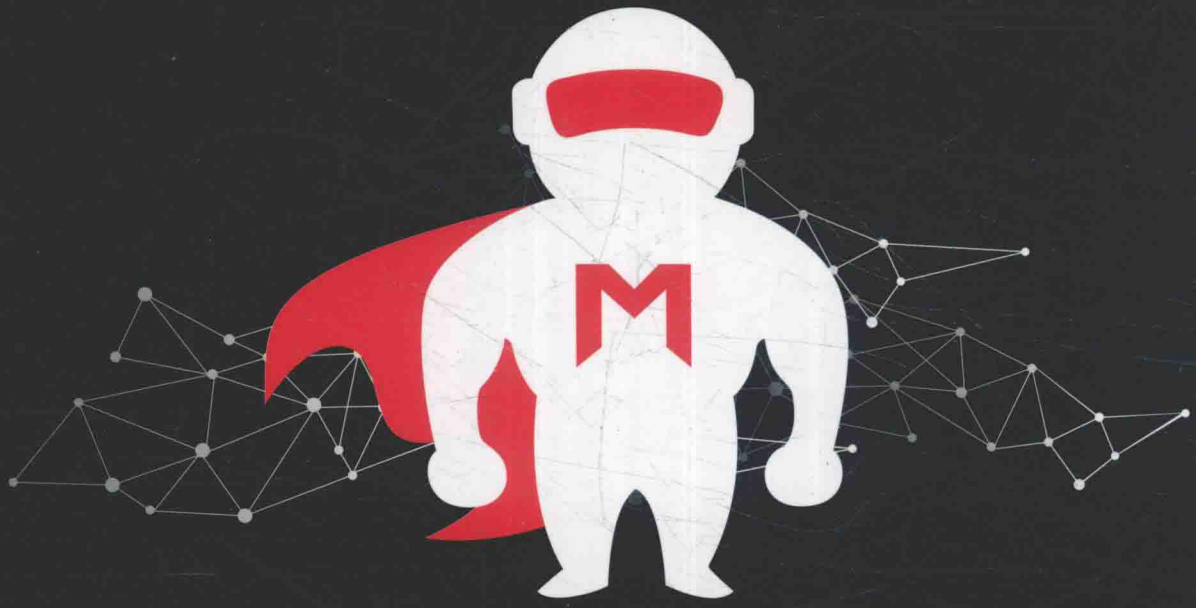
Broadview
www.broadview.com.cn

安全技术大系

云虚拟化安全攻防实践

唐青昊 毛大鹏 著

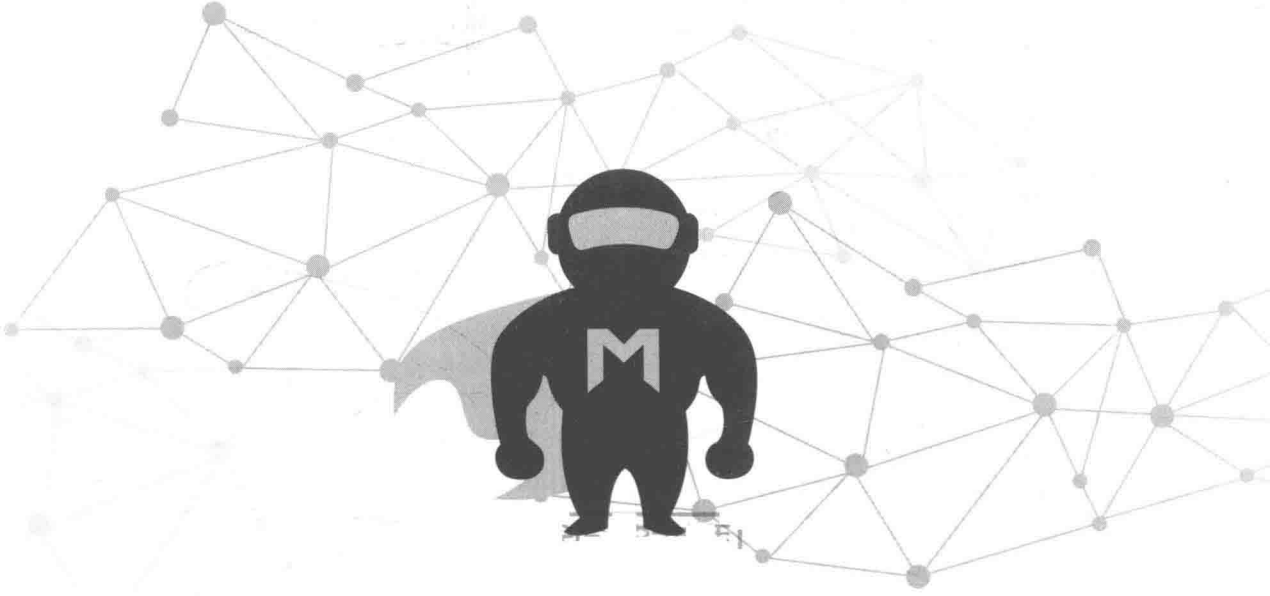


中国工信出版集团
電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

安全技术大系

云虚拟化安全攻防实践

唐青昊 毛大鹏 著



電子工業出版社
Publishing House of Electronics Industry
北京•BEIJING

内 容 简 介

2017 年，全世界云计算市场已经达到千亿美元量级。云计算因其形态不断丰富而在企业、政府的现在和未来布局中都占据着重要位置。作为云生态的关键部分，Hypervisor 使人类具备了对计算机硬件资源更细粒度的掌控能力。主流的 Hypervisor 产品，如 KVM、Xen、Docker 等已经主导了现有公有云和私有云市场。了解这些 Hypervisor 产品的安全知识，掌握对这些产品的分析方法，无论是对于安全领域的爱好者，还是云计算行业的从业人员都是大有裨益的。

本书涵盖多种 Hypervisor 产品的调试分析过程，通过抽丝剥茧的方式深入剖析了 Hypervisor 安全攻防技术，重点介绍了 Hypervisor 漏洞的利用方法和防护手段。希望以此书推动整个云生态的安全建设，为构筑未来互联网的安全基石做一些微小的工作。

图书在版编目（CIP）数据

云虚拟化安全攻防实践 / 唐青昊，毛大鹏著. —北京：电子工业出版社，2018.4
（安全技术大系）
ISBN 978-7-121-33748-2

Ⅰ. ①云… Ⅱ. ①唐… ②毛… Ⅲ. ①计算机网络－网络安全 Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字(2018)第 036189 号

