计算机科学
COMPUTER SCIENCE

MTDCD:一种对抗网络入侵的混合防御机制

高春刚，王永杰，熊鑫立

引用本文

高春刚，王永杰，熊鑫立. MTDCD:一种对抗网络入侵的混合防御机制[J]. 计算机科学, 2022, 49(7): 324-331.

GAO Chun-gang, WANG Yong-jie, XIONG Xin-li. MTDCD:A Hybrid Defense Mechanism Against Network Intrusion [J]. Computer Science, 2022, 49(7): 324-331.

计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.210600193

MTDCD:一种对抗网络入侵的混合防御机制

高春刚　王永杰　熊鑫立
国防科技大学电子对抗学院　合肥 230037
安徽省网络安全态势感知与评估重点实验室　合肥 230037
(gangchungaog9432@nudt.edu.cn)

摘　要　移动目标防御和网络欺骗防御均是通过增加攻击者获取的信息的不确定性来保护己方系统和网络,该方法能够在一定程度上减缓网络入侵。然而,单一的移动目标防御技术无法阻止利用多元信息进行网络入侵的攻击者,同时,部署的诱饵节点可能会被攻击者识别和标记,降低了防御效能。因此,提出了融合移动目标防御和网络欺骗防御的混合防御机制 MTDCD,并通过深入分析实际网络对抗,构建了网络入侵威胁模型,最后基于 Urn 模型建立了防御有效性评估模型,并从虚拟网络拓扑大小、诱饵节点的欺骗概率、IP 地址随机化周期、IP 地址转移概率等多个方面评估了所提混合防御机制 MTDCD 的防御效能,为后续防御策略设计提供了一定的参考和指导。

关键词:移动目标防御;网络欺骗防御;网络入侵;有效性评估
中图法分类号　TP309

MTDCD:A Hybrid Defense Mechanism Against Network Intrusion

GAO Chun-gang,WANG Yong-jie and XIONG Xin-li
College of Electronic Engineering,National University of Defense Technology,Hefei 230037,China
Anhui Key Laboratory of Cyberspace Security Situation Awareness and Evaluation,Hefei 230037,China

Abstract　Both moving target defense and cyber deception defense protect their own systems and networks by increasing the uncertainty of information acquired by attackers. They can slow down network reconnaissance attacks to a certain extent. However, a single moving target defense technology cannot prevent attackers who use multiple information to conduct network intrusions. Meanwhile, the deployed decoy node may be identified and marked by the attacker, thereby reducing the defense effectiveness. Therefore, this paper proposes a hybrid defense mechanism combining moving target defense and cyber deception defens. Through in-depth analysis of actual network confrontation, a network intrusion threat model is constructed. Finally, a defense effectiveness evaluation model based on the Urn model is built. In addition, this paper evaluates the defense performance of the proposed hybrid defense method from multiple aspects such as virtual network topology size, deception probability of decoy nodes, IP address randomization period, IP address transfer probability, etc., and provides reference and guidance for subsequent defense strategy design.

Keywords　Moving target defense, Cyber deception defense, Network intrusion, Effectiveness assessment

1　引言

攻击者在发动网络入侵之前通常需要进行网络侦查,以收集目标网络的信息,包括 IP 地址、开放端口、操作系统和协议等。然而,传统的网络防御技术大多通过入侵检测、防火墙等技术来保护网络及系统安全,这些技术都是静态化的,高级持续性威胁(Advanced Persistent Threat,APT)[1]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测试,直到达到最终目标[2]。

为了阻止或减缓网络入侵,学术界和安全人员开始将目光聚焦于主动防御方法。移动目标防御(Moving Target Defense,MTD)[3]作为"改变游戏规则"的革命性技术之一被提出。MTD 的思想是使系统动态化,通过增加系统的多样性、动态性和随机性来增加攻击者的攻击难度和攻击成本,从而提高系统的安全性[4]。IP 地址[5]、端口[6-7]、运行平台[8-9]、内存布局[10]等诸多网络要素被用来实施具体的 MTD 技术。网络欺骗防御(Cyber Deception Defense,CDD)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[11]。防御者通过部署虚假节点[12]、模拟虚假的操作系统指纹[13]以及伪造虚假的数据[14]等,使攻击者探测到错误信息,致使攻击失败。

然而,移动目标防御和网络欺骗防御都存在各自的不足。单一的 MTD 技术能够在一定程度上抵御简单的攻击,但

到稿日期:2021-06-28　返修日期:2021-12-15
通信作者:王永杰(wangyongjie17@nudt.edu.cn)

APT 攻击者通常会综合分析网络中的多元信息（如 IP 地址、端口、操作系统信息、潜在漏洞等），以识别和追踪主机，因此单一参数的变化无法有效抵御 APT 攻击。为解决此问题，研究人员综合多个参数进行多重跳变来提高防御效能[15]，但多个参数的变换往往会相互干扰，影响系统正常运行。网络欺骗防御通过设置陷阱，来误导攻击者攻击错误的目标，但熟练的攻击者能够通过分析指纹信息、网络差异等来区分真实主机和诱饵，并将诱饵节点加入黑名单，导致诱饵节点失去欺骗效果[16]。

为弥补移动目标防御和网络欺骗防御的缺点，一些学者提出结合移动目标防御和网络欺骗防御的混合防御方法，Sun 等[17]提出在网络中部署诱饵节点，以降低攻击者扫描到真实主机的概率，并利用 IP 地址随机化技术动态改变真实主机和诱饵节点的 IP 地址，提高诱饵节点的生存率。Xing 等[18]和 Zhao 等[19]提出了一种自适应欺骗防御机制，该机制通过预测攻击者的行为，自适应地调整欺骗视图。但上述研究并没有考虑两种防御技术相互干扰的情况，IP 地址随机化在一定程度上降低了诱饵节点的欺骗效果。因此，若要充分发挥两种技术的优势，不能只是将这两种技术简单叠加，而需要制定合理的策略，实现两种技术的有机融合。

