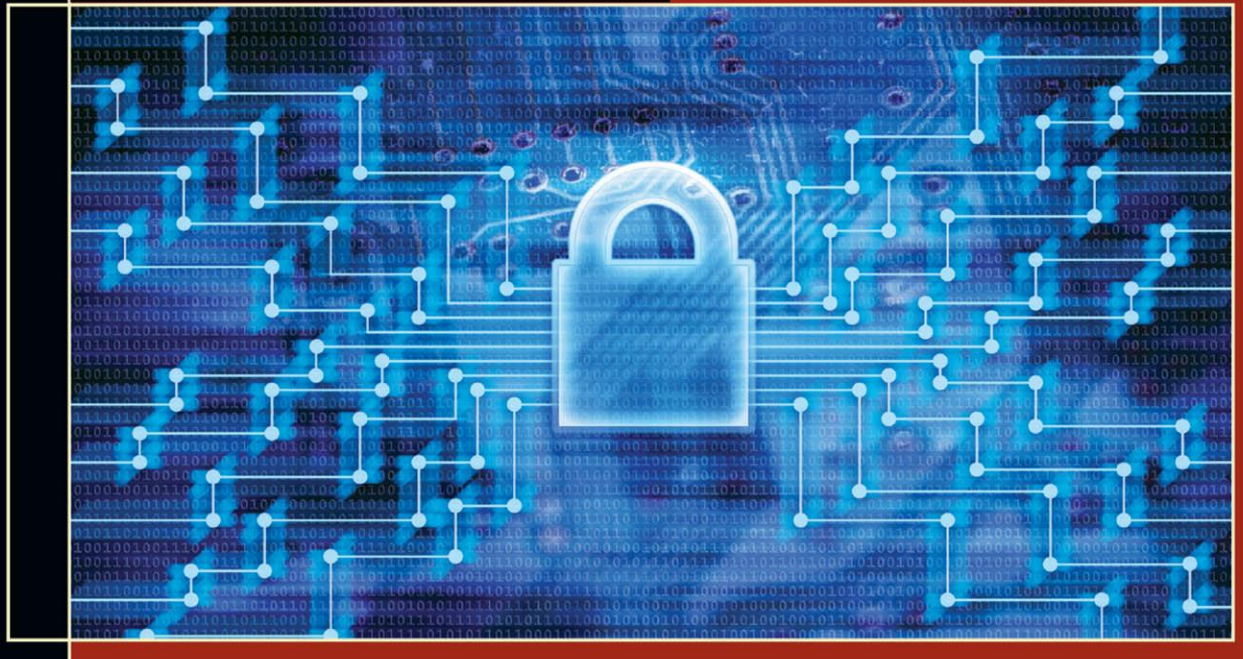
SECOND EDITION

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

The McGraw-Hill Companies

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.

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)2] 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

This page intentionally left blank

Contents