cisco

Official Cert Guide

Learn, prepare, and practice for exam success

CCNA网络安全运营 SECFND 210-250 认证考试指南

[美] 奥马尔·桑托斯（Omar Santos）
[美] 约瑟夫·穆尼斯（Joseph Muniz） 著
[意] 斯蒂法诺·德·克雷森佐（Stefano De Crescenzo）

孙余强 王涛 译

ciscopress.com

中国工信出版集团 人民邮电出版社 POSTS & TELECOM PRESS

CCNA网络安全运营
SECFND 210-250
认证考试指南

本书旨在帮助读者掌握CCNA SECFND 210-250认证考试的主题，具体包括：

- 网络概念；
- 安全概念；
- 密码学；
- 基于主机的分析；
- 安全监控。

本书是CCNA网络安全运营SECFND 210-250认证考试的官方学习资料，旨在帮助读者顺利通过该考试。本书介绍了一些备考提示和技巧，可以帮助读者识别自己的薄弱环节，提高对概念的理解和动手能力。

本书包括下述内容：

- 一个成熟的备考日程安排，以帮助读者通过考试；
- “摸底测试”，用于评估在学习每章时需要花费的时间；
- 每章末尾的“练习题”，帮助读者彻底掌握每章中的关键知识；
- 配套资源Pearson IT Certification Practice Test软件带有200多道考试习题，支持自定义使用模式，还可以生成一个详细的成绩报告。

本书因其详细程度、学习计划、评估特性、具有挑战性的复习题以及动手练习而备受推崇，它会帮助你掌握所有的概念和技术，让你顺利通过考试。

Omar Santos，Cisco产品安全事故响应团队（PSIRT）工程师。在调查和解决网络安全漏洞期间，领导并指点工程师和事故经理（incident manager）是他的主要职责。他曾为财富500强公司和美国政府设计、实施和支持安全网络，并在Cisco全球安全技术实践和TAC部门任职。

Joseph Muniz，思科系统的安全架构师和研究员。他在为财富500强企业和美国政府设计安全解决方案和安全体系结构方面享有丰富的经验。他参与并出版了多部作品。

Stefano De Crescenzo，Cisco产品安全事故响应团队（PSIRT）事故经理。他专注于Cisco产品漏洞管理和取证，以及关键基础设施设备中的恶意软件检测和完整性保证。他为Cisco IOS、IOS-XE和ASA编写了完整性保证指南。

本书是Cisco Press出版的认证考试指南系列丛书之一。该系列丛书提供了Cisco 官方开发的备考资料，供Cisco认证考生评估、复习和练习使用，从而帮助他们找到不足、督促学习，并增强通过考试的信心。

CCNA

ciscopress.com

分类建议：计算机 / 网络技术

人民邮电出版社网址：www.ptpress.com.cn

ISBN 978-7-115-52232-0

ISBN 978-7-115-52232-0

定价：129.00 元

CCNA网络安全运营
SECFND 210-250
认证考试指南

[美]奥马尔·桑托斯（Omar Santos）
[美]约瑟夫·穆尼斯（Joseph Muniz） 著
[意]斯蒂法诺·德·克雷森佐（Stefano De Crescenzo）
孙余强 王涛 译

人民邮电出版社
北京

图书在版编目（CIP）数据

CCNA网络安全运营SECFND 210-250认证考试指南 /（美）奥马尔·桑托斯（Omar Santos），（美）约瑟夫·穆尼斯（Joseph Muniz），（意）斯蒂法诺·德·克雷森佐（Stefano De Crescenzo）著；孙余强，王涛译. -- 北京：人民邮电出版社，2019.12
ISBN 978-7-115-52232-0

Ⅰ. ①C… Ⅱ. ①奥… ②约… ③斯… ④孙… ⑤王… Ⅲ. ①计算机网络－安全技术－资格考试－自学参考资料 Ⅳ. ①TP393.08

中国版本图书馆CIP数据核字(2019)第223944号

版权声明

◆ 著　[美]奥马尔·桑托斯（Omar Santos）
[美]约瑟夫·穆尼斯（Joseph Muniz）
[意]斯蒂法诺·德·克雷森佐（Stefano De Crescenzo）
译　孙余强　王　涛
责任编辑　陈聪聪
责任印制　焦志炜

◆ 人民邮电出版社出版发行　北京市丰台区成寿寺路 11 号
邮编　100164　电子邮件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
大厂聚鑫印刷有限责任公司印刷

