一种基于拟态防御机制的SDN虚拟蜜网

廉 哲,殷肖川,席 茜,谭 韧
空军工程大学 信息与导航学院,西安 710077

摘 要:针对传统蜜网部署不方便,流量控制困难,蜜网动态调整较复杂的缺陷,利用SDN技术灵活的控制机制与容器高速、轻量的技术特性,设计了具有动态可调整特性的SDN虚拟蜜网,结合拟态防御机制为SDN虚拟蜜网提供动态调整的依据,并通过博弈论验证了基于拟态防御机制的SDN虚拟蜜网的有效性。利用Containernet仿真实验平台搭建出SDN虚拟蜜网,并设计实现了基于拟态防御机制的动态跳变,通过实验验证了该蜜网的可行性。

关键词:软件定义网路;拟态防御;容器技术;虚拟蜜网;动态跳变
文献标志码:A **中图分类号:**TP393.08 doi:10.3778/j.issn.1002-8331.1709-0175

廉哲,殷肖川,席茜,等.一种基于拟态防御机制的SDN虚拟蜜网.计算机工程与应用,2019,55(1):109-114.
LIAN Zhe, YIN Xiaochuan, XI Xi, et al. SDN virtual honeynet based on mimic defense mechanism. Computer Engineering and Applications, 2019, 55(1):109-114.

SDN Virtual Honeynet Based on Mimic Defense Mechanism

LIAN Zhe, YIN Xiaochuan, XI Xi, TAN Ren
Information and Navigation College, Air Force Engineering University, Xi'an 710077, China

Abstract: The traditional honeynet has many drawbacks such as inconvenient deployment, difficult flow control and complex dynamic adjustment. SDN technology has flexible controlling mechanism and container with high speed and lightweight. A SDN virtual honeynet is designed by using these advantages. It will provide dynamic adjustment basis to SDN virtual honeynet by using the mimic defense mechanism. The effectiveness of the SDN virtual honeynet is verified based on the game theory. At last, the SDN virtual honeynet is established using Containernet simulation platform, and the dynamic jumping change is designed and implemented based on mimic defense mechanism. The feasibility of the honeynet is verified through experiments.

Key words: software defined networking; mimic defense; container technology; virtual honeynet; dynamic jump

1 引言

网络信息安全已经成为互联网时代人们的重点关注对象,传统的网络防御技术如防火墙[1]、入侵检测[2]等存在着网络攻防不平衡的问题:一方面因为攻击方处于隐蔽,存在未知的威胁和漏洞;另一方面因为现有的防御体系基本上都是依靠现有、已知的一些漏洞、病毒等,需要一定的先验知识[3]。蜜网是一种十分有效的防御机制,它可以通过诱骗攻击者使攻击者误以为蜜罐主机就是真实服务主机,从而起到保护真实服务主机的作用[4]。但是传统的蜜网存在流量控制困难,物理机部署复杂的问题,本文结合SDN[5](Software Defined Networking, SDN)以及容器技术[6]构建了一种SDN虚拟蜜网,通过软件定义网络拓扑,利用虚拟化技术和SDN控制器实现蜜网的部署与流量控制。为了实现主动防御,本文结合拟态防御机制,构建一种基于拟态防御机制的SDN虚拟蜜网,并利用博弈论对SDN虚拟蜜网进行理论分析,验证了这种防御手段的有效性,最后通过实验验证了该方法的可行性。

基金项目:陕西省工业科技攻关项目(No.2016GY-087)。
作者简介:廉哲(1994—),男,硕士生,研究领域为网络与信息安全,E-mail:lianzkgd@163.com;殷肖川(1961—),男,教授,研究领域为网络与信息安全;席茜(1993—),女,硕士生,研究领域为网络与信息安全、数据挖掘;谭韧(1993—),男,硕士生,研究领域为网络与信息安全。
收稿日期:2017-09-13 **修回日期:**2017-11-01 **文章编号:**1002-8331(2019)01-0109-06
CNKI **网络出版:**2018-03-13, http://kns.cnki.net/kcms/detail/11.2127.TP.20180313.0847.008.html

