

# 基于蜜场的 Openstack 安全系统

焦宏宇,何利文,黄俊

(南京邮电大学 计算机学院,江苏 南京 210046)

**摘要:**随着云计算的普及,大量采用 Openstack 的私有云出现在现今网络中,同时虚拟机被普遍用于部署公司业务,Openstack 上大量虚拟机的安全问题也变得日益严峻。蜜场作为主动安全防御的技术,既能为 Openstack 上部署的虚拟机带来安全保障,同时能记录下黑客的行为作为反向追踪依据。由于 Openstack 虚拟化网络与传统物理网络有很大的区别,所以根据 Openstack 虚拟化网络的特殊性设计出一个新型的蜜场系统。首先将网络攻击流量重定向与虚拟化紧密结合,将异常流量通过虚拟化网络重定向到蜜场中;其次将异常检测系统用于检测流量,增大了业务系统的安全性;最后根据虚拟机灵活配置的特性,设计出动态蜜罐部署系统。实验结果表明,该系统能够有效地检测出异常流量,并将其正确地重定向到蜜场中,同时在蜜场中的蜜罐上记录下黑客的攻击行为用于后续分析。

**关键词:**Openstack;蜜场;虚拟机;虚拟网络;重定向;蜜罐

**中图分类号:**TP302

**文献标识码:**A

**文章编号:**1673-629X(2018)10-0092-05

**doi:**10.3969/j.issn.1673-629X.2018.10.019

## Openstack Security System Based on Honeyfarm

JIAO Hong-yu, HE Li-wen, HUANG Jun

(School of Computer Science, Nanjing University of Posts and Telecommunications,  
Nanjing 210046, China)

**Abstract:** With the popularization of cloud computing, a large number of private clouds adopting Openstack appear in today's network. Meanwhile, virtual machines are widely used to deploy company business, so the security of a large number of virtual machines on Openstack is becoming increasingly serious. As an active security defense technology, Honeyfarm can not only provide security for virtual machines deployed on Openstack, but also record the hacker's behavior as the basis of reverse tracking. Because Openstack virtualized network is quite different from traditional physical network, a new Honeyfarm system is designed according to the particularity of Openstack virtualized network. Firstly, the network attack traffic redirection is closely combined with virtualization, and abnormal traffic is redirected to Honeyfarm through virtualized network. Secondly, the abnormal detection system is used to detect the flow, which increases the security of the business system. Finally, the dynamic Honeypot deployment system is designed according to the flexible configuration of the virtual machine. The experiment shows that the system can detect the abnormal flow effectively and redirect it to the Honeyfarm correctly. Meanwhile, the hacker's attack behavior is recorded on the Honeypot in the Honeyfarm for subsequent analysis.

**Key words:** Openstack; Honeyfarm; virtual machine; virtual network; redirection; Honeypot

## 0 引言

近年来,云计算、大数据被社会各界广泛关注并快速发展。作为提供 ISSA 服务的开源云平台 Openstack<sup>[1]</sup>也被很多公司作为构建私有云的管理平台。随之而来,Openstack 的安全问题也日益严峻。由于 Openstack 本身并没有有效的安全机制防止网络上的攻击,会造成很大的安全隐患。蜜场技术作为网络安

全领域的核心技术,结合了蜜罐技术<sup>[2]</sup>和异常检测机制,在大型分布式网络中集中部署蜜罐,对各个子网安全威胁进行收集。但是蜜场系统受安全性、性能和保真度这三个因素的相互制约而无法广泛应用。基于蜜场技术的 Openstack 安全模块研究就是在这种背景下进行的,它不仅为私有云提供了更高的安全性,而且解决了蜜场系统搭建的安全性、保真度与性能这三个相