◆ 开本：800×1000　1/16
印张：34
字数：719 千字　2019 年 12 月第 1 版
印数：1－2 000 册　2019 年 12 月河北第 1 次印刷
著作权合同登记号　图字：01-2018-8411 号

定价：129.00 元

读者服务热线：(010)81055410　印装质量热线：(010)81055316
反盗版热线：(010)81055315
广告经营许可证：京东工商广登字 20170147 号

内容提要

本书是 CCNA SECFND 210-250 认证考试的官方认证指南，旨在帮助读者掌握该考试的所有主题，为顺利通过考试打下基础。

本书分为 14 章，其内容包括网络协议和网络设备基本知识、网络安全设备和云服务、安全原理、访问控制简介、安全运维管理简介、密码学和公钥基础设施（PKI）基础知识、虚拟专用网路（VPN）简介、基于 Windows 的分析、基于 Linux 和 macOS 的分析、端点安全技术、网络和主机洞察技术、安全监控所面临的操作方面的难题、攻击和漏洞的种类以及安全逃避技术。为了帮助读者更好地深入掌握各章所学的知识，每章开头的“摸底测验”可以帮助读者评估知识能力并确定如何分配有限的学习时间。每章末尾的“备考任务”还总结了本章的考试要点以及课后练习，以方便读者参考和复习。

本书主要面向备考 CCNA SECFND 210-250 认证考试的考生，全书紧密围绕考试主题，在内容的组织和编写上切实凸显了认证考试需求。此外，本书内容的实用性很强，有志于从事网络安全运营工作的读者也可以通过本书顺利入门。

关于作者

Omar Santos 活跃于网络安全社区，在网络安全行业的多个倡议性组织和标准组织担任领导职务。他的主要工作是积极帮助企业、学术机构、州政府、地方执法机构以及其他参与机构提升自己的关键基础设施的安全性。

Omar 不但出版过多部专著，发布过大量的视频课程，还是诸多白皮书、论文以及安全配置和最佳做法指南的作者。Omar 是 Cisco 产品安全事故响应团队（Product Security Incident Response Team，PSIRT）的首席工程师，在调查和解决网络安全漏洞期间，领导并指点工程师和事故经理（incident manager）是他的主要职责。

Joseph Muniz 是一位安全研究员，在 Cisco 公司任架构师一职。他在设计财富 500 强企业及美国政府的安全解决方案/安全体系结构方面享有丰富的经验。Joseph 目前的工作使他能够从领先的安全厂商和众多客户那里了解到网络安全的最新趋势。Joseph 的研究成果包括名为“社交媒体欺骗（Social Media Deception）”的 RSA 演讲（该演讲的内容被许多消息来源引用，可搜关键字“Emily Williams Social Engineering”进一步了解），以及他在《PenTest》杂志上发表的各种安全主题的文章。

Joseph 拥有一家安全博客网站。该网站提供了各种与安全、黑客攻击和产品实现有关的热门资源。他写过几本涉及各种渗透测试和安全主题的图书。

Stefano De Crescenzo 是 Cisco 产品安全事故响应团队的高级事故经理，专攻产品漏洞管理和 Cisco 产品漏洞检验。他发表过多篇与安全最佳做法及安全取证有关的博文和白皮书。他活跃于安全社区，曾在多场安全会议上发表过演讲。

Stefano 的主要研究领域包括检测重要基础设施设备中运行的恶意软件以及完整性保障，他是多篇 Cisco IOS、IOS-XE 以及 ASA 的完整性保障指南的作者。

Stefano 拥有意大利米兰理工大学（Politecnico di Milano）电信工程专业的理科学士和硕士学位，以及丹麦技术大学（Danish Technical University，Denmark）通信专业的硕士学位。目前，他在比利时 Vlerick 商学院（Vlerick Business School in Belgium）攻读工商行政管理硕士学位。他还持有 CCIE 安全证书以及 CISSP、CISM 证书。

关于技术审稿人

Pavan Reddy 是 Cisco 安全服务部门的安全负责人。Pavan 在金融服务、医疗保健、服务提供商和零售领域拥有 20 多年的安全和网络咨询经验。他最近参与的项目涉及技术安全策略和架构、网络隔离策略、威胁情报分析、分布式拒绝服务缓解架构，以及 DNS 架构和安全。Pavan 拥有多张 CCIE 证书，握有计算机工程学士学位。