2　相关研究

蜜网技术从提出到现在已经发展到第三代,其核心技术在于其昂贵的蜜墙技术[7]。当前蜜网系统对于网络攻击方进行诱骗主要是依靠模拟仿真的方式或者通过保持与真实系统一致,在真实系统基础上构建具有高交互性的蜜网。DTK[8]和LaBrea[9]通过构建网络服务绑定到指定端口,模拟成网络服务的攻击目标,诱骗攻击方对其进行攻击扫描,但这种机制交互性较低,无法识别未知的攻击,HoneyBow[10]基于真实的服务系统构建高交互性蜜网,但是对硬件设备依赖性强,硬件设备必须需要一定标准的接口,部署成本较高且可扩展性较差。DecoyPort[11]系统建议将攻击方重定向到蜜罐,在每台计算机上创建诱饵端口,并将流量重定向到蜜罐,但仍然存在攻击者对一些系统忽略的端口进行攻击的机会,并且现在黑客技术也在提升,传统的蜜网容易被黑客识别并有可能被加以利用,反而造成更大的损害。诸葛建伟在文献[4]中对蜜罐技术的发展研究趋势进行了分析与预测,提出现在的蜜网技术在仿真性与可控性之间存在很大的矛盾,提出具有可定制与扩展性的蜜网架构与具有自适应能力的动态蜜网具有研究意义。胡毅勋[12]等在2015年提出了Openflow协议下的动态虚拟蜜网系统,运用Openflow交换机验证了虚拟蜜网系统转发时延低、动态性强的特性。邬江兴[13]提出的网络空间拟态防御对于解决攻防不平衡,实现主动防御具有重要意义。仝青[14]等人提出了拟态防御Web服务器并设计实验验证了其防御技术的可行性和有效性。因此,本文在前人研究的基础上,研究设计了一种新的蜜网机制,使用SDN网络架构构建虚拟蜜网,利用SDN架构数据控制层与数据传输层分离的特性,解决传统蜜网无法根据需求动态调整以及扩展性不足的问题,将拟态防御机制应用于SDN虚拟蜜网,构建具有主动防御机制的拟态蜜网,并通过博弈理论分析验证拟态虚拟蜜网的有效性,最后通过实验构建拟态SDN虚拟蜜网,验证了方案的可行性。

3　基于拟态防御的SDN虚拟蜜网

3.1　SDN虚拟蜜网

为了解决传统蜜网流量控制困难,物理机部署不方便,动态性与扩展性不足的问题,提出一种基于SDN的虚拟蜜网,SDN网络架构是当前研究最前沿的网络技术,对未来网络发展具有重要意义,本文在前人研究基础上,将SDN网络架构运用于蜜网的构建,首先对于网络流量的重定向技术与动态调整,提出了新的方案,SDN网络架构实现了数据控制与数据传输的解耦合,利用控制层的控制技术,实现软件定义流量转发,实现蜜网流量的监控和动态迁移,并且利用Docker容器代替传统虚拟机,使服务主机更加轻量级,动态转换更加高速。

SDN虚拟蜜网网络架构[15]如图1所示,利用SDN网络架构构建虚拟蜜网,需要从三个层面对网络进行构建:

(1)基础设施层

基础设施层由网络设备组成,底层虚拟设备通过容器技术与OpenvSwitch(OVS)交换机技术进行实现,可以达到快速进行动态调整的目的,实现虚拟蜜网的动态性。将服务节点利用Docker容器来部署,Docker容器是一种轻量级的虚拟化技术,与传统的虚拟化技术相比,它能让更多数量的应用程序在同一硬件上运行并简化了管理和部署应用程序的任务,能够实现高速、轻量的目标。交换节点利用虚拟交换机OVS来部署,利用OVS虚拟交换机能够实现OpenFlow协议,可以通过流表管理交换机的行为,通过与Docker容器连接组成SDN底层设施,将真实服务与蜜罐服务部署于底层。

(2)控制层

控制层实现网络的集中控制与管理,利用当前流行的OpenDaylight(ODL)控制器,实现对OVS交换机中流表的控制,拥有全局网络视图,简化了网络设计和运维,优化网络资源,实现实时快速响应和业务快速部署,解决了传统蜜网流量控制困难的问题。

(3)应用层

应用层由各网络应用服务组成,用户通过控制层开放的接口开发各种网络应用,根据业务需求修改网络转发行为,实现可编程控制的虚拟蜜网,根据用户需求将底层设备进行映射到应用层供外部用户访问,向外界提供可动态调整、具有主动防御功能的虚拟蜜网。