收稿日期:2017-11-17

修回日期:2018-03-06

网络出版时间:2018-05-28

**基金项目:**江苏省“六大人才高峰”高层次人才项目(2014-WLW-005);南京邮电大学引进人才科研启动基金(NY212012);中兴通讯研究基金(项目批准号-2015 外)

**作者简介:**焦宏宇(1994-),男,硕士研究生,研究方向为云计算应用技术;何利文,博士,南京邮电大学特聘教授,CCF 会员(28059M),研究方向为网络与信息安全、图像处理、云计算和大数据的技术与应用等。

网络出版地址: <http://cnki.net/kcms/detail/61.1450.TP.20180525.1558.040.html>

互制约因素带来的难题,让蜜场系统具有了更高的实用价值。

但是目前很多的蜜场都是用于传统物理网络,对于虚拟化网络中的应用不是很成熟。文献[3]介绍了通过构建 SDN 蜜网,利用 OpenDaylight 控制器良好的可扩展性和可控性,解决了传统蜜网难以实现流量控制、部署不便、调整复杂等问题。文献[4]建立了一个称为 Potemkin 的原型蜂窝系统,利用虚拟机,激进的内存共享以及后期绑定资源来实现这一目标。虽然还不成熟,但 Potemkin 在实际测试中模拟了超过 64 000 个互联网蜜罐,仅仅是使用少量的物理服务器。

1 网络攻击流量重定向

重定向<sup>[5]</sup>是蜜场系统中的关键组成部分。它的作用是将进入 Openstack 系统的所有流量进行分类,并将不同的流量重定向到不同的系统中去。首先,监听非业务地址以及端口,非业务的流量会直接重定向到蜜场中;其次,业务流量会交由异常检测系统进行分析,检测到的异常流量会直接重定向到蜜场中;最后,由异常检测系统检测出的正常流量才会转发到业务系统中。但是现有的网络攻击检测与网络流量的重定向机制,存在较多不足,无法很好地满足蜜场的需要。同时现有的重定向机制无法很好地工作在 Openstack 虚拟化的网络环境中<sup>[6]</sup>。

1.1 网络攻击检测系统

黑客进行攻击之前,一般都会进行网络扫描。网络扫描通常扫描的是一个目的 IP 地址段,这些地址段中有些 IP 是未被使用的,端口扫描通常扫的是已有 IP 地址的主机上的大量端口,有些端口并未使用,即未开启相应服务。对于非活跃 IP 地址以及非开放端口的访问,统称为非业务访问,这些访问通常是攻击流量。对于非业务流量的重定向,可以引诱攻击这对蜜罐进行攻击。如果黑客通过某种方法得知业务系统地址,根据业务系统的漏洞对服务进行攻击,可达到一定的目的。对业务子网中活跃主机上开放服务的访问,叫做业务访问,也包含各种各样的攻击。

所以,针对子网的网络攻击流,不仅包含非业务流量,也包含业务流量。因此网络攻击检测机制包含了对于非业务流量以及业务流量的检测机制。

1.1.1 非业务访问监听模块

非业务访问监听,需要确定哪些是非业务的流量,一般体现为未使用的 IP+Port,需要去探测业务子网中哪些地址和端口是未使用的。这两个参数主要体现在虚拟机是不是运行状态以及运行状态的虚拟机上开启的端口有哪些。

对于虚拟机的状态,在传统网络中或使用 Ping 进

行存活状态检测,而在 Openstack 中所有虚拟机的状态都会由系统检测记录到相应的数据库中,可以直接拉取子网内虚拟机状态信息,分析出哪些 IP 地址是运行中主机使用的。

对于运行中虚拟机的端口是否开放,可以先拉取虚拟机安全组配置,将放行的端口取出,对应运行中主机放行的端口进行主动探测,将探测出来的运行主机对应的开放端口记录下来。

以上两个机制可以获取到子网业务地址与端口,根据这些信息建立虚拟机开放服务信息库。非业务监听模块如图 1 所示。

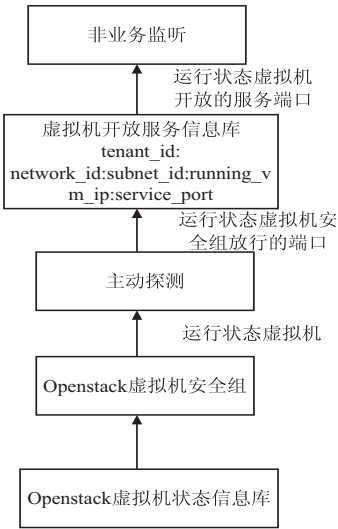


图 1 非业务监听模块

1.1.2 针对业务访问的异常检测模块

业务访问中很可能会包含各种各样的攻击,对这些攻击进行检测的有效方式是采用入侵检测技术,入侵检测技术可以检测出某些未知攻击。在业务子网中部署基于支持向量机(SVM)的入侵检测系统<sup>[7]</sup>,经过模拟仿真实验验证选取最佳的 SVM 参数。当入侵检测系统检测出异常流量后,对这股流量需要重定向到蜜场中。同时异常检测系统会将攻击信息记录到事件数据库中,其中包括最重要的信息是攻击源的 IP 和 Port,将该信息其存入黑名单列表中,并设置一个超时时间,在超时时间内该 IP:Port 发来的流量都会被视为攻击流量直接重定向到蜜场中,不再经过异常检测系统,减轻了系统压力。

