

# THE NETWORK SECURITY TEST LAB

A Step-by-Step Guide



MICHAEL GREGG

WILEY



# **The Network Security Test Lab**





# The Network Security Test Lab

---

A Step-by-Step Guide

Michael Gregg

WILEY

## The Network Security Test Lab: A Step-by-Step Guide

Published by

**John Wiley & Sons, Inc.**

10475 Crosspoint Boulevard

Indianapolis, IN 46256

[www.wiley.com](http://www.wiley.com)

Copyright © 2015 by John Wiley & Sons, Inc., Indianapolis, Indiana

Published simultaneously in Canada

ISBN: 978-1-118-98705-6

ISBN: 978-1-118-98715-5 (ebk)

ISBN: 978-1-118-98713-1 (ebk)

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning or otherwise, except as permitted under Sections 107 or 108 of the 1976 United States Copyright Act, without either the prior written permission of the Publisher, or authorization through payment of the appropriate per-copy fee to the Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923, (978) 750-8400, fax (978) 646-8600. Requests to the Publisher for permission should be addressed to the Permissions Department, John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, (201) 748-6011, fax (201) 748-6008, or online at <http://www.wiley.com/go/permissions>.

**Limit of Liability/Disclaimer of Warranty:** The publisher and the author make no representations or warranties with respect to the accuracy or completeness of the contents of this work and specifically disclaim all warranties, including without limitation warranties of fitness for a particular purpose. No warranty may be created or extended by sales or promotional materials. The advice and strategies contained herein may not be suitable for every situation. This work is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional services. If professional assistance is required, the services of a competent professional person should be sought. Neither the publisher nor the author shall be liable for damages arising herefrom. The fact that an organization or Web site is referred to in this work as a citation and/or a potential source of further information does not mean that the author or the publisher endorses the information the organization or website may provide or recommendations it may make. Further, readers should be aware that Internet websites listed in this work may have changed or disappeared between when this work was written and when it is read.

For general information on our other products and services please contact our Customer Care Department within the United States at (877) 762-2974, outside the United States at (317) 572-3993 or fax (317) 572-4002.

Wiley publishes in a variety of print and electronic formats and by print-on-demand. Some material included with standard print versions of this book may not be included in e-books or in print-on-demand. If this book refers to media such as a CD or DVD that is not included in the version you purchased, you may download this material at <http://booksupport.wiley.com>. For more information about Wiley products, visit [www.wiley.com](http://www.wiley.com).

**Library of Congress Control Number:** 2015946971

**Trademarks:** Wiley and the Wiley logo are trademarks or registered trademarks of John Wiley & Sons, Inc. and/or its affiliates, in the United States and other countries, and may not be used without written permission. All other trademarks are the property of their respective owners. John Wiley & Sons, Inc. is not associated with any product or vendor mentioned in this book.



## About the Author

**Mr. Michael Gregg** is the CEO of Superior Solutions, Inc., a Houston based IT security-consulting firm. He has more than 20 years experience in the IT field and holds two associate's degrees, a bachelor's degree, a master's degree, and many IT certifications such as: CISSP, CISA, CISM, MCSE, and CEH. Michael has authored/co-authored more than 20 books. Some include: *Inside Network Security Assessment*, SAMS 2005; *Hack the Stack*, Syngress 2006; *Security Administrator Street Smarts*, Syngress 2011; and *How to Build Your Own Network Security Lab*, Wiley 2008.

Michael has testified before the United States Congress on privacy and security breaches. He also testified before the Missouri State Attorney General's committee on cybercrime and the rise of cell phone hacking. He has spoken at major IT/Security conferences such as the NCUA auditors conference in Arlington, Virginia. He is frequently cited by major print publications as a cybersecurity expert and has also appeared as an expert commentator for network broadcast outlets and print publications such as CNN, FOX, CBS, NBC, ABC, The Huffington Post, Kiplinger's, and The New York Times.

Michael enjoys giving back to the community; some of his civic engagements include Habitat for Humanity and United Way.