Ron Taylor 在信息安全领域工作近 20 年。其中有 10 年他都在从事咨询工作，积累了众多领域的宝贵经验。2008 年，他加入 Cisco 全球认证团队（Global Certification Team），任信息保障方向的 SME 一职。2012 年，他调入安全研究与运营部门（PSIRT），主要负责 Cisco 产品和服务的渗透测试。他参与设计并教授 Cisco 公司为其全球的内部开发和测试团队提供的安全培训课程。此外，他还作为产品安全测试方向的 SME，为许多产品团队提供过咨询。目前，他的职位是 Cisco 公司的系统咨询工程师，专攻安全产品线。他拥有 GPEN、GWEB、GCIA、GCIH、GWAPT、RHCE、CCSP、CCNA、CISSP 和 MCSE 等证书。Ron 的头衔有 Cisco 安全黑带、SANS 导师、Raleigh BSides 安全会议的联合创始人兼主席，以及 Defcon 的 Packet Hacking Village 团队成员。

献辞

谨将本书献给我的爱妻 Jeannette 和两个孩子 Hannah 和 Derek，感谢你们在本书的整个写作过程中给予的启发和支持。

还要将本书献给了我的父亲 Jose 和亡母 Generosa。没有你们的知识、智慧和教导，今天我就实现不了我一直努力争取的目标。

——Omar Santos

谨将本书献给我的亡父 Raymond Muniz。你未等到我出人头地（大学毕业、著书立说）的那天就离开了我。我得因为在高中退出足球队而向你道歉。在以后的生活中，我又重返绿茵场，现在每个星期至少踢两场比赛。你的辛勤付出得到了回报，但愿你能泉下有知。

——Joseph Muniz

谨将本书献给我的妻子 Nevena 和一对漂亮的女儿 Sara 和 Tea，感谢你们在本书的整个写作过程中给予的支持和启发。说具体一点，Tea 是在我开始写第 1 章的前几个礼拜出生的，她与本书的关系要更密切一点。

我还要将本书献给我的母亲 Mariagrazia 和妹妹 Francesca，你们在我外出写作时，对我和我的妻儿照顾有加。还要将本书献给我的亡父 Cataldo。

——Stefano De Crescenzo

致谢

我要感谢本书的技术审稿人 Pavan Reddy 和 Ron Taylor，感谢你们所付出的时间和提出的技术建议。你们检验了我们的工作成果，为本书的成功做出了贡献。还要感谢 Cisco Press 团队，尤其要感谢 Mary Beth Ray、Denise Lincoln 和 Christopher Cleveland，感谢你们的耐心、指导和关照。非常感谢你们所付出的努力。最后，我还要感谢 Cisco 安全研究和运营团队、Cisco 高级威胁分析（Cisco Advanced Threat Analytics）以及 Cisco Talos。有好几位网络安全行业的“大牛”都在那里工作，为我们 Cisco 公司的客户（这样的客户经常处于疲于奔命的状态）提供支持，你们每天都在创造奇迹。你们是真正的无名英雄，我很荣幸在同一战壕里与你们并肩战斗，捍卫客户和 Cisco 公司的利益。

——Omar Santos

首先，我要感谢 Omar 和 Stefano 邀请我写作本书。我真的很喜欢和你们这些家伙一起共事，希望将来我们能有更多的合作。其次，我还要感谢 Cisco Press 团队和本书的技术审稿人 Pavan Reddy 和 Ron Taylor，正是由于你们无微不至的关照，我们每一个人在写作过程中才能保持很高的水准并感到轻松愉快。嘿，Ron，你实现了这一切并拥有了 CTR 漫画。Green 先生，2016 年对你来说很棒。

我还要感谢所有让我成材的重要人物。

最后，还有一句话要讲给 7 岁的 Raylin Muniz 听：希望有一天你能实现自己的梦想，就像我完成本书这样。

——Joseph Muniz

我要感谢在本书的写作过程中成为我好伙伴的 Omar 和 Joey。尤其还得感谢我的妻子，感谢你在整个写作过程中对我的支持，感谢你帮助检查我的工作成果。

要是没有 Cisco Press 团队特别是 Chris Cleveland 的帮助，本书将不可能完成。Chris Cleveland 的指导尤为可贵。非常感谢本书的技术审稿人 Pavan 和 Ron，感谢你们提出的坦诚而又中肯的建议！非常感谢 Eric Vyncke 提出的众多建议。

