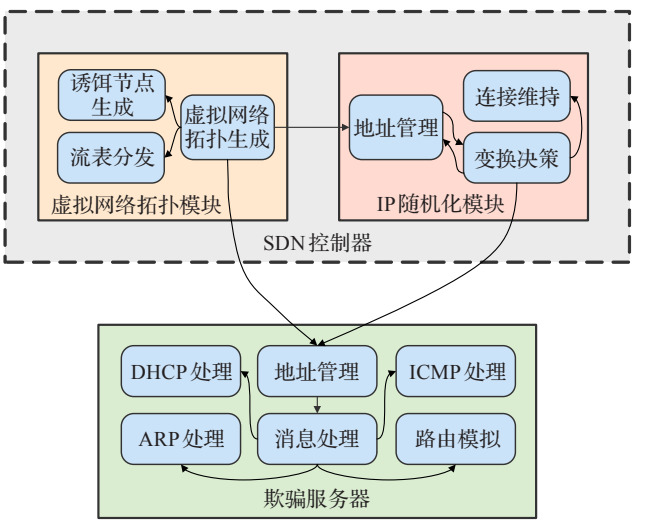

图 2　系统架构

Fig.2　System structure

3.1　虚拟网络拓扑模块

虚拟网络拓扑模块主要负责生成虚拟网络拓扑以及根据虚拟网络拓扑的规范分发流表,包括虚拟网络拓扑生成模块、诱饵节点生成模块和流表分发模块三个子模块。

虚拟网络拓扑生成模块负责提供虚拟网络拓扑规范,即描述主机、诱饵节点的真实和虚拟的地址信息,以及它们之间的连接性。包括:

(1)目标主机的真实 IP 地址、虚拟 IP 地址、真实 MAC 地址和交换机端口。

(2)内网主机的真实 IP 地址、虚拟 IP 地址、真实 MAC 地址和交换机端口。

(3)诱饵节点的真实 IP 地址、虚拟 IP 地址、真实 MAC 地址、虚拟 MAC 地址和交换机端口。

(4)目标主机到内网主机和诱饵节点的虚拟路径

信息。

诱饵节点生成模块负责根据虚拟网络拓扑规范生成大量的诱饵节点。在实际部署中,受限于硬件资源,不能部署大量的蜜罐主机。为了使网络拓扑规模足够大,采用一对多映射的方式生成诱饵节点。在虚拟网络拓扑配置文件中为一个蜜罐主机分配多个虚拟IP,在响应扫描探测时,由SDN控制器将虚拟IP反向映射到其母体蜜罐,由母体蜜罐响应具体的探测行为。

流表分发模块监听来自交换机的PackIn报文,根据虚拟网络拓扑的规范动态生成特定的流表,并将其推送到SDN交换机以控制网络传输。为了引导和控制网络传输,采取反应式流表生成方法,而不是主动式方法,即在到达SDN交换机中的数据包与存储在交换机中的任何流表都不匹配时,SDN控制器动态生成流规则。

算法1给出了虚拟网络拓扑模块的报文处理算法实现。虚拟网络拓扑模块实时监听来自交换机的PackIn消息,分析数据包的源和目的地址以及数据包类型,根据虚拟网络拓扑规范生成特定的流表并添加流表动作,包括重写数据包头,完成真实IP与虚拟IP的转换以及指定转发出口。报文处理算法的时间复杂度在于对于收到的PackIn报文需要查询报文类型和源地址,查询类型的复杂度为1,查询源地址需要遍历虚拟网络拓扑中的所有节点,复杂度为 n (n 为虚拟网络拓扑中的节点数量),因此报文处理算法的时间复杂度为 n 。

算法1 虚拟网络拓扑模块报文处理算法

```
输入:PackIn报文,虚拟网络拓扑
输出:PackOut报文
if PackIn.src=target.addr then//处理来自目标主机报文
  if PackIn.type=ARP then//处理ARP报文
    OutFlow.action is outport=server.switchport
    InFlow.action is outport=ingressport
  end if
  if PackIn.type=IP then//处理IP报文
    OutFlow.action is srcIP=target.rIP and dstIP=dst.rIP
    InFlow.action is srcIP=dst.vIP and dstIP=target.vIP
  end if
end if
else then//处理来自内网主机的报文
  if PackIn.type=ARP then//处理ARP报文
    OutFlow.action is outport=server.switchport
    InFlow.action is outport=ingressport
  end if
    if PackIn.type=IP then//处理IP报文
      if PackIn.dst=target.rIP then
        OutFlow.action is srcIP=src.vIP and dstIP=
target.vIP
        InFlow.action is srcIP=target.rIP and dstIP=src.rIP
      end if
    else then
      OutFlow.action is outport=dst_node.switchport
      InFlow.action is outport=src_node.switchport
    end if
```