**Project Editor**

Sydney Argenta

**Technical Editor**

Rob Shimonski

**Production Manager**

Kathleen Wisor

**Copy Editor**

Marylouise Wiack

**Manager of Content Development  
& Assembly**

Mary Beth Wakefield

**Marketing Director**

David Mayhew

**Marketing Manager**

Carrie Sherrill

**Professional Technology &  
Strategy Director**

Barry Pruett

**Business Manager**

Amy Knies

**Associate Publisher**

Jim Minatel

**Project Coordinator, Cover**

Brent Savage

**Proofreader**

Nancy Carrasco

**Indexer**

Johnna VanHoose Dinse

**Cover Designer**

Wiley

**Cover Image**

©iStock.com/alphaspirit





# Acknowledgments

I would like to acknowledge Christine, Betty, Curly, and all my family. Also, a special thanks to everyone at Wiley. It has been a great pleasure to have worked with you on this book. I am grateful for the help and support from Carol Long, Sydney Argenta, Debbie Dahlin, and Rob Shimonski.





# Contents

<b>Introduction</b>	<b>xxi</b>
<b>Chapter 1 Building a Hardware and Software Test Platform</b>	<b>1</b>
Why Build a Lab?	2
Hardware Requirements	4
Physical Hardware	5
Equipment You Already Have	6
New Equipment Purchases	7
Used Equipment Purchases	7
Online Auctions	8
Thrift Stores	9
Company Sales	10
Virtual Hardware	10
VMware	12
VirtualBox	15
Hacker Hardware	16
Software Requirements	18
Operating Systems	19
Microsoft Windows	19
Linux	20
Navigating in Linux	23
Linux Basics	25
Mac OS X	28
Software and Applications	28
Learning Applications	29
Hacking Software	31
Summary	32
Key Terms	33
Exercises	34

	Equipment Checklist	34
	Installing VMware Workstation	35
	Exploring Linux Operating System Options	35
	Using VMware to Build a Windows Image	35
	Using VMware Converter to Create a Virtual Machine	36
	Exploring Other Operating System Options	37
	Running Kali from VMware	37
	Installing Tools on Your Windows Virtual Machine	38
<b>Chapter 2</b>	<b>Passive Information Gathering</b>	<b>39</b>
	Starting at the Source	40
	Scrutinizing Key Employees	43
	Dumpster Diving (Electronic)	45
	Analyzing Web Page Coding	48
	Exploiting Website Authentication Methods	51
	Mining Job Ads and Analyzing Financial Data	53
	Using Google to Mine Sensitive Information	56
	Exploring Domain Ownership	57
	WHOIS	59
	Regional Internet Registries	61
	Domain Name System	63
	Identifying Web Server Software	66
	Web Server Location	69
	Summary	70
	Key Terms	70
	Exercises	72
	IP Address and Domain Identification	72
	Information Gathering	72
	Google Hacking	74
	Banner Grabbing	74
	Telnet	75
	Netcat	75
	VisualRoute	76
<b>Chapter 3</b>	<b>Analyzing Network Traffic</b>	<b>77</b>
	Why Packet Analysis Is Important	77
	How to Capture Network Traffic	78
	Promiscuous Mode	78
	Hubs and Switches	79
	Hubbing Out and Using Taps	79
	Switches	79
	Capturing Network Traffic	82
	Managed and Unmanaged Switches	83
	ARP Cache Poisoning	85
	Flooding	91
	DHCP Redirection	92
	Redirection and Interception with ICMP	94