——Stefano De Crescenzo

前言

恭喜！若你正在阅读本书，则拥有了一本秘籍，可以帮助你做到以下几点。

- 改进对网络安全基础知识的认识和理解。
- 提升与实施网络安全有关的技能水平。
- 备战 CCNA Cyber Ops SECFND 认证考试。

无论读者是要备战 CCNA Cyber Ops 认证考试，还是只想转行从事网络安全相关工作，都能从本书获得备考或入门所要掌握的知识。写作本书之时，我们顾及到了读者心中所想，会与读者共同探索制定网络加固方案之道以及如何顺利实现网络安全运维。本书的内容不但专注于应对 CCNA Cyber Ops SECFND 考试，而且还将实战中的最佳做法和具体案例相结合，旨在成为读者的自学指南，引领读者踏上网络安全之旅。

CCNA Cyber Ops SECFND 210-250 考试是获取 CCNA Cyber Ops 证书的必考科目。本书涵盖了 Cisco 考试大纲中罗列的所有主题，每一章都包含考试要点和备考准备，以帮助读者掌握相关内容。

关于 210-250 CCNA Cyber Ops SECFND 考试

CCNA Cyber Ops SECFND 210-250 考试是获取 CCNA Cyber Ops 证书的两项必考科目中的第一项，考试的内容与胜任安全运营中心（SOC）助理级安全分析员这一职位所要掌握的知识保持一致。SECFND 考试会测试考生对网络安全基本原理、基础知识以及核心技能的理解，以便通过第二项必考科目 SECOPS 来掌握助理级安全分析员理应具备的更为全面的知识。

CCNA Cyber Ops SECFND 210-250 考试是一项由 55～60 道题构成的计算机形式的考试，考试时长为 90 分钟。由于所有考试信息均由 Cisco 公司管理，因此考试内容可能会随时发生变化，考生应时刻关注 Cisco 公司官网对考试的更新。

关于本书

本书与 210-250 SECFND 考试的各项内容紧密契合，通过多种途径来帮助读者理解各项考试内容并为考试做好准备。

本书的目标和使用方法

本书会给出各种重要考点，来让读者发现需要多加复习的考试内容，引领读者充分理解并牢记相关细节，能够让读者自证已经掌握了相应的考点。也就是说，本书并不打算让

读者单凭死记硬背来通过考试，而是要让读者能真正学习并理解相关考点。本书将通过以下方法来帮助读者通过 SECFND 考试。

- 帮助读者发现自己尚未掌握的考点。
- 通过注解和案例分析来填补读者的知识空白。
- 提供习题来增强读者回忆及推断考题答案的能力。
- 通过配套网站上的模拟试题，让读者感受真实的考试氛围。

本书的内容结构

本书的核心内容共分 14 章，每一章都涵盖了 CCNA Cyber Ops SECFND 考试的部分考点。本书的核心内容分为 4 个部分，每个部分的主题如下所示。

第一部分：网络概念

- **第 1 章：网络协议和网络设备基本知识**，涵盖网络技术基本知识，包括对 OSI 参考模型和各种协议（比如，IP、TCP、UDP、ICMP、DNS、DHCP、ARP 等）的介绍。本章还将介绍各种网络基础设施设备（比如，路由器、交换机、HUB、无线接入点和无线 LAN 控制器）的基本运作原理。
- **第 2 章：网络安全设备和云服务**，涵盖防火墙、入侵防御系统（IPS）、高级恶意软件防护（AMP）系统的基本知识，以及 Cisco 网络安全设备（WSA）、Cisco 云网络安全（CWS）系统、Cisco E-mail 安全设备（ESA）、Cisco 云 E-mail 安全（CES）服务的基本知识。本章将会介绍以数据包过滤器的方式应用于网络设备接口的 ACL 的运作原理，比较具备数据包过滤功能的深度包检测技术与状态化防火墙技术之间的区别，细究线内流量检测与流量监听/流量镜像之间的区别。本章还会比较在执行网络流量分析时，从分路器/流量镜像获取的数据和从 NetFlow 获取的数据在特征上有什么差异。

第二部分：安全概念

- **第 3 章：安全原理**，涵盖了纵深防御战略的原理，从概念上对风险、威胁、漏洞和（利用漏洞发动的）攻击进行了比较和澄清。本章将会定义威胁制造者（threat actor）、runbook automation（RBA）、监管（证据）链、逆向工程、滑动窗口异常检测、个人身份信息（Personally Identifiable Information，PII）、受保护的健康信息（Protected Health Information，PHI）等诸多术语，解释最低权限原则以及如何落实职责分离。本章还将介绍风险评分、风险加权、风险降低等概念，以及如何开展全面的风险评估。
- **第 4 章：访问控制简介**，涵盖访问控制和管理的基本概念。本章会简述认证、授权和记账的原理，介绍几种较为常用的访问控制模式，包括自主访问控制（DAC）、强制访问控制（MAC）、基于角色的访问控制（RBAC）和基于属性

