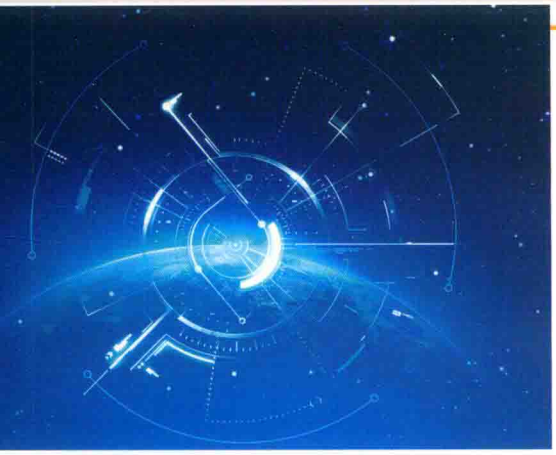

# 基于虚拟化的计算机网络安全技术

JIYU XUNIHUA DE
JISUANJI WANGLUO
ANQUAN JISHU

秦燊 · 著

延边大学出版社

# 基于虚拟化的计算机网络安全技术

秦燊 著

延边大学出版社

**图书在版编目（CIP）数据**

基于虚拟化的计算机网络安全技术 / 秦燊著. -- 延吉 : 延边大学出版社, 2019.9
ISBN 978-7-5688-7800-5

Ⅰ. ①基… Ⅱ. ①秦… Ⅲ. ①计算机网络－安全技术 Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字(2019)第 206456 号

**基于虚拟化的计算机网络安全技术**

---

著　　者：秦　燊
责任编辑：崔福顺
封面设计：延大兴业
出版发行：延边大学出版社
社　　址：吉林省延吉市公园路 977 号　　邮　　编：133002
网　　址：http://www.ydcbs.com　　E-mail：ydcbs@ydcbs.com
电　　话：0433-2732435　　传　　真：0433-2732434
制　　作：山东延大兴业文化传媒有限责任公司
印　　刷：天津雅泽印刷有限公司
开　　本：787×1092　1/16
印　　张：24.5
字　　数：350 千字
版　　次：2020 年 6 月第 1 版
印　　次：2020 年 6 月第 1 次印刷
书　　号：ISBN 978-7-5688-7800-5

---

定价：98.00 元

# 内容提要

本专著研究了如何基于 EVE-NG、VMware、OpenStack 等虚拟化技术搭建计算机网络安全实验平台，快速创建计算机网络安全防护联动实验环境，并在此基础上，从计算机网络硬件安全和软件安全两方面入手，全面研究了计算机网络所面临的安全问题，安全防护方法和网络渗透测试技术。本专著将基于虚拟化的计算机网络安全技术研究成果应用到了教学改革中，创建了基于虚拟化的网络安全项目场景和实验环境，该项目场景和实验环境可与笔者的著作（兼教材）《计算机网络安全防护技术》配合使用。

# 作者简介


秦燊，男，广西灵川人，广西师范大学教育硕士，主要研究方向为计算机网络安全、人工智能。本书为2017年度广西高校中青年教师基础能力提升项目《计算机网络安全防护技术研究》，项目编号2017KY1271和2019年度广西教育科学“十三五”规划资助经费重点课题（A类）《基于虚拟化技术的计算机网络课程教学改革实践研究》，课题编号2019A024的研究成果。

# 前　言

随着云计算、大数据时代的到来，虚拟化技术得到了广泛的应用，成为未来发展的一大趋势。虚拟化技术的发展有利于科研人员对计算机网络安全展开深入的研究，也有利于计算机网络安全专业知识的普及，为计算机网络安全等课程的教学及课内外实验带来了极大的便利。

计算机网络安全技术涉及计算机网络的硬件安全、软件安全、局域网安全、广域网安全等方方面面。要研究计算机网络安全的相关知识，实施相关实验，就要架设出小型局域网、大型广域网的硬件环境，并创建被攻击对象的软件环境，如 Windows 服务器靶机、Linux 服务器靶机、Web 服务器靶机等，创建对这些靶机实施网络安全渗透测试攻击的 Kali Linux 系统软件环境。在一台个人电脑上构造出这样规模的环境，在过去是不太现实的。过去利用虚拟化技术只能单独模拟服务器，或单独模拟路由器等网络设备，或单独模拟防火墙等安全设备，要将它们互联起来，组成一个项目环境，存在较大的困难。