Preventing Packet Capture	94
Dynamic Address Inspection	95
DHCP Snooping	95
Preventing VLAN Hopping	96
Detecting Packet Capture	97
Wireshark	99
Wireshark Basics	99
Filtering and Decoding Traffic	102
Basic Data Capture—A Layer-by-Layer Review	108
Physical—Data-Link Layer	108
Network-Internet Layer	110
Transport—Host-Host Layer	111
Application Layer	115
Other Network Analysis Tools	115
Summary	118
Key Terms	118
Exercises	119
Fun with Packets	119
Packet Analysis with tcpdump	120
Packet Filters	121
Making a One-Way Data Cable	122
<b>Chapter 4</b>	<b>125</b>
<b>Detecting Live Systems and Analyzing Results</b>	<b>125</b>
TCP/IP Basics	125
The Network Access Layer	127
The Internet Layer	128
The Host-to-Host Layer	132
Transmission Control Protocol	132
User Datagram Protocol	134
The Application Layer	134
Detecting Live Systems with ICMP	138
ICMP—Ping	138
Traceroute	142
Port Scanning	147
TCP and UDP Port Scanning	147
Advanced Port-Scanning Techniques	151
Idle Scan	151
Analyzing Port Scans	155
Port-Scanning Tools	156
Nmap	157
SuperScan	160
Other Scanning Tools	161
OS Fingerprinting	161
Passive Fingerprinting	162
Active Fingerprinting	164
How Nmap OS Fingerprinting Works	165
Scanning Countermeasures	167

Summary	171
Key Terms	171
Exercises	172
Understanding Wireshark	172
Interpreting TCP Flags	174
Performing an ICMP Packet Decode	175
Port Scanning with Nmap	176
Traceroute	177
An Analysis of a Port Scan	178
OS Fingerprinting	179
<b>Chapter 5 Enumerating Systems</b>	<b>181</b>
Enumeration	181
Router and Firewall Enumeration	182
Router Enumeration	182
Firewall Enumeration	187
Router and Firewall Enumeration Countermeasures	191
Windows Enumeration	191
Server Message Block and Interprocess Communication	194
Enumeration and the IPC\$ Share	195
Windows Enumeration Countermeasures	195
Linux/Unix Enumeration	196
Enumeration of Application Layer Protocols	197
Simple Network Management Protocol	197
SNMP Enumeration Countermeasures	200
Enumeration of Other Applications	200
Advanced Enumeration	202
SCADA Systems	202
User Agent Strings	210
Mapping the Attack Surface	213
Password Speculation and Cracking	213
Sniffing Password Hashes	216
Exploiting a Vulnerability	218
Protecting Passwords	221
Summary	221
Key Terms	222
Exercises	223
SNMP Enumeration	223
Enumerating Routing Protocols	225
Enumeration with DumpSec	227
Identifying User Agent Strings	227
Browser Enumeration	229
<b>Chapter 6 Automating Encryption and Tunneling Techniques</b>	<b>231</b>
Encryption	232
Secret Key Encryption	233
Data Encryption Standard	235
Triple DES	236

Advanced Encryption Standard	237
One-Way Functions (Hashes)	237
MD Series	238
SHA	238
Public Key Encryption	238
RSA	239
Diffie-Hellman	239
El Gamal	240
Elliptic Curve Cryptography	240
Hybrid Cryptosystems	241
Public Key Authentication	241
Public Key Infrastructure	242
Certificate Authority	242
Registration Authority	242
Certificate Revocation List	243
Digital Certificates	243
Certificate Distribution System	244
Encryption Role in Authentication	244
Password Authentication	245
Password Hashing	246
Challenge-Response	249
Session Authentication	250
Session Cookies	250
Basic Authentication	251
Certificate-Based Authentication	251
Tunneling Techniques to Obscure Traffic	252
Internet Layer Tunneling	252
Transport Layer Tunneling	254
Application Layer Tunneling	256
Attacking Encryption and Authentication	259
Extracting Passwords	259
Password Cracking	260
Dictionary Attack	261
Brute-Force Attack	261
Rainbow Table	263
Other Cryptographic Attacks	263
Summary	264
Key Terms	264
Exercises	266
CrypTool	266
Extract an E-mail Username and Password	268
RainbowCrack	268
John the Ripper	270
<b>Chapter 7 Automated Attack and Penetration Tools</b>	<b>273</b>
Why Attack and Penetration Tools Are Important	274
Vulnerability Assessment Tools	274