为验证防御方法的有效性，需要对其防御效能进行评估。按照评估所采用的模型和方法，可以将现有的主动防御效能评估模型分为 3 类，包括基于仿真模拟的评估、基于实验实例的评估和基于数学模型的评估。Prakash 等[20]通过仿真程序建立了一个抽象网络攻防场景，Eeuwen 等[21]建立了基于软件定义网络和虚拟化的系统级实验测试环境。基于仿真模拟和实验实例的评估方法虽然具有较高的可信度，但其依赖环境特征，准确性和通用性较差，且进行评估需要具体的技术实现代码或仿真代码，可在防御方法部署后进行评估分析使用，但对于防御技术部署前的效能分析来说成本太高。

基于数学模型的评估方法利用概率模型、博弈论、随机过程模型以及图模型等数学工具对不同的网络防御技术进行效能评估。Carroll 等[22]和 Crouse 等[23]提出了基于 Urn 模型的防御有效性评估模型，该模型分析了基于蜜罐的防御和基于移动目标防御的防御性能，并对每一种防御的参数进行了定量分析。Xiong 等[24]提出了基于球入箱模型和生成函数的有效性评估模型，该模型对多种移动目标防御策略进行了有效性评估。但上述研究仅针对攻击者扫描探测阶段进行了有效性评估，无法真实地反映防御方法针对网络入侵整个过程的防御有效性。

基于上述分析，为有效抵抗网络入侵，本文提出了一种融合移动目标防御和网络欺骗防御的混合防御机制 MTDCD（MTD Enhanced Defense of Cyber Deception），并基于 Urn 模型评估了 MTDCD 应对网络入侵的防御有效性。首先，针对移动目标防御和网络欺骗防御同时使用时存在相互干扰的问题，提出了 MTDCD 防御方法，实现了 IP 地址随机化和虚拟网络拓扑的有机融合；其次，通过深入分析网络入侵的行为特征来构建威胁模型，真实反映网络入侵的整个过程；最后，形式化定义网络攻防过程，并引入 Urn 模型，根据虚拟网络拓扑大小、诱饵节点的欺骗概率、IP 地址随机化周期、IP 地址转移概率等多个参数量化评估 MTDCD 的防御有效性，并研究如何提高其防御效能，为后续防御策略设计提供一定的参考和指导。

2 MTDCD 防御模型

为抵抗攻击者对目标网络的网络入侵，系统首先将网络内主机的真实 IP 地址转换为虚拟 IP 地址并生成大量的诱饵节点，使攻击者探测到的目标网络为与真实网络完全不同的虚拟网络拓扑，从而混淆攻击者获取的信息。图 1 为由真实网络拓扑生成虚拟网络拓扑的示意图，其中 h_0 为攻击者在外网占领的主机，h_1，h_2，…，h_6 为内网中的真实主机，b 为蜜罐。构造的虚拟网络拓扑比真实的网络规模大了很多，目的是延长攻击者发现真实主机的时间。在生成的虚拟网络拓扑中，真实主机分布在各个子网，诱饵节点由蜜罐映射生成，一个蜜罐可以映射生成多个诱饵节点。

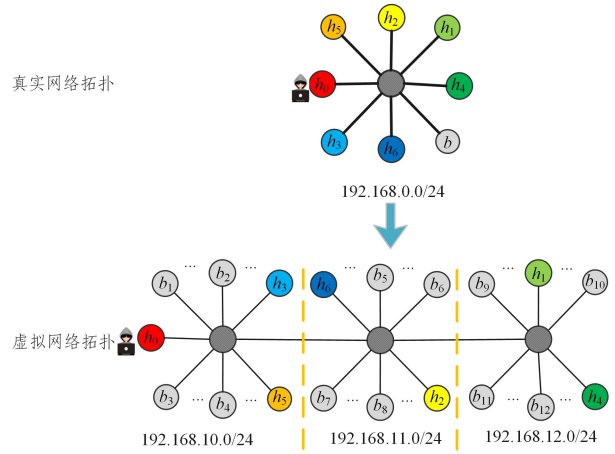

图 1 虚拟网络拓扑生成示意图

Fig. 1 Schematic diagram of virtual network topology generation

攻击者通过分析网络中主机的指纹信息（包括 IP 地址、端口、操作系统信息、潜在漏洞等）来识别和追踪主机。对于网络中的每一个真实主机，存在与其指纹相似的诱饵节点。攻击者有一定的概率识别出诱饵节点，这与攻击者的能力和诱饵节点的真实度有关。如果攻击者识别出诱饵节点，则将其拉入黑名单，在接下来的扫描探测中不再访问；如果没有识别出诱饵节点，则将其当作真实主机发起攻击。这是因为，在正常情况下，诱饵节点与其他节点没有交互，所以一旦有节点向其发起连接，就可以判定该节点为不正常主机，切断连接并封禁其 IP，此时攻击失败。然而，攻击者经过长时间的探测和分析，最终可以确定网络中的诱饵节点并绕过，此时诱饵节点失去了防御效果，因此本文在虚拟网络拓扑的基础上融合 IP 地址随机化技术，构建动态虚拟网络拓扑，以获取更好的防御效果。

IP 地址随机化技术通过周期性地变换网络中节点的 IP 地址，使攻击者在一段时间内获取的信息失效。每次 IP 地址随机化事件发生时，在从未使用的 IP 地址池中，随机选择一个 IP 地址替换节点当前的 IP 地址，并将当前的 IP 地址放回未使用的 IP 地址池中。而在网络欺骗场景中，如果只对真实主机进行 IP 地址随机化，攻击者即可根据 IP 地址是否发生

变化来识别真实主机和诱饵节点，从而将诱饵节点拉入黑名单。文献[17]对真实主机和诱饵节点同时实施 IP 地址随机化，使得攻击者无法根据 IP 地址的变化来区分真实主机和诱饵节点，提高了诱饵节点的存活率。然而，对诱饵节点实施 IP 地址随机化，会出现攻击者已经探测到诱饵节点且被诱饵节点欺骗却没有成功命中的情况，降低了诱饵节点的欺骗效果。

针对上述问题，本文提出了 MTDCD 防御模型，将 IP 地址随机化分为 IP 地址变换、IP 地址转移、IP 地址保持 3 种策略，它们的定义如下。

定义 1(IP 地址变换) 在从未使用的 IP 地址池中随机选择一个 IP 地址替换节点当前的 IP 地址，并将当前的 IP 地址放回未使用的 IP 地址池中。

定义 2(IP 地址转移) 在从未使用的 IP 地址池中随机选择一个 IP 地址替换主机当前的 IP 地址，并将当前的 IP 地址转移至与其指纹相似的诱饵节点上。