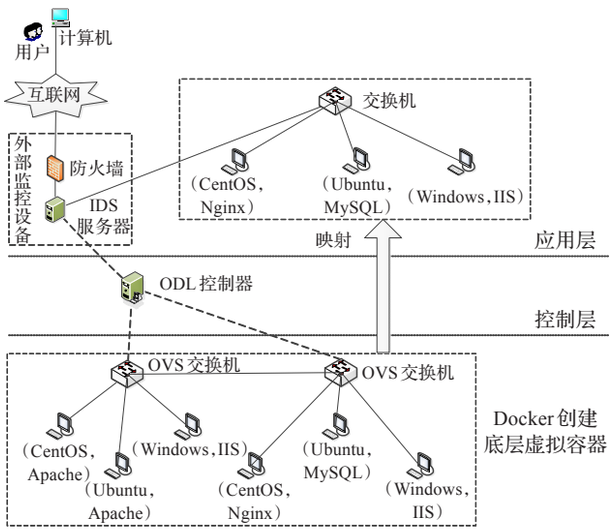

图1　SDN虚拟蜜网架构

3.2　拟态虚拟蜜网

漏洞是计算机系统存在安全威胁的根本原因[16],根据国家信息安全漏洞库的统计[17],通过归纳整理可知,近

年来每年新增安全漏洞均在5 500以上，中危和高危漏洞占的比例较多，近年来每年新增漏洞数量如图2所示。

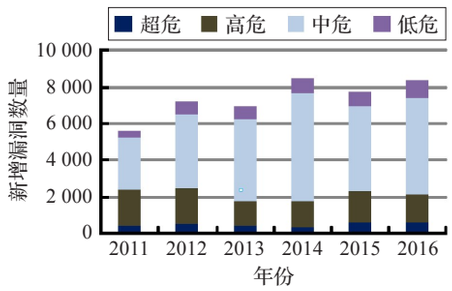

图2　2011—2016年新增漏洞数量

一般的攻击链可以归纳为攻击探测、漏洞挖掘、权限提升、攻击植入、痕迹消除。邬江兴在文献[13]中提出，拟态安全防御即是指防御方在主动或被动的触发条件下，动态或伪随机地选择执行各种硬件和软件变体，使得攻击者观察到的硬件执行环境和软件工作状况具有不确定性，基于漏洞或后门的攻击链不易被构建，从而达成降低系统安全风险的目的[9]。

为了实现SDN虚拟蜜网的动态性和随机性，利用拟态防御机制，将蜜网物理层的容器进行异构冗余处理，由于容器是一种轻量级虚拟化技术，可以在一台服务主机设置多台冗余蜜罐主机。例如需要提供的服务为Web服务，可以提供Web服务的方法有很多，在保证服务功能一致的条件下，不同操作系统利用不同的软件，可以达到相同的效果。首先，操作系统可以有很多种选择，包括Windows server、Win7、Ubuntu、red hat、centos等，当选择好操作系统之后，提供服务的软件也包含很多种，例如Apache、IIS、Nginx等。可以为真实服务主机提供多种类型的冗余蜜罐容器，包括相同操作系统不同服务软件、不同操作系统不同服务软件、不同操作系统相同服务软件、相同操作系统相同服务软件但提供不同端口和漏洞等等，当攻击者想要攻击真实服务时，这些冗余的蜜罐容器都可以用来替换真实服务主机，利用ODL控制器对容器进行动态、伪随机地调整，实现拟态蜜网，使得攻击者对于攻击目标的攻击探测、漏洞挖掘不能顺利进行，从而阻断攻击者的攻击链，达到主动防御的目的。

4　拟态蜜网博弈理论分析

为了验证拟态SDN虚拟蜜网的有效性，本文利用博弈理论进行分析[18]，对于蜜网防护来说，是攻击方与防御方参与的非合作不完全信息博弈，对于服务方来说，由于其最优策略随着访问方的类型变化而变化，所以需要通过分析计算得到攻防双方的贝叶斯纳什均衡策略。本文对拟态蜜网进行博弈理论分析如下。

局中人包括：$P=\{Ser,Vis\}=$ {服务方，攻击方}，其中 $Ser=\{S_r,S_h\}=$ {真实服务，蜜罐服务}，$Vis=\{V_n,V_a\}=$ {普通用户，攻击者}。