结合第2章的分析可知,虚拟网络拓扑与真实网络是严格分离的,通过在DMZ的服务器上部署虚拟网络拓扑,攻击者探测到的内网主机IP地址皆为虚拟IP地址,且其观察到的网络地址空间规模更大,同时还能使攻击者探测到诱饵节点,从而延迟攻击者探测到真实主机的时间。而对于DMZ对于内网中的主机,仍然使用真实IP地址进行交互,因此不会对网络的正常功能造成影响。

3.2 IP随机化模块

为了进一步增加网络欺骗系统的防御效能,创建IP随机化模块。IP随机化模块负责协调网络中主机和诱饵节点的地址变换,包括地址管理模块、变换决策模块和连接维持模块三个子模块。

地址管理模块负责根据虚拟网络拓扑规范实时统计每个子网中的主机和诱饵节点、每个子网中的还未使用的IP地址以及为子网内的主机和诱饵节点分配IP地址,确保在IP地址分配中不会相互干扰。

变换决策模块负责设置IP地址随机化的的周期以及虚拟网络拓扑的构造方法。可以根据实际网络系统状态设定IP地址随机化的周期,兼顾网络性能和安全性。变换决策模块也可以根据实际情况确定虚拟网络拓扑的大小、子网数、每个子网中诱饵节点的数量以及主机在网络中的位置。

连接维持模块负责地址变换时正常的服务不会中断,保证地址变换对用户的透明。通过前面的分析可知,网络欺骗系统的部署,使得攻击者在DMZ的服务器上探测到地址不断变化的内网拓扑,而内网中的主机通过DMZ服务器的真实IP地址访问服务。并且因为IP地址随机化只改变虚拟IP地址,真实IP地址始终不变,所以内网中的主机始终可以通过DMZ服务器的真实IP地址访问它。然而,IP地址随机化改变了内网主机的虚拟IP地址,主机向服务器发送的请求无法收到回复,主机需要重新对服务器发起连接,这带来了网络延迟。连接维持模块通过在流表中设定空闲存活时间字段 $idel\_timeout$ 来确保正常的服务不会中断。 $idel\_timeout$ 正比于IP地址随机化周期 T ,即 $idel\_timeout=\alpha T$,其中 $0<\alpha<1$ 。只要两个节点的交互间隔时间小于空闲存活时间,流表就不会消失,两个节点之间的连接就可以维持。空闲存活时间的大小影响网络安全性和网络性能。算法2给出了IP地址随机化模块的地址分配算法实现。首先确定变换的周期 T ,网络中的子网,每个子网中的主机和诱饵节点,每个子网中未使用的IP地址。每次变换时,针对每个子网中的每个节点,从子网

内未使用的IP地址中随机选择一个作为节点的虚拟IP地址,并更新虚拟网络拓扑的信息。地址分配算法的时间复杂度在于需要变换虚拟网络拓扑中每一个节点的IP地址,因此时间复杂度为 n 。

算法2　IP地址随机化模块地址分配算法

输入:变换周期 T,子网信息 *subnetlist*,每个子网内的节点信息 *hostdict* ,子网内还未使用的IP地址 *ipdict*

输出: *ipdict* , *hostdict* ,虚拟网络拓扑 *vnt*

```
if time=T do
  for net in subnetlist do
    for host in hostdict[net] do
      ip=net+random(start,end)
      if ip in ipdict do
        host.vIP=ip
        update ipdict
        update hostdict
        update vnt
      end if
    end for
  end for
end if
```

