Preface 1

Chapter 1 : Up and Running with BackTrack 7
Introduction 8
Installing BackTrack to a hard disk drive 8
Installing BackTrack to a USB drive with persistent memory 13
Installing BackTrack on VirtualBox 16
Installing BackTrack Using Vmware Tools 21
Fixing the splash screen 23
Changing the root password 23
Starting network services 24
Setting up the wireless network 26

Chapter 2 : Customizing BackTrack 29
Introduction 30
Preparing kernel headers 30
Installing Broadcom drivers 31
Installing and configuration ATI video card drivers 34
Installing and configuration NVIDIA video card drivers 38
Applying updates and configuring extra security tools 41
Setting up ProxyChains 43
Directory encryption 45

Chapter 8 : Voice over IP (VoIP) 221
Introduction 222
Using Svmap 223
Finding valid extensions 225
Monitoring, capturing and eavesdropping on VoIP traffic 228
Using VoIPong 232
Mastering UCSniff 234
Mastering Xplico 240
Capturing SIP authentication 242
Mastering VoIP Hopper 244
Causing a denial of service 246
Attacking VoIP uisng Metasploit 247
Sniffing DECT phones 249

Chapter 9 : Password Cracking 253
Introduction 254
Online password attacks 255
Cracking HTTP passwords 259
Gaining router access 263
Password profiling 267
Cracking a Windows password using John the Ripper 274
Using dictionary attacks 275
Using rainbow tables 279
Using NVIDIA Compute Unified Device Architecture (CUDA) 281
Using ATI Stream 284
Physical access attacks 287

Chapter 3 : Information Gathering 49
Introduction 50
Service enumeration 50
Determing the network range 54
Identifying active machines 58
Finding open ports 59
Operating system fingerprinting 62
Service fingerprinting 63
Threat assessment with Maltego 65
Mapping the network 70

Chapter 4 : Vulnerability Identification 77
Introduction 78
Installing, configuring, and starting Nessus 79
Nessus – finding local vulnerabilities 82
Nessus – finding network vulnerabilities 86
Nessus – finding linux-specific vulnerabilities 91
Nessus – finding Windows-specific vulnerabilities 95
Installing, configuring, and starting OpenVAS 99
OpenVAS – finding local vulnerabilities 106
OpenVAS – finding network vulnerabilies 112
OpenVAS – finding Linux-specific vulnerabilities 117
OpenVAS – finding Window-specific vulnerabilities 122

Chapter 5 : Exploitation 129
Introduction 130
Implementing exploits from BackTrack 130
Installing and configurating Metasploitable 133
Mastering Armitage – the graphical management tool for Metasploit 138
Mastering the Metasploit Console (MSFCONSOLE) 141
Mastering the Metasploit CLI (MSFCLI) 144
Mastering Meterpreter 148
Metasploitable MySQL 151
Metsaploitable PostgreSQL 154
Metasploitable Tomcat 158
Metasploitable PDF 160
Implementing the browser_autopwn module 163

Chapter 6 : Privilege Escalation 167
Introduction 168
Using impersonating tokens 168
Local privilege escalation attack 171
Mastering the Social-Engineering Toolkit (SET) 172
Collecting victims' data 179
Cleaning up the tracks 181
Creating a persistent backdoor 183
Man-in-the-middle attack (MITM) 186

Chapter 7 : Wireless Network Analysis 191
Introduction 192
Cracking a WEP wireless network 192
Cracking a WPA/WPA2 wireless network 197
Automating wireless network cracking 200
Accessing clients using a fake AP 203
URL traffic manipulation 206
Port redirection 207
Sniffing network traffic 209
Access. ıg an e-mail by stealing cookies 214

Chapter 10 : BackTrack Forensics 289
Introduction 290
Intrusion detection and log analysis 290
Recursive directory encryption/decryption 295
Rescanning for signs of rootkits 300
Recovering data from a problematic source 303
Retrieving a Window password 307
Resetting a Windows-password 311
Looking at the Windows registry entries 313

Conclusion 315