应用新的虚拟化技术，则完美地解决了这个问题。本专著分别对个人电脑虚拟化和大型服务器虚拟化进行了研究。从个人电脑虚拟化的角度，本专著通过对新技术 EVE-NG 的研究应用，运用最新的虚拟化技术，整合了 VMware Workstation、EVE-NG、Kali Linux 网络安全渗透测试系统、Metasploit 网络安全渗透测试工具，Windows 服务器靶机，Linux 服务器靶机，DVWA 网站靶机，使科研人员、在校师生以及网络安全爱好者在一台

个人电脑上就能仿真出各种规模的计算机网络安全实验的环境，创建功能强大的仿真虚拟环境，创建出以前无法搭建的仿真项目实训环境，让科研人员的研究及师生的项目实践不再受网络设备和实验场所的限制，无论何时、何地，只要有电脑就可以自己建立虚拟网络实验室，研究和运用最新的、最实用的知识。除了对个人电脑虚拟化在网络安全技术上的应用研究，本专著还探讨了为大型服务器搭建 OpenStack 云计算 IaaS 架构平台的方法及应用，基于个人电脑虚拟化的网络安全技术迁移到大型服务器上，能服务于更多用户，满足大量科研人员进行科学研究或全班师生进行教学实训的需求。

通过虚拟化技术 EVE-NG 构建的实验环境支持厂商的虚拟化产品，如安全设备、网络设备等产品，是由厂商采用虚拟化技术设计实现并在现实中销售与应用的虚拟化产品，并非模拟设备。将它们免费用于实验时，仅有速度上的限制，并无功能上的限制，采用这些虚拟化产品能与真实应用实现零差距对接。过去的虚拟化技术应用还只是处于模拟阶段，与真实技术还是有一定区别，特别是防火墙等网络安全设备，与真实设备相比，从版本到功能，都有差别。随着虚拟化技术在云计算中的广泛应用，各大厂商生产的网络及安全设备产品不但有硬件版的，也有虚拟化版的，虚拟化产品既作为产品销售，也能在 EVE 仿真虚拟环境中运行。这样的虚拟化产品，可以使科研工作者和广大师生完整操控与真实生产环境一致的实验环境，实现与企业工作环境的零距离对接。

本专著通过研究 EVE-NG 等相关的虚拟化技术及使用方法，找到快速构建计算机网络安全联动实验环境的虚拟实验平台的方法及步骤，创建出了功能强大的仿真虚拟环境，搭建了实验平台。基于虚拟化技术构建的计

算机网络安全实验平台，可以实施各种计算机网络安全实验项目。针对新的虚拟化技术对硬件要求较高的特点，本专著还研究了硬盘扩容、扩大虚拟内存等方法，使一些新的虚拟化技术得以在内存只有 8G 的 PC 上加以实现和应用。

基于该虚拟化实验平台，本专著从计算机网络硬件安全和软件安全两方面入手，展开了对计算机网络安全技术的全面研究，涉及计算机网络所面临的安全问题、安全防护方法和网络渗透测试技术等方面。具体包括企业级防火墙的应用，穿越防火墙的网络攻击与防御,入侵检测系统的应用，局域网安全技术，MAC 地址泛洪攻击，ARP 攻击，DHCP Snooping 技术，服务器安全技术，数据加密技术的原理与应用，DH 算法，数据指纹，HMAC 算法，数字签名，公钥基础结构，虚拟专用网技术的原理与应用，IPSEC 技术，GRE Over IPSec 技术，VTI 技术， SSL 技术，网络安全渗透测试的原理与应用，Metasploit 渗透测试，Web 安全技术的原理与应用，XSS 攻击，SQL 注入攻击，CSRF 漏洞攻击等方面的知识、技能及防护措施。

具体来说，防火墙安全技术主要包括防火墙接口的配置技术、防火墙路由协议的配置技术、防火墙远程安全网管的技术、防火墙安全防护技术等。通过配置防火墙，保护公司内网和 DMZ 区域的安全，可有效地控制内网用户对 DMZ 区域和外网的访问。通过对防火墙的 Policy-map 进行配置，可控制穿越防火墙的流量，防范穿越防火墙的攻击，防御外网对内网发动泪滴攻击、IP 分片攻击以及死亡之 ping 等攻击。

我们不但需要防火墙这样的门卫，还需要入侵检测系统（IDS）这样的摄像头，部署到内网的各处，及时识别出不正常的行为流量，配合防火墙对内部网络进行管理和防护。入侵检测系统有硬件和软件版本，本专著以

