

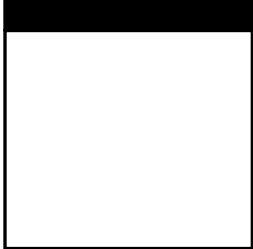
The CEH™ Prep Guide: The Comprehensive Guide to Certified Ethical Hacking

Ronald L. Krutz
Russell Dean Vines



Wiley Publishing, Inc.

The CEH™ Prep Guide: The Comprehensive Guide to Certified Ethical Hacking



The CEH™ Prep Guide: The Comprehensive Guide to Certified Ethical Hacking

Ronald L. Krutz
Russell Dean Vines



Wiley Publishing, Inc.

The CEH™ Prep Guide: The Comprehensive Guide to Certified Ethical Hacking

Published by
Wiley Publishing, Inc.
10475 Crosspoint Boulevard
Indianapolis, IN 46256
www.wiley.com

Copyright © 2007 by Ronald L. Krutz and Russell Dean Vines.

Published by Wiley Publishing, Inc., Indianapolis, Indiana

Published simultaneously in Canada

ISBN: 978-0-470-13592-1

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 Legal Department, Wiley Publishing, Inc., 10475 Crosspoint Blvd., Indianapolis, IN 46256, (317) 572-3447, fax (317) 572-4355, 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 Website 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 or to obtain technical support, please contact our Customer Care Department within the U.S. at (800) 762-2974, outside the U.S. at (317) 572-3993 or fax (317) 572-4002.

Library of Congress Cataloging-in-Publication Data

Krutz, Ronald L., 1938-

The CEH prep guide : the comprehensive guide to certified ethical hacking / Ronald L. Krutz, Russell Dean Vines.
p. cm.

Includes index.

ISBN 978-0-470-13592-1 (cloth/cd-rom)

1. Computer security—Testing—Examinations—Study guides. 2. Computer networks—Security measures—Examinations—Study guides. 3. Computer networks—Examinations—Study guides. 4. Computer hackers. I. Vines, Russell Dean, 1952– II. Title. III. Title: Comprehensive guide to certified ethical hacking.

QA76.9.A25.K79 2007

005.8--dc22

2007033354

Trademarks: Wiley, the Wiley logo, the Sybex logo, and related trade dress 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. CEH and the CEH logo are trademarks of EC-Council. All rights reserved. All other trademarks are the property of their respective owners. Wiley Publishing, Inc., is not associated with any product or vendor mentioned in this book.

Wiley also publishes its books in a variety of electronic formats. Some content that appears in print may not be available in electronic books.

*In memory of all I loved who have
passed and whom I dearly miss.*

– R.L.K.

To Elzy, now and forever.

– R.D.V.



About the Authors

RONALD L. KRUTZ, Ph.D., P.E., CISSP, ISSEP. Dr. Krutz is the Chief Knowledge Officer of Cybrinth, LLC. Cybrinth provides innovative information protection, analysis, assurance, and management services to government and the commercial sector. Prior to holding this position, he was a Senior Information Security Researcher in the Advanced Technology Research Center of Lockheed Martin/Sytex, Inc. In this capacity, he worked with a team responsible for advancing the state of the art in information systems security. He has more than 40 years of experience in distributed computing systems, computer architectures, real-time systems, information assurance methodologies, and information security training.

He has been an information security consultant at REALTECH Systems Corporation and BAE Systems, an associate director of the Carnegie Mellon Research Institute (CMRI), and a professor in the Carnegie Mellon University Department of Electrical and Computer Engineering. Dr. Krutz founded the CMRI Cybersecurity Center and was founder and director of the CMRI Computer, Automation, and Robotics Group. He is a former lead instructor for the (ISC)² CISSP Common Body of Knowledge review seminars. Dr. Krutz is also a Distinguished Visiting Lecturer at the University of New Haven Henry C. Lee College of Criminal Justice and Forensic Sciences, a part-time instructor in the University of Pittsburgh Department of Electrical and Computer Engineering, and a Registered Professional Engineer.