Source Code Assessment Tools	275
Application Assessment Tools	276
System Assessment Tools	276
Attributes of a Good System Assessment Tool	278
Nessus	279
Automated Exploit Tools	286
Metasploit	286
Armitage	287
Metasploit Console	288
Metasploit Command-Line Interface	289
Updating Metasploit	290
BeEF	290
Core Impact	291
CANVAS	292
Determining Which Tools to Use	292
Picking the Right Platform	292
Summary	293
Key Terms	294
Exercises	294
Exploring N-Stalker, a Vulnerability Assessment Tool	294
Exploring Searchsploit on Kali Linux	295
Metasploit Kali	296
<b>Chapter 8 Securing Wireless Systems</b>	<b>299</b>
Wi-Fi Basics	300
Wireless Clients and NICs	301
Wireless Access Points	302
Wireless Communication Standards	302
Bluetooth Basics	304
Wi-Fi Security	305
Wired Equivalent Privacy	305
Wi-Fi Protected Access	307
802.1x Authentication	309
Wireless LAN Threats	310
Wardriving	310
NetStumbler	312
Kismet	314
Eavesdropping	314
Rogue and Unauthorized Access Points	318
Denial of Service	319
Exploiting Wireless Networks	320
Finding and Assessing the Network	320
Setting Up Airodump	321
Configuring Aireplay	321
Deauthentication and ARP Injection	322
Capturing IVs and Cracking the WEP KEY	322
Other Wireless Attack Tools	323

Exploiting Bluetooth	324
Securing Wireless Networks	324
Defense in Depth	325
Misuse Detection	326
Summary	326
Key Terms	327
Exercises	328
Using NetStumbler	328
Using Wireshark to Capture Wireless Traffic	329
<b>Chapter 9    An Introduction to Malware</b>	<b>331</b>
History of Malware	331
Types of Malware	334
Viruses	334
Worms	337
Logic Bombs	338
Backdoors and Trojans	338
Packers, Crypters, and Wrappers	340
Rootkits	343
Crimeware Kits	345
Botnets	347
Advanced Persistent Threats	350
Spyware and Adware	350
Common Attack Vectors	351
Social Engineering	351
Faking It!	352
Pretending through Email	352
Defenses against Malware	353
Antivirus	353
File Integrity Verification	355
User Education	355
Summary	356
Key Terms	356
Exercises	357
Virus Signatures	357
Building Trojans	358
Rootkits	358
Finding Malware	362
<b>Chapter 10    Detecting Intrusions and Analyzing Malware</b>	<b>365</b>
An Overview of Intrusion Detection	365
IDS Types and Components	367
IDS Engines	368
An Overview of Snort	370
Platform Compatibility	371
Limiting Access to the IDS	371
Verification of Configuration	372

Building Snort Rules	373
The Rule Header	374
Logging with Snort	375
Rule Options	376
Advanced Snort: Detecting Buffer Overflows	377
Responding to Attacks and Intrusions	379
Analyzing Malware	381
Tracking Malware to Its Source	382
Identifying Domains and Malicious Sites	382
Building a Testbed	386
Virtual and Physical Targets	386
Operating Systems	387
Network Isolation	387
Testbed Tools	388
Malware Analysis Techniques	390
Static Analysis	390
Dynamic Analysis	394
Summary	397
Key Terms	397
Exercises	398
Building a Snort Windows System	398
Analyzing Malware Communication	400
Analyzing Malware with VirusTotal	401
<b>Chapter 11 Forensic Detection</b>	<b>403</b>
Computer Forensics	404
Acquisition	405
Drive Removal and Hashing	407
Drive-Wiping	409
Logical and Physical Copies	410
Logical Copies	411
Physical Copies	411
Imaging the Drive	412
Authentication	413
Trace-Evidence Analysis	416
Browser Cache	418
Email Evidence	419
Deleted or Overwritten Files and Evidence	421
Other Trace Evidence	422
Hiding Techniques	422
Common File-Hiding Techniques	423
Advanced File-Hiding Techniques	425
Steganography	426
Detecting Steganographic Tools	429
Antiforensics	430
Summary	431
Key Terms	431

Exercises	432
Detecting Hidden Files	432
Basic File-Hiding	432
Advanced File-Hiding	433
Reading Email Headers	433
Use S-Tools to Embed and Encrypt a Message	435
<b>Index</b>	<b>439</b>





# Introduction

Welcome to *The Network Security Test Lab*. With this book, you can increase your hands-on IT security skills. The techniques and tools discussed in this book can benefit IT security designers and implementers. IT security designers will benefit as they learn more about specific tools and their capabilities. Implementers will gain firsthand experience from installing and practicing using software tools needed to secure information assets.

