Table of Contents

Preface 1

Chapter 1: Wireless Lab Setup 7

Hardware requirements 8
Software requirements 8
Installing BackTrack 8
Time for action – installing BackTrack 9
Setting up the access point 12
Time for action – configuring the access point 12
Setting up the wireless card 15
Time for action – configuring your wireless card 16
Connecting to the access point 17
Time for action – configuring your wireless card 18
Summary 22

Chapter 2: WLAN and Its Inherent Insecurities 23

Revisiting WLAN frames 24
Time for action – creating a monitor mode interface 26
Time for action – sniffing wireless packets 29
Time for action – viewing Management, Control, and Data frames 32
Time for action – sniffing data packets for our network 36
Time for action – packet injection 40
Important note on WLAN sniffing and injection 42
Time for action – experimenting with your Alfa card 42
Role of regulatory domains in wireless 45
Time for action – experimenting with your Alfa card 45
Summary 49

Chapter 3: Bypassing WLAN Authentication 51

Hidden SSIDs 51
Time for action – uncovering hidden SSIDs 52

This material is copyright and is licensed for the sole use by Haran, Varun on 21st September 2011
-, -, -, -

MAC filters 57
Time for action – beating MAC filters 57
Open Authentication 60
Time for action – bypassing Open Authentication 60
Shared Key Authentication 62
Time for action – bypassing Shared Authentication 63
Summary 71

Chapter 4: WLAN Encryption Flaws 73
WLAN encryption 73
WEP encryption 74
Time for action – cracking WEP 74
WPA/WPA2 82
Time for action – cracking WPA-PSK weak passphrase 85
Speeding up WPA/WPA2 PSK cracking 89
Time for action – speeding up the cracking process 90
Decrypting WEP and WPA packets 94
Time for action – decrypting WEP and WPA packets 94
Connecting to WEP and WPA networks 96
Time for action – connecting to a WEP network 96
Time for action – connecting to a WPA network 97
Summary 99

Chapter 5: Attacks on the WLAN Infrastructure 101
Default accounts and credentials on the access point 101
Time for action – cracking default accounts on the access points 102
Denial of service attacks 104
Time for action – De-Authentication DoS attack 104
Evil twin and access point MAC spoofing 107
Time for action – evil twin with MAC spoofing 108
Rogue access point 112
Time for action – Rogue access point 112
Summary 116

Chapter 6: Attacking the Client 117
Honeypot and Mis-Association attacks 118
Time for action – orchestrating a Mis-Association attack 118
Caffe Latte attack 124
Time for action – conducting the Caffe Latte attack 124
De-Authentication and Dis-Association attacks 129
Time for action – De-Authenticating the client 129
Hirte attack 133
Time for action – cracking WEP with the Hirte attack 133

This material is copyright and is licensed for the sole use by Haran, Varun on 21st September 2011
-, -, -, -

AP-less WPA-Personal cracking 135
Time for action – AP-less WPA cracking 137
Summary 140
Chapter 7: Advanced WLAN Attacks 141
Man-in-the-Middle attack 141
Time for action – Man-in-the-Middle attack 142
Wireless Eavesdropping using MITM 147
Time for action – wireless eavesdropping 147
Session Hijacking over wireless 152
Time for action – session hijacking over wireless 153
Finding security configurations on the client 156
Time for action – enumerating wireless security profiles 157
Summary 161
Chapter 8: Attacking WPA-Enterprise and RADIUS 163
Setting up FreeRadius-WPE 163
Time for action – setting up the AP with FreeRadius-WPE 164
Attacking PEAP 168
Time for action – cracking PEAP 168
Attacking EAP-TTLS 173
Time for action – cracking EAP-TTLS 174
Security best practices for Enterprises 176
Summary 177
Chapter 9: WLAN Penetration Testing Methodology 179
Wireless penetration testing 179
Planning 180
Discovery 180
Time for action – discovering wireless devices 181
Attack 183
Finding rogue access points 183
Finding unauthorized clients 185
Cracking the encryption 186
Compromising clients 189
Reporting 191
Summary 192
Appendix A: Conclusion and Road Ahead 193
Wrapping up 193
Building an advanced Wi-Fi lab 194
Staying up-to-date 196
Conclusion 197

This material is copyright and is licensed for the sole use by Haran, Varun on 21st September 2011
-, -, -, -

Appendix B: Pop Quiz Answers 199
Chapter 1, Wireless Lab Setup 199
Chapter 2, WLAN and its Inherent Insecurities 199
Chapter 3, Bypassing WLAN Authentication 200
Chapter 4, WLAN Encryption Flaws 200
Chapter 5, Attacks on the WLAN Infrastructure 200
Chapter 6, Attacking the Client 201
Chapter 7, Advanced WLAN Attacks 201
Chapter 8, Attacking WPA Enterprise and RADIUS 201
Chapter 9, Wireless Penetrating Testing Methodology 202
Index 203

This material is copyright and is licensed for the sole use by Haran, Varun on 21st September 2011
-, -, -, -