1.2 网络流量重定向系统

Openstack 虚拟化网络与物理网络存在很多不同之处。物理网络是由传统物理网络设备和物理服务器组成,数据包由网络设备进行转发。而 Openstack 虚拟化网络较为复杂,Openstack 所有的外部网络的流量和 Openstack 内同租户跨网段的流量都是要经过 neutron 节点,通过不同租户命名空间的 router 进行路由的。该组件会基于每个租户虚拟化出基于不同命名空

间(namespace)的路由器(router),所有该租户下的虚拟机去往外网的通信都会在该router上面做NAT,同租户下的跨网段通信也由该router进行路由。由于Openstack网络的特殊性,物理网络的重定向设计不适合Openstack的网络模式。

文中采用重定向器作为中间设备,桥接业务系统租户命名空间router和蜜场网络租户命名空间router,进行重定向以及相关的路由。当一个新的租户网络被创建时,Openstack在该租户网络所在neutron节点上,创建相应命名空间的router,同时会新建一个redirect桥接到该新建租户的router和蜜场租户的router上。redirect会对不同类型的数据包进行相关修改,不同租户命名空间的router负责相关数据包的路由,具体流程如图2所示。

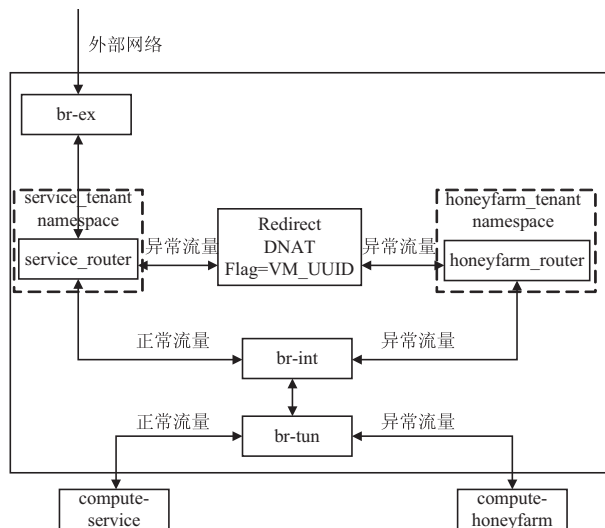


图2 网络流量重定向系统

1. 当外部流量进来之后会到达业务系统租户(service\_tenant)命名空间下的service\_router,service\_router会将所有流量都转发到redirect上;

2. redirect根据流量分类进行相关操作,如果是非业务流量直接DNAT发给honeyfarm\_router;如果是针对业务系统的攻击流量会进行DNAT发给honeyfarm\_router;如果是业务系统的正常流量,会直接转发给service\_router,不做任何操作;

3. 同时redirect会给非正常业务流量打上相应标记<sup>[8]</sup>,标记该流量是针对Openstack业务系统中的哪台虚拟机的流量。因为VM的UUID可以唯一标识一台虚拟机,所以采用UUID来标识该流量,以便针对业务系统的攻击流量转发到蜜场网关,蜜场网关可以结合这个标记和自身的相关数据库进行转发;

4. 所有进入蜜场的流量回包会经过蜜场系统租户(honeyfarm\_tenant)命名空间下的honeyfarm\_router,该router将流量发给redirect,redirect对流量进行SNAT,发给service\_router进行路由;

5. 所有正常的业务流量,直接由service\_router路由给业务系统,回包也是由service\_router进行路由。

## 2 蜜场系统

利用Openstack中每个租户隔离的特性,将蜜场单独放入一个租户中,使它逻辑上与其他业务系统所在的租户隔离。蜜场系统应该具备数据安全控制的机制、数据捕获机制以及动态部署蜜罐的机制<sup>[9]</sup>。