策划编辑：郑柳洁
责任编辑：葛　娜
印　　刷：三河市鑫金马印装有限公司
装　　订：三河市鑫金马印装有限公司
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　邮编：100036
开　　本：787×980　1/16　印张：21.75　字数：388 千字
版　　次：2018 年 4 月第 1 版
印　　次：2018 年 4 月第 1 次印刷
定　　价：69.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888，88258888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

本书咨询联系方式：010-51260888-819，faq@phei.com.cn。

好评袭来

虚拟化系统是云计算的核心，对这个领域的安全攻防研究非常有意义。本书结合了作者多年的研究和实践，深入浅出，值得一读。

腾讯云副总裁　黎巍

虚拟化安全是云安全的重要核心，对于普通安全从业者往往显得晦涩难懂，但又随着网络攻防愈演愈烈而愈发重要。青昊和大鹏的这本书全面介绍了主流虚拟化系统的攻防对抗技术，给这个深奥的领域绘制了一份重要的地图，为有志于在云安全方向进行深入研究的同行提供了难得的指南。

百度首席安全科学家，北京大学客座教授，CISO发展中心理事长　韦韬

随着云计算的兴起，虚拟化安全越来越重要。本书聚焦在虚拟化安全攻防，内容丰富、通俗易懂，是学习虚拟化安全不可多得的佳作。

腾讯安全云鼎实验室　董志强

云计算是互联网行业中的新兴业态，头部厂商的技术表现为封闭性，基本不对外公开细节，安全研究者们想切入有一定的门槛，而本书正好开辟了一条蹊径，帮助大家理解云计算中最广泛的底层技术——虚拟化的安全，对有志于从事云安全领域的读者来说是性价比极高的参考读物。