IP随机化模块可以与虚拟网络拓扑模块有机结合,不会相互抵触、相互牵制,而是相互协调。IP随机化模块利用虚拟网络拓扑模块生成的虚拟网络拓扑规范完成节点IP地址的实时统计和变换,并将变换后的信息反馈到虚拟网络拓扑模块。从防御效能上看,现有研究中虚拟网络拓扑存在静态性,APT攻击者可以长期潜伏在网络中寻找攻击目标,同时识别诱饵节点并且其拉入黑名单,因此随着攻击者不断探测,虚拟网络拓扑的防御效能会逐渐降低。本文提出的防御方法通过IP地址随机化变换网络中节点的IP地址,使得攻击者在一段时间内探测到的信息失效,攻击者只能重新开始探测,从而提高了节点的存活率。现有研究中,IP地址随机化需要频繁的变换,这对系统性能带来巨大的损耗。本文提出的防御方法,通过部署比真实网络大得多的虚拟网络拓扑,能够延长攻击者探测到真实主机的时间,因此不需要频繁地变换就可以达到较好的防御效果。

3.3　欺骗服务器

欺骗服务器负责根据虚拟网络视图的规范制作响应来欺骗恶意扫描程序。包括地址管理模块、消息处理模块、DHCP处理模块、ARP处理模块、ICMP处理模块、路由模拟模块。

地址管理模块负责确保与SDN控制器维护相同的虚拟网络拓扑规范。

消息处理模块负责解析接收到的数据包,并根据数据包的类型发往相应的模块处理。

DHCP处理模块、ARP处理模块、ICMP处理模块和路由模拟模块负责对恶意扫描程序的请求做出欺骗性的响应。以路由模拟模块为例介绍它们是实现欺骗的。

步骤1　恶意扫描程序使用tarceroute向节点发送探测数据包,依次将数据包的TTL设置为1,2,…。

步骤2　虚拟网络拓扑模块将数据包转发到欺骗服务器,并由消息处理子模块发往路由模拟子模块处理。

步骤3　虚拟网络拓扑规范中描述了网络中两个主机之间的虚拟的路由信息,路由模拟模块首先根据虚拟路由信息向源主机发送ICMP超时报文,证明数据包经过了虚拟路由。

步骤4　路由模拟模块根据目的主机的虚拟IP生成ICMP端口不可达报文,证明数据包已到达目的地。

通过上述过程,路由模拟模块可以基于虚拟网络拓扑的规范模拟两个节点之间的多跳路径,使得攻击者无法获取节点在网络中的真实位置。

3.4　系统可扩展性

SDN已经在许多著名的科研项目中得到应用和部署,谷歌的数据中心B4[25]是SDN应用在大规模网络中的成功案例,通过在数据中心部署基于OpenFlow的集中式流量工程服务,使得网络更稳定,链路带宽利用率更高。面对更为庞大的流量请求和网络监控统计等需求,分布式的多控制器部署成为提升控制平面规模可扩展的有效方式[26-27]。因此通过分布式控制平面的方式部署,可以实现更大规模的IP地址随机化。网络欺骗系统的分布式控制平面部署模型如图3所示,包括SDN主控制器和SDN子控制器。SDN主控制器负责模拟虚拟网络拓扑和管理分布式控制平面。SDN子控制器负责控制子网中的网络流量,每个子控制器对本地交换设备的控制不需要向其他控制器通告。当IP地址随机化时间发生时,SDN主控制器将虚拟网络拓扑的变化发往各个子控制器,各子控制器进行同步更新。因此,所有控制器都能实时掌握全局网络信息,但实际上只是负责局部区域网络。