### 2.1 数据控制安全策略

当蜜场内的蜜罐机器被黑客攻陷后,为了防止黑客使用这些蜜罐作为跳板向外攻击别的节点,造成二次危害,在蜜场内做安全控制是非常有必要的<sup>[10]</sup>。蜜场的目的是吸引黑客的攻击,所以进入蜜场的流量是不能限制的,只需要限制出向的流量即可。所有从蜜场中出去的流量都会被认为与黑客交互的流量,都需要进行限制。一般会将单位时间内出向的流量大小以及出向的连接数限制到一个合理的值。这些参数可以直接在蜜场网关的iptables上进行统一配置,其可以限制多种协议的连接数以及流量大小,比如TCP、UDP、ICMP等。数据控制安全策略的配置文件为rc.firewall,如在rc.firewall设置规则:

```
##set the connection outbound limits for different protocols
SCALE="day" #记录单位,也可以是秒、分、小时等
TCPRATE="15" #每记时单位中允许的TCP连接数
UDPRATE="20" #每记时单位中允许的UDP连接数
ICMPRATE="50" #每记时单位中允许的ICMP连接数
OTHERRATE="15" #每记时单位中允许的其他IP新协议连接数
```

```
STOP_OUT="no" #如果不想允许任何向外连接,可以将这个参数设为"yes"
```

通过此规则设置,可以较好地限制对外连接数量。

### 2.2 数据捕获机制

部署蜜场最主要的目的是记录攻击者的相关数据,比如攻击行为、攻击数据包,然后用收集到的这些数据进行分析和反向追踪。所以如何收集这些数据也至关重要。

数据捕获机制是在蜜场网关和蜜罐上捕获数据的。蜜场网关是所有数据出入蜜场的必经之地,所以蜜场网关上捕获的数据是最全面的。在蜜场网关利用iptables可以记录所有经过蜜场网关的连接,同时给不同的流量打上不同的标记,使用tcpdump抓包工具抓取相应标记的数据包,以便后续分类和分析<sup>[11]</sup>。在蜜罐上通过运行sebek来记录攻击者的攻击行为,比如击键记录、所读取的数据以及运行了哪些程序。

### 2.3 动态蜜罐部署机制

动态部署蜜罐最关键的一点是怎样学习周围的网络环境。传统的方法<sup>[12]</sup>有两种,方法一是积极主动地



进行探测,从而确定周围存在一些什么样的操作系统。然而这种方法存在一些不足。首先,它引入了额外的网络活动,不可避免会影响到网络带宽;其次,为能够了解网络的变化情况,必须持续对网络进行扫描,这可能使得系统中的某些服务甚至整个服务被关闭。方法二是采用被动采集的方法获取周围的网络环境。这种方法基于每种操作系统的 IP 协议栈不同的特点,缺点在于不能精确判断出网络环境,操作系统众多,有些操作系统仅通过数据包内的某些字段是判断不出来的。而且上述两种方法都是针对物理网络的,对于 Openstack 这种多租户隔离的网络是不行的。所以采用直接从 Openstack 虚拟机状态数据库中获取虚拟机镜像信息的方法较为合适。

2.3.1 如何探测网络环境

根据 Openstack 的特点,它作为一个对虚拟机、虚拟网络等的管理平台,会记录下很多虚拟机相关的数据到数据库中,比如虚拟机的状态信息、创建虚拟机的镜像等。在蜜场网关上监听虚拟机相关操作的 nova-api 接口,根据不同的调用参数做出相应的操作。如果是新建虚拟机的调用,一旦有新建虚拟机的操作,就会立即根据新建虚拟机使用的镜像,在蜜场中创建相同的操作系统的虚拟机作为 honeypot,该 honeypot 的 UUID 与业务虚拟机的 UUID 的对应关系会存到 honeypot\_vm 的数据库中;如果有删除的操作,会立即删除相应的 honeypot 同时更新 honey\_vm 数据库;如果有关机、挂起或者扫描到 vm 状态不为运行中,这时会在数据库中给该 vm 对应的条目设置一个计时器,如果该计时器到期之前 vm 状态还不是运行中,就会删除该 vm 对应的 honeypot 以及数据库条目。同时,蜜场网关会定期对 Openstack 的虚拟机状态信息数据库进行扫描,如果有些业务虚拟机的 UUID 在 honey\_vm 的数据库中不存在,就会根据该虚拟机的镜像在 honeyfarm 中创建相应的蜜罐。这是针对同一时间有大量的虚拟机新建操作,可能无法及时创建相应的蜜罐的问题,采用定期扫描的方法进行补充。

