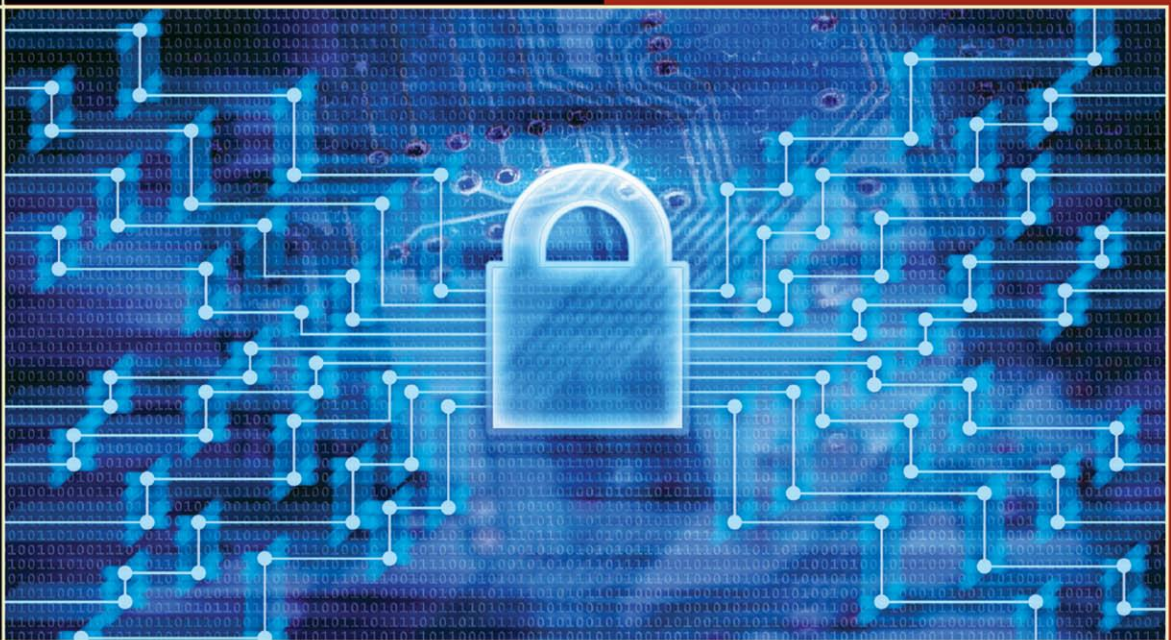


SECOND EDITION

# Principles of Computer Security

*CompTIA Security+™ and Beyond*

LAB MANUAL



VINCENT NESTLER

CompTIA Security+

GREGORY WHITE, PH.D.

WM. ARTHUR CONKLIN, PH.D.

CompTIA Security+, CISSP®

Mc  
Graw  
Hill

# **Principles of Computer Security: CompTIA Security+™ and Beyond Lab Manual**

## **Second Edition**

**Vincent Nestler  
Wm. Arthur Conklin  
Gregory White  
Matthew Hirsch**



New York Chicago San Francisco  
Lisbon London Madrid Mexico City  
Milan New Delhi San Juan  
Seoul Singapore Sydney Toronto

Copyright © 2011 by The McGraw-Hill Companies. All rights reserved. Except as permitted under the United States Copyright Act of 1976, no part of this publication may be reproduced or distributed in any form or by any means, or stored in a database or retrieval system, without the prior written permission of the publisher.

ISBN: 978-0-07-174857-5

MHID: 0-07-174857-1

The material in this eBook also appears in the print version of this title: ISBN: 978-0-07-174856-8,  
MHID: 0-07-174856-3.

All trademarks are trademarks of their respective owners. Rather than put a trademark symbol after every occurrence of a trademarked name, we use names in an editorial fashion only, and to the benefit of the trademark owner, with no intention of infringement of the trademark. Where such designations appear in this book, they have been printed with initial caps.

McGraw-Hill eBooks are available at special quantity discounts to use as premiums and sales promotions, or for use in corporate training programs. To contact a representative please e-mail us at [bulksales@mcgraw-hill.com](mailto:bulksales@mcgraw-hill.com).

Information has been obtained by McGraw-Hill from sources believed to be reliable. However, because of the possibility of human or mechanical error by our sources, McGraw-Hill, or others, McGraw-Hill does not guarantee the accuracy, adequacy, or completeness of any information and is not responsible for any errors or omissions or the results obtained from the use of such information.

#### TERMS OF USE

This is a copyrighted work and The McGraw-Hill Companies, Inc. (“McGrawHill”) and its licensors reserve all rights in and to the work. Use of this work is subject to these terms. Except as permitted under the Copyright Act of 1976 and the right to store and retrieve one copy of the work, you may not decompile, disassemble, reverse engineer, reproduce, modify, create derivative works based upon, transmit, distribute, disseminate, sell, publish or sublicense the work or any part of it without McGraw-Hill’s prior consent. You may use the work for your own noncommercial and personal use; any other use of the work is strictly prohibited. Your right to use the work may be terminated if you fail to comply with these terms.