Dr. Krutz is the author of ten best-selling publications in the area of information systems security, and is a consulting editor for John Wiley and Sons for its information security book series. Dr. Krutz holds B.S., M.S., and Ph.D. degrees in Electrical and Computer Engineering.

RUSSELL DEAN VINES, CISSP, CISM, Security +, CCNA, MCSE, MCNE. Mr. Vines is Chief Security Advisor for Gotham Technology Group, LLC. He has been active in the prevention, detection, and remediation of security vulnerabilities for international corporations, including government, finance, and new media organizations, for many years. He has headed computer security departments and managed worldwide information systems networks for prominent technology, entertainment, and nonprofit corporations worldwide.

Mr. Vines is the author or co-author of ten best-selling information system security publications, and is a consulting editor for John Wiley and Sons for its information security book series. He is currently writing *Composing Digital Music For Dummies*, to be published in February, 2008.

Mr. Vines's early professional years were illuminated not by the flicker of a computer monitor but by the bright lights of Nevada casino show rooms. After receiving a *Down Beat* magazine scholarship to Boston's Berklee College of Music, he performed as a sideman for a variety of well-known entertainers, including George Benson, John Denver, Sammy Davis Jr., and Dean Martin.

In addition to composing and arranging hundreds of pieces of jazz and contemporary music recorded and performed by his own big band and others, he also founded and managed a scholastic music publishing company and worked as an artist-in-residence for the *National Endowment for the Arts* (NEA) in communities throughout the West. He still performs and teaches music in the New York City area and is a member of the American Federation of Musicians Local #802 and the International Association for Jazz Education.

You can find Mr. Vines's blog at <http://rdvgroup.blogspot.com>.



Credits

Executive Editor

Carol Long

Development Editor

Christopher J. Rivera

Production Editor

William A. Barton

Copy Editor

C.M. Jones

Editorial Manager

Mary Beth Wakefield

Production Manager

Tim Tate

**Vice President and Executive Group
Publisher**

Richard Swadley

Vice President and Publisher

Joseph B. Wikert

Project Coordinator, Cover

Adrienne Martinez

Compositor

Laurie Stewart,
Happenstance Type-O-Rama

Proofreading

Jen Larsen, Word One

Indexing

Johnna VanHoose Dinse

Anniversary Logo Design

Richard Pacifico



Contents

Foreword	xxiii
Acknowledgments	xxv
Introduction	xxvii
Part I The Business and Legal Issues of Ethical Hacking	1
Chapter 1 Introduction to Ethical Hacking	3
Terminology	3
Hackers, Crackers, and Other Related Terms	5
Hactivism	5
Threats	6
Hacking History	7
Ethical Hacking Objectives and Motivations	8
Steps in Malicious Hacking	8
Reconnaissance	10
Scanning	10
Acquiring Access	11
Maintaining Access	11
Covering, Clearing Tracks, and Installing Back Doors	11
Hacker and Ethical Hacker Characteristics and Operations	12
Skills Needed by an Ethical Hacker	12
Steps in an Infosec Evaluation	13
Types of Information System Security Testing	14
Ethical Hacking Outputs	15
Protections and Obligations for the Ethical Hacker	15
Related Types of Computer Crime	17
Assessment Questions	19

Chapter 2	Legality and Ethics	25
	Law and Legal Systems	25
	Administrative Law	26
	Common Law Organization	26
	Statutory Law	26
	U.S. Common Law System Categories	27
	Computer Security Crime Laws	27
	Privacy Principles and Laws	34
	Computer Crime Penalties	35
	Ethics	35
	Assessment Questions	40
Chapter 3	Penetration Testing for Business	47
	Penetration Testing from a Business Perspective	47
	Penetration Test Approach and Results	48
	Valuating Assets	48
	Penetration Testing Steps Summarized	50
	Selecting a Penetration Testing Consulting Organization	53
	Justification of Penetration Testing through Risk Analysis	54
	Risk Analysis Process	55
	Typical Threats and Attacks	56
	Impact Determination	58
	Management Responsibilities in Risk Analysis Relating to Penetration Testing	61
	Assessment Questions	64
Part II	The Pre-Attack Phases	71
Chapter 4	Footprinting	73
	Gathering Information	74
	Whois	74
	Nslookup	78
	Open Source Searching	79
	Locating the Network Range	79
	Determining the Network Range with ARIN	80
	Traceroute and TTL	80
	Email Tracking Programs	85
	Assessment Questions	86
Chapter 5	Scanning	91
	Identifying Active Machines	92
	Ping	92
	Ping Sweeps	93
	Ping Tools	93
	Identifying Open Ports and Available Services	94
	Port Scanning	95
	TCP/UDP Scanning Types	96
	Determining the Operating System	101