2.3.2 蜜罐系统模板

根据 Openstack 相关的状态信息去创建 honeypot,相对于去探测或者抓取虚拟机发送的数据包判断更为准确快速<sup>[13]</sup>,同时不会占用大量的网络带宽,也不需要耗费抓取数据的资源。但是根据系统镜像创建的 honeypot 有个缺点,就是其上没有业务服务,不能很好地吸引和留住黑客。所以,采用虚拟机快照的方式去创建 honeypot,当虚拟机创建之后定期对虚拟机进行快照,利用快照去创建蜜罐,这样可以复制虚拟机的部分业务服务,使得蜜罐更像真实业务系统,更为真实,提高与黑客的交互数据度。

3 基于蜜场的 Openstack 安全系统设计

将蜜场和 Openstack 进行有机结合,设置出一个基于虚拟化网络的新型蜜场系统。其中,网络攻击检测系统中的非业务流量监听模块负责监听非业务流量,异常检测模块负责对业务流量进行异常分析;网络流量重定向系统中的重定向模块负责对于非业务流量监听模块监听到的流量和异常检测模块检测出的异常流量进行重定向,将流量重定向到蜜场中进行交互,路由模块负责正常流量和重定向后的攻击流量的路由;蜜场系统中的动态蜜罐部署机制根据业务系统的虚拟机状态动态地配置蜜罐以及根据虚拟机的快照进行蜜罐的创建。基于蜜场的 Openstack 安全系统设计框架如图 3 所示。

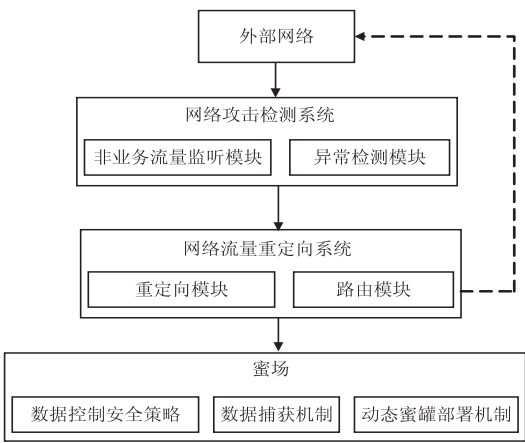


图 3 基于蜜场的 Openstack 安全系统设计

系统的工作流程如下:网络攻击检测系统进行流量分析,将流量分类;由重定向系统将分类后的流量进行重定向,正常流量路由到业务系统,攻击流量路由到蜜场;蜜场中的蜜罐负责和外部攻击进行交互;根据虚拟机状态和快照,动态地部署蜜罐系统。

4 实验及结果分析

在 Openstack 上部署改进的蜜场环境<sup>[14]</sup>,创建一个小型业务租户与子网作为实验平台。蜜场环境由一个蜜场网关以及蜜罐系统组成;业务子网由重定向和若干业务主机组成,每个业务主机上有若干对外开放的服务,可通过 Internet 访问。在重定向上允许非业务探测、网络入侵检测、网络流量重定向和日志记录系统,在蜜场网关上启动动态蜜罐部署的服务、Firewall 以及流记录器。经过一段时间的运行,各子系统工作正常,实验结果及分析如下:

重定向的网络流正确地到达了蜜场环境。经过对比,在重定向网关的流信息库中,被重定向的流(非业务流量、异常流量)在蜜场网关的流记录中都能找到,反之亦然,说明重定向系统是正常工作的。

蜜场中的蜜罐以及 honeypot\_vm 数据记录均正

确。经过对比,在 honeypot\_vm 数据库的记录和相关的蜜罐均能正确匹配,并且蜜罐的系统模板与服务系统的快照一样,说明动态蜜罐部署的机制是正常的。

根据蜜场网关以及蜜罐上监测系统的日志记录得到一些攻击数据。图 4 展示了 24 小时内被重定向经过蜜场网关的网络流量统计图,图 5 是 24 小时内 Openstack 虚拟化网络内的各类型网络流量统计对比图。可以看到:有较大比例的网络流量为非业务访问被重定向到蜜场;小部分流量为未知源的攻击流;少部分流量为已知源攻击流,也被重定向到蜜场;还有高度可疑的蜜罐对 Internet 访问流,说明攻击者对蜜罐攻击成功。

