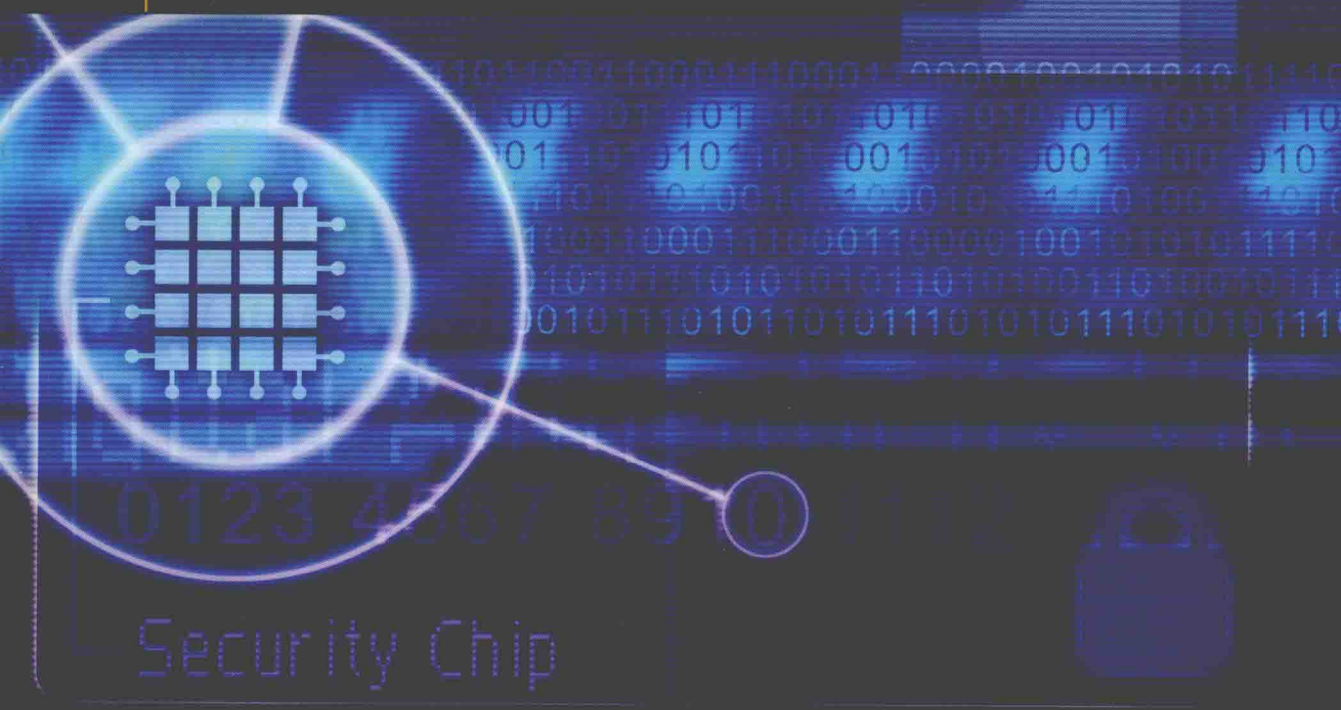
Information Assurance
& Security Series



Vincent J. Nestler Wm. Arthur Conklin Gregory B. White Matthew P. Hirsch

COMPUTER SECURITY

LAB MANUAL

Computer Security Lab Manual

Vincent J. Nestler
Wm. Arthur Conklin
Gregory B. White
Matthew P. Hirsch

Boston Burr Ridge, IL Dubuque, IA Madison, WI New York San Francisco St. Louis
Bangkok Bogotá Caracas Kuala Lumpur Lisbon London Madrid Mexico City
Milan Montreal New Delhi Santiago Seoul Singapore Sydney Taipei Toronto

COMPUTER SECURITY LAB MANUAL

This book is printed on acid-free paper.