相比 IP 地址变换，IP 地址转移增加了诱饵节点被攻击的概率。同时，因为诱饵节点和真实主机的指纹相似，当发生 IP 地址转移时，从攻击者的角度来看，真实主机的 IP 地址并没有发生变化。为了确保攻击者无法根据 IP 地址变化规律区分真实主机和诱饵节点，在 IP 地址随机化发生时，需要部分诱饵节点的 IP 地址不发生变化，因此定义了 IP 地址保持策略。

定义 3(IP 地址保持) 当 IP 地址随机化发生时，保持诱饵节点的 IP 地址不变。

相比现有研究，MTDCD 防御模型通过实施 IP 地址转移策略，不仅减轻了 IP 地址随机化对诱饵节点的欺骗效果的干扰，而且进一步增加了攻击者接触到诱饵节点的概率。通过同时实施上述 3 种策略，以确保攻击者无法根据 IP 地址的变化来区分真实主机和诱饵节点。

图 2 给出了在 MTDCD 防御模型中，IP 地址随机化发生前后两个周期的网络系统状态。每个格子代表一个 IP 地址，其中 h_1，h_2 和 h_3 为真实主机，b_1，b_2 和 b_3 分别为与 h_1，h_2 和 h_3 指纹相似的诱饵节点，其余为未使用的 IP 地址，系统周期性地执行 IP 地址随机化，图中节点所处位置的变化代表节点 IP 地址的变化。在 T_2 周期内，主机 h_1，h_2 和 h_3 的 IP 地址变换为 T_1 周期内未使用的 IP 地址，主机 h_1 的 IP 地址转移至诱饵节点 b_1，诱饵节点 b_2 的 IP 地址未发生变换，诱饵节点 b_3 的 IP 地址变换为 T_1 周期未使用的 IP 地址。

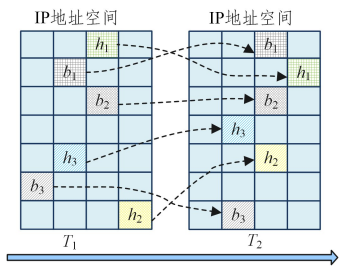

图 2 MTDCD 防御模型示意图

Fig. 2 Schematic diagram of MTDCD defense model

3 网络入侵威胁模型

攻击者进行网络入侵的目的通常为窃取或破坏目标网络的重要资产，但攻击者在外部网络很难直接攻击目标网络中存储有重要资产的主机，攻击者首先需要在目标网络中建立立足点，即在内网中占领至少一台主机，从而为后续的攻击奠定基础。因此，本文构建的威胁模型为针对在目标网络中建立立足点的网络入侵行为。

洛克希德-马丁公司提出了网络杀伤链(Cyber Kill Chain)模型[25]，该模型用于描述针对性的多阶段攻击，如图 3 所示，分别为扫描侦查、武器构建、载荷投递、漏洞利用、安装植入、命令与控制以及目标达成。

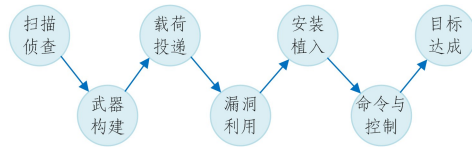

图 3 网络杀伤链

Fig. 3 Cyber kill chain

攻击者建立立足点可以分为 3 个阶段：扫描探测、攻击准备和攻击实施，分别对应网络杀伤链的扫描侦查、武器构建以及载荷投递和漏洞利用。在扫描探测阶段，攻击者对目标网络进行若干次扫描，以获取活跃主机、开放端口、操作系统指纹、漏洞等信息；在攻击准备阶段，攻击者对获取的目标网络信息进行分析，并构建对应的网络攻击武器；攻击者完成攻击准备后，会对网络中的脆弱性主机实施攻击。相比前两个阶段，攻击实施阶段的时间非常短，可以忽略不计，因此建立立足点的时间包括攻击准备时间和扫描探测时间。通常攻击者使用自动化工具进行扫描探测，因此扫描探测阶段和攻击准备阶段可以同时进行。

基于以上分析，本文对威胁模型提出了几点假设：

(1)假设攻击者知道网络中存在诱饵节点，且具有一定的诱饵节点识别能力；

(2)攻击者已知目标网络的 IP 地址范围，但 IP 地址是随机分配给所有节点的，攻击者仅凭 IP 地址无法区分真实主机和诱饵节点；

(3)攻击者的目标是追踪定位至少一台真实主机，并将其作为进一步入侵的立足点，在此过程中检测并绕过诱饵节点；

(4)攻击者联合多元网络信息(如开放端口、运行服务、操作系统信息、漏洞等)追踪定位网络中的节点，这些信息构成了节点的指纹；

(5)攻击者具有很强的漏洞分析和利用能力，对探测到的每一个节点都能研制出攻击武器；

(6)由于快速扫描容易被检测到[26]，因此攻击者的扫描探测具有低速率、隐蔽性和持久性；

(7)攻击者采取隐蔽扫描的方式探测目标网络，在扫描探测阶段，诱饵节点难以感知到攻击者，而在攻击实施阶段，攻击者有明显的攻击行为，诱饵节点很容易检测到攻击者。

攻击者建立立足点的过程如图 4 所示。攻击者在扫描探测阶段对目标网络进行若干次探测，每次随机探测一个 IP

地址。攻击者探测到活跃节点后，首先会分析该节点是否为诱饵节点，若攻击者判断该节点为诱饵节点，则将其 IP 地址加入黑名单；若攻击者判断该节点为真实主机，则会进行攻击准备，包括漏洞分析和武器制作。如果攻击者在节点 IP 地址发生变换之前实施攻击，则可以成功命中，攻击结束，否则重新进行扫描探测。