Debian 系统上运行一款开源的 IDS 产品 snort 为例，深入研究了入侵检测系统（IDS）及其应用。

局域网设备安全技术应用，主要涉及的硬件设备是交换机。通过配置交换机的 Port-Security 属性，使用交换机的 DHCP Snooping 技术，启用交换机的 DAI 检查等技术手段，可有效地防范 MAC 地址泛洪攻击、DHCP 攻击及 ARP 欺骗等攻击，实现对这些攻击的有效防御。

除了对各种计算机网络设备的硬件安全进行研究，本专著还研究了计算机网络的软件系统安全，包括了网络协议、网络操作系统安全、网络应用软件安全、加密技术、VPN 技术、网络渗透测试技术等。

TCP/IP 等网络协议本身存在一定的缺陷，IP 数据包不需要认证的缺陷使得攻击者可冒充其他用户实施 IP 欺骗攻击；各种操作系统的源代码或多或少都存在一些漏洞，例如 Windows 操作系统的 RPC 缓冲区漏洞，导致了冲击波病毒的攻击。Web 应用服务器漏洞的存在，导致了 XSS 跨站脚本攻击、网站用户 Cookie 窃取、网站页面篡改、SQL 注入攻击、用户名认证攻击、CSRF 漏洞等攻击。

加密技术、VPN 技术、Web 安全技术以及渗透测试等技术是保障计算机网络软件安全的重要手段。

加密技术包括古典加密技术、对称加密技术（如 DES、3DES、AES 等）、非对称加密技术（如 RSA）、公钥基础架构 PKI 技术、HASH 算法、HMAC、数据指纹、数字签名、PGP 加密软件、SSL、HTTPS 等。

运用 VPN 技术可保证总部与分部之间，出差员工和在家办公员工与公司内网之间网络的安全性。VPN 技术包括通过路由器、防火墙实现 IPSEC VPN、GRE Over IPSec VPN、SVTI VPN、SSL VPN 等虚拟专用网技术。

运用 Web 安全技术，分析 Web 动态网站的源代码，分析网络数据库的调用存储方式，加强安全防范，可有效地抵御针对 Web 网站的 XSS 跨站脚本、SQL 注入、CSRF 漏洞等攻击。

网络渗透测试技术，主要涉及操作系统、数据库、应用软件等的安全。通过信息收集，扫描获取开放的主机、端口、漏洞，然后使用网络安全渗透测试工具对 Windows 服务器、Linux 服务器进行渗透测试，可修补和提升系统的安全性。

基于这些研究内容，笔者创建了相应的基于虚拟化的网络安全项目场景和实验环境，并出版了著作（兼教材）《计算机网络安全防护技术》，通过对它们的合理配合使用，可有效地促进教学改革，提高学生的学习兴趣和学习前沿知识的能力以及动手操作能力，发挥学生的潜能，增强学生的就业竞争力和发展潜力。

# 目 录

# 第一章　基于虚拟化的研究基础

## 第一节　虚拟化技术及其研究现状

虚拟化技术是在真机性能未能充分利用的基础上提出来的，目的是最大限度地屏蔽软硬件资源的差异性，把物理资源转变为可灵活分配、统一管理的逻辑资源，实现资源的自动化分配。虚拟化技术有很多优点，通过它能有效利用各种资源，快速地部署操作系统和应用软件，减少系统对硬件的依赖和由于硬件快速更新带来的影响，降低运营维护的成本。因此，众多大型企业、公共服务机构纷纷将现有的系统向虚拟化平台迁移。

虚拟化技术是“云计算”最重要的基础技术之一。“云”是互联网的一个隐喻，“云计算”使用互联网来接入存储、运行远程服务器端的服务及应用。云计算可分为三层，分别是基础设施即服务（Infrastructure as a Service，IaaS），平台即服务（Platform as a Service，PaaS），软件即服务（Software as a Service，SaaS）。基础设施即服务（IaaS）在最下端，平台即服务（PaaS）在中间，软件即服务（SaaS）在顶端。国内提供 IaaS 服务的机构有阿里云、腾讯云、华为云、Ucloud、中国电信、青云等，提供 PaaS 服务的有阿里云、腾讯云、新浪云、Ucloud 等，提供 SaaS 服务的有北森、用友、金蝶、商派等。以前，企事业单位架设网站、新增网络服务等，需要购买服务器等硬件，现在阿里云或其他服务商提供云计算 IaaS 服务，可

以将硬件外包，由提供 IaaS 服务的云计算公司提供场外服务器，存储和网络硬件供企事业单位租用，任何时候都可利用这些硬件来运行其应用，从而节省维护成本和办公场地成本。