	Scanning Tools	101
	Vulnerable Ports	104
	Port Scanning Issues	105
	Banner Grabbing	105
	War Dialing	107
	War Driving and War Walking	107
	Wireless Scanners	108
	Wireless Packet Sniffers	109
	Fingerprinting	109
	Passive Fingerprinting	110
	Mapping the Network	111
	Assessment Questions	112
Chapter 6	Enumerating	117
	Protection Rings	117
	Windows Architecture	119
	Windows Security Elements	120
	SAM Database	122
	Local Security Authority Subsystem Service	123
	NetBIOS	124
	Active Directory (AD)	124
	Enumerating Techniques for Windows	125
	NetBIOS Enumerating	126
	Net View	126
	NBTSTAT	128
	Nbtscan	129
	User2sid and Sid2user	130
	Other Tools	131
	SNMP Enumeration	132
	SNMPutil	132
	Other SNMP Enumeration Tools	133
	DNS Zone Transfer	134
	Active Directory Enumeration	135
	Countermeasures	136
	NetBIOS Null Sessions	137
	SNMP Enumeration Countermeasures	137
	DNS Zone Transfer Countermeasures	138
	Assessment Questions	139
Part III	Attack Techniques and Tools	143
Chapter 7	System Hacking Techniques	145
	Password Guessing	146
	Automated Password Guessing	147
	Password Sniffing	147
	L0phtcrack	148
	KerbCrack	148

Alternate Means	149
Keystroke Loggers	149
Hardware Keyloggers	151
Software Keyloggers	151
Keylogging Tools	152
Redirecting SMB	152
Privilege Escalation	153
Password Cracking	154
Password Cracking Techniques	155
Dictionary Attack	156
Brute Force Attack	156
Hybrid Attack	156
Rainbow Attack	157
Stealing SAM	157
Cracking Tools	157
Covering Tracks	159
Disabling Auditing	159
Clearing the Event Log	159
Planting Rootkits	160
File Hiding	161
Countermeasures	162
Assessment Questions	164

Chapter 8 Trojans, Backdoors, and Sniffers 169

Trojans and Backdoors	169
Trojan Types	170
Remote Access Trojans (RATs)	171
Trojan Attack Vectors	172
Wrappers	174
Covert Communication	175
Trusted Computer System Evaluation Criteria (TCSEC)	175
Covert Storage Channel	176
Covert Timing Channel	176
Covert Communication Tools	177
Port Redirection	178
NetCat	178
Reverse Telnet	179
Datapipe	179
Fpipe	180
Rinetd	180
Trojan Tools and Creation Kits	180
Tini	181
QAZ	181
Donald Dick	181
NetBus	181

Back Orifice 2000	181
SubSeven	182
Other Notables	182
Anti-Trojan Software and Countermeasures	183
Windows File Protection (WFP)	183
Tripwire	183
Fport	184
TCPView	184
Process Viewer	190
Inzider	193
Sniffers	193
Sniffing Exploits	194
ARP Spoofing	195
MAC Flooding	197
DNS Spoofing or Poisoning	198
Sniffing Tools	198
Snort	198
Dsniff	198
Ethereal	199
MAC Flooding Tools	199
ARP Poisoning Tools	199
Other Sniffing Tools	200
Assessment Questions	201
Chapter 9 Denial of Service Attacks and Session Hijacking	207
Denial of Service/Distributed Denial of Service (DoS/DDoS)	207
DOS Attacks	208
DDoS Attacks	210
Prevention of DoS Attacks	213
Prevention of DDoS Attacks	214
Session Hijacking	215
The TCP/IP Protocol Stack	216
Layered Protocol Roles	218
Sequence Numbers	219
Session Hijacking Steps	220
Tools for Session Hijacking	221
Protecting Against Session Hijacking	223
Assessment Questions	224
Chapter 10 Penetration Testing Steps	231
Penetration Testing Overview	231
Legal and Ethical Implications	232
The Three Pretest Phases	233
Footprinting	233
Scanning	234
Enumerating	235