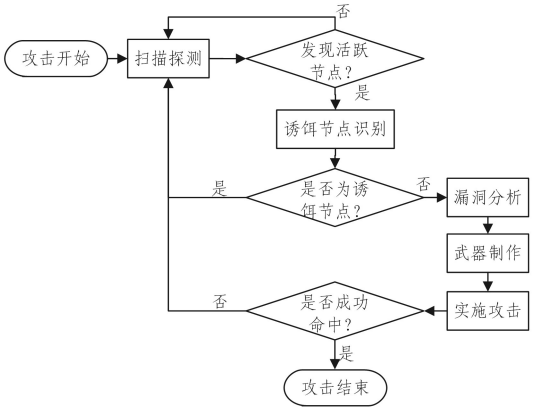

图 4 立足点建立过程

Fig. 4 Foothold building process

4 MTDCD 防御有效性评估模型

为了分析 MTDCD 的有效性，在前两节提出的防御模型和威胁模型的基础上，形式化构建网络攻防场景，分析网络攻防结果，并建立有效性评估概率模型，以此量化评估 MTDCD 的防御有效性。

4.1 网络攻防场景分析

定义 MTDCD 防御场景下的网络攻防模型 $CADM=\{N,\Omega,S,T,R\}$，其中各变量的具体定义如下。

(1) $N=\{N_h,N_b\}$ 为虚拟网络拓扑节点集合，其中 $N_h=\{h_1,h_2,\cdots,h_m\}$ 为真实主机集合，$N_b=\{b_1,b_2,\cdots,b_e\}$ 为诱饵节点集合。对于真实主机 h_i，存在与其指纹相似的诱饵节点 b_j，记作 $b_j \parallel h_i$。

(2) $\Omega=\{\Omega_D,\Omega_A\}$ 为参与者集合，其中 Ω_D 为防御者，即第 2 节定义的防御模型；Ω_A 为攻击者，即第 3 节定义的威胁模型。

(3) $S=\{S_D,S_A\}$ 为攻防策略集合，其中 $S_D=\{S_{D_h^1},S_{D_h^2},S_{D_b^1},S_{D_b^2}\}$ 为防御者策略，根据第 2 节分析可知，$S_{D_h^1}$ 为对真实主机采取 IP 地址变换策略，$S_{D_h^2}$ 为对真实主机采取 IP 地址转移策略，$S_{D_b^1}$ 为对诱饵节点采取 IP 地址变换策略，$S_{D_b^2}$ 为对诱饵节点采取 IP 地址保持策略。$S_A=\{S_{A_\forall^0},S_{A_h^1},S_{A_b^1},S_{A_b^2}\}$ 为攻击者策略，根据第 3 节分析可知，$S_{A_\forall^0}$ 为对任意一个节点进行扫描探测，针对真实主机的攻击策略 $S_{A_h^1}$ 为对真实主机实施攻击，针对诱饵节点的攻击策略 $S_{A_b^1}$ 和 $S_{A_b^2}$ 分别为对诱饵节点实施攻击和绕过诱饵节点。

(4) $T=\{T_\tau,T_s,T_a\}$ 为实施时间集合，其中，T_τ 为 IP 地址随机化周期，T_s 为攻击者扫描探测一个节点的时间，T_a 为攻击者的攻击准备时间。

(5) $R=\{r_0,r_1,r_2\}$ 为网络攻防结果集合，其中，r_0 表示攻击者没有攻击到任何节点，r_1 表示攻击者成功攻击真实主机，r_2 表示攻击者攻击到诱饵节点。

定义攻击者函数为 $f_A(T_s,T_a,S_A)$，防御者函数为 $f_D(T_\tau,S_D)$，MTDCD 防御场景下的网络攻防过程可表示为：

$$N_i\mid_{Z_{t-1}}^{C_{t-1}} \xrightarrow[f_A(T_s,T_a,S_A)]{f_D(T_\tau,S_D)} N_i\mid_{Z_t}^{C_t} \tag{1}$$

其中，$N_i\mid_{Z_t}^{C_t}$ 为节点 N_i 在 t 时刻的状态集合，C_t 和 Z_t 分别为攻击者行为和防御者行为对节点的作用。$C_t=\{C_0,C_1\}$，其中 C_0 表示攻击者对节点不实施攻击，C_1 表示攻击者对节点实施攻击。$Z_t=\{Z_0,Z_1,Z_2\}$，其中 Z_0 表示节点的 IP 地址没有发生变化，Z_1 表示节点发生 IP 地址变换，Z_2 表示节点发生 IP 地址转移。网络攻防结果由攻击者和防御者采取的策略和实施时间共同决定。

针对真实主机的网络攻防过程如式(2)所示：

$$h_i\mid_{Z_{t-1}}^{C_{t-1}} \xrightarrow[f_A(T_s,T_a,S_A)]{f_D(T_\tau,S_D)} h_i\mid_{Z_t}^{C_t} \tag{2}$$

$h_i\mid_{Z_t}^{C_t}=\{h_i\mid_{Z_0}^{C_0},h_i\mid_{Z_1}^{C_0},h_i\mid_{Z_2}^{C_0},h_i\mid_{Z_0}^{C_1},h_i\mid_{Z_1}^{C_1},h_i\mid_{Z_2}^{C_1}\}$ 为主机 h_i 在 t 时刻的状态集合。

分析攻防结果可知，$h_i\mid_{Z_0}^{C_0}$，$h_i\mid_{Z_1}^{C_0}$ 和 $h_i\mid_{Z_2}^{C_0}$ 均为攻击者没有扫描探测到主机 h_i 的情况，因此攻防结果为 r_0；$h_i\mid_{Z_0}^{C_1}$ 为攻击者在 IP 地址随机化之前实施攻击的情况，可以成功攻击到主机 h_i，攻防结果为 r_1；$h_i\mid_{Z_1}^{C_1}$ 为攻击者实施攻击之前主机 h_i 发生了 IP 地址变换的情况，攻击者不能命中主机，攻防结果为 r_0；$h_i\mid_{Z_2}^{C_1}$ 为攻击者实施攻击之前主机 h_i 发生了 IP 地址转移的情况，攻击者命中诱饵节点，攻击失败，攻防结果为 r_2。

针对诱饵节点的网络攻防过程如式(3)所示：

$$b_j\mid_{Z_{t-1}}^{C_{t-1}} \xrightarrow[f_A(T_s,T_a,S_A)]{f_D(T_\tau,S_D)} b_j\mid_{Z_t}^{C_t} \tag{3}$$

$b_j\mid_{Z_t}^{C_t}=\{b_j\mid_{Z_0}^{C_0},b_j\mid_{Z_1}^{C_0},b_j\mid_{Z_0}^{C_1},b_j\mid_{Z_1}^{C_1}\}$ 为诱饵节点 b_j 在 t 时刻的状态集合。