局中人策略：$S_{Ser}=\{S_0,S_1\}=$ {不提供服务，提供服务}，$S_{Vis}=\{V_0,V_1\}=$ {不访问服务，访问服务}。

局中人收益：首先，当真实服务提供服务时，如果普通用户访问，则双方收益都为局中人收益：首先，当真实服务提供服务时，如果普通用户访问，则双方收益都为 $\alpha(\alpha>0)$，否则收益为 $-\alpha$，如果攻击者访问，则服务方除了本身提供的服务受到影响，其他性能也会遭到不同程度的破坏，则收益为 $-\mu\alpha-\beta$（其中 $0<\mu<1$ 表示服务本身受到的影响程度，$\beta>0$，表示除自身服务外其它性能遭到的破坏程度），攻击者收益为 $\mu\alpha+\beta-\gamma$（其中 $\gamma>0$ 表示攻击者的攻击成本）；当蜜罐服务提供服务时，如果普通用户访问，则蜜罐服务收益为0，普通用户收益为 $-\alpha$，如果攻击者访问，则蜜罐收益为 λ（$\lambda>0$ 表示蜜罐对攻击者的诱骗收益），攻击者收益 $-\lambda-\gamma$。攻防双方收益如表1所示。

表1　攻防双方收益表

		V_n		V_a	
		V_0	V_1	V_0	V_1
S_r	S_0	0，0	$-\alpha,-\alpha$	0，0	$0,-\gamma$
	S_1	0，0	α,α	0，0	$-\mu\alpha-\beta,\mu\alpha+\beta-\gamma$
S_h	S_0	0，0	$0,-\alpha$	0，0	$0,-\gamma$
	S_1	0，0	$0,-\alpha$	0，0	$\lambda,-\lambda-\gamma$

在进行攻防博弈时，服务方存在四种策略组合 (S_0,S_0)，(S_0,S_1)，(S_1,S_0)，(S_1,S_1)，其中 (S_a,S_b) 代表真实服务与蜜罐服务的策略组合，同样，访问方也存在四种策略组合 (V_0,V_0)，(V_0,V_1)，(V_1,V_0)，(V_1,V_1)，其中 (V_a,V_b) 代表普通用户与攻击者的策略组合。在进行博弈之前，攻防双方会对双方类型有一个先验概率判断，本文假设 $P(S_h)=p$，$P(S_r)=1-p$，$P(V_a)=q$，$P(V_n)=1-q$，在局中人观测到对方的行为后，利用贝叶斯法则得到其后验概率，并计算出各局中人的期望收益，通过比较计算得出使得各方期望收益取得极大值时的占优策略。

对于服务方而言，最期望双方局中人策略为 $\{(S_1,S_1),(V_1,V_0)\}$，即真实服务与蜜罐服务同时提供服务，普通用户正常访问，而攻击者不攻击。本文主要对策略 $\{(S_1,S_1),(V_1,V_0)\}$ 进行博弈分析，判断是否存在博弈均衡。首先，以访问者组合策略 (V_1,V_0) 为例，分析攻防博弈，由表1可以看出，对于蜜罐服务，无论访问方是什么类型，提供服务都是绝对占优策略；对于真实服务，观测得到访问方的策略为 (V_1,V_0) 后，可以得到访问方类型的后验概率 $P(V_n|V_1)=1-p$，$P(V_a|V_0)=p$，则真实服务的期望收益为：

$$E_{S_r}(S_1)=P(V_n|V_1)\times\alpha+P(V_a|V_0)\times0=(1-p)\times\alpha+p\times0=(1-p)\alpha \quad (1)$$

$$E_{S_r}(S_0)=P(V_n|V_1)\times(-\alpha)+P(V_a|V_0)\times 0=$$
$$(1-p)\times(-\alpha)+p\times 0=(p-1)\alpha \quad (2)$$

由公式(1)、(2)可以得到当 $p<1$ 时，$E_{S_r}(S_1)>E_{S_r}(S_0)$，即真实服务提供服务是绝对占优策略。由以上可以得出在访问方访问策略为 (V_1,V_0) 时，真实服务与蜜罐服务都提供服务是占优策略。