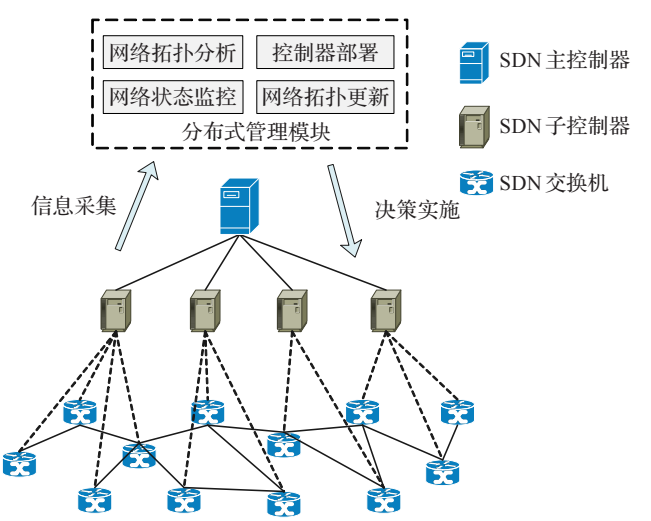

图3　分布式控制平面部署模型

Fig.3　Distributed control plane deployment model

4　实验评估与分析

本章将评估MTD增强的网络欺骗系统的有效性及其产生的开销。实验评估在Ubuntu20.04.1操作系统环境下进行，虚拟机内存为4 GB，使用mininet[28]搭建基于SDN的网络系统，SDN控制器使用POX控制器，交换机使用Open Vswitch。实验部署了无防御(NO VNT)、虚拟网络拓扑(VNT)、IP地址随机化(IPR)、动态虚拟网络拓扑(DVNT)四种防御方法，通过对比实验分析本文提出的防御方法的有效性。

真实网络拓扑如所图4所示，红色节点为已经被攻击者占领的主机、蓝色节点为6个普通客户端，灰色节点为蜜罐，绿色节点为SDN交换机。网段地址为192.168.0.0/24，网络中的6个普通客户端和蜜罐均存在可利用的漏洞。

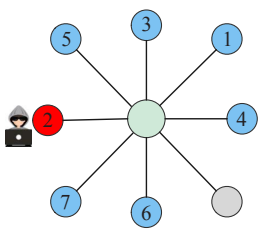

图4　真实网络拓扑

Fig.4　Real network topology

虚拟网络拓扑的参数如表1所示，虚拟网络拓扑包含3个子网，网段地址分别为192.168.10.0/24、192.168.11.0/24、192.168.12.0/24，真实脆弱性主机平均分布在地址空间上，子网中的诱饵节点数分别为17、18、16。

表1　虚拟网络拓扑参数

Table 1　Parameters of virtual network topology

参数名称	参数值
子网数	3
每个子网中的真实主机数	2(192.168.10.0/24) 2(192.168.11.0/24) 2(192.168.12.0/24)
每个子网中的诱饵节点数	17(192.168.10.0/24) 18(192.168.11.0/24) 16(192.168.12.0/24)

部署的虚拟网络拓扑如图5所示，红色节点为已经被攻击者占领的主机，蓝色节点为普通客户端，即真实脆弱性主机，灰色节点为蜜罐，黄色节点为虚拟路由。虚拟网络拓扑的结构与真实网络拓扑完全不同，可以最大程度地欺骗攻击者。

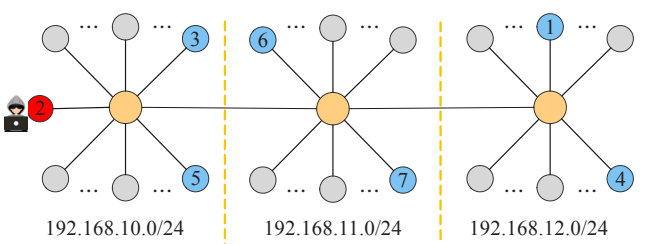

图5　虚拟网络拓扑

Fig.5　Virtual network topology

IP地址随机化参数如表2所示，IPR的地址变换周期为30 s。为了分析地址变换周期对防御有效性和系统开销的影响，实验部署了两种IP地址随机化增强的虚拟网络拓扑，分别为地址变换周期为30 s的动态虚拟网络拓扑(DVNT_30)和地址变换周期为10 s的动态虚拟网络拓扑(DVNT_10)，地址变换方式均为随机变换，即每个周期都在未使用的IP地址集内随机选择一个分配给主机。

表2　IP地址随机化参数

Table 2　Parameters of IP address randomization

类型	参数名称	参数值
IPR	变换周期/s	30
	变换方式	random
DVNT_30	变换周期/s	30
	变换方式	random
DVNT_10	变换周期/s	10
	变换方式	random