## Overview of the Book and Technology

---

This book is designed for individuals who need to better understand the functionality of security tools. Its objective is to help guide those individuals in learning when and how specific tools should be deployed and what any of the tools' specific limitations are. This book is for you if any of the following are true:

- You want to learn more about specific security tools.
- You lack hands-on experience in using security tools.
- You want to get the skills needed to advance at work or move into a new position.
- You love to tinker or expand your skills with computer software and hardware.
- You are studying for a certification and want to gain additional skills.

## How This Book Is Organized

---

The contents of this book are structured as follows:

- **Chapter 1, “Building a Hardware and Software Test Platform”**—Guides you through the process of building a hardware test platform.
- **Chapter 2, “Passive Information Gathering”**—Reviews the many ways that information can be passively gathered. This process starts at the organization’s website, and then moves to WHOIS records. This starting point allows you to build a complete profile of the organization.
- **Chapter 3, “Analyzing Network Traffic”**—Reviews methods and techniques for packet analysis. You will learn firsthand how common packet analysis tools such as Wireshark, Capsa, and Netwitness are used.
- **Chapter 4, “Detecting Live Systems and Analyzing Results”**—Once IP ranges have been discovered and potential systems have been identified, you will move quickly to using a host of tools to determine the status of live systems. Learn how Internet Control Message Protocol (ICMP) and other protocols work, while using both Linux and Windows lab systems.
- **Chapter 5, “Enumerating Systems”**—Explores how small weaknesses can be used to exploit a system and gain a foothold or operational control of a system. You will learn firsthand how to apply effective countermeasures by changing default banners, hardening systems, and disabling unwanted services.
- **Chapter 6, “Automating Encryption and Tunneling Techniques”**—Provides insight into how cryptographic systems are used to secure information and items such as passwords. You learn firsthand how these systems are attacked and which tools are used.
- **Chapter 7, “Automated Attack and Penetration Tools”**—Presents you with an overview of how attack and penetration tools work. These are the same tools that may be used against real networks, so it is important to understand how they work and their capabilities.
- **Chapter 8, “Securing Wireless Systems”**—Offers an overview of the challenges you’ll face protecting wireless networks. Although wireless systems are easy to deploy, they can present a real security challenge.
- **Chapter 9 “An Introduction to Malware”**—Takes you through a review of malware and demonstrates how to remove and control virulent code. You learn how to run rootkit detectors and spyware tools, and use integrity-verification programs.

- **Chapter 10, “Detecting Intrusions and Analyzing Malware”**—Introduces intrusion detection systems (IDSs) and discusses the ways in which malware can be analyzed. This chapter gives you the skills needed to set up and configure Snort and use tools such as IdaPro.
- **Chapter 11, “Forensic Detection”**—Reviews the skills needed to deal with the aftermath of a security breach. Forensics requires the ability to acquire, authenticate, and analyze data. You learn about basic forensic procedures and tools to analyze intrusions after security breaches.

## Who Should Read This Book

---

This book is designed for the individual with intermediate skills. While this book is focused on those who seek to set up and build a working security test lab, this does not mean that others cannot benefit from it. If you already have the hardware and software needed to review specific tools and techniques, Chapter 2 is a good starting point. For other even more advanced individuals, specific chapters can be used to gain additional skills and knowledge. As an example, if you are looking to learn more about password hashing and password cracking, proceed to Chapter 6. If you are specifically interested in wireless systems, Chapter 8 is for you. So, whereas some readers may want to read the book from start to finish, there is nothing to prevent you from moving around as needed.