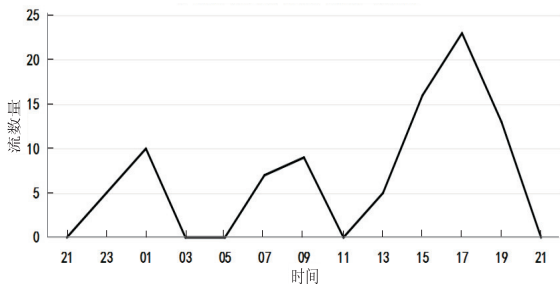


图 4 24 小时内经过蜜场网关的流量统计图

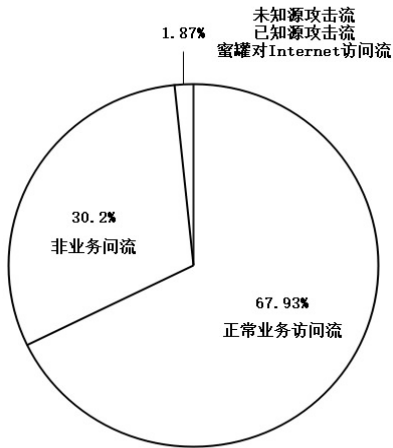


图 5 24 小时内各类型网络流量统计对比图

系统潜在问题:时间延迟。当未知攻击源实施对业务系统的首次攻击,依次经过异常检测系统检测,重定向和蜜场网关分发流量到蜜罐,这些动作均有短时间延迟。

## 5 结束语

对面向虚拟化环境的蜜场进行了研究,结合 Openstack 虚拟网络和 Openstack 对虚拟机状态的记录,设计出了针对虚拟化环境中的重定向实现机制以

及动态蜜罐部署机制。实验结果表明,该新型蜜场系统很好地解决了虚拟化环境的安全问题。下一步的工作将是在蜜场环境中对重定向的攻击流进行取证分析,这涉及到跟踪攻击行为和攻击取证等一系列技术,在这些技术研究的基础上,最终将实现虚拟化环境中基于蜜场的网络主动安全防护系统。

## 参考文献:

- [1] KUMAR R, GUPTA N, CHARU S, et al. Open source solution for cloud computing platform using OpenStack[J]. International Journal of Computer Science and Mobile Computing, 2014, 3(5): 89-98.
- [2] 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.
- [3] 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, 18(3): 79-84.
- [4] VRABLE M, MA J, CHEN J, et al. Scalability, fidelity, and containment in the potemkin virtual honeyfarm[J]. ACM SIGOPS Operating Systems Review, 2005, 39(5): 148-162.
- [5] CHEN J, MCCULLOUGH J, SNOEREN A C. Universal Honeyfarm containment[M]. [s. l.]: [s. n.], 2007: 213-220.
- [6] JIANG Xuxian, XU Dongyan, WANG Yimin. Collapsar: a VM-based honeyfarm and reverse honeyfarm architecture for network attack capture and detention[J]. Journal of Parallel and Distributed Computing, 2006, 66(9): 1165-1180.
- [7] 武小年,彭小金,杨宇洋,等. 入侵检测中基于 SVM 的两级特征选择方法[J]. 通信学报, 2015, 36(4): 19-26.
- [8] KREIBICH C, CROWCROFT J. Honeycomb: creating intrusion detection signatures using honeypots[J]. ACM SIGCOMM Computer Communication Review, 2004, 34(1): 51-56.
- [9] 石乐义,李 婕,刘 昕,等. 基于动态阵列蜜罐的协同网络防御策略研究[J]. 通信学报, 2012, 33(11): 159-164.
- [10] 项国富,金 海,邹德清,等. 基于虚拟化的安全监控[J]. 软件学报, 2012, 23(8): 2173-2187.
- [11] 胡双双. 基于蜜网的攻击行为分析[D]. 北京:北京邮电大学, 2015.
- [12] 向全青. 基于网络扫描技术的动态蜜罐网络设计与实现[J]. 信息技术, 2013(6): 157-161.
- [13] JAIN P, SARDANA A. A hybrid honeyfarm based technique for defense against worm attacks[C]//World congress on information and communication technologies. Mumbai, India: IEEE, 2011: 1084-1089.
- [14] 李小宁,李 磊,金连文,等. 基于 OpenStack 构建私有云计算平台[J]. 电信科学, 2017(9): 1-8.