4.1　有效性

首先评估部署虚拟网络拓扑对于延长攻击者发现真实脆弱性主机的时间的有效性。攻击者进行内网渗透时通常首先使用扫描器(如Nmap、Metasploit等)对内网进行探测，获取网络中存活性主机、网络结构等信息，为下一步攻击做准备。实验模拟攻击者使用Nmap探测网络中的存活性主机，扫描方式为随机扫描，且IP地址为平均分布，即每个IP地址只扫描一次。在模拟攻击者扫描探测的同时，记录攻击者探测到真实脆弱性主机的时间，最后通过统计攻击者探测到的真实脆弱性主机的时间来评估系统的有效性。为保证实验结果的可靠性，共进行了100次重复实验。

表3为在没有部署虚拟网络拓扑(NO VNT)和部署了虚拟网络拓扑(VNT)的网络下，攻击者扫描出真实脆弱性主机所花费的时间对比。在100次重复实验中，攻击者在这两种情况下，攻击者发现真实脆弱性主机的最短时间相同，但最长时间和平均时间VNT均为NO VNT的7倍以上。

表3　不同网络下攻击者发现真实脆弱性主机的时间

Table 3　Time of attacker discovering real vulnerable host under different networks

s

网络	最小时间	最大时间	平均时间
NO VNT	15	155	44
VNT	15	1 102	341

图6为NO VNT和VNT的网络下，攻击者扫描出真实脆弱性主机的概率随时间的变化。分析实验结果，在NO VNT的网络下，攻击者扫描40 s时，发现真实脆

弱性主机的概率为52%,而在VNT的网络下,攻击者发现真实脆弱性主机的概率仅为8%;在NO VNT的网络下,攻击者有100%的概率发现真实脆弱性主机的时间为320 s,而在VNT的网络下,则需要1 280 s。

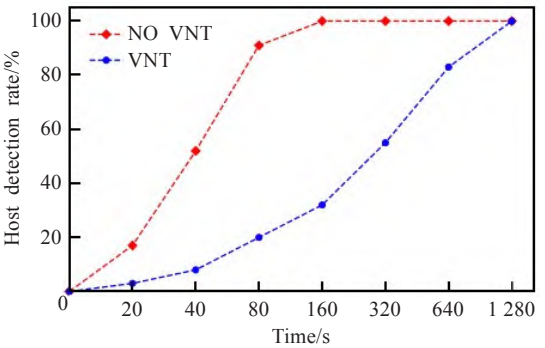

图6　不同网络下攻击者发现真实脆弱性主机的概率

Fig.6　Probability of attacker discovering realvulnerable host under different networks

通过部署虚拟网络拓扑,大大延长了攻击者发现脆弱性主机的时间,提高了攻击者的时间成本。但只要时间充足,APT攻击者仍然可以攻下网络中的所有主机。IP地址随机化可以使攻击者在一段时间内探测到的信息失效,因此在虚拟网络拓扑的基础上融合IP地址随机化技术,同时评估在部署NO VNT、VNT、IPR和DVNT_30的网络下,攻击者成功攻击主机的个数随时间变化。假设攻击者具有丰富的攻击资源,对网络中主机的每一个漏洞都有利用工具,且攻击者具有很强的漏洞分析能力,发现漏洞后能在较短的时间内成功利用。实验模拟攻击者首先使用Nmap探测网络中的存活性主机,当攻击者探测到真实脆弱性主机时,经过一段时间的攻击准备,向其发起攻击。与此同时,记录攻击者成功攻击真实脆弱性主机的时间,最后通过统计攻击者成功攻击真实脆弱性主机的时间来评估系统的有效性。为了贴近真实渗透场景,假设攻击者探测到脆弱性主机到发起攻击的时间为10~60 s内的一个随机时间,地址变换的周期为30 s。

图7为攻击者在部署了上述四种防御方法的网络下,攻击者成功攻击真实脆弱性主机的个数随时间的变化。对比实验结果,相比于NO VNT,VNT将攻击者成功攻击一个脆弱性主机的时间平均延长至8倍,这是因为虚拟网络拓扑中存在大量诱饵节点,攻击者分析利用诱饵节点的漏洞浪费了更多的时间;相比于NO VNT,IPR将攻击者成功攻击脆弱性主机的概率降低了33%,这是因为当攻击者对脆弱性主机的漏洞进行利用时,其IP地址很可能已经过时;相比于VNT和IPR,DVNT_30不仅进一步延长了攻击者成功攻击真实脆弱性主机的时间,而且将攻击者成功攻击的概率降低83%。