分析攻防结果可知，$b_j\mid_{Z_0}^{C_0}$ 和 $b_j\mid_{Z_1}^{C_0}$ 包括攻击者没有扫描探测到诱饵节点 b_j 或攻击者扫描探测到 b_j 但识别出其为诱饵节点这两种情况，攻防结果为 r_0；$b_j\mid_{Z_0}^{C_1}$ 为攻击者扫描探测到 b_j 且识别出其为诱饵节点的情况，因此攻防结果为 r_2；$b_j\mid_{Z_1}^{C_1}$ 为攻击者向诱饵节点 b_j 实施攻击之前 b_j 的 IP 地址发生变换的情况，因此攻防结果为 r_0，这种情况会降低诱饵节点的欺骗效果。

4.2 防御有效性评估模型

为评估 MTDCD 的防御有效性，本文建立了攻击者成功概率模型，其定义如下。

定义 4(攻击者成功概率) 攻击者在内网中成功建立立足点的概率，即攻击者至少成功攻击内网中一个真实主机的概率。相同条件下，攻击者的攻击成功概率越低，说明系统的防御有效性越好。

用于概率建模的常用工具为 Urn 模型[27]，其已在物理学、通信和计算机科学中得到广泛应用，用于确定一组给定事件的统计分布。本节基于 Urn 模型建立攻击者成功概率模型。

根据以上分析可知，部署的网络攻防场景具有以下特性：

(1)网络的真实地址空间为 n_r,虚拟地址空间为 n_v;

(2)网络中有 $m<n_r$ 个真实主机,虚拟网络拓扑中有 $e<n_v$ 个诱饵节点;

(3)攻击者被诱饵节点欺骗的概率为 ε,$0\leqslant\varepsilon\leqslant1$;

(4)对于单个节点,攻击者扫描探测时间为 T_s,攻击准备阶段时间为 T_a;

(5)攻击者已知地址空间大小,并连续进行 k 次探测以获取网络中的真实主机;

(6)攻击者的目标是建立立足点,即在 k 次探测中,至少探测到一台易受攻击的计算机;

(7)攻击者在 k 次探测中成功探测到的主机数量为 X_k^s,攻击者成功攻击的主机数量为 X_k^a;

(8)IP 地址随机化周期是攻击准备时间的 λ 倍,因为 IP 地址随机化周期太短会严重影响网络性能,因此本文只考虑 IP 地址随机化周期大于攻击准备时间的情况,即 $\lambda>1$;

(9)在一次 IP 地址随机化事件中,真实主机发生 IP 地址转移的概率为 α,为确保攻击者无法根据 IP 地址变化规律来区分真实主机和诱饵节点,诱饵节点和真实主机发生 IP 地址变换的概率均为 $1-\alpha$。

文献[23]详细分析了无防御场景下的攻击者成功概率模型,因此不再赘述。在无防御场景下,攻击者连续进行 k 次扫描探测,成功探测到 x 个真实主机的概率为:

$$P(X_k=x)=\frac{C_m^x\cdot C_{n_r-m}^{k-x}}{C_{n_r}^k} \tag{4}$$

因此攻击者攻击成功的概率为:

$$P(X_k\geqslant1)=1-P(X_k^a=0)=1-\frac{C_{n_r-m}^k}{C_{n_r}^k} \tag{5}$$

在 MTDCD 防御场景下,可以将攻击者成功概率模型建模为包含 n_v 个弹球的 Urn 模型,包括 m 个绿色弹珠、εe 个红色弹珠和 $n_v-m-\varepsilon e$ 个蓝色弹珠,它们分别代表真实主机、成功欺骗攻击者的诱饵节点和地址空间中剩余的 IP 地址。在每个回合,攻击者会取出一个弹珠,并且不放回,但因为 IP 地址随机化事件会使攻击者获取的信息失效,相当于周期性地将已取出的弹珠全部放回,因此攻击者成功的条件为至少取到一个绿色弹珠且没有取到任何红色弹珠。

假设系统周期性地执行 IP 地址随机化事件,且攻击者的扫描探测时间 T_s 是固定的,则攻击者在每个周期的探测数为:

$$L=\frac{T_\tau}{T_s} \tag{6}$$

攻击者总的探测数 $k=J\times L+\delta$,其中 $J=\left\lfloor\frac{k}{L}\right\rfloor$ 为攻击者进行 k 次探测需要的周期数,δ 为剩余的探测数。攻击者成功的条件为攻击者至少在一个周期成功攻击真实主机,且攻击者在 J 个周期和剩余 δ 次探测中都没有攻击诱饵节点。

攻击者有两种失败的情况,一种是攻击者没有成功攻击到任何节点,即攻击者既没有成功攻击到真实主机也没有成功攻击到诱饵节点;另一种情况是攻击者攻击到诱饵节点。

J 个周期内,攻击者成功的概率无法直接计算得出,需要首先计算攻击者在 J 个周期内没有成功攻击到任何节点的概率和攻击者在 J 个周期内攻击到诱饵节点的概率。

首先分析单个周期的情况。由前面的分析可知,IP 地址随机化的部署,使得攻击者成功攻击到至少一个真实主机的概率进一步减小。单个周期内,攻击者没有成功攻击到任何节点的概率 $P_{T_{no}}$ 可以表示为:

$$P_{T_{no}}=1-P_{T_h}-P_{T_b} \tag{7}$$

P_{T_h} 为攻击者成功攻击到至少一个真实主机且没有攻击诱饵节点的概率。

因为 IP 地址随机化周期是攻击准备时间的 λ 倍,所以攻击者成功探测到主机但在攻击实施阶段没有成功命中的概率为:

$$P_{T_h}^{no}=\sum_{x=1}^{m}\frac{C_m^xC_{n_r-m-\varepsilon e}^{L-x}}{C_{n_r}^L}\cdot\frac{1}{\lambda} \tag{8}$$

因此易知:

$$P_{T_h}=\sum_{x=1}^{m}\frac{C_m^xC_{n_r-m-\varepsilon e}^{L-x}}{C_{n_r}^L}\cdot\left(1-\frac{1}{\lambda}\right) \tag{9}$$