在从服务方视角得到占优策略后，下一步需要继续讨论在服务方策略为 (S_1,S_1) 时访问方是否存在博弈均衡，对于访问方可以得到服务方类型的后验概率 $P(S_r|S_1)=1-q$，$P(S_h|S_1)=q$，则访问方的期望收益为：

$$E_{V_n}(V_1)=P(S_r|S_1)\times\alpha+P(S_h|S_1)\times(-\alpha)=$$
$$(1-q)\times\alpha+q\times(-\alpha)=(1-2q)\alpha \quad (3)$$
$$E_{V_n}(V_0)=P(S_r|S_1)\times 0+P(S_h|S_1)\times 0=0 \quad (4)$$
$$E_{V_a}(V_1)=P(S_r|S_1)\times(\mu\alpha+\beta-\gamma)+P(S_h|S_1)\times(-\lambda-\gamma)=$$
$$(1-q)\times(\mu\alpha+\beta-\gamma)+q\times(-\lambda-\gamma)=$$
$$\mu\alpha+\beta-\gamma-q(\mu\alpha+\beta+\lambda) \quad (5)$$
$$E_{V_a}(V_0)=P(S_r|S_1)\times 0+P(S_h|S_1)\times 0=0 \quad (6)$$

由公式(3)、(4)可以得到当 $q<1/2$ 时，$E_{V_n}(V_1)>E_{V_n}(V_0)$，即普通用户访问服务是占优策略，否则不访问服务是占优策略。由公式(5)、(6)可以得到当 $q>(\mu\alpha+\beta-\gamma)/(\mu\alpha+\beta+\lambda)$ 时，$E_{V_a}(V_1)<E_{V_a}(V_0)$，即攻击者不攻击服务是占优策略，否则攻击服务是占优策略。所以当 $(\mu\alpha+\beta-\gamma)/(\mu\alpha+\beta+\lambda)<q<1/2$ 时，在服务方策略为 (S_1,S_1) 时，访问方普通用户访问服务，攻击者不攻击是占优策略。

综上所述，在 $p<1$，$(\mu\alpha+\beta-\gamma)/(\mu\alpha+\beta+\lambda)<q<1/2$ 时，真实服务与蜜罐服务同时提供服务，访问方普通用户正常访问而攻击者不攻击这一理想策略组合可以达到贝叶斯纳什均衡，此时的博弈均衡条件只与蜜罐存在的概率 q 有关而与攻击者攻击概率 p 无关，所以可以都得到结论：拟态SDN虚拟蜜网防御可以达到主动防御的目的。进一步分析博弈均衡条件，由 $(\mu\alpha+\beta-\gamma)/(\mu\alpha+\beta+\lambda)<q<1/2$ 可以得到 $(\mu\alpha+\beta-\gamma)/(\mu\alpha+\beta+\lambda)<1/2$ 即攻击者收益/(真实服务损失+蜜罐收益)$<1/2$，意味着蜜罐的收益需要远大于攻击者的收益以及真实服务所受的损失。这就需要对蜜罐进行充分的设计与利用，通过不同冗余拟态蜜罐尽可能多的对攻击方进行诱骗并获取对方的信息，这些将在后续的研究中继续加以分析和利用。

5　实验

5.1　实验部署

本文利用虚拟机软件VMware 12进行仿真实验，首先在虚拟机上安装Ubuntu16.04系统，在Ubuntu系统上安装SDN控制器ODL的Beryllium版本，并且安装Containernet[19]工具进行仿真实验。在Containernet工具下编写Python脚本进行SDN虚拟蜜网的设计，通过Containernet部署SDN虚拟蜜网可以实现容器技术的利用，能够比较方便的实现拟态SDN虚拟蜜网的构建，利用ODL控制器实现虚拟蜜网中流量的控制和转发，可以方便快捷的对流量进行控制，解决传统蜜网流量控制的问题。

5.2　仿真测试与分析

测试的目的是为了验证基于拟态防御机制的SDN虚拟蜜网的可行性，首先应该搭建好SDN虚拟蜜网，在其基础上测试能否实现拟态防御机制，从而验证基于拟态防御机制的SDN虚拟蜜网的可行性。

利用Containernet创建两个openflow交换机，每个交换机连接两个docker容器，用于模拟部署真实服务和蜜罐服务，如图3所示，是通过编写Python脚本，利用提前构建好的Docker镜像来生成SDN蜜网。