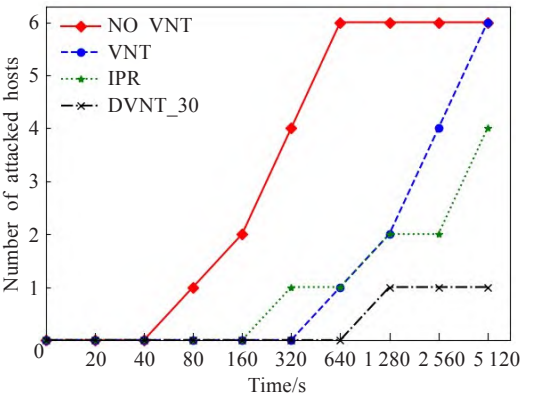

图7　不同网络下主机被成功攻击的个数

Fig.7　Number of hosts successfully attacked under different networks

4.2　系统开销

MTD增强的网络欺骗系统极大地提高了网络的安全性,但也难免对网络性能造成一定影响,因此需要对系统开销进行评估分析。使用Netperf来测量系统对网络吞吐量和网络延迟的影响,比较4种不同系统配置下的性能:NO VNT、VNT、DVNT_30和DVNT_10。

评估系统对网络吞吐量的影响。在目标主机上运行Netperf服务端,在客户机上运行Netperf客户端,使用TCP_STREAM模拟客户端向服务端的批量数据传输,测量网络吞吐量,进行了10次重复实验,每次实验进行8组测试,每组数据大小由8 Byte到1 024 Byte不等。

图8为四种不同网络下系统吞吐量的对比,分析实验结果,与没有部署虚拟网络拓扑的网络情况对比,部署了虚拟网络拓扑的网络吞吐量减少了2.2%到11.5%,平均减少了5%;部署了地址变换周期为30 s的动态虚拟网络拓扑的网络吞吐量减少了2.4%到14.1%,平均减少了7.1%;部署了地址变换周期为10 s的动态虚拟网络拓扑的网络吞吐量减少了3.3%到15.9%,平均减少了8.2%。

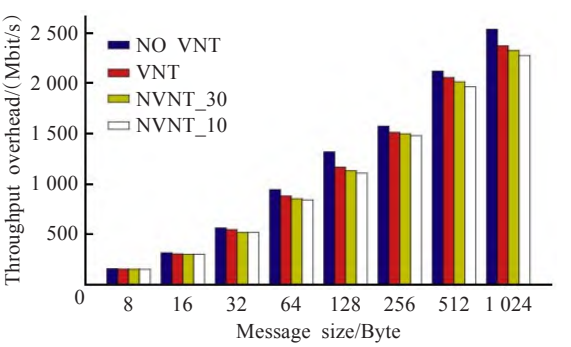

图8　不同网络下的网络吞吐量

Fig.8　Network throughput under different networks

评估系统对网络延迟的影响。在目标主机上运行Netperf服务端,在客户机上运行Netperf客户端,使用TCP_RR模拟客户端和服务端request/response模式,客户端向服务端发出查询分组,服务端接收到请求返回结果数据,测量网络延迟,数据大小由8 KB到1 024 KB不

等，进行了10组重复实验。

图9为四种不同网络下系统吞吐量的对比，分析实验结果，部署了虚拟网络拓扑的网络延迟增加了2.2%到10.4%，平均增加了5.4%；部署了地址变换周期为30 s的动态虚拟网络拓扑的网络延迟增加了3%到12.3%，平均增加了6.6%；部署了地址变换周期为10 s的动态虚拟网络拓扑的网络延迟增加了3.5%到12.8%，平均增加了7.4%。