美团点评集团安全部高级总监　赵彦

云计算以摧枯拉朽之势变革传统IT，云安全也在变革传统安全。虚拟化与云计算引入了新的安全风险，随着云计算的普及，这种风险随之放大。但受制于现状，懂云计算又懂云安全的复合人才远无法满足要求。而本书既覆盖了虚拟化技术的核心基础知识，又包含了云安全攻防分析内容，“鱼与熊掌兼得”，是云安全领域值得推荐的好书。

360企业安全集团云安全事业部总经理　刘浩

前言

在过去数年中，云计算给互联网带来了巨大变革，在可预见的五年中，云计算依然会影响互联网领域的方方面面。全社会对公有云和私有云的大规模应用，使得过去分散的数据存储和代码运算在云计算场景下更为集中，因此保证云计算平台的安全稳定运行就成为各个云服务供应商的基本诉求。

在云计算平台所面临的各种安全风险中，来自于虚拟机内部的威胁一直被忽视。这种类型的威胁通常会导致云计算平台的内部网络被侵入、核心数据被窃取，甚至会导致该云计算平台的众多租户受到影响。为了应对这种来自于云虚拟化领域的威胁，美国的Google公司、Microsoft公司，以及中国的奇虎360公司、阿里巴巴集团、腾讯公司在过去的两年时间中都投入了安全团队进行研究并不断公开最新成果。通过这些公司的共同投入，云虚拟化安全的价值被更多的公司所认可，可喜的是众多云供应商已经开始采购云虚拟化安全的企业级防御产品。

作为云虚拟化安全攻防研究项目的直接参与人员，在过去两年中，我看到有更多的国际大型安全会议开始接受与云相关的议题，也看到了在Pwn2Own这个安全界的奥运会比赛中加入了虚拟化平台攻击项目。这些正在发生的变化不断验证虚拟化安全对云生态安全的重要性。因此，对于云计算生态中的从业人员、安全行业的从业人员，以及关注互联网历程的每一个人，了解云虚拟化安全将是有趣的且是有必要的。

《云虚拟化安全攻防实践》这本书中包含了在2015—2017年我在多个国际安全会议上分享的议题，以及我在完成Pwn2Own 2017 VMware Workstation比赛的过程中积累的方法。相信这些核心内容可以帮助读者快速了解云虚拟化安全的精髓。

本书的前6章由唐青昊完成，第7章由毛大鹏完成。本书的第1章介绍了虚拟化技术的基础概念；第2~6章分别对Docker、VMware Workstation、QEMU和KVM、Xen、Hyper-V这几种主流的虚拟化系统的脆弱性进行了分析；第7章介绍了虚拟化系统的

防御技术。本书不但为行业从业人员准备了大量深入而精彩的虚拟化系统代码分析、漏洞代码分析，而且为毫无云计算基础的读者提供了相当篇幅的分析方法介绍、基础工具介绍。希望这种深浅搭配的内容可以满足读者的需求。

在本书成书之际，感谢为本书面世而不辞辛劳的郑柳洁编辑，感谢提出云计算安全方向的奇虎360公司技术总裁谭晓生先生，感谢一直以来在背后提供支持的家人。

唐青昊

目录

第 1 章　认识 Hypervisor

作为云生态的核心，Hypervisor使人类具备了对计算机硬件资源更细粒度的掌控能力。在Hypervisor被应用之前，服务器都是由操作系统中的进程直接使用CPU、内存、硬盘等硬件资源的，由于企业业务划分及地域性因素，绝大多数的计算或者存储资源未被100%使用，造成极大的浪费。Hypervisor的出现，一举解决了这个问题，通过在过去分散的服务器中部署Hypervisor，将全部硬件资源进行集约化管理。假设有一台配置24核心、128GB内存、12TB硬盘的服务器，在部署单机版本Hypervisor之后，可以根据业务用途切分成尽可能多的虚拟机，如32台配置4GB内存、200GB硬盘的虚拟机。Hypervisor自20世纪70年代开始出现在学术论文中，历经在大型机、PC、服务器上多年的技术演进，目前体系已经相当完善。

