

**CEH Certified Ethical Hacker Certification Exam**  
**Preparation Course in a Book for Passing the CEH**  
**Certified Ethical Hacker Exam:**

The 'How to Pass on Your First Try' Certification Study Guide

**Notice of Rights:** *Copyright © The Art Of Service. All rights reserved. No part of this book may be reproduced or transmitted in any form by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of the publisher.*

**Notice of Liability:** *The information in this book is distributed on an “As Is” basis without warranty. While every precaution has been taken in the preparation of the book, neither the author nor the publisher shall have any liability to any person or entity with respect to any loss or damage caused or alleged to be caused directly or indirectly by the instructions contained in this book or by the products described in it.*

**Trademarks:** *Many of the designations used by manufacturers and sellers to distinguish their products are claimed as trademarks. Where those designations appear in this book, and the publisher was aware of a trademark claim, the designations appear as requested by the owner of the trademark. All other product names and services identified throughout this book are used in editorial fashion only and for the benefit of such companies with no intention of infringement of the trademark. No such use, or the use of any trade name, is intended to convey endorsement or other affiliation with this book.*

## Foreword

*The Art of Service is an Accredited Training Organization and has been training IT professionals since 1998. The strategies and content in this book are a result of experience and understanding of the Certified Ethical Hacker methods, and the exam requirements.*

*This Exam Preparation book is intended for those preparing for the Certified Ethical Hacker Exam. This book is **not** a replacement for completing the course. This is a study aid to assist those who have completed an accredited course and preparing for the exam. Do not underestimate the value of your own notes and study aids. The more you have, the more prepared you will be.*

*While it is not possible to pre-empt every question and content that MAY be asked in the CEH exam, this book covers the main concepts covered within the Certified Ethical Hacker discipline.*

*The CEH exam certifies individuals in the specific network security discipline of Ethical Hacking from a vendor-neutral perspective. The Certified Ethical Hacker certification will fortify the application knowledge of security officers, auditors, security professionals, site administrators, and anyone who is concerned about the integrity of the network infrastructure. A Certified Ethical Hacker is a skilled professional who understands and knows how to look for the weaknesses and vulnerabilities in target systems and uses the same knowledge and tools as a malicious hacker.*

*Due to licensing rights, we are unable to provide actual CEH Exam. However, the study notes and sample exam questions in this book will allow you to appropriately prepare for the CEH exam.*

*The Art of Service*

<http://www.theartofservice.com/>

## **Write a Review and Receive a Bonus Emereo eBook of Your Choice**

### ***Up to \$99 RRP – Absolutely Free***

*If you recently bought this book we would love to hear from you – submit a review of this title and you'll receive an additional free ebook of your choice from our catalog at <http://www.emereo.org>.*

### ***How Does it Work?***

*Submit your review of this title via the online store where you purchased it. For example, to post a review on Amazon, just log in to your account and click on the 'Create Your Own Review' button (under 'Customer Reviews') on the relevant product page (you'll find plenty of example product reviews on Amazon). If you purchased from a different online store, simply follow their procedures.*

### ***What Happens When I Submit my Review?***

*Once you have submitted your review, send us an email via [review@emereo.org](mailto:review@emereo.org), and include a link to your review and a link to the free eBook you'd like as our thank-you (from <http://www.emereo.org> – choose any book you like from the catalog, up to \$99 RRP). You will then receive a reply email back from us, complete with your bonus ebook download link. It's that simple!*

## 2 Table of Contents

1	Foreword .....	1
2	Table of Contents .....	3
3	Cisco Certified Entry Networking Technician .....	12
4	Exam Specifics .....	13
5	Exam Prerequisites.....	13
6	Ethics.....	14
6.1	Terminology .....	14
6.2	The Ethical Hacker .....	15
6.3	Security and Hacking .....	15
6.3.1	Foundation of Security – C.A.I.A .....	15
6.3.2	Phases of Ethical Hacking.....	16
6.4	Hacking Technologies .....	16
6.5	Phase of Ethical Hacking.....	17
6.5.1	Reconnaissance.....	17
6.5.2	Scanning.....	18
6.5.3	Gaining Access .....	18
6.5.4	Maintaining Access .....	19
6.5.5	Covering Tracks .....	19
6.6	Hacker Classes .....	20
6.6.1	Black Hats.....	20
6.6.2	White Hats .....	20
6.6.3	Gray Hats.....	20
6.7	Hactivism.....	21
6.8	Skills of an Ethical Hacker .....	21
6.8.1	Focus of an Ethical Hacker.....	21
6.8.2	Profile of an Ethical Hacker .....	21
6.8.3	Actions of an Ethical Hacker.....	22
6.8.4	Skills of an Ethical Hacker .....	22
6.9	Vulnerability Research .....	23
6.10	Methods of a Ethical Hacker .....	23
6.10.1	Preparation .....	24
6.10.2	Conduct Security Evaluation .....	24
6.10.3	Conclusion .....	25
6.10.4	Issues for Ethical Hacking .....	25
6.11	Legal Implications .....	25
6.11.1	Crime Statistics .....	25
6.11.2	United States Federal Code on Computer Crimes.....	26