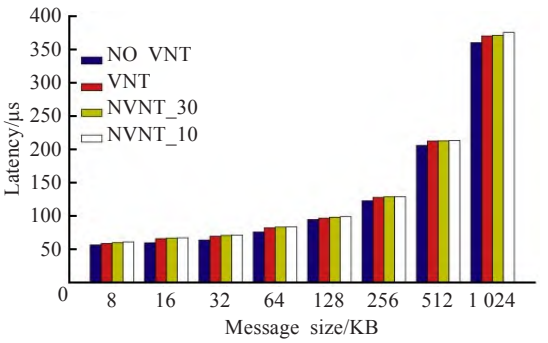

图9　不同网络下的网络延迟

Fig.9　Network delay under different networks

由实验结果可以看出，造成额外系统开销的最大的原因在于虚拟网络拓扑，因为每个数据包到达交换机都需要重写数据包头。变换造成的系统开销时因为每次地址变换后，原来的虚拟地址对应的流表会消失，在新的数据包到达交换机时，需要重新安装新的流表。额外的时间开销为SDN控制器根据虚拟网络拓扑描述执行查找操作的时间以及安装流表的时间。同时在一定时间内，地址变换的频率越高，重新安装流表的次数越多，造成的额外时间开销也就越大。分析实验结果可以发现，地址变换造成的额外开销较小，这是因为IP随机化地址是在虚拟网络拓扑的基础上实现的，系统的额外开销要小于单独使用虚拟网络拓扑和IP随机化造成的系统开销的总和。

4.3　基于网络杀伤链模型的有效性评估

洛克希德-马丁公司提出网络杀伤链来描述网络入侵活动。该模型将网络入侵分为七个阶段，分别为侦查、武器化、投送、漏洞利用、安装、命令与控制、控守目标，越早打断网络杀伤链就能越有效地阻止网络攻击。本节根据一个网络攻击实例，使用网络杀伤链模型来分析MTD增强的网络欺骗防御系统的有效性。攻击者已经获取DMZ中某台服务器的管理员权限，并以此为跳板探测内网，并进行横向渗透，目的为获取内网中数据库服务器中的数据资源。

在侦查和武器化阶段，攻击者需要识别和确定目标，并根据目标的环境信息决定采取的方法。本系统在此阶段通过创建虚拟网络拓扑延长攻击者的侦查时间，并通过诱饵节点提供虚假服务，误导攻击者武器的研制以挫败攻击。

在投送、漏洞利用和安装阶段，攻击者要将生成的攻击代码发送到目标主机并运行以建立初步的立足点。本系统在此阶段通过IP随机化技术改变目标主机的IP地址，使得攻击代码被投送到错误的目标。

在命令控制和控守目标阶段，攻击者控制系统以作为跳板进一步渗透或获取系统上的资源。本系统在此阶段通过诱饵节点使得攻击者获取欺骗性数据资源或通过IP随机化技术破坏攻击者与目标主机的连接。

5　结束语

本文提出一个MTD增强的网络欺骗系统来防御内网侦查。针对的目标为利用门户网站的漏洞已入侵目标网络中一个主机并进行内网横向渗透的攻击者。系统的防御方法为对其显示一个与真实网络完全不同的虚拟网络拓扑，混淆攻击者通过探测获取的目标网络信息，从而增加攻击者探测到真实脆弱性主机的时间，同时动态变换虚拟网络拓扑中节点的IP地址，使攻击者在一段时间内获取的信息失效，降低攻击者攻击成功的概率。最后基于Mininet和POX控制器实现网络欺骗原型系统，并通过对比实验对系统进行评估。评估实验结果表明，该系统能够有效地防御网络侦查攻击，同时具有可接受的系统性能开销。

参考文献：

[1] 徐焱，贾晓璐.内网安全攻防：渗透测试实战指南[J].中国信息化，2020，310(2)：99.
XU Y，JIA X L.Intranet security attack and defense：a practical guide to penetration testing[J].China Information Technology，2020，310(2)：99.

[2] PING C，DESMET L，HUYGENS C.A study on advanced persistent threats[C]//IFIP International Conference on Communications and Multimedia Security.Berlin Heidelberg：Springer，2014.

[3] BOWERS K，VAN DIJK M，GRIFFIN R，et al.Defending against the unknown enemy：applying flipit to system security[C]//Proceedings of the 3rd Conference on the Decision and Game Theory for Security(GameSec)，2012：248-263.

[4] WANG C，LU Z.Cyber deception：overview and the road ahead[J].IEEE Security & Privacy，2018，16(2)：80-85.

[5] 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.
JIA Z P，FANG B X，LIU C G，et al.Survey on cyber deception[J].Journal on Communications，2017，38(12)：128-143.

[6] UITTO J，RAUTI S，LAURÉN S，et al.A survey on anti-honeypot and anti-introspection methods[C]//World Conference on Information Systems & Technologies，2017.