THE WORK IS PROVIDED “AS IS.” McGRAW-HILL AND ITS LICENSORS MAKE NO GUARANTEES OR WARRANTIES AS TO THE ACCURACY, ADEQUACY OR COMPLETENESS OF OR RESULTS TO BE OBTAINED FROM USING THE WORK, INCLUDING ANY INFORMATION THAT CAN BE ACCESSED THROUGH THE WORK VIA HYPERLINK OR OTHERWISE, AND EXPRESSLY DISCLAIM ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. McGraw-Hill and its licensors do not warrant or guarantee that the functions contained in the work will meet your requirements or that its operation will be uninterrupted or error free. Neither McGraw-Hill nor its licensors shall be liable to you or anyone else for any inaccuracy, error or omission, regardless of cause, in the work or for any damages resulting therefrom. McGraw-Hill has no responsibility for the content of any information accessed through the work. Under no circumstances shall McGraw-Hill and/or its licensors be liable for any indirect, incidental, special, punitive, consequential or similar damages that result from the use of or inability to use the work, even if any of them has been advised of the possibility of such damages. This limitation of liability shall apply to any claim or cause whatsoever whether such claim or cause arises in contract, tort or otherwise.

*To my mother, for giving me that deep-seated feeling  
that comes from knowing a mother's love.*

—Vincent Nestler

*To Mike Meyers, forever reminding me of the power  
of hands-on learning, and to Tiffany and Susan,  
who made those sessions a lot more fun.*

—Art Conklin

# About the Authors

**Vincent Nestler**, M.S. Network Security, Capitol College, and M.A.T. Education, Columbia University, is a network engineering consultant and technical trainer with over 20 years of experience in network administration and security. Mr. Nestler served as a Data Communications Maintenance Officer in the U.S. Marine Corps Reserve. During his service, he designed and implemented the training for Marines assigned to the Defense Information Systems Agency (DISA) Computer Emergency Response Team. He also served as the Assistant Operations Officer (training) for the Joint Broadcast System, during its transition to DISA. Since 2007, Mr. Nestler has been integral to training CyberCorps students at the National Information Assurance Training and Education Center (NIATEC) at Idaho State University. He has developed the curriculum for 2 year, 4 year, and graduate programs in Networking and Information Assurance. He is currently a Professor of Practice in Information Assurance at Capitol College. Mr. Nestler's professional certifications include the Security+, Network +, and A+.

**Wm. Arthur Conklin**, Ph.D., is an assistant professor in the College of Technology and Director of the Center for Information Security Research and Education at the University of Houston. Dr. Conklin has terminal degrees from the Naval Postgraduate School in electrical engineering and The University of Texas at San Antonio in business administration. Dr. Conklin's research interests lie in the areas of software assurance and the application of systems theory to security issues associated with critical infrastructures. His dissertation was on the motivating factors for home users in adopting security on their own PCs. He has coauthored four books on information security and has written and presented numerous conference and academic journal papers. He has over ten years of teaching experience at the college level and has assisted in building two information security programs that have been recognized by the NSA and DHS as National Centers of Academic Excellence in Information Assurance Education. A former U.S. Navy officer, he was also previously the Technical Director at the Center for Infrastructure Assurance and Security at The University of Texas at San Antonio.

**Gregory White**, Ph.D., has been involved in computer and network security since 1986. He spent 30 years on active duty or in the Reserves with the U.S. Air Force. He obtained his Ph.D. in computer science from Texas A&M University in 1995. His dissertation topic was in the area of computer network intrusion detection, and he continues to conduct research in this area today. He is currently the Director for the Center for Infrastructure Assurance and Security (CIAS) and is an associate professor of computer science at The University of Texas at San Antonio. Dr. White has written and presented numerous articles and conference papers on security. He is also the coauthor of five textbooks on computer and network security and has written chapters for two other security books. Dr. White continues to be active in security research. His current research initiatives include efforts in high-speed intrusion detection, community infrastructure protection, and visualization of community and organization security postures.

**Matthew Hirsch**, M.S. Network Security, Capitol College, B.A. Physics, State University of New York (SUNY) New Paltz, has worked in the information security operations group for a large financial firm (which prefers to remain unnamed), in data distribution for firms including Deutsche Bank and Sanwa Securities, and in systems/network administration for Market Arts Software. Formerly an adjunct professor at Capitol College, Katharine Gibbs School, and DeVry, Mr. Hirsch also enjoys a long-term association with Dorsai, a New York City nonprofit ISP/hosting firm.