6.11.3	Crimes and Criminal Procedure Section 1029 .....	26
6.11.4	Crimes and Criminal Procedure Section 1030 .....	28
7	Footprinting.....	33
7.1	Defining Footprinting .....	33
7.1.1	Google Hacking.....	34
7.2	Gathering Information.....	34
7.2.1	The Information Gathering Methodology .....	34
7.2.2	Uncovering Initial Information .....	34
7.2.3	Locating Network Ranges .....	35
7.3	Competitive Intelligence .....	36
7.4	DNS Enumeration .....	36
7.5	Lookups .....	37
7.5.1	Whois.....	37
7.5.2	Nslookup.....	37
7.5.3	ARIN .....	38
7.5.4	SmartWhois.....	38
7.6	Types of DNS Records.....	39
7.7	Using traceroute.....	39
7.7.1	NeoTrace (McAfee Visual Trace) .....	40
7.7.2	VisualLookout.....	40
7.8	E-mail Tracking .....	41
7.8.1	emailTrackerPro.....	41
7.8.2	Mail Tracking.....	41
7.9	Web Spiders.....	41
8	Social Engineering.....	42
8.1	Defining Social Engineering .....	42
8.2	Common Types of Attacks .....	42
8.2.1	Human-Based Attacks.....	42
8.2.2	Computer-Based Attacks.....	43
8.3	Insider Attacks.....	43
8.4	Identity Theft .....	43
8.5	Phishing .....	43
8.6	Online Scams.....	44
8.7	URL Obfuscation.....	44
8.8	Countermeasures.....	44
9	Scanning .....	45
9.1	Define Scanning.....	45
9.1.1	Port Scanning.....	45
9.1.2	Network Scanning .....	46
9.1.3	Vulnerability Scanning.....	47
9.1.4	Detection of Scanning .....	47

- 9.1.5 Passive Scans..... 47
- 9.1.6 Active Scans ..... 47
- 9.1.7 Interactive Scans..... 48
- 9.2 CEH Scanning Methodology ..... 48
  - 9.2.1 Method..... 48
- 9.3 Ping Sweeps ..... 48
  - 9.3.1 Technique Used ..... 49
  - 9.3.2 Detecting Ping Sweeps ..... 49
  - 9.3.3 Identifying Open Ports and Services ..... 50
  - 9.3.4 Countering Port Scans ..... 50
- 9.4 Nmap Command Switches ..... 50
  - 9.4.1 Port States ..... 51
  - 9.4.2 Common Scan Methods..... 51
  - 9.4.3 Common NMAP Commands ..... 51
- 9.5 Types of Scans ..... 52
  - 9.5.1 SYN scans ..... 52
  - 9.5.2 XMAS scans..... 53
  - 9.5.3 FIN scans..... 53
  - 9.5.4 NULL scans..... 53
  - 9.5.5 IDLE scans..... 53
- 9.6 TCP Communication Flag Types..... 54
  - 9.6.1 TCP Flag Types ..... 54
  - 9.6.2 TCP Scan Types ..... 54
  - 9.6.3 Hacking Tools ..... 55
- 9.7 War Dialers ..... 56
  - 9.7.1 Tools Used..... 56
- 9.8 Banner Grabbing and OF Fingerprinting Techniques ..... 56
  - 9.8.1 Banner Grabbing..... 57
  - 9.8.2 Fingerprinting ..... 57
- 9.9 Proxy Servers..... 57
  - 9.9.1 Tools for Hackers ..... 58
- 9.10 Anonymizers..... 58
- 9.11 HTTP Tunneling Techniques ..... 58
  - 9.11.1 Hacking Tools Used ..... 59
- 9.12 IP Spoofing Techniques..... 59
- 10 Enumeration ..... 60
  - 10.1 Define Enumeration ..... 60
    - 10.1.1 Hacking Tools Used ..... 61
  - 10.2 Null Sessions..... 61
    - 10.2.1 Connecting a Null Session ..... 62
    - 10.2.2 Countermeasures Available ..... 62