[7] JAJODIA S,GHOSH A K,SWARUP V,et al.Moving target defense[M].New York:Springer,2011:23-35.
[8] XU J,GUO P,ZHAO M,et al.Comparing different moving target defense techniques[C]//Proceedings of ACM Workshop on Moving Target Defense,2014:97-107.
[9] AL-SHAER E.Toward network configuration randomization for moving target defense[M]//Moving target defense.[S.l.]:Springer,2011:153-159.
[10] FEAMSTER N,REXFORD J,ZEGURA E.The road to SDN:an intellectual history of programmable networks[J].Computer Communication Review:A Quarterly Publication of the Special Interest Group on Data Communication,2014(2):87-98.
[11] AKIYAMA M,YAGI T,HARIU T,et al.Honey circulator:distributing credential honeytoken for introspection of web-based attack cycle[J].International Journal of Information Security,2018,17:135-151.
[12] ACHLEITNER S,PORTA T L,MCDANIEL P,et al.Cyber deception:virtual networks to defend insider reconnaissance[C]//2016 International Workshop,2016.
[13] ZHAN S,YAN G.Ensuring deception consistency for FTP services hardened against advanced persistent threats[C]//The 5th ACM Workshop,2018.
[14] RRUSHI J L.NIC displays to thwart malware attacks mounted from within the OS[J].Computers & Security,2016,61:59-71.
[15] RUBIO-MEDRANO C E,DOUP A,YAN S,et al.HoneyPLC:a next-generation honeypot for industrial control systems[C]//2020 ACM SIGSAC Conference on Computer and Communications Security,2020.
[16] ZHE L,YIN X,REN T A N,et al.SDN virtual honeynet for network attack information acquisition[J].DEStech Transactions on Computer Science and Engineering,2017,2:123-125.
[17] KONG T,WANG L,MA D,et al.Automated honeynet deployment strategy for active defense in container-based cloud[C]//2020 IEEE 22nd International Conference on High Performance Computing and Communications;IEEE 18th International Conference on Smart City;IEEE 6th International Conference on Data Science and Systems(HPCC/SmartCity/DSS),2020.
[18] NIAKANLAHIJI A,JAFARIAN J H,CHU B T,et al.HoneyBug:personalized cyber deception for Web applications[C]//Hawaii International Conference on System Sciences 2020(HICSS 53),2020.
[19] SENGUPTA S,CHOWDHARY A,SABUR A,et al.A survey of moving target defenses for network security[J].IEEE Communications Surveys & Tutorials,2019,22(3):1909-1941.
[20] YANG Y,CHENG L.An SDN-based MTD model[J].Concurrency and Computation:Practice and Experience,2018,31.
[21] LIU Z,HE Y,WANG W,et al.AEH-MTD:adaptive moving target defense scheme for SDN[C]//2019 IEEE International Conference on Smart Internet of Things(SmartIoT),2019.
[22] NARANTUYA J,YOON S,LIM H,et al.SDN-based IP shuffling moving target defense with multiple SDN controllers[C]//2019 49th Annual IEEE/IFIP International Conference on Dependable Systems and Networks-Supplemental Volume(DSN-S),2019.
[23] WANG P,ZHOU M,DING Z.A two-layer IP hopping-based moving target defense approach to enhancing the security of mobile ad-hoc networks[J].Sensors,2021,21(7):2355.
[24] DADHEECH K,CHOUDHARY A,BHATIA G.De-militarized zone:a next level to network security[C]//2018 Second International Conference on Inventive Communication and Computational Technologies(ICICCT),2018:595-600.
[25] JAIN S,KUMAR A,MANDAL S,et al.B4:experience with a globally-deployed software defined WAN[C]//Computer Communication Review,2013:3-14.
[26] DAS T,GURUSAMY M.Controller placement for resilient network state synchronization in multi-controller SDN[J].IEEE Communications Letters,2020,24(6):1299-1303.
[27] TZENG Y Y,SHEN C A.An integrated multi-controller management framework for highly reliable software defined networking[J].Telecommunication Systems,2021,77:377-388.
[28] OLIVEIRA R,SCHWEITZER C M,SHINODA A A,et al.Using mininet for emulation and prototyping software-defined networks[C]//Communications & Computing,2014.