P_{T_b} 为攻击者攻击到至少一个诱饵节点的概率。

$$P_{T_b}=\left(1-\frac{C_{n_v-\varepsilon e}^L}{C_{n_v}^L}\right)\cdot\left(1-\frac{1}{\lambda}\cdot(1-\alpha)\right) \tag{10}$$

因此单个周期内,攻击者没有成功攻击到任何节点的概率为:

$$P_{T_{no}}=1-\sum_{x=1}^{m}\frac{C_m^x\cdot C_{n_r-m-\varepsilon e}^{L-x}}{C_{n_r}^L}\cdot\left(1-\frac{1}{\lambda}\right)-\left(1-\frac{C_{n_v-\varepsilon e}^L}{C_{n_v}^L}\right)\cdot\left(1-\frac{1-\alpha}{\lambda}\right) \tag{11}$$

IP 地址转移将上一个周期的真实主机 IP 地址转移至诱饵节点,由此可知,在下一个周期内,攻击者攻击到诱饵节点的概率为:

$$\begin{aligned}P_{T_b}^*&=P_{T_b}+P_{T_h}^{no}\cdot\alpha\\&=\left(1-\frac{C_{n_v-\varepsilon e}^L}{C_{n_v}^L}\right)\cdot\left(1-\frac{1-\alpha}{\lambda}\right)+\sum_{x=1}^{m}\frac{C_m^xC_{n_r-m-\varepsilon e}^{L-x}}{C_{n_r}^L}\cdot\frac{\alpha}{\lambda}\end{aligned} \tag{12}$$

在上一个周期被探测到的主机,在下一个周期仍然被探测到的概率为 $\frac{L}{n_v}$。因为攻击者在上一个周期针对该主机已经进行了攻击准备工作,若攻击者在下一个周期再次探测到该主机,则不需要重新进行攻击准备,可以直接实施攻击。因此,攻击者在第 j 个周期成功攻击到至少一个主机的概率为:

$$\begin{aligned}P_{T_h}^j&=P_{T_h}+P_{T_h}^{no}\cdot(1-\alpha)\cdot\frac{L}{n_v}\cdot j\\&=\sum_{x=1}^{m}\frac{C_m^xC_{n_r-m-\varepsilon e}^{L-x}}{C_{n_r}^L}\cdot\left(1-\frac{1}{\lambda}\right)+\sum_{x=1}^{m}\frac{C_m^xC_{n_r-m-\varepsilon e}^{L-x}}{C_{n_r}^L}\cdot\frac{1}{\lambda}\cdot\frac{L}{n_v}\cdot j\end{aligned} \tag{13}$$

因此在第 j 个周期,攻击者没有成功攻击到任何节点的概率为:

$$\begin{aligned}P_{T_{no}}^j&=1-P_{T_h}^j-P_{T_b}^*\\&=1-\sum_{x=1}^{m}\frac{C_m^xC_{n_v-m-\varepsilon e}^{L-x}}{C_{n_v}^L}\cdot\left(1-\frac{1}{\lambda}\right)-\sum_{x=1}^{m}\frac{C_m^xC_{n_v-m-\varepsilon e}^{L-x}}{C_{n_v}^L}\cdot\frac{1}{\lambda}\cdot\frac{L}{n_v}\cdot j-\left(1-\frac{C_{n_v-\varepsilon e}^L}{C_{n_v}^L}\right)\cdot\left(1-\frac{1-\alpha}{\lambda}\right)-\sum_{x=1}^{m}\frac{C_m^xC_{n_r-m-\varepsilon e}^{L-x}}{C_{n_r}^L}\cdot\frac{\alpha}{\lambda}\end{aligned} \tag{14}$$

攻击者在 J 个周期成功的概率 $P_{T_h}^J$ 可以表示为：

$$P_{T_h}^J = 1 - P_{T_{\text{no}}}^J - P_{T_b}^J \tag{15}$$

其中，$P_{T_{\text{no}}}^J$ 为攻击者在 J 个周期都没有成功攻击到任何节点的概率，$P_{T_b}^J$ 为攻击者在 J 个周期都没有攻击到诱饵节点的概率。因此攻击者在 J 个周期成功的概率为：

$$\begin{aligned} P_{T_h}^J &= P(X_{JL} \geqslant 1) \\ &= 1 - P_{T_{\text{no}}} \cdot \prod_{j=1}^{J-1} P_{T_{\text{no}}}^j - (1 - (1 - P_{T_b}) \cdot (1 - P_{T_b}^*)^{J-1}) \end{aligned} \tag{16}$$

此外还有剩余 δ 次探测，同理可求得攻击者接触到至少一个蜜罐的概率为：

$$P_{\delta_b} = 1 - \frac{C_{n_v - \omega}^{\delta}}{C_{n_v}^{\delta}} \tag{17}$$

剩余 δ 次探测中，攻击者没有成功攻击到任何节点的概率为：

$$\begin{aligned} P_{\delta_{\text{no}}} &= 1 - P_{\delta_h} - P_{\delta_b} \\ &= \frac{C_{n_v - \omega}^{\delta}}{C_{n_v}^{L}} - \sum_{x=1}^{m} \frac{C_m^x \cdot C_{n_v - m - \omega}^{\delta - x}}{C_{n_v}^{L}} \cdot \left(1 - \frac{1}{\lambda}\right) \end{aligned} \tag{18}$$

因此，连续进行 k 次侦查，攻击者成功的概率为：

$$\begin{aligned} P(X_k \geqslant 1) = 1 - P_{T_{\text{no}}} \cdot \prod_{j=1}^{J-1} P_{T_{\text{no}}}^j \cdot P_{\delta_{\text{no}}} - (1 - (1 - P_{T_b}) \cdot \\ (1 - P_{T_b}^*)^{J-1} \cdot (1 - P_{\delta_b})) \end{aligned} \tag{19}$$

5 结果和分析

第 4 节推导了 MTDCD 的防御有效性评估模型。本节将根据虚拟网络拓扑大小、诱饵节点的欺骗概率、IP 地址随机化周期、IP 地址转移概率等多个参数量化评估防御方法的有效性，分析不同参数的变化对防御有效性的影响，以指导防御技术的实现和部署。