读者可通过本章了解云计算的起源、Hypervisor在云计算场景中扮演的角色，Hypervisor的分类，以及Hypervisor所使用到的虚拟化技术。在后续章节中将对各主流Hypervisor进行安全性分析。

1.1　云计算的起源

早在2006年，亚马逊就推出了亚马逊云计算服务（AWS，Amazon Web Service），到2016年第四季度，该服务净销售额已经达到24亿美元。在过去的12年间（2006—2017年），云计算概念不断延展，深入各个领域的方方面面，从最初仅在美国顶级互联网公司中应用，发展到目前被全球政府、企业广泛接受。毫无疑问，围绕云计算概念，已经形成一个完整的生态系统。云计算生态的出现，是计算机技术变革和互联网商业模式发展的共同结果，符合人类对资源精细化管控的趋势。

本节将介绍构筑起目前市场格局的关键阶段和典型产品，帮助读者建立起对云计算生态的初步印象。

1.1.1 分时计算

云计算具体依赖的底层架构均由已存在多年的技术演化而来。计算机在诞生之初，是非常昂贵的大型设备，在任何时间只能为单个用户运行单个程序。随着计算机运行速度的提升，同时支持多个用户的系统成为必然。20世纪60年代，分时计算的概念应运而生，即每个用户的程序的运行状态可以被实时保存，并按照时钟快速切换。分时计算的本质是将计算机资源作为基础设施，可以看作云计算的早期版本。

1.1.2 虚拟化

“虚拟化[1]（Virtualization）”一词最早出现在20世纪60年代，指一种隐藏了物理特性的抽象的计算技术，也被称为“硬件虚拟化”“平台虚拟化”“服务器虚拟化”。控制虚拟化的软件被称为“虚拟机管理程序”（Hypervisor）。使用虚拟机管理程序可以在特定的硬件平台上创建模拟的计算机环境，即虚拟机（Virtual Machine），而特定的硬件平台被称为“宿主机”。一般情况下，在宿主机和虚拟机上均会运行操作系统软件，以方便操作计算资源。

1.1.3 Web 2.0 和分布式文件系统

Web 2.0的概念最早出现在21世纪初，相对于人们只能被动观看的Web 1.0网站，Web 2.0网站鼓励用户在虚拟社区中进行交互并创造内容，例如国内的新浪微博、百度百科就是典型的Web 2.0网站。

Web 2.0为互联网数据[2]带来了几何级数的增长，分布式文件系统被设计出来用于更方便地扩展存储。不同于NFS、Ext等本地系统，分布式文件系统通常使用网络协议进行文件块访问操作。分布式文件系统拥有和本地文件系统同样丰富的接口，可以实现对文件的枚举、读取、写入、删除等操作。

---

1 参考https://en.wikipedia.org/wiki/Hardware_virtualization

2 参考https://en.wikipedia.org/wiki/Clustered_file_system

1.1.4 云计算元年

2006年可以被视为云计算元年，2006年8月9日在搜索引擎战略会议（Search Engine Strategies Conference）中，谷歌公司CEO艾瑞克（Eric Schmidt）首次提出“云计算”一词，如图1-1所示。

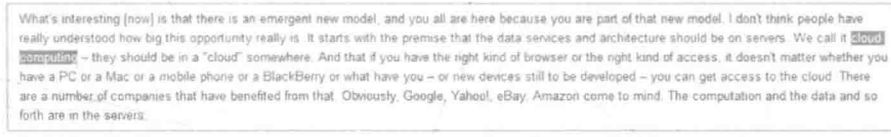

What's interesting [now] is that there is an emergent new model, and you all are here because you are part of that new model. I don't think people have really understood how big this opportunity really is. It starts with the premise that the data services and architecture should be on servers. We call it cloud computing – they should be in a "cloud" somewhere. And that if you have the right kind of browser or the right kind of access, it doesn't matter whether you have a PC or a Mac or a mobile phone or a BlackBerry or what have you – or new devices still to be developed – you can get access to the cloud. There are a number of companies that have benefited from that. Obviously, Google, Yahoo!, eBay, Amazon come to mind. The computation and the data and so forth are in the servers.