Penetration Testing Tools and Techniques	235
Port Scanners	236
Vulnerability Scanners	237
Password Crackers	237
Trojan Horses	238
Buffer Overflows	239
SQL Injection Attack	239
Cross Site Scripting (XSS)	240
Wireless Network Penetration Testing	241
WLAN Vulnerabilities	241
SSID Issues	242
WEP Weaknesses	242
MAC Address Vulnerabilities	243
Wireless Scanning Tools	243
Social Engineering	245
Intrusion Detection System (IDS)	246
Assessment Questions	248
Chapter 11 Linux Hacking Tools	251
Linux History	251
Scanning Networks with Linux Tools	253
NMap	253
Nessus	254
Cheops and Cheops-ng	254
Linux Hacking Tools	256
John the Ripper	256
SARA	257
Sniffit	257
HPing	257
Linux Rootkits	258
Linux Security Tools	259
Linux Firewalls	259
IPChains	259
IPTables	259
Linux Application Security Tools	260
Linux Intrusion Detection Systems (IDS)	260
Linux Encryption Tools	261
Linux Log and Traffic Monitors	262
Port Scan Detection Tools	263
Assessment Questions	264
Chapter 12 Social Engineering and Physical Security	267
Social Engineering	267
Human-Based (Person-to-Person) Social Engineering	268
Computer-Based Social Engineering	268
Example Social Engineering Attacks	269

Motivations for Individuals to Respond to Social Engineers	270
Reverse Social Engineering	270
Phishing	271
Hidden Frames	271
URL Obfuscation	272
HTML Image Mapping	272
Identity Theft	272
Defending Against Social Engineering Attacks	273
Physical Security	276
Physical Security Implementation	277
Company Facility Controls and Issues	277
Company Personnel Controls	278
Environmental Controls	278
Heating, Ventilation, and Air Conditioning (HVAC)	279
Fire Safety Controls	279
Access Controls	282
Fax Machines	286
Physical Facility Controls	286
Assessment Questions	290
 Part IV Web Server and Database Attacks	 299
Chapter 13 Web Server Hacking and Web Application Vulnerabilities	301
Web Server Hacking	301
Client to Server Data Exchange	302
Web Servers	304
Web Server Security Issues	304
ISAPI and DLL	304
IIS Attacks	305
Apache Attacks	307
Hacking Tools	308
Patch Management	309
Web Application Vulnerabilities	310
Related Hacking Tools	312
Ncat	312
Black Widow	313
Instant Source	313
Wget	313
Websleuth	313
Nikto	314
Wikto	314
Nessus	315
Network Utilities	315
Countermeasures	316
Assessment Questions	318