1 2 3 4 5 6 7 8 9 0 DOC/DOC 0 9 8 7 6 5

ISBN: 0-07-225508-0

Editorial director: *Michael Lange*
Publisher: *David Culverwell*
Sponsoring editor: *Thomas Casson*
Developmental editor: *Jonathan Plant*
Editorial assistant: *Lindsay Roth*
Marketing Manager: *Lynn Kalb*
Lead project manager: *Pat Frederickson*
Senior production supervisor: *Sesha Bolisetty*
Design coordinator: *Cara David*
Cover Designer: *Brian Perveneckis*
Cover Photos: © *Getty Images*
Compositor: *International Typesetting and Composition*
Typeface: 11/14 *Eureka*
Printer: *R. R. Donnelley*

Library of Congress Cataloging-in-Publication Data

Computer security lab manual / Vincent J. Nestler . . . [et al.].
p. cm.
ISBN 0-07-225508-0 (alk. paper)
1. Computer security—Management—Handbooks, manuals, etc. 2. Data protection—Handbooks, manuals, etc. I. Nestler, Vincent J.
QA76.9.A25C6555 2006
005.8—dc22 2005049595

www.mhhe.com

This book is dedicated to you, the aspiring information security professionals who will be assuming frontline positions in defending the nation's infrastructures. Your work will enable information systems to safely and securely fulfill the promise of the information age. Study hard—you play a key role in our nation's future.

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 15 years of experience in network administration and security. Served as a Data Communications Maintenance Officer in the U.S. Marine Corps Reserve. Designed and implemented the training for Marines assigned to the Defense Information Systems Agency (DISA) Computer Emergency Response Team. Served as the Assistant Operations Officer (training) for the Joint Broadcast System during its transition to DISA. Developed the curriculum for the Computer Network Operations program. Adjunct professor of Networking and Security at Capitol College, DeVry Institute of Technology, and The Katharine Gibbs School. Professional certifications include the Red Hat Certified Engineer, Microsoft Certified Trainer, Microsoft Certified Systems Engineer, Cisco Certified Network Associate, and Security+.

Wm. Arthur Conklin is a Research Assistant Professor at the Center for Infrastructure Assurance and Security at The University of Texas at San Antonio (UTSA). He is doctoral candidate in Business Administration, specializing in Information Systems/Information Assurance. Mr. Conklin has a B.A. from Washington University in St. Louis, an M.B.A. from UTSA, and two graduate degrees in electrical engineering from the U.S. Naval Postgraduate School in Monterey, California. His research interests are in the area of security issues in distributed systems. Mr. Conklin is a 10-year veteran of the U.S. Navy, serving as a surface warfare officer and engineering duty officer, and has over 10 years' experience in software engineering and project management. He is co-author of McGraw-Hill's *Security+ Certification All-in-One Exam Guide* and *Principles of Computer Security: Security+ and Beyond.*

Dr. Gregory White has been involved in computer and network security since 1986. He spent 19 years with the Air Force and is currently in the Air Force Reserves. He obtained his Ph.D. in Computer Science from Texas A&M University in 1995. He currently serves as the Interim Director and Technical Director for the Center for Infrastructure Assurance and Security and is an Associate Professor of Computer Science at The University of Texas at San Antonio (UTSA). His current research initiatives include an examination of organizational issues affecting computer security, high-speed intrusion detection, infrastructure protection, and methods to determine a return on investment from security. He is the co-author of several books on computer security and numerous articles and conference publications.

Matthew Hirsch, M.S. Network Security, Capitol College. B.A. Physics, State University of New York (SUNY) New Paltz. Adjunct Professor, Computer Network Operations Department

of The Katharine Gibbs School. Over 15 years of experience as systems and network administrator. Systems Administrator for Deutsche Bank. Systems/Network Administrator for Sanwa Securities and Market Arts Software. Volunteer administrator for Dorsai, a New York City non-profit ISP. Built a mostly secure, some would say insanely secure, firewall for Market Arts in 1994.

About the Technical Editor

Mike Casper's primary role is that of Information Security Manager in the financial services industry, responsible for the compliance and oversight of service providers. He has extensive knowledge and experience in evaluating the security posture of vendors across the globe. Mike also has nine years' experience as a higher-education instructor, based out of Pennsylvania and North Carolina. One of Mike's accomplishments includes being a contributing author of the CompTIA Security+ Examination. His list of certifications includes CompTIA Security+, Security Certified Network Specialist (SCNP), and Certified Information Systems Security Professional (CISSP).