## Tools You Will Need

---

Your desire to learn is the most important thing you have as you start to read this book. I try to use open source “free” software as much as possible. After all, the goal of this book is to try to make this as affordable as possible for those wanting to increase their skills. Because the developers of many free tools do not have the development funds that those who make commercial tools do, these tools can be somewhat erratic. The upside is that, if you are comfortable with coding or developing scripts, many of the tools can be customized. This gives them a wider range of usability than many commercial tools.

Tools are only half the picture. You will also need operating systems to launch tools and others to act as targets. A mixture of Linux and Windows systems will be needed for this task. We will delve into many of these issues in the first chapter. You may also want to explore sites like <http://www.linuxlinks.com/distributions>. There is more on this in the next section.

## What's on the Wiley Website

---

To make the process as easy as possible for you to get started, some of the basic tools you will need are available on the Wiley website that has been setup for this book at [www.wiley.com/go/networksecuritytestlab](http://www.wiley.com/go/networksecuritytestlab).

## Summary (From Here, Up Next, and So On)

---

*The Network Security Test Lab* is designed to take readers to the next stage of personal knowledge and skill development. Rather than presenting just the concept or discussing the tools that fit in a specific category, *The Network Security Test Lab* takes these topics and provides real-world implementation details. Learning how to apply higher-level security skills is an essential skill needed to pursue an advanced security career, and to make progress toward obtaining more complex security certifications, including CISSP, CASP, GSEC, CEH, CHFI, and the like. I hope that you enjoy this book, and please let me know how it helps you advance in the field of cyber security.

# Building a Hardware and Software Test Platform

This book is designed for those who need to better understand the importance of IT security. This chapter walks you through what you need to set up a hardware/software test platform. As a child, you may have loved to take things apart, TVs, radios, computers, and so on, in a quest to better understand how they worked. Your tools probably included soldering irons, screwdrivers—maybe even a hammer! That is similar to what you will be doing throughout this book. While you won't be using a hammer, you will be looking at protocols and applications to understand how they work. You will also examine some common tools that will make your analysis easier. The objective is to help you become a better network analyst, and improve and sharpen your IT security skills.

Because no two networks are the same, and because they change over time, it is impossible to come up with a one-size-fits-all list of hardware and software that will do the job for you. Networks serve the enterprises that own them, and enterprises must change over time. In addition, the scale of operation impacts security considerations. If you pursue a career as a security consultant, your goals (and inevitably your needs) will differ, depending on whether you work for a large multinational corporation (and even here, your goals and needs will depend on the type of industry) or a small office/home office (SOHO) operation or a small business. Clearly, a whole spectrum of possibilities exists here.

This chapter provides the first step in building your own network security lab. You will start to examine the types of hardware and gear that you can use

to build such a test environment, and then look at the operating systems and software you should consider loading on your new equipment.

## Why Build a Lab?

---

A laboratory is as vital to a computer-security specialist as it is to a chemist or biologist. It is the studio in which you can control a large number of variables that come to bear upon the outcome of your experiments. And network security, especially, is a field in which the researcher must understand how a diverse range of technologies behave at many levels. For a moment, just consider the importance of the production network to most organizations. They must rely on an always-on functioning, which means that many tests and evaluations must be developed in a lab on a network that has been specifically designed for such experiments.

**NOTE** A laboratory is a controlled environment in which unexpected events are nonexistent or at least minimized. Having a lab provides a consequence-free setting in which damage that might result from experimentation is localized (and can, it is hoped, be easily corrected).

Consider something as basic as patch management. Very few organizations move directly from downloading a patch to installing it in the production environment. The first step is to test the patch. The most agreed-upon way to accomplish this is to install it on a test network or system. This allows problems to be researched and compatibility ensured. You might also want to consider a typical penetration test. It may be that the penetration-testing team has developed a new exploit or written a specific piece of code for this unique assignment. Will the team begin by deploying this code on the client's network? Hopefully not. The typical approach would be to deploy the code on a test network to verify that it will function as designed. The last thing the penetration test team needs is to be responsible for a major outage on the client's network. These types of events are not good for future business.