Chapter 14 SQL Injection Vulnerabilities	327
SQL Injection Testing and Attacks	327
Preparing for an Attack	328
Conducting an Attack	329
Lack of Strong Typing	330
Union Select Statements	331
Acquiring Table Column Names	333
Stored Procedures	333
Extended Stored Procedures	334
Server System Tables	335
SQL Injection Prevention and Remediation	335
Automated SQL Injection Tools	336
Assessment Questions	339
 Chapter 15 Cryptography	 347
Symmetric Key Cryptography	348
Symmetric Key Encipherment	348
Substitution Cipher	348
Vernam Cipher (One-Time Pad)	350
Transposition (Permutation) Cipher	350
The Exclusive Or (XOR) Function	350
Symmetric Key Cryptography Characteristics	351
Data Encryption Standard (DES)	351
Triple DES	352
The Advanced Encryption Standard (AES)	352
The Blowfish Algorithm	353
The Twofish Algorithm	353
The IDEA Cipher	353
RC5/RC6	353
Public Key Cryptosystems	353
One-Way Functions	354
Public Key Algorithms	354
RSA	354
El Gamal	355
Elliptic Curve (EC)	355
Summaries of Public Key Cryptosystem Approaches	356
Digital Signatures	356
Hash Function	357
Developing the Digital Signature	357
The U.S. Digital Signature Standard (DSS)	358
MD5	359
Public Key Certificates	359
Digital Certificates	359
Public Key Infrastructure (PKI)	362
Cryptanalysis	363
Managing Encryption Keys	364
Email Security	365

Electronic Transaction Security	366
Wireless Security	366
Disk Encryption	369
Hacking Tools	369
Assessment Questions	371
Chapter 16 Cracking Web Passwords	379
Authentication	379
Authentication Methods	380
Basic Authentication	380
Digest Authentication	381
NTLM (NT LAN Manager) Authentication	382
Negotiate Authentication	382
Certificate Based Authentication	382
Forms-Based Authentication	383
RSA Secure Token	383
Biometrics	384
Password Considerations and Issues	384
Selecting Passwords	385
Protecting Passwords	385
Password Cracking	386
Computer Password Cracking and Support Tools	387
Web Password Cracking Tools	388
Countermeasures	389
Assessment Questions	392
Part V Advanced Topics	399
Chapter 17 Wireless Network Attacks and Countermeasures	401
Wireless Technology	401
The Cellular Phone Network	402
Worldwide Cellular via LEO Satellites	402
Cellular Network Elements	403
Global Wireless Transmission Systems	404
AMPS	404
TDMA	404
CDMA	404
GSM	405
CDPD	405
NMT	406
TACS	406
PDC	406
General Packet Radio Service (GPRS)	406
Enhanced Data Rates for Global Evolution (EDGE)	406
Wireless Networking	406
Direct Sequence Spread Spectrum (DSSS)	407
Frequency Hopping Spread Spectrum (FHSS)	407

The IEEE 802.11 Family	408
WLAN Operational Modes	410
Ad Hoc Mode	410
Infrastructure Mode	410
Association Frames	412
Service Set Identifier (SSID)	412
Bluetooth	413
BT Security	413
BT Attacks	415
The Wireless Application Protocol (WAP)	415
Wired Equivalent Privacy (WEP)	417
WEP Encryption	417
WEP Decryption	420
RC4	421
WEP Authentication Methods	421
Open System Authentication	422
Shared Key Authentication	422
Media Access Control Authentication	424
WEP Key Management	424
WEP Cracking	425
WPA and WPA2	425
802.1x and EAP	426
Extensible Authentication Protocol (EAP)	427
EAP Transport Level Security (EAP-TLS)	427
Lightweight Extensible Authentication Protocol (LEAP)	427
WLAN Threats	427
Denial of Service Attacks	428
SSID Problems	429
The Broadcast Bubble	429
War Driving	430
Rogue Access Points	430
MAC Spoofing	431
Wireless Hacking Tools	431
NetStumbler	432
AiroPeek	432
AirSnort	434
Kismet	434
WEPCrack	435
Other WLAN Tools	435
Securing WLANs	436
Standards and Policy Solutions	437
MAC Address Filtering	437
SSID Solutions	438
Antenna Placement	439
VLANS	439
Wireless VPNs	440