Acknowledgments

Over the last several months a number of people pitched in to help develop this lab manual, many of whom stayed up late nights and weekends testing and tweaking. I would like to thank:

Themis Trilivas, Demetrious Orellano, and Rishi Rattan for testing, researching, and giving me the student perspective.

Patricia Markey for her work with testing and capturing images, and her attention to detail.

Rachel Fox for her help in editing my early drafts.

The weekend crew: Rich Rosenbluth, Lena Martinez, Don Walsh, Mike Dimeglio, Ed Clottin, Peter Chiu, Lou Breviario, Victor Rios, George Banks, and Mohammed Diop.

Dee Mike, who, aside from spending many hours testing, editing, and researching, has been a dear friend. Your friendship and support throughout the process was more than any friend could ask for.

Thanks to Dean Keith Hoell, whose support both administratively and as a friend was greatly appreciated.

Thanks to Corinne Tate, making the equipment and facilities available for developing the manual.

Thank you to Dr. Corey Schou for the opportunity to develop my vision of technical security training in this manual.

Thank you to Dr. David Ward, who has been many things to me—my commanding officer, mentor, and colleague. His guidance has always been sage.

Thank you, James and Sonja Hillestad, for being mentors to me and always reminding me to take a Sabbath.

To my friends and students. I could not have done it without you.

—Vincent Nestler

Children are our most important effort, and to Jennifer I dedicate this work with love.

—Wm. Arthur Conklin

To my parents, Charles and Nellie White, who from my youth taught me the importance of education and instilled in me a love for learning.

—Dr. Gregory White

To the staff at Dorsai for their patience and mentorship. Shai!

—Matthew Hirsch

Book Introduction

I hear and I forget.

I see and I remember.

I do and I understand.

—Confucius

The success of a learning endeavor rests on several factors including the complexity of the material and the level of direct involvement on the part of the student. It takes more than passive attendance at a lecture to learn most complex subjects. To truly learn and understand all of the elements of a complex issue requires exploration that comes from more intimate involvement with the material.

Computer security is a complex subject with many composite domains, overlapping principles, and highly specific, detailed technical aspects. Developing skilled professionals in computer security requires that several components be addressed, namely technical and principle-based knowledge, coupled with practical experience using that knowledge in operational situations. This book is designed to assist in simulating the practical experience portion of the knowledge base of computer security.

This book is not a stand-alone reference designed to cover all aspects of computer security. It is designed to act together with a principles-based text, such as McGraw-Hill's *Principles of Computer Security: Security+ and Beyond*. Together in a well-balanced curriculum they provide a foundation for understanding basic computer security concepts and skills.

Pedagogical Design

Four Questions in Security

This book is laid out in four sections, each corresponding to a question associated with networks and computer security. These questions act as a structured framework designed to build upon each previous section as we strive to develop a hands-on understanding of computer security principles. The sections and questions are:

Section 1—How does the network work?

Section 2—How is the network vulnerable and what are the threats?

Section 3—How do we prevent harm to the network?

Section 4—How do we detect and respond to attacks on the network?

These four questions build upon one another. First, it is important to understand how a network works before you can see the vulnerabilities that it has. After studying the vulnerabilities and the threats that act upon them, we must look to the methods for preventing harm to the network. Lastly, even in the most secure environments, we must prepare for the worst and ask how can we detect and how should we respond to attacks.

Lab Exercise Design

This laboratory book is specifically designed to allow flexibility on the part of instructors. There is flexibility in regards to equipment and setup, as they can be performed on a Windows, Linux, or Mac platform with the use of virtual machines. There is flexibility in regards to equipment quantity as both stand-alone networks and virtual networks can be employed. Lastly, there is flexibility in lab selection, as it is not expected that every lab will be employed, but rather a selection of appropriate labs may be taken to support specific concepts in the principles portion of coursework.

The lab exercises are designed to teach skills and concepts in computer and network security. There are several features of each lab that allow for flexibility while not losing focus on important concepts.