## 第二节　科研与教学中常用的虚拟化要素

目前，科研和教学中常用的虚拟化要素有桌面操作系统虚拟化软件、网络设备虚拟软件和仿真虚拟环境。

### 一、桌面操作系统虚拟化软件

用于桌面操作系统虚拟化的软件主要有 Virtual PC、VMware workstation、开源虚拟机 QEMU 等。在教学领域中，用得最广泛的是 VMware workstation。该软件的主要优点是：支持在同一台真机上安装和同时运行多个虚拟机，每个虚拟机可以是同种或不同种的操作系统；通过该软件创建的虚拟机，独立于真机系统；有快照功能，可在同一台虚拟机上搭建多个不同的场景，并实现不同场景的迅速切换；可实现完全克隆和链接克隆，迅速生成一个同样的系统。

### 二、网络设备虚拟软件

常见的网络设备虚拟软件主要有 Boson Netsim for CCNA(CCNP)、HW-RouteSim、Packet Tracer、Dynamips、Zebra、GNS3 等。这些网络设备模拟软件有些适用于入门教学，如思科模拟器 Packet Tracer，它的命令集比真实系统有所减少，功能有所删减，并增加了适合于初学者的抓包模拟和动画

显示等功能；有些则采用真实的 Cisco IOS 来模拟网络设备，命令集与真实路由器完全一样，可开展一些复杂实验，如 Dynamips、GNS3 等。

### 三、仿真虚拟环境（EVE-NG）

EVE-NG 是近期才出现的虚拟化实验环境，全称是 Emulated Virtual Environment - Next Generation，意为下一代的仿真虚拟环境。它是在 Unetlab 1.0 的基础上发展起来的。各厂商的虚拟化网络产品都能在 EVE-NG 上运行，如思科、华为、Check Point、Juniper、Palo Alto、山石网科等公司的虚拟化网络设备，都能在 EVE-NG 环境下运行。在 EVE-NG 环境下，能实现虚拟化设备与真实网络以及 VMware workstation 下的虚拟机的互联。EVE-NG 是深度定制的 Ubuntu 操作系统，可以直接安装在 x86 架构的物理主机上，也可选用它的 ova 版本，通过 VMware 等虚拟化软件将其导入并运行。

## 第三节　虚拟化是行业发展的趋势

虚拟化是行业发展的趋势，相关科研技术及相关课程教学向虚拟化切换势在必行。目前，计算机网络安全防护等计算机网络专业相关课程的教学主要还是基于单独硬件平台设计的，但随着云计算、虚拟化技术的兴起，单独硬件平台已逐渐被虚拟化技术取代，网络、存储、服务、应用等虚拟化成为行业发展趋势。虚拟化技术在计算机网络安全防护等课程教学中应用是重要和迫切的。

首先，应用虚拟化技术可解决科研设备不足、教学实训设备不足、教学内容陈旧等问题。因为硬件更新快，科研经费有限，实验室的更新往往

跟不上硬件更新的速度，教学内容常常滞后于现实应用。若在科研及教学实训中采用最新的虚拟化产品，则可使得学生的学习与现实应用同步。

其次，应用虚拟化技术可以解决实训场景不易搭建、不易重复利用以及用真实设备无法为实训的不同阶段设置断点的问题。利用虚拟机搭建场景，为不同场景作快照，可实现不同实训场景的迅速模拟。在科研过程及教学实训过程中使用真机设备，可能会由于操作失误而花大量时间重新搭建场景，而虚拟机只需用很短的时间简单恢复为某断点处的状态便可继续进行科学研究或教学实训。

再次，通过对网络设备、网络安全设备和桌面操作系统的虚拟化产品进行联合应用研究，可建立仿真的虚拟网络，建立相关科研场景、教学场景和实验场景，并进一步通过快照促进科研、教学和实验的优化。对于科研工作者而言，在实验过程中，可根据自己的科研进度灵活地选择实验场景进行研究；对于教师而言，只需快速回到某个教学场景快照便可进行教学，大大提高课堂效率；对于学生而言，在实验过程中，可根据自己的学习进度灵活地选择实验场景开展实验。另外，可将科研场所和课堂教学延伸到课外，科研工作者的研究、教师的备课、学生的课后实验等都将不再受到网络设备和实验场所的限制，在有电脑的地方，都可以通过建立仿真的虚拟网络，进行网络组建、网络安全部署与防护等，大大提高科研工作者的科研效率，提高教师的备课效率，提高学生的动手操作能力和就业竞争力。