Wireless RADIUS	441
Dynamic WEP Keys	441
Enable WEP, WPA2, EAP, and 802.1x	442
Site Surveys and IDS	442
Assessment Questions	444
Chapter 18 Firewalls, Intrusion Detection Systems, and Honeypots	449
Firewalls	449
Firewall Types	449
Proxy Firewall	450
Packet Level Filtering Firewall	450
Stateful Inspection Firewalls	451
Hardware and Software Firewalls	452
Firewall Architectures	452
Packet-Filtering Routers	452
Dual-Homed Hosts	452
Screened Host	453
Screened-Subnet Firewalls	454
Firewall Identification	454
Banner Grabbing	455
Port Scanning	456
Firewall Ports	457
Scanning with TCP	457
Scanning with UDP	457
Firewalking	457
Breaching and Bypassing Firewalls	458
Hping	458
Traceroute	458
Covert Channeling	459
ACK Tunneling	459
HTTP Tunneling	459
Firewall Backdoors	460
Firewall Informer	460
Intrusion Detection and Response	461
Host-Based ID Systems	461
Network-Based ID systems	461
IDS Detection Methods	462
Statistical Anomaly Detection	462
Pattern Matching Detection	462
Protocol Detection	463
IDS Responses	463
Using an IDS in a Switched Environment	463
Evading IDSs	464
Tools for Evading and Testing IDSs	465
Intrusion Prevention Systems	466
SNORT 2.x	466
Cisco Security Agent	467

Incident Handling	467
Computer Incident Response Team	467
Incident Notification	469
Honeypots	469
Honeypot Applications	470
Discovering Honeypots	471
Assessment Questions	472
Chapter 19 Viruses, Worms, and Buffer Overflows	483
Viruses	483
The Virus Lifecycle	484
Macro Viruses	484
Polymorphic Viruses	484
Stealth Viruses	485
Spyware	485
Web Bugs	486
Spambots	486
Pop-Up Downloads	486
Drive-By Downloads	487
Bogus Spyware Removal Programs	487
Multistage and Blended Threats	488
Worms	488
Virus and Worm Examples	489
Chernobyl	489
Explore.Zip	489
LoveLetter	489
Melissa Virus	489
Nimda Virus	490
Pretty Park	490
BugBear	491
Klez	491
SirCam Worm	491
Code Red Worm	492
Other Worms of Interest	492
Buffer Overflows	492
Preventing Malicious Code and Buffer Overflows	494
Virus Scanners	494
Virus Prevention	494
Virus Detection	494
Defending Against Buffer Overflows	495
Assessment Questions	496
Appendix A Answers to Assessment Questions	499
Appendix B Glossary of Terms and Acronyms	625
Appendix C What's on the CD	707
Index	711



Foreword

Shortly after I became the first computer crime instructor at the Los Angeles Police Department, Dr. Andrew Gross and I were recruited by a forward thinking director of security to conduct what we now refer to as ethical hacking. Dr. Gross had gained some celebrity for being on the team that had tracked down and arrested the notorious hacker Kevin Mitnick, and I had become known for being able to tell a search warrant execution squad what kind of networked computer equipment they would find at a crime scene before they kicked the door down.

After accepting the challenge to conduct the ethical hack of the famous organization, I conducted a literature review to find a good book to guide us through our efforts. To my surprise, my research revealed no single book that covered all the issues that Dr. Gross and I were facing in ethical hacking. I wound up having to write the legal release for the ethical hacking based on advice from a fellow instructor who was a former prosecutor.

Some time later while I was teaching advanced Internet investigation for the SEARCH Group, a non-profit organization owned by the Department of Justice, I started teaching ethical hacking to local, State, and Federal law enforcement officers by having them hack into a secure government information system. Again, I did a literature review to find a text book for our officers to use to study ethical hacking, and found no single book that was suitable for our needs. We had to resort to providing a few papers to the officers and to having experts in the various disciplines give lectures to them on the issues. Again, I had to write the release for the ethical hacking myself.

Those of us who have come to be known as pioneers in the field of information security and ethical hacking have spent years being frustrated that we

could not place in the hands of students one single book that covered all the essential issues of our field.

Then a breakthrough occurred for us with the publication of *The CISSP and CAP Prep Guide*, by Krutz and Vines. Finally someone had rounded up the latest information spanning the critical disciplines of the information security field and placed it in a single readable book. It is a book that both our law enforcement students and university students will really read and learn from.