图1-1 艾瑞克首次提出“云计算”[1]

同年8月24日，亚马逊公司发布即将推出弹性计算云（Elastic Compute Cloud，EC2）beta版本的公告（如图1-2所示），标志着云计算概念第一次被应用在商业服务中。在这份公告中，“可伸缩的计算和存储”这个标志性的特点首次被提及。


Announcing Amazon Elastic Compute Cloud (Amazon EC2) - beta

Posted On: Aug 24, 2006

Amazon Elastic Compute Cloud (Amazon EC2) is a web service that provides resizable compute capacity in the cloud. It is designed to make web-scale computing easier for developers. Just as Amazon Simple Storage Service (Amazon S3) enables storage in the cloud, Amazon EC2 enables "compute" in the cloud. Amazon EC2's simple web service interface allows you to obtain and configure capacity with minimal friction. It provides you with complete control of your computing resources and lets you run on Amazon's proven computing environment. Amazon EC2 reduces the time required to obtain and boot new server instances to minutes, allowing you to quickly scale capacity, both up and down, as your computing requirements change. Amazon EC2 changes the economics of computing by allowing you to pay only for capacity that you actually use.

图1-2 亚马逊公司推出弹性计算云服务

1.1.5 云计算在中国

中国最早进军云计算领域的大型互联网企业是阿里巴巴公司和新浪公司。2009年9月，阿里云在杭州成立，其云产品在2010年的“双11”在线购物促销活动中得到使用。同年11月，新浪公司推出云计算产品SAE（Sina App Engine），允许互联网产品的开发人员使用新浪提供的软件开发工具包开发网页程序。

1 引用自https://www.google.com/press/podium/ses2006.html

1.1.6 典型的云计算产品

目前构建云计算生态的关键产品占据了市场的绝大部分份额，它们的成长史就是并不长的云生态历史，它们的规划也是云计算生态将要到达的未来。

这些扮演关键角色的产品包括亚马逊公司的AWS，一款被全球广泛使用的公有云计算服务；NASA和Racespace共同发起的OpenStack项目，提供了开源的云计算管理平台；Docker公司的Docker产品，一款流行的开源应用容器引擎；传统PC巨头微软公司推出的公有云平台Azure和个人虚拟系统产品Hyper-V；VMware 公司推出的面向私有云的ESXi/ESX产品和个人虚拟系统VMware Workstation产品。下面来详细介绍这些产品。

亚马逊公司提供的AWS是世界上最早发布、最早投入使用的公有云服务平台，它的中文官网地址是https://aws.amazon.com/cn/，网站首页如图1-3所示。

图1-3 AWS官网部分截图

AWS对云计算的定义是，一种通过互联网交付的IT资源与应用交付方式[1]。基于这个定义，在AWS的漫长发展历史中，所提供的关键服务包括Amazon Elastic Compute Cloud（简称EC2，2006年8月发布的资源可延展的虚拟计算服务）、Amazon Simple Storage Service（简称S3，2006年3月发布的云存储服务）和其他服务，涉及负载均衡、