## About the Series Editor

**Corey D. Schou**, Ph.D., is the University Professor of Informatics and the Associate Dean of the College of Business at Idaho State University. He has been involved in establishing computer security and information assurance training and standards for 25 years. His research interests include information assurance, ethics, privacy, and collaborative decision making. He was responsible for compiling and editing computer security standards and training materials for the Committee on National Security Systems (CNSS). Throughout his career, Dr. Schou has remained an active classroom teacher despite his research and service commitments. He is the founding director of the Informatics Research Institute and the National Information Assurance Training and Education Center (NIATEC) that was designated a National Center of Academic Excellence in Information Assurance Education. In 1996, his research center was cited by the Information Systems Security Association (ISSA) for Outstanding Contributions to the Security Profession and he was selected as the Educator of the Year by the Federal Information Systems Security Educators Association (FISSEA). In 1997, the Masie Institute and TechLearn Consortium recognized his contributions to distance education. In 2001, Dr. Schou was honored by the International Information Systems Security Certification Consortium [(ISC)<sup>2</sup>] with the Tipton award for his work in professionalization of computer security and his development of the generally accepted common body of knowledge (CBK) used in the certification of information assurance professionals. Dr. Schou serves as the chair of the Colloquium for Information Systems Security Education (CISSE). Under his leadership, the Colloquium creates an environment for exchange and dialogue among leaders in government, industry, and academia concerning information security and information assurance education. In addition, he is the editor of *Information Systems Security* and serves on the board of several professional organizations.

## About the Technical Editor

**Chris Crayton** (CompTIA A+, CompTIA Network+, MCSE) is an author, editor, technical consultant, and trainer. Mr. Crayton has worked as a computer and networking instructor at Keiser University, where he was awarded 2001 Teacher of the Year, as network administrator for Protocol, an eCRM company, and as a computer and network specialist at Eastman Kodak. Mr. Crayton has authored several print and online books on PC repair, CompTIA A+, CompTIA Security+, and Microsoft Windows Vista. Mr. Crayton has served as technical editor on numerous professional technical titles for many of the leading publishing companies, including *CompTIA A+ All-in-One Exam Guide*, and has most recently contributed to *Mike Meyers CompTIA A+ Test Bank* and *Mike Meyers' CompTIA Network+ Certification Passport*.

*This page intentionally left blank*

# Contents at a Glance

<b>PART I</b>	<b>NETWORKING BASICS: HOW DO NETWORKS WORK?</b> .....	<b>I</b>
<i>Chapter 1</i>	WORKSTATION NETWORK CONFIGURATION AND CONNECTIVITY .....	3
<i>Chapter 2</i>	NETWORK TRANSPORTS .....	35
<i>Chapter 3</i>	NETWORK APPLICATIONS .....	59
<b>PART II</b>	<b>VULNERABILITIES AND THREATS: HOW CAN SYSTEMS BE COMPROMISED?</b> .....	<b>83</b>
<i>Chapter 4</i>	PENETRATION TESTING .....	85
<i>Chapter 5</i>	ATTACKS AGAINST APPLICATIONS .....	121
<i>Chapter 6</i>	MORE ATTACKS: TROJAN ATTACKS, MITM, STEGANOGRAPHY .....	141
<b>PART III</b>	<b>PREVENTION: HOW DO WE PREVENT HARM TO NETWORKS?</b> ...	<b>165</b>
<i>Chapter 7</i>	HARDENING THE HOST COMPUTER .....	167
<i>Chapter 8</i>	SECURING NETWORK COMMUNICATIONS .....	191
<b>PART IV</b>	<b>DETECTION AND RESPONSE: HOW DO WE DETECT AND RESPOND TO ATTACKS?</b> .....	<b>253</b>
<i>Chapter 9</i>	PREPARING FOR AND DETECTING ATTACKS .....	255
<i>Chapter 10</i>	DIGITAL FORENSICS .....	301
	INDEX .....	321



*This page intentionally left blank*

# Contents

	ACKNOWLEDGMENTS	xv
	INTRODUCTION	xvi
	ADDITIONAL RESOURCES FOR TEACHERS	xx
<b>PART I</b>	<b>NETWORKING BASICS: HOW DO NETWORKS WORK?</b>	<b>I</b>
Chapter 1	WORKSTATION NETWORK CONFIGURATION AND CONNECTIVITY	3
	Lab 1.1: Network Workstation Client Configuration	5
	Lab 1.1w: Windows Client Configuration	6
	Lab 1.1l: Linux Client Configuration	11
	Lab 1.1 Analysis Questions	16
	Lab 1.1 Key Terms Quiz	17
	Lab 1.2: Computer Name Resolution	19
	Lab 1.2w: Name Resolution in Windows	20
	Lab 1.2 Analysis Questions	24
	Lab 1.2 Key Terms Quiz	25
	Lab 1.3: IPv6 Basics	26
	Lab 1.3w: Windows IPv6 Basics (netsh/ping6)	27
	Lab 1.3 Analysis Questions	32
	Lab 1.3 Key Terms Quiz	32
Chapter 2	NETWORK TRANSPORTS	35
	Lab 2.1: Network Communication Analysis	36
	Lab 2.1w: Network Communication Analysis in Windows	39
	Lab 2.1 Analysis Questions	47
	Lab 2.1 Key Terms Quiz	47
	Lab 2.2: Port Connection Status	49
	Lab 2.2w: Windows-Based Port Connection Status	49
	Lab 2.2l: Linux-Based Port Connection Status	52
	Lab 2.2 Analysis Questions	56
	Lab 2.2 Key Terms Quiz	57