Now with the publication of this book, *The CEH Prep Guide*, Ronald Krutz and Russell Vines have given us a single book on ethical hacking that will be a similar benchmark in the field. This is the book I wish I could have given to the hundreds of officers that I taught how to penetrate highly secured government and military information systems.

— *Deputy Ross Mayfield*
Practitioner in Residence
National Security Program
University of New Haven



Acknowledgments

I want to thank my wife, Hilda, for her continuous support during this project.

— R.L.K.

I would like to thank all my friends, and especially my wife, Elzy, for their continual support.

— R.D.V.

Both authors would like to express a special thanks to Carol Long and Christopher J. Rivera of John Wiley and Sons for their support and assistance in developing this text.



Introduction

The EC-Council (www.eccouncil.org) Certified Ethical Hacker (CEH) certification is designed to qualify skilled information system security professionals in performing ethical attacks against target information systems to assist an organization in developing preemptive approaches against hackers. A CEH understands the tools and methods used by malicious individuals against networks and applies his or her skills to help organizations identify vulnerabilities in their systems.

The *CEH Prep Guide* prepares candidates for the CEH certification examination by providing in-depth coverage of the latest hacking techniques required to pass the qualifying CEH 312-50 or ECO-350 examinations. The subject matter is presented in a concise, professional manner in an easy-to-understand format and includes review questions at the end of each chapter to test a candidate's knowledge of the material. The included CD, with many hundreds of questions and answers, also serves as a self-paced examination review and knowledge reinforcement tool.

In addition to technical content, the *CEH Prep Guide* emphasizes the legal and ethical requirements associated with ethical hacking and the increased professional responsibility that goes along with the CEH certification.

Because this book provides a focused presentation of the CEH material, it is extremely valuable to professionals seeking to advance their careers, levels of competence, and recognition in the Ethical Hacking and penetration testing field. The knowledge gained is applicable to commercial, industrial, military, and government organizations.

The CEH certification also makes an individual a much-desired employee to an organization. This professional brings the knowledge of security threats, penetration testing, vulnerability analysis, risk mitigation, business-related issues,

and countermeasures to an organization along with the means to upgrade an organization's defenses in an effective and cost-efficient manner. The CEH has knowledge of both offensive and defense measures in order to protect an organization's information systems.

Exam Eligibility

To sit for the CEH certification examination, a candidate must either have attended a CEH course at an EC-Council Accredited Training Center or prepare through self-study. In the self-study path, the candidate must have at least two years of information system security experience endorsed by his or her employer. If the candidate does not have two years of experience but has educational experience, he or she can submit a request to EC-Council for consideration on a case-by-case basis.

No matter which path the CEH candidate chooses, the CEH Prep Guide is a valuable tool for acquiring the necessary knowledge to prepare for and pass the CEH exam. The clear and detailed explanations of key ethical hacking topics along with the hundreds of review questions greatly increase the candidate's chances of success when taking the CEH examination.

The CEH Examination Application Form (ECO-350) can be downloaded from the EC-Council website (www.eccouncil.org/CEH.htm) and the completed form should be faxed to the EC-Council at +1-212-202-3500 for verification. After verification, the candidate will receive an eligibility voucher number that can be used to register and schedule the test at any Authorized Prometric Testing Center globally. The cost of the examination is USD 250.

EC-Council offers two examinations: Exam 312-50 and Exam ECO-350. Only students who have undergone training at an EC-Council Accredited Training Center are eligible to appear for the Web-based Prometric Prime Exam 312-50. Self-study candidates are authorized to sit for the ECO-350 Exam at an Authorized Prometric Testing Center. Both exams are identical in source and lead to the CEH certification.

The examination comprises 150 questions with a four hour time period in which to complete the exam. The exam duration is four and one half hours for Non-English speaking countries. A score of 70 percent is required to pass the exam.

The CEH Exam can be retaken with no restrictions or waiting period, if necessary. The CEH certification is valid for 2 years and EC-Council Professional Education Credits (EPE) are required to maintain the certification. If the candidate passes the examination, he or she will receive a welcome kit in eight week's time.

Additional information can be found at the EC-Council website.