设置真实网络的地址范围为一个 C 段，网络中共有 20 个真实主机，虚拟网络拓扑由若干个子网组成，每个子网地址范围为一个 C 段。假设攻击者的能力固定，对于单个节点，攻击者的攻击准备时间是扫描探测时间的 10 倍。

5.1 虚拟网络拓扑大小

为评估虚拟网络拓扑大小对防御有效性的影响，设置无防御(NO Defense)，MTDCD_256_3，MTDCD_512_3，MTDCD_1024_3 这 4 种场景(其中 MTDCD_256_3 表示 IP 地址范围为 256，IP 地址随机化的周期为攻击准备时间 3 倍，以此类推)。每个子网中诱饵节点数量为 20，诱饵节点的欺骗成功率为 20%，IP 地址转移的概率为 50%。

图 5 给出了在上述 4 种场景下，随着攻击者扫描探测次数的增加，攻击者成功概率的变化情况。在无防御的场景下，经过 51 次扫描，攻击者的成功概率可达到 99%；而在部署了 MTDCD 的场景下，随着攻击者扫描探测次数的增加，攻击者成功的概率先增大后减小。这是因为攻击者探测的次数越多，接触到诱饵节点的概率就越大，而一旦接触到诱饵节点，攻击者就会失败。在 MTDCD_256_3 场景下，攻击者经过 21 次扫描探测，攻击成功的概率达到最大，为 40%；在 MTDCD_512_3 场景下，攻击者经过 45 次扫描探测，攻击成功的概率达到最大，为 31%；在 MTDCD_1024_3 场景下，攻击者经过 51 次扫描探测，攻击成功的概率达到最大，为 22%。通过分析可以看出，扩大虚拟网络拓扑地址范围，不仅可以降低攻击者的攻击成功概率，还可以增加攻击者的时间成本。同时还可以发现，在部署了 MTDCD 的场景下，随着攻击者扫描探测次数的增加，攻击者成功的概率呈周期性变化，且变化周期与 IP 地址随机化周期一致。

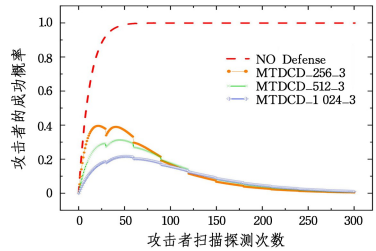

图 5 不同虚拟网络拓扑下攻击者的成功概率

Fig. 5 Attacker's success probability in different virtual network topologies

5.2 诱饵节点欺骗概率

诱饵节点的存在使攻击者不能随意探测网络，攻击者的成功概率还受网络中诱饵节点的欺骗概率的影响。设置无防御、诱饵节点欺骗率分别为 10%(Deception 10%)，20%(Deception 20%)和 80%(Deception 80%)的 4 种 MTDCD 防御场景，虚拟网络拓扑均包含 2 个子网，且每个子网中的诱饵节点数为 10，诱饵节点的欺骗成功率为 10%，IP 地址随机化的周期均为 5 倍攻击准备时间，IP 地址转移的概率为 50%。

图 6 给出了在上述 4 种场景下，随着攻击者扫描探测次数的增加，攻击者成功概率的变化。在诱饵节点的欺骗成功率为 10%时，攻击者的攻击成功概率最大为 60%；而当诱饵节点的欺骗率为 20%时，攻击者的攻击成功概率最大为 47%；当诱饵节点的欺骗率为 80%时，攻击者的攻击成功概率最大为 24%。可以看出，攻击者成功的概率随着诱饵节点欺骗概率的增加而降低，这说明提高诱饵节点的仿真度，增加诱饵节点的欺骗概率，能够有效提升虚拟网络拓扑的防御有效性。

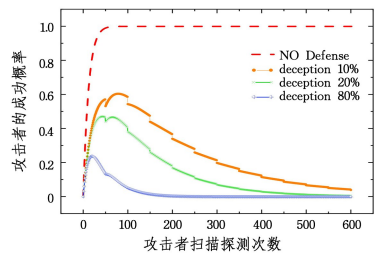

图 6 不同欺骗成功率下攻击者的成功概率

Fig. 6 Attacker's success probability in different deception success rates

5.3 IP 地址随机化周期

IP 地址随机化可以使攻击者在一段时间内获取的信息失效，使其不得不重新开始探测，因此需要分析 IP 地址随机化频率的大小对防御有效性的影响。设置无防御、MTDCD_

512_5 和 MTDCD_512_2 这 3 种场景，虚拟网络拓扑中每个子网的诱饵节点数为 10，诱饵节点的欺骗成功率为 20%，IP 地址转移的概率为 50%。

图 7 给出了上述 3 种场景下，随着攻击者扫描探测次数的增加，攻击者成功概率的变化。在攻击者扫描探测次数相同的情况下，IP 地址随机化周期越大，攻击者的成功概率越大，因此可以通过减小 IP 地址随机化周期来提高防御效能。

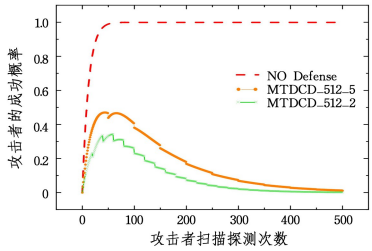

图 7 不同 IP 地址随机化周期下攻击者的成功概率

Fig. 7 Attacker's success probability in different IP address randomization cycles

5.4 IP 地址转移概率

每当 IP 地址随机化事件发生时，真实主机的 IP 地址以一定概率转移至诱饵节点，为分析 IP 地址转移概率对攻击者成功概率的影响，设置无防御、MTDCD_1024_8、MTDCD_1024_4 和 MTDCD_1024_2 这 4 种场景，虚拟网络拓扑中每个子网中的诱饵节点数为 10，诱饵节点的欺骗成功率为 20%。

图 8 给出了上述 4 种场景下，随着 IP 地址转移概率的增加，攻击者成功概率的变化。通过分析结果可以看出，随着 IP 地址转移概率的增加，攻击者成功的概率逐渐减小，且 IP 地址随机化周期越小，IP 地址转移概率对攻击者成功概率的影响越大。