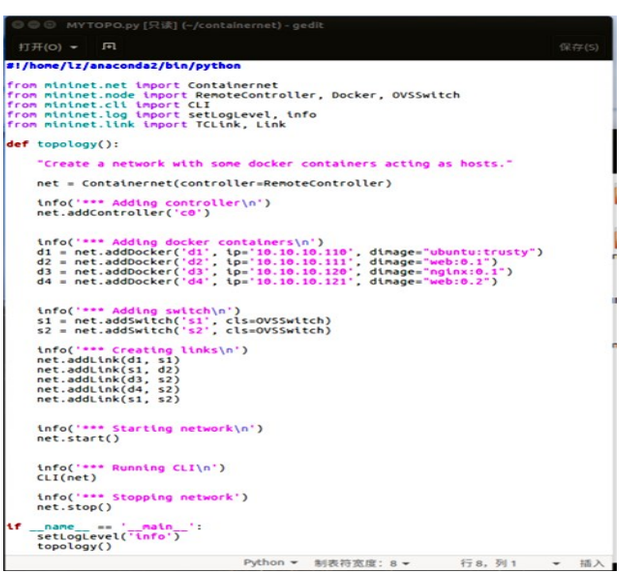

图3　自定义网络拓扑Python脚本

拓扑图由ODL控制器可以监测得到，如图4所示，其中，左边两个容器，左上是模拟访问主机，左下是模拟真实服务主机，真实服务主机是在Ubuntu14.04上装有Apache服务，并下载一个静态网页界面作为测试用例。右边交换机连接两个容器作为冗余蜜罐服务，其中右上容器是在Ubuntu14.04上装有Nginx服务并自定义了一个欢迎测试网站，右下容器同样在Ubuntu16.04上装有Apache服务并部署测试网站，并将Apache访问的日志数据挂载到宿主机可以访问的数据卷中，进一步加深对Docker容器技术的理解和应用。

部署好SDN虚拟蜜网后，首先进行连通性测试，ODL控制器初始默认网络中的流表为空，SDN蜜网中各主机无法进行正常通信访问，需要利用ODL添加流表规则，将两个交换机各端口连通。连通之后如图5所

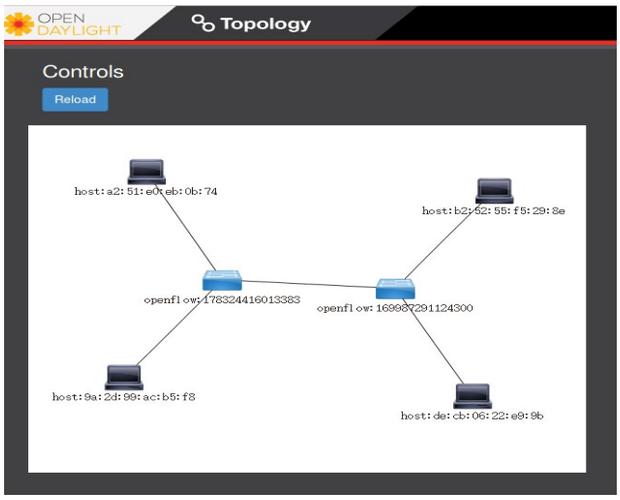

图4　SDN虚拟蜜网拓扑图

示,由访问主机对其他主机执行ping命令,发现都可以连通,自此完成SDN虚拟蜜网的搭建。

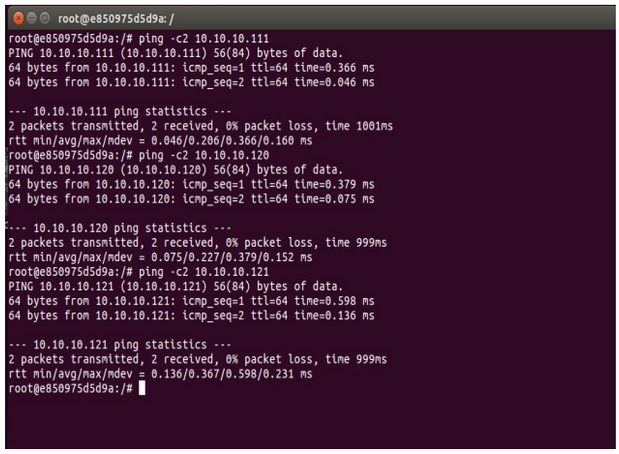

图5　SDN虚拟蜜网连通测试效果图

在完成SDN虚拟蜜网的搭建后,为了验证拟态SDN虚拟蜜网的可行性,接下来需要对网络中的流量进行迁移,实现功能不变条件下服务主机的跳变。在之前部署的SDN虚拟蜜网中,真实服务主机与蜜罐服务主机分处于不同交换机上,需要利用ODL控制器添加流表规则实现流量的迁移,从而实现服务的跳变进而达到拟态防御的目的。

