

Computer Security Lab Manual

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

ĐẠI HỌC QUỐC GIA HÀ NỘI
TRUNG TÂM THÔNG TIN THƯ VIỆN

A - D0/04902

McGraw-Hill
Irwin

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

Contents

	ABOUT THE AUTHORS	IV
	ACKNOWLEDGMENTS	VI
	BOOK INTRODUCTION	XIII
SECTION 1	NETWORKING BASICS: HOW DO NETWORKS WORK?	I
Chapter 1	WORKSTATION NETWORK CONFIGURATION AND CONNECTIVITY	3
	Lab 1: Network Workstation Client Configuration	6
	Lab 1a: Windows Client Configuration (ipconfig/ping/arp)	8
	Lab 1b: Linux Client Configuration (ifconfig/ping/arp)	15
	Lab 2: Computer Name Resolution	27
	Lab 2a: Windows (nslookup)	28
	Lab 2b: Linux (nslookup)	34
	Lab 3: Network Routing Basics (routing)	43
	Lab 3c: Network Routing Basics	43
	Lab 4: Network Communication Analysis	58
	Lab 4a: Windows Network Communication Analysis (Ethereal)	59
	Lab 4b: Linux Network Communication Analysis (Ethereal)	66
Chapter 2	TCP/UDP BASICS	79
	Lab 5: TCP Basics	80
	Lab 5a: TCP Three-Way Handshake in Windows	84
	Lab 5b: TCP Three-Way Handshake in Linux	89
	Lab 6: UDP Basics	98
	Lab 6a: Windows UDP Basics	100
	Lab 6b: Linux UDP Basics	103

Chapter 3	NETWORK APPLICATIONS	111
	Lab 7: FTP Communications	114
	Lab 7a: Windows FTP Communication (FTP-HTTP)	115
	Lab 7b: Linux FTP Communication (FTP-HTTP)	121
	Lab 8: Port Connection Status	132
	Lab 8a: Windows-Based Port Connection Status (netstat)	133
	Lab 8b: Linux-Based Port Connection Status (netstat)	138
	Lab 9: E-mail Protocols—SMTP and POP	147
	Lab 9b: Linux E-mail—SMTP and POP	148
	Lab 9c: Windows E-mail—SMTP and POP	154
	Lab 10: E-mail Client Software	165
	Lab 10b: Linux E-mail Client Software (Evolution)	166
	Lab 10c: Windows E-mail Client Software (Outlook Express)	173
	Lab 11a: Windows Network Management (Net Command)	183
SECTION 2	VULNERABILITIES AND THREATS—HOW CAN NETWORKS BE COMPROMISED?	195
Chapter 4	SCANNING AND ENUMERATING THE NETWORK FOR TARGETS	197
	Lab 12: IP Address and Port Scanning, Service Identity Determination	199
	Lab 12a: Nmap—IP Scanning in Windows	201
	Lab 12b: Nmap—IP Scanning in Linux	209
	Lab 13d: Researching System Vulnerabilities	222
	Lab 14: GUI-Based Vulnerability Scanners	230
	Lab 14a: NeWT—Using a Vulnerability Scanner in Windows	231
	Lab 14b: Nessus—Using a Vulnerability Scanner in Linux	239

Chapter 5	ATTACKS—WEB SERVER, E-MAIL, DOS, AND TROJAN ATTACKS	253
	Lab 15: Web Server Exploits	255
	Lab 15a: Web Server Exploits	256
	Lab 16: E-mail System Exploits	266
	Lab 16b: Exploiting E-mail Vulnerabilities in Linux	268
	Lab 16c: Exploiting E-mail Vulnerabilities in Windows	275
	Lab 17: Denial of Service Exploits	288
	Lab 17a: Windows Denial of Service SMBDie	289
	Lab 17b: Linux Denial of Service Syn Flood	294
	Lab 18: Trojan Attacks	305
	Lab 18a: Using the Netbus Trojan	306
	Lab 18a2: Using the SubSeven Trojan	314
Chapter 6	ESCALATING PRIVILEGE—SNIFFING, KEYLOGGING, PASSWORD-CRACKING ATTACKS	327
	Lab 19: Intercepting and Sniffing Network Traffic	329
	Lab 19b: Sniffing Network Traffic in Linux	330
	Lab 19c: Sniffing Network Traffic in Windows	334
	Lab 20: Keystroke Logging	343
	Lab 20a: Keystroke Logging in Windows	344
	Lab 20b: Keystroke Logging in Linux	348
	Lab 21: Password Cracking	356
	Lab 21a: Password Cracking in Windows	358
	Lab 21b: Password Cracking in Linux	363