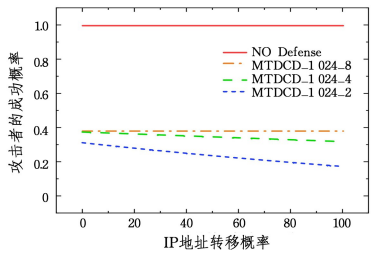

图 8 IP 地址转移概率对攻击者成功概率的影响

Fig. 8 Impact of IP address transfer probability on attacker's success probability

结束语 本文针对攻击者网络入侵的行为特点，提出了结合移动目标防御和网络欺骗防御的 MTDCD 防御机制，通过深入分析网络入侵过程，建立威胁模型，并基于 Urn 模型建立了防御有效性评估模型，最后根据虚拟网络拓扑大小、诱饵节点的欺骗概率、IP 地址随机化周期、IP 地址转移概率等多个参数量化评估了防御方法的有效性。通过严密的理论分析和实验验证，证明了本文提出的 MTDCD 防御机制能够有效缓解网络入侵，并为后续防御策略的设计提供一定的参考和指导。下一步将建立仿真环境，通过仿真实验来评估 MTDCD 的防御性能和系统开销。

参 考 文 献

[1] PING C, DESMET L, HUYGENS C. A Study on Advanced Persistent Threats[C]// IFIP International Conference on Communications and Multimedia Security. Berlin: Springer, 2014: 63-72.

[2] BOWERS K, VAN D 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(Game Security). 2012: 248-263.

[3] CHONG F, LEE R, ACQUISTI A, et al. National cyber leap year summit 2009: Co-chairs' report[J/OL]. https://www.nitrd.gov/nitrdgroups/index.php? title=Category: National_Cyber_Leap_Year_ Summit_2009.

[4] 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.

[5] CHANG S Y, PARK Y, BABU B. Fast IP Hopping Randomization to Secure Hop-by-Hop Access in SDN[J]. IEEE Transactions on Network and Service Management, 2018, 16(1): 308-320.

[6] LUO Y B, WANG B S, WANG X F, et al. RPAH: Random Port and Address Hopping for Thwarting Internal and External Adversaries[C]// IEEE Trustcom/bigdatase/ispa. IEEE, 2015.

[7] CUNHA V A, CORUJO D, BARRACA J P, et al. TOTP Moving Target Defense for sensitive network services[J]. Pervasive and Mobile Computing, 2021, 74(4): 101412.

[8] DEBROY S, CALYAM P, NGUYEN M, et al. Frequency-minimal moving target defense using software-defined networking [C]// International Conference on Computing. IEEE, 2016: 1-6.

[9] TORQUATO M, MACIEL P, VIEIRA M. Security and Availability Modeling of VM Migration as Moving Target Defense [C]// 25th IEEE Pacific Rim International Symposium on Dependable Computing. IEEE, 2020: 50-59.

[10] MARS J, LAURENZANO M, TANG L. Runtime compiler environment with dynamic co-located code execution U. S. Patent 9921859[P]. 2018-03-20.

[11] JIA Z P, FANG B X, LIU C G, et al. Overview of Network Deception Techniques [J]. Journal on Communications, 2017, 38(12): 128-143.

[12] SUN J, LIU S, SUN K. A scalable high fidelity decoy framework against sophisticated cyber attacks[C]// Proceedings of the 6th ACM Workshop on Moving Target Defense. ACM, 2019: 37-46.

[13] WANG S, WANG J H, PEI Q Q, et al. Active deception defense method based on dynamic camouflage network[J]. Journal on Communications, 2020(2): 97-111.

[14] ALBANESE M, BATTISTA E, JAJODIA S. Deceiving Attackers by Creating a Virtual Attack Surface[M]. Berlin: Springer International Publishing, 2016: 167-199.

[15] ZHAO Z, GONG D F, LU B, et al. SDN-Based Double Hopping

Communication against Sniffer Attack[J/OL]. Mathematical Problems in Engineering. https://doi.org/10.1155/2016/8927169.

[16] UITTO J,RAUTI S,LAURÉN S,et al. A Survey on Anti-honeypot and Anti-introspection Methods[C]// World Conference on Information Systems & Technologies. Cham:Springer,2017:125-134.

[17] SUN J,SUN K. DESIR:Decoy-enhanced seamless IP randomization[C]// IEEE INFOCOM. IEEE,2016:1-9.

[18] XING J,YANG M,ZHOU H,et al. Hiding and Trapping:A Deceptive Approach for Defending against Network Reconnaissance with Software-Defined Network[C]// 2019 IEEE 38th International Performance Computing and Communications Conference(IPCCC). IEEE,2020:1-8.

[19] ZHAO J L,ZHANG G M,XING C Y,et al. An adaptive spoofing defense mechanism against network reconnaissance [J]. Computer Science,2020,47(12):304-310.

[20] PRAKASH A,WELLMAN M P. Empirical Game-Theoretic Analysis for Moving Target Defense[C]// ACM Workshop on Moving Target Defense. ACM,2015:57-65.

[21] EEUWEN B V,STOUT W,URIAS V. MTD assessment framework with cyberattack modeling[C]// 2016 IEEE International Carnahan Conference on Security Technology(ICCST). IEEE,2016:1-8.

[22] CARROLL T E,CROUSE M,FULP E W,et al. Analysis of network address shuffling as a moving target defense[C]// IEEE International Conference on Communications. IEEE,2014:701-706.

[23] CROUSE M,PROSSER B,FULP E W. Probabilistic Performance Analysis of Moving Target and Deception Reconnaissance Defenses[C]// ACM Workshop on Moving Target Defense. ACM,2015:21-29.

[24] XIONG X L,XU W G,ZHAO G S. The Effectiveness Assessment for Network Based MTD Strategies[C]// Proceedings of the 8th International Conference on Communication and Network Security. 2018:7-11.

[25] DALZIEL H. Cyber Kill Chain[J]. Securing Social Media in the Enterprise,2015,12(6),7-15.

[26] STAFFORD J S. Behavior-based worm detection[D]. Eugene:University of Oregon,2012.

[27] HAIGH J. Polya Urn Models[J]. Journal of the Royal Statistical Society Series A(Statistics in Society),2010,172(4):932-942.

GAO Chun-gang, born in 1996, postgraduate. His main research interests include network security and active defense.

WANG Yong-jie, born in 1974, Ph. D, professor. His main research interests include network security and active defense.

(责任编辑:何杨)