在本实验中,当访问主机d1访问真实服务d2时,可以正常访问其业务,如图6所示,为了实现拟态防御,首先需要将访问者发出的数据包的目的ip与目的mac修改为蜜罐服务d3的ip地址与mac地址,当d3处理完数据包往回传送时,需要将源ip与源mac修改为d2的ip地址与mac地址,这样实际上是访问者d1与蜜罐服务d3在进行交互,但访问者并没有察觉,如图7所示是添加流表规则后,数据包进行重定向后访问者d1访问d2时返回的数据。两次d1访问d2得到的结果不同,当有攻击者欲利用真实服务d2的漏洞进行攻击时,可以给d3运用冗余机制使用不同的手段提供相同的服务,并将流量迁移到d3,从而阻断攻击者攻击链,达到保护真实服务的作用,证明蜜罐服务起到了作用,达到了拟态防御的目的,验证了基于拟态防御的SDN虚拟蜜网的可行性。

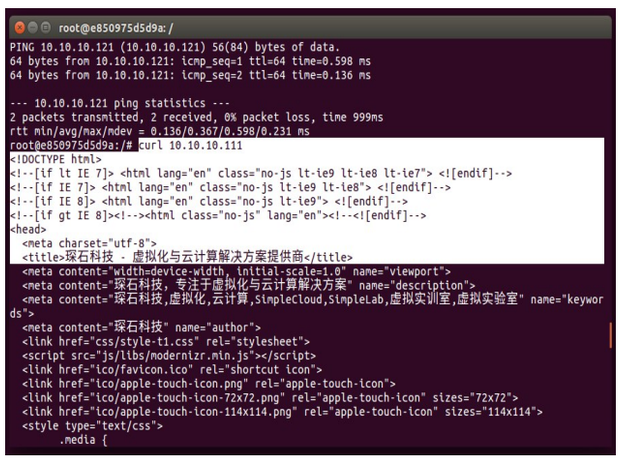

图6　数据重定向前访问主机d1访问d2服务

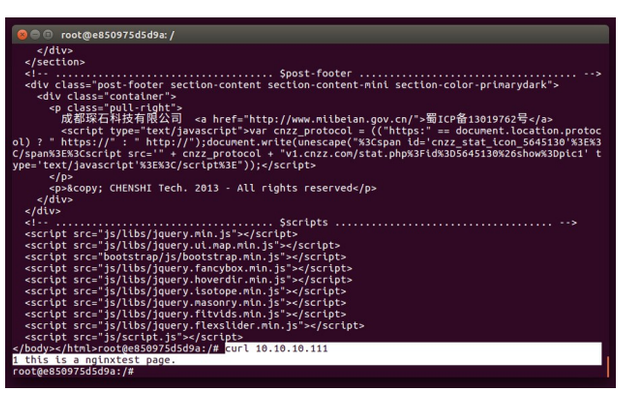

图7　数据重定向后访问主机d1访问d2服务

6　结束语

本文在前人研究的基础上,将拟态防御机制与SDN相关技术结合,设计了基于拟态防御机制的SDN虚拟蜜网。利用最新的容器技术代替传统虚拟蜜网的虚拟机,解决了传统蜜网部署不方便,流量控制困难的缺陷,并且可以很方便地根据需要添加或者删除各类服务容器。在搭建好SDN虚拟蜜网的基础上,结合拟态防御机制设计了基于拟态防御的SDN虚拟蜜网,并通过博弈论论证了基于拟态防御机制的SDN虚拟蜜网的有效性,最后利用Containernet工具进行仿真实验,通过拟态防御中的冗余机制设置蜜罐容器,利用ODL控制器设置并发送流表控制OVS交换机,在保证功能不变的前提下实现网络数据包的重定向,从而验证了基于拟态防御机制的SDN虚拟蜜网的可行性。在后期的研究过程中,可以利用ODL控制器对网络中的流量进行监测和分析,进一步诱骗攻击者对蜜网进行攻击,并通过分析得到攻击者的攻击信息。这样,一方面可以获取更多

的攻击方信息,为网络态势分析与呈现提供依据;另一方面可以根据攻击者信息制定相应防御策略,实现主动防御。

参考文献:

[1] Wang X,Tang H,Paterson A H.Research on the application of firewall in network security[J].Plant Cell,2011,23(1):27-37.