的访问控制（ABAC）。此外，本章还将介绍访问控制的各种具体实现，比如，AAA 协议、端口安全、802.1X、Cisco TrustSec 技术、入侵防御和检测技术，以及恶意软件防护技术。

- **第 5 章：安全运维管理简介**，涵盖安全运维管理的基本知识。具体而言，本章将会简述身份管理、协议和技术、资产安全管理、变更和配置管理、移动设备管理、事件和日志管理，涉及安全信息和事件管理（SIEM）技术、漏洞管理和补丁管理。

第三部分：密码学

- **第 6 章：密码学和公钥基础设施（PKI）基础知识**，涵盖业界常用的各种哈希和加密算法。本章会比较对称和非对称加密算法之间的区别，介绍公钥基础结构（PKI）和 PKI 的运作方式，以及 IPSec、SSL 和 TLS 协议。
- **第 7 章：虚拟专用网络（VPN）简介**，涵盖远程访问和站点到站点 VPN 技术、各种部署方案，以及 Cisco 提供的 VPN 解决方案。

第四部分：基于主机的分析

- **第 8 章：基于 Windows 的分析**，涵盖 Windows 操作系统如何处理应用程序的基本概念，包括该操作系统如何使用内存以及如何处理资源等细节。这些知识对确保 Windows 系统的性能最大化和安全性至关重要。
- **第 9 章：基于 Linux 和 macOS 的分析**，涵盖 UNIX 环境的内部运作机制，涉及进程执行和事件记录。了解 UNIX 环境的内部运作机制，既可以提高自己的技术能力，还可以制定用于加固基于 Linux 和基于 macOS 的系统的策略。
- **第 10 章：端点安全技术**，涵盖端点安全技术（比如，基于主机的入侵检测技术、基于主机的防火墙技术、应用层级白名单技术和黑名单技术，以及基于系统的沙箱技术）的运作机制。

第五部分：安全监控和攻击方法

- **第 11 章：网络和主机洞察技术**，涵盖如何鉴别由网络和基于主机的洞察技术或工具（包括 NetFlow、传统防火墙、下一代防火墙、抓包工具、应用程序的可视化及控制技术，以及 Web 和邮件内容过滤工具）提供的各种数据。本章还将概述在执行安全运维和安全监视时，如何执行抓包任务，如何分析会话数据、事务日志和安全告警数据。
- **第 12 章：安全监控所面临的操作方面的难题**，涵盖安全监控所面临的各种操作方面的难题，包括与使用 Tor、访问控制列表、隧道技术、对等到对等（P2P）通信技术、封装技术，以及负载均衡技术有关的难题。
- **第 13 章：攻击和漏洞的种类**，介绍各种网络安全攻击和漏洞，以及当今的威

胁制造者如何利用漏洞发动各种攻击。

- **第 14 章：安全逃避技术**，介绍攻击者“隐身”以及逃避各种检测和取证技术的手段，涉及易受攻击的网络环境中的加密攻击、资源耗竭攻击、流量隔离攻击、协议操纵攻击以及轴心攻击。

第六部分：附录

- **附录：摸底测验和课后练习答案**，给出了从第 1 章至第 14 章的摸底测试题和课后练习题的答案。

Pearson Test Prep 软件使用说明

在首次使用 Pearson Test Prep 软件时，需要遵循如下步骤。

1．从异步社区下载并安装完 Pearson Test Prep （培生测试备考）软件之后，运行该软件。

2．在 My Products 选项卡下选择 Activate New Project（激活新产品）按钮。

3．在弹出的 Activate Product Wizard（激活产品向导），输入本书提供的激活码，然后单击 Activate 按钮。

4．单击 Next 按钮，然后单击 Finish 按钮，将考试数据下载到应用程序中。

5．接下来就可以使用这个软件了。

注意，该软件在启动时将提示用户是否更新（Update）到新版本，建议根据实际需求单击 Update 或 Cancel 按钮。建议单击 Cancel 按钮，取消更新。若单击 Update 按钮，软件可能会进入“未响应”状态。

目录