Building a lab requires you to become familiar with the basics of wiring, signal distribution, switching, and routing. You also need to understand how you might tap into a data stream to analyze or, potentially, attack the network. The mix of common network protocols must be understood; only by knowing what is normal on the network can you recognize and isolate strange behavior. Consider some of the other items that might motivate you to construct such a lab:

- Certification
- Job advancement
- Knowledge

- Experimentation
- Evaluation of new tools

To varying degrees, networking- and security-related certifications require knowledge of the hardware and software of modern networks. There is no better vehicle for learning about networking and security issues firsthand than to design and build your own network lab. This provides a place where you can add and remove devices at will and reconfigure hardware and software to your liking. You can observe the interaction between the systems and networking devices in detail.

Advancing in your field is almost never an accident. The IT industry is an area of constant change, and the best way to build a career path in the world of IT is to build your skill set. By mastering these technologies, you will be able to identify the knowledgeable people on the job or at a customer's site, and align yourself with them. You might even uncover some gifts that you did not previously realize you possessed, such as a love for hexadecimal—well, maybe.

Building a lab demonstrates your desire and ability to study and control networks. One key item that potential employers always consider is whether a candidate has the drive to get the job done. Building your own security lab can help demonstrate to employers that you are looking for more than just a job: You want a career. As you use the network resources in your lab, you will invariably add to your knowledge and understanding of the technologies that you employ. Learning is a natural consequence.

Experimentation is a practical necessity if you are to fully understand many of the tools and methods employed by security professionals and hackers alike. Just consider the fact that there are many manuals that explain how Windows Server 2012 works, or how a Check Point firewall works, but no manual can account for every single situation and what is 'unique' to any environment you encounter. Some combinations and interactions are simply unknown. By building your own lab, you will discover that when deployed in complex modern networks, many things do not work the way the documentation says they will. And many times, it does not suffice to simply understand *what* happens; you need to appreciate the timing and sequence of events. This requires the control that a laboratory environment provides.

Because IT is an industry of continual change, new software, new security tools, new hacking techniques, and new networking gizmos constantly appear. A network security lab provides you with a forum in which to try these things out. You certainly don't want to risk corrupting a computer that you depend on every day to do your job. And you don't want to negatively impact the work of others; doing so is a good way to quickly put the brakes on your budding career.

A laboratory thus provides a place where you can try new things. This is a setting in which you can gain a detailed understanding of how things are put together and how they normally interact. It is an environment in which you can likely predict the outcome of your experiments, and if an outcome is unexpected, you can then isolate the cause.

**BUILDING YOUR OWN SECURITY LAB**

A common question among students and those preparing for certification is, “How do I really prepare for the job or promotion I am seeking?” The answer is always the same: know the material, but also get all the hands-on experience you can. Many times they don’t have enough money in their IT budget, or they are a struggling student. That is totally understandable. Yet the fact remains that there is no way to pick up many of the needed skills by reading alone. And many tests cannot be conducted on a live Internet-connected network.

With a little work and effort, you can find the equipment required to practice necessary skills at a reasonable price—network professionals have been doing this for years. There are even sites such as [certificationkits.com](http://certificationkits.com) that are set up exclusively to provide students with a full set of networking gear needed to complete a Cisco Certified Network Associate (CCNA) or a Cisco Certified Network Professional (CCNP) certification.

---

## Hardware Requirements

---

Before you can get started with any testing, you need to assemble some hardware. Your goal, as always, will be to do this as inexpensively as possible. Many things might be included in a network security laboratory. Some of these items are mandatory (for example, cables), and some things can be added according to your needs and as they become available or affordable. Although it is possible to contain everything within one computer, your requirements will vary from time to time based on the scenario that you are modeling.

Here are some of the things that will likely end up in your mix:

- Computers
- Networking tools
- Cables
- Network-attached storage (NAS)
- Hubs
- Switches
- Routers
- Removable disk storage
- Internet connection
- Cisco equipment
- Firewalls
- Wireless access points