- 10.2.3 SNMP Enumeration..... 63
- 10.2.4 Hacking Tools Used ..... 64
- 10.2.5 SNMP Countermeasures..... 64
- 10.3 Windows 2000 DNS Zone Transfer..... 64
  - 10.3.1 Zone Transfer Countermeasures..... 65
  - 10.3.2 LDAP Enumeration..... 65
- 10.4 Performing Enumeration ..... 66
  - 10.4.1 System Hacking ..... 66
- 10.5 Password Cracking Techniques..... 66
  - 10.5.1 LanManager Hash..... 67
  - 10.5.2 Windows 2000 Passwords ..... 68
  - 10.5.3 SMB Logon Redirection ..... 68
  - 10.5.4 SMB Relay MITM Attacks..... 69
  - 10.5.5 NetBIOS DoS Attacks ..... 69
  - 10.5.6 Countermeasures Against Password Cracking..... 69
- 10.6 Types of Passwords..... 70
  - 10.6.1 Types of Password Attacks ..... 71
  - 10.6.2 Passive Online Attacks..... 71
  - 10.6.3 Active Online Attacks ..... 72
  - 10.6.4 Offline attacks ..... 73
  - 10.6.5 Non-electronic Attacks ..... 74
- 10.7 Escalating Privileges..... 74
  - 10.7.1 Executing Applications ..... 74
  - 10.7.2 Buffer Overflows..... 75
- 10.8 Spyware Technologies..... 75
  - 10.8.1 Other Spyware Technologies ..... 75
- 10.9 Hiding Files..... 76
  - 10.9.1 Alternate Data Streams ..... 76
  - 10.9.2 Countermeasures to NTFS Streaming..... 77
- 10.10 Rootkits..... 77
  - 10.10.1 Rootkits on Windows 2000 and NP..... 77
  - 10.10.2 Rootkits Embedded TCP/IP Stack ..... 78
  - 10.10.3 Countermeasures to Rootkits..... 78
- 10.11 Steganography ..... 79
  - 10.11.1 Stenography Tools..... 79
  - 10.11.2 Countermeasures to Stegnography ..... 79
- 10.12 Covering Tracks..... 80
  - 10.12.1 Disabling Audits..... 80
  - 10.12.2 Clearing the Event Log ..... 80
- 11 Trojans and Backdoors ..... 81
  - 11.1 Defining Trojans..... 81

11.2	Overt and Covert Channels.....	82
11.3	Types of Trojans .....	83
11.4	Netcat Trojans .....	83
11.5	Wrapping .....	84
11.6	Reverse-Connecting Trojans .....	84
11.7	Preventing Trojans.....	84
11.8	Trojan Evading Techniques .....	85
12	Virus and Worms .....	86
12.1	Differences Between Viruses and Worms .....	86
12.2	Types of Viruses .....	86
12.2.1	What Can Be Infected .....	86
12.2.2	How Viruses Infect .....	87
12.3	Antivirus Evasion Techniques.....	87
12.4	Virus Detection Methods.....	88
13	Sniffers .....	89
13.1	Susceptible Protocols .....	89
13.2	Defining Sniffing.....	89
13.3	ARP Poisoning.....	90
13.3.1	Preventing ARP Spoofing.....	90
13.4	Ethernet Filters.....	91
13.5	MAC Flooding.....	91
13.6	DNS Spoofing.....	91
13.6.1	How DNS Spoofing Works .....	92
13.6.2	Types of DNS Spoofing.....	92
13.7	Sniffing Countermeasures .....	92
14	Denial of Service.....	93
14.1	Types of DoS Attacks .....	93
14.2	DDoS Attacks .....	93
14.3	BOTs/BOTNETS.....	94
14.3.1	Using BOTs.....	94
14.3.2	Using BOTNETs.....	95
14.4	Smurf Attacks .....	95
14.5	SYN Flooding .....	95
14.5.1	Preventing SYN Floods .....	96
14.6	DoS/DDoS Countermeasures .....	96
15	Session Hijacking .....	97
15.1	Spoofing vs. Hijacking.....	97
15.2	Types of Session Hijacking.....	97
15.3	Sequence Prediction.....	98
15.3.1	Sequence Numbering.....	98
15.3.2	Sequence Predictions .....	98