[2] Leu F Y,Tsai K L,Hsiao Y T,et al.An internal intrusion detection and protection system by using data mining and forensic techniques[J].IEEE Systems Journal,2017,11(2):427-438.

[3] Zhang Y,Zhang Y,Zhang Y,et al.Game-theory-based active defense for intrusion detection in cyber-physical embedded systems[J].ACM Transactions on Embedded Computing Systems,2016,16(1):18.

[4] 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(自然科学版),2013,24(4):825-842.

[5] Sezer S,Scott-Hayward S,Chouhan P K,et al.Are we ready for SDN? Implementation challenges for software-defined networks[J].IEEE Communications Magazine,2013,51(7):36-43.

[6] Liu X,Hu Z Y.Design and implementation of Web cluster based on Docker container[J].Electronic Design Engineering,2016,24(8):117-119.

[7] Fan W,Fernández D,Du Z.Versatile virtual honeynet management framework[J].IET Information Security,2017,11(1):38-45.

[8] Cohen F.The deception toolkit[EB/OL].(2012)[2017-08-01].http://all.net/dtk/index.html.

[9] Liston L.Welcome to my tarpit:The tactical and strategic use of LaBrea[EB/OL].(2011)[2017-08-01].http://www.hackbusters.net/LaBrea/LaBrea.txt.

[10] 诸葛建伟,韩心慧,周勇林,等.HoneyBow:一个基于高交互式蜜罐技术的恶意代码自动捕获器[J].通信学报,2007,28(12):8-13.

[11] More A,Tapaswi S.A software router based predictive honeypot roaming scheme for network security and attack analysis[C]//Proceeedings of International Conference on Innovations in Information Technology,2013:221-226.

[12] 胡毅勋,郑康锋,武斌,等.Openflow下的动态虚拟蜜网系统[J].北京邮电大学学报,2015(6):104-108.

[13] 邬江兴.网络空间拟态安全防御[J].保密科学技术,2014(10):4-9.

[14] 仝青,张铮,张为华,等.拟态防御Web服务器设计与实现[J].软件学报,2017,28(4):883-897.

[15] 廉哲,殷肖川,谭韧,等.面向网络攻击态势的SDN虚拟蜜网[J].空军工程大学学报(自然科学版),2017(3):79-84.

[16] Subrahmanian V S,Ovelgonne M,Dumitras T,et al.The global cyber-vulnerability report[M].[S.l.]:Springer International Publishing,2015.

[17] 中国国家信息安全漏洞库[EB/OL].[2017-08-01].http://www.cnnvd.org.cn.

[18] Manshaei M H,Zhu Q,Alpcan T,et al.Game theory meets network security and privacy[J].ACM Computing Surveys,2013,45(3):1-39.

[19] Peuster M,Karl H,Rossem S V.MeDICINE:Rapid prototyping of production-ready network services in multi-PoP environments[C]//Proceeedings of Network Function Virtualization and Software Defined Networks,2017.

(上接第83页)

[13] Xiao D,Eltabakh M,Kong X.Bermuda:An efficient mapreduce triangle listing algorithm for web-scale graphs[C]//Proceeedings of International Conference on Scientific and Statistical Database Management,2016:10.

[14] Qin L,Yu J X,Chang L,et al.Scalable big graph processing in MapReduce[C]//Proceeedings of SIGMOD,2014:827-838.

[15] Gabriel E,Fagg G E,Bosilca G,et al.Open MPI:Goals,concept,and design of a next generation MPI implementation[C]//Recent Advances in Parallel Virtual Machine and Message Passing Interface,European Pvm/mpi Users' Group Meeting,Budapest,Hungary,September 19-22,2004:97-104.

[16] Gropp W,Lusk E,Doss N,et al.A high-performance,portable implementation of the MPI message passing interface standard[J].Parallel Computing,1996,22(6):789-828.

[17] Plimpton S J,Devine K D.MapReduce in MPI for large-scale graph algorithms[J].Parallel Computing,2010,37(9):610-632.

[18] Patwary M A.Scalable parallel OPTICS data clustering using graph algorithmic techniques[C]//High Performance Computing,Networking,Storage and Analysis,2013:1-12.

[19] Cazals F,Karande C.A note on the problem of reporting maximal cliques[J].Theoretical Computer Science,2008,407(1):564-568.

[20] Regneri M.Finding all cliques of an undirected graph[R].Seminar—"Current Trends in Ie" Ws,Jun,2007.