Labs Written for Windows and Linux

Most lab exercises are written for both Windows and Linux operating systems. This not only allows the students to work in the operating system with which they are familiar, but can serve to bridge the gap between understanding how each operating system works.

Each Lab Exercise Stands Alone

While the labs build upon one another in terms of content and skills covered, they stand alone with respect to configuration and settings. This allows for maximum flexibility in relation to the sequence and repetition of labs.

Labs Are Presented in Progressive Sequence

While the lab manual is broken down into four sections, each section is further broken down into chapters that divide the content into logical groupings. See Figure 1. This will help the student new to network security develop his knowledge and awareness of the skills and concepts in a progressive manner.

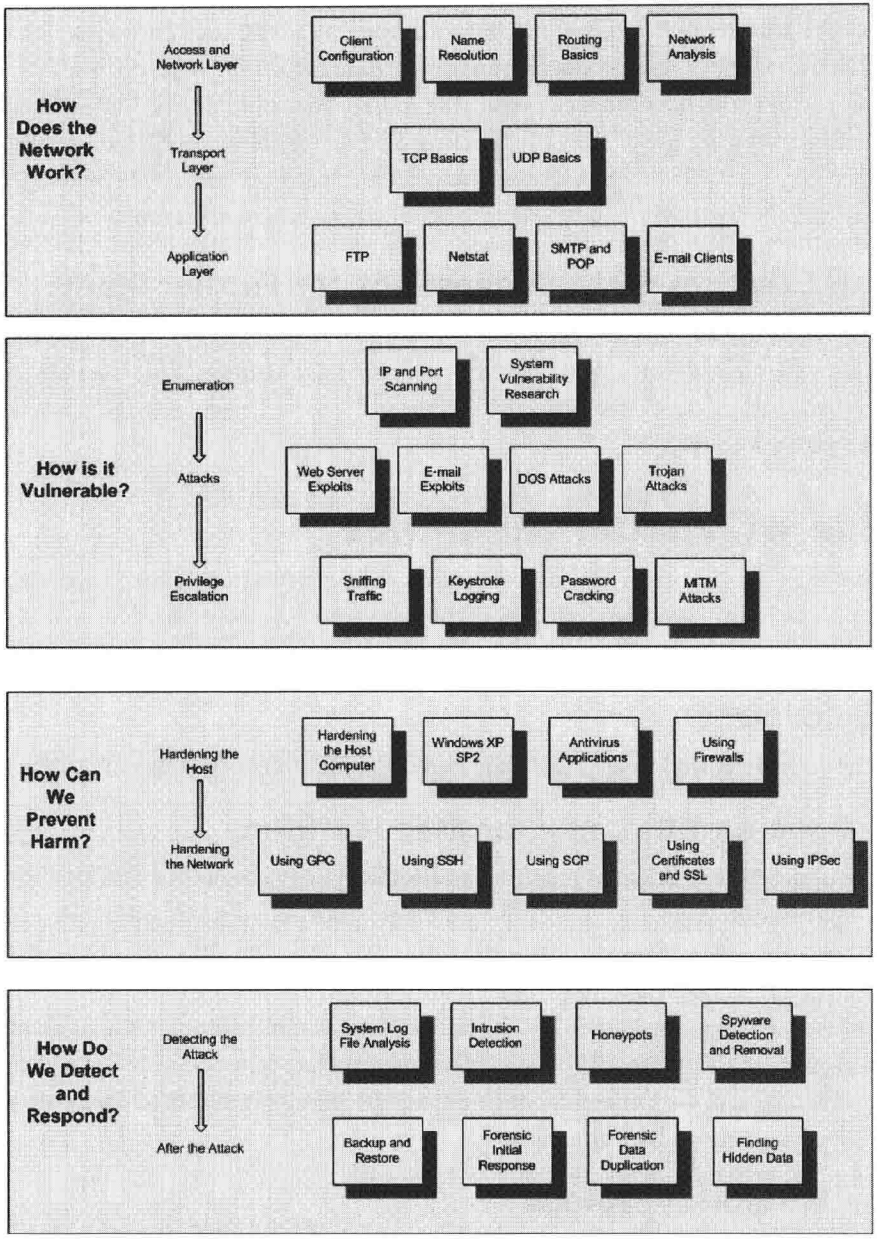


Figure 1: Lab exercises

Labs Can Be Done in Sequence by Topic

Not only are the lab exercises grouped by content according to the four questions, but references to later lab exercises that relate to the current one are included. See Figure 2. For example, you may want to perform the lab exercises pertaining to FTP. You could do the FTP lab from Section 1, which demonstrates the use of FTP; the Sniffing lab from Section 2, which demonstrates a vulnerability of FTP; the SCP lab from Section 3, which demonstrates hardening by encrypting the file transfer; and the log analysis lab from Section 4, which can reveal attacks on an FTP server.

Most Lab Exercises Have Suggestions for Further Study

At the end of each lab there are suggestions for further investigation. These sections point the student in the right direction to discover more. For the student who is advanced and completes labs ahead of time, these suggested labs offer a challenge, though they need not be required for other students.

The Use of Virtual Machines

While all the labs can be performed on computers configured as explained in the accompanying Web site, it is highly recommended that the lab be performed on virtual machines such as Microsoft Virtual PC or VMWare. There are several advantages to using virtual machines.

Easy Deployment

Once the virtual machines are created, they can be copied to all the lab computers.

Can Be Done on PC, Linux, or Mac Platform

As long as you meet the minimum resource and software requirements, the labs can be done on both PCs, Linux, or Macs.

One Student, One PC, Multiple Machines

If you use physical PCs to set up the lab, it will require at a minimum 3 PCs to create the network necessary to complete all the labs. This means that in a classroom of 30 computers, only 10 lab exercises can be worked on at one time. By using virtual machines, all 30 computers can be used running 30 labs at a time.

Labs Are Portable—Laptops

The use of virtual machines gives you the added benefit of having a network security lab on your laptop. This means that the student does not necessarily have to go to the lab to do the exercises; he can take the lab with him where ever he goes.