1 https://wenku.baidu.com/view/ef0bf608fab069dc51220152.html

数据库、数据分析、应用服务、管理部署、容器等领域。EC2部署了大量定制后的 Xen 虚拟机，从而可以帮助用户在短短几分钟内创建虚拟机（在AWS中称为instance，即实例）。EC2使用两种不同类型的数据存储方式，分别是本地存储和网络存储。S3是AWS解决海量数据存储的关键产品，用户可以通过网络接口访问S3。S3在稳定性和持久性方面性能卓越，发布至今，累计传输了达万亿规模的对象数据。AWS改变了传统的IT业务模式，将自建软硬件设施转化为购买在线服务。AWS的一大特点是按需付费，即用即付。AWS的定价方式和水电费相似，客户只需为所使用的服务付费，这样就省去了购买服务器、软件许可或者租赁设施的费用。

OpenStack是一个以IaaS模式部署的开源云计算软件平台[1]。与AWS不同，OpenStack并不是付费的产品或者服务，并且可以在官网（https://releases.openstack.org/）获取全部代码。OpenStack软件由NASA参与推出，目标是帮助用户提供可以在标准硬件上运行的云计算服务。在2010年首次推出后，主流操作系统如Ubuntu Linux、Debian、SUSE、Red Hat、Oracle Solaris、Oracle Linux逐步将其引入。在OpenStack的架构（如图1-4所示）中，包含了极丰富的组件，提供计算、存储、网络、身份认证等服务。这些组件都有单独的项目代码名称。OpenStack的界面是由Web程序实现的，它的代码名称是Horizon。用户在Web界面进行操作即可管理整个云，如开启虚拟机、配置网络等。OpenStack的计算组件又称Nova，用于管理虚拟机，用户可以使用该组件对虚拟机进行开启、关闭、重启、暂停、迁移、销毁、配置调整等操作。网络组件的代码名称是Neutron，用户使用该组件的接口即可定义云环境的网络结构，包括配置路由、DHCP、DNS等。存储组件的代码名称是Swift，用于进行对象存储和检索，比如存储镜像或者进行卷的备份等。OpenStack项目聚合了众多的先进“大脑”，并且获得了包括Dell、Cisco等多家巨头的支持，提供了多种云基础组件和各类功能强大的辅助组件（包括负载均衡、消息队列、服务部署等），打造了一艘开源云计算平台的“航空母舰”，在整个云生态发展过程中占据不可或缺的位置。

1 引用官网介绍

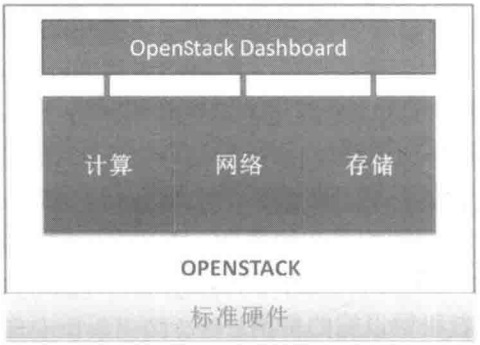


图1-4 OpenStack架构图

作为PC时代毫无争议的巨无霸，微软公司在云计算时代依然表现抢眼。2008年，微软即发布Azure服务进军云计算市场，2014年最终改名为Mircosoft Azure。Azure 在技术架构上是基于Mircosoft Hyper-V的。Hyper-V是微软云产品及云服务最核心的Hypervisor系统，最早出现在Windows Server 2008中。与微软以往的封闭风格略有不同的是，Hyper-V不但可以运行Windows操作系统的虚拟机，也在版本更迭的过程中支持一些Linux/UNIX操作系统。Hyper-V系统架构如图1-5所示[1]。Azure在计算、存储、数据库、网络、监控、安全这六个方面都提供了丰富的服务。其中包括许多具有特色的组件，如数据库方面的Azure DocumentDB，这是由微软实现的NoSQL产品，不同于主流的NoSQL产品MongoDB，DocumentDB以PaaS形式提供服务，而且借助Azure实现了优异的伸缩能力。Mircosoft Azure云服务，借助微软在x86平台积累的良好口碑，加上一如既往的卓越架构能力和产品互操作性，相信在云时代会延续霸主的角色。

1 图片引用自https://docs.microsoft.com/en-us/virtualization/hyper-v-on-windows/reference/hyper-v-architecture