15.4	Dangers Posed By Session Hijacking .....	99
15.5	Prevent Session Hijacking .....	99
16	Hacking Web Servers .....	100
16.1	Types of Web Server Vulnerabilities .....	100
16.2	Attacks Against Web Servers.....	100
16.3	IIS Unicode Exploits.....	101
16.4	Patch Management.....	102
16.5	Web Application Scanners.....	102
16.6	Metasploit Framework.....	102
16.7	Web Server Hardening .....	103
17	Web Application Vulnerabilities.....	104
17.1	Web Applications .....	104
17.2	Web Application Hacking .....	104
17.3	Anatomy of an Attack.....	105
17.4	Web Application Threats.....	105
17.5	Google Hacking .....	106
17.6	Web Application Countermeasures.....	106
18	Web Based Password Cracking Techniques .....	107
18.1	Authentication Types .....	107
18.2	Password Cracker .....	107
18.3	Using a Password Cracker .....	108
18.4	Password Attacks - Classification .....	108
18.5	Password Cracking Countermeasures.....	108
19	SQL Injection.....	109
19.1	SQL Injection.....	109
19.2	Conducting SQL Injection .....	109
19.3	SQL Server Vulnerabilities.....	110
19.4	SQL Injection Countermeasures .....	110
20	Buffer Overflows .....	111
20.1	Types of Buffer Overflows.....	111
20.2	Stack-Based Buffer Overflows .....	111
21	Wireless Hacking.....	113
21.1	WEP, WPA Authentication Systems .....	113
21.1.1	Wired Equivalent Privacy (WEP) .....	113
21.1.2	Wi-Fi Protected Access (WPA).....	114
21.2	Wireless Sniffers and SSID, MAC Spoofing.....	115
21.3	Rogue Access Points.....	115
21.4	Wireless Hacking Techniques.....	116
21.5	Securing Wireless Networks .....	116
22	Physical Security .....	117
22.1	Physical Security Breach Incidents .....	117

22.2	Physical Security .....	117
22.2.1	Physical Measures .....	118
22.2.2	Technical Measures .....	118
22.2.3	Operational Measures .....	119
22.3	Need for Physical Security .....	119
22.4	Accountability for Physical Security .....	119
22.5	Factors Affecting Physical Security .....	120
23	Linux Hacking .....	121
23.1	Linux Kernels Compilation .....	121
23.1.1	Linux Basics .....	121
23.1.2	Linux Kernels .....	122
23.1.3	Compiling Linux Kernels .....	122
23.2	Understand GCC Compilation Commands .....	123
23.3	LKM modules .....	123
23.4	Linux Hardening Methods .....	124
24	Evading IDS, Honeypots and Firewalls .....	125
24.1	Intrusion Detection Systems and Evasion Techniques .....	125
24.1.1	Types of IDS .....	125
24.1.2	Using IDS .....	126
24.2	Firewall and Honeypot Evasion Techniques .....	127
24.2.1	Evading Firewalls and Honeypots .....	127
25	Cryptography .....	128
25.1	Cryptography and Encryption Techniques .....	128
25.2	Public and Private Keys .....	129
25.3	Algorithms .....	129
25.3.1	Types of Algorithm .....	130
26	Penetration Testing Methodologies .....	131
26.1	Security Assessments .....	131
26.2	Penetration Testing Methodologies .....	132
26.3	Penetration Testing Steps .....	132
26.3.1	Pre-Attack Phase .....	133
26.3.2	Attack Phase .....	133
26.3.3	Post-Attack Phase .....	134
26.4	Pen-Test Legal Framework .....	135
26.5	Pen-Test Deliverables .....	135
26.6	Automated Penetration Testing Tools .....	136
27	Practice Exam .....	137
27.1	Refresher “Warm up Questions” .....	137
28	Answer Guide .....	148
28.1	Answers to Questions .....	148
29	References .....	154