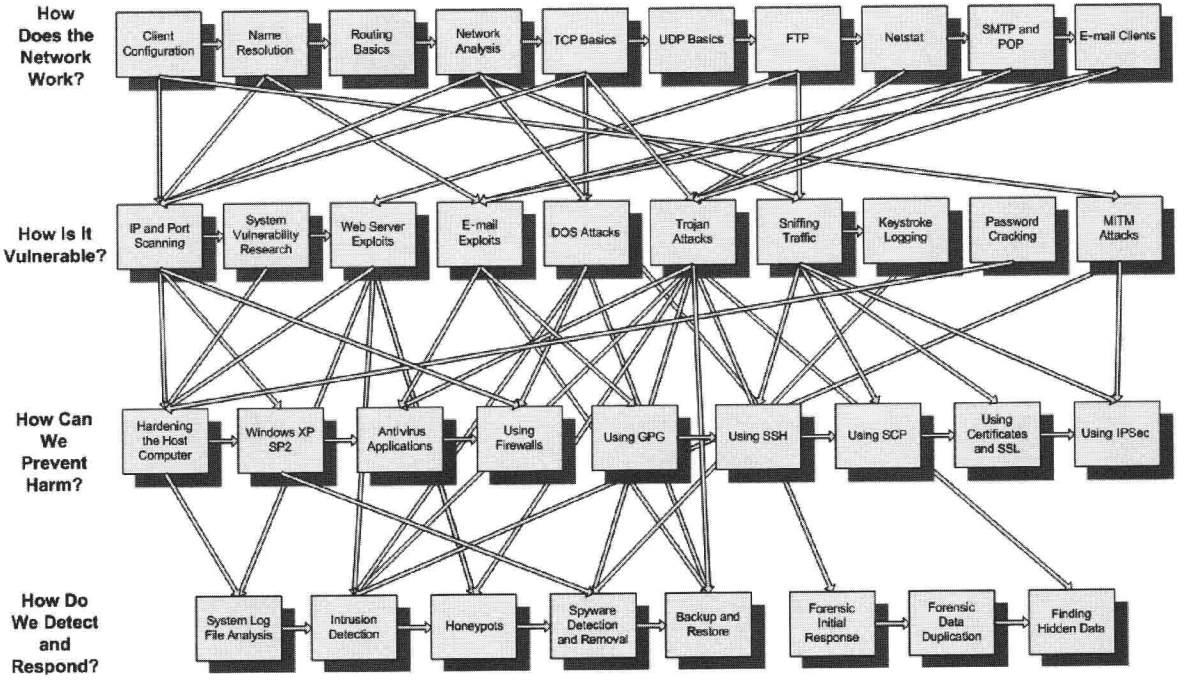


Figure 2: Lab exercises by topic

Easy Rollback

When properly configured, at the end of each lab exercise there is no need to uninstall or re-image computers. All that is needed is to exit the virtual machine without saving the changes. If the virtual hard drive has been modified, copying the original file back is a simple process.

Unlimited Potential for Further Experimentation

Unlike a simulation, each virtual machine is using the actual operating systems and as such can be used to develop new techniques and/or test out other security concepts and software with relatively little difficulty.

Security Lab Setup

All lab exercises have a letter designation of a, b, c, or d. The "a" labs are Windows-based exercises, "b" labs are Linux-based exercises, and "c" labs are mixed Windows and Linux exercises. Labs with the a, b, or c designation are intended to be performed on a closed network or virtual PC. The "d" labs are labs that need to be performed on a computer with Internet access. See Figure 3.

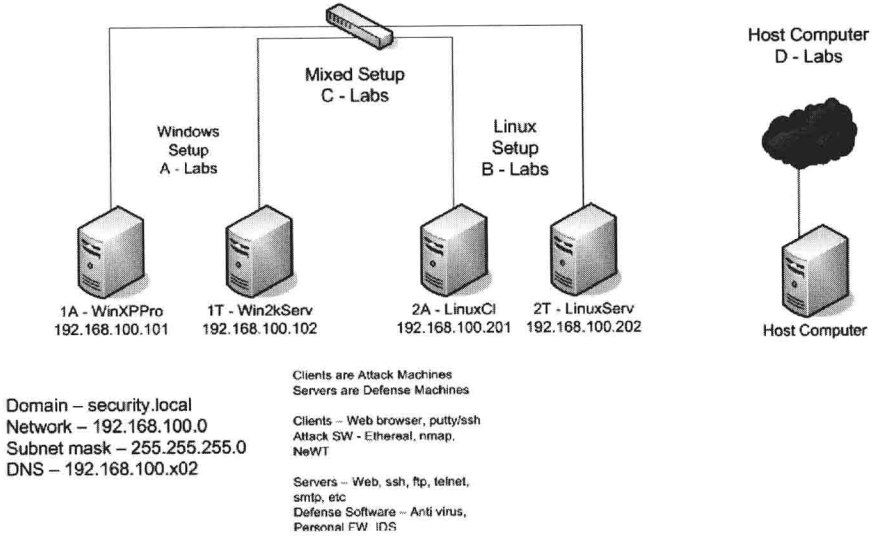


Figure 3: Lab setup diagram

The "a" Labs

These labs involve a Windows XP Professional PC and a Windows 2000 Server. In general the XP PC will be the attacker and the server will be the defender.

The "b" Labs

These labs involve a Red Hat 9 version of Linux. One will be configured as a client and one as a server. In general the Linux client will be the attacker and the server will be the defender.

The "c" Labs

These labs will involve a combination of Windows and Linux PCs. The Linux PC is used as an SSH and mail server.

The "d" Labs

These labs involve a host PC that has Internet access. While most exercises are designed to be done without Internet access, a few do require connectivity. The Internet connection allows students to do research and see the effects of spyware as they exist in real life.

Note that all computers are configured with weak passwords intentionally. This is for ease of lab use and to demonstrate the hazards of weak passwords. Creating and using more robust passwords is covered in Section 3.

Security Lab Requirements and Instructions

Detailed requirements and instructions for the security lab setup can be found at www.securitylabmanual.com. The requirements and instructions vary based upon the platform and base OS you intend to use.

★ Note

As many vendors improve their software, the availability of the versions used in this manual may no longer be available. As such, a few lab exercises may not work exactly as written but should still work in general. Please visit www.securitylabmanual.com for updates and other information.

Contents