

WiFi Hacking

TABLE OF CONTENTS

Preface	1	Introduction	30	WPA /WPA2	99	Time for action – De-Authenticating the client	156	Introduction	218
Introduction	2	Revisiting WLAN frames	31	Time for action – cracking WPA-PSK weak passphrase	102	Hirte attack	161	Wireless penetration testing	218
What this book covers	3	Time for action – creating a monitor mode interface	34	Speeding up WPA/ WPA2 PSK cracking	107	Time for action –cracking WEP with the Hirte attack	161	Planning	219
What you need for this book	6	Time for action – sniffing wireless packets	37	Time for action – speeding up the cracking process	108	AP-less WPA-Personal cracking	164	Discovery	220
Who this book is for	7	Time for action – viewing Management, Control, and Data frames	40	Decrypting WEP and WPA packets	112	Time for action – AP-less WPA cracking	166	Time for action – discovering wireless devices	220
Reader feedback	8	Time for action – sniffing data packets for our network	45	Time for action – decrypting WEP an WPA packets	113	Summary	169	Attack	223
Errata	8	Time for action – packet injection	49	Connecting to WEP and WPA networks	115	Chapter 7 . Advanced WLAN Attacks	171	Finding rogue access points	223
Chapter 1 . Wireless Lab Setup	9	Important note on WLAN sniffing and injection	51	Time for action – connecting to a WEP network	115	Introduction	172	Finding unauthorized clients	226
Introduction	10	Time for action – experimenting with your Alfa card	52	Time for action – connecting to a WPA network	116	Man-in-the-Middle attack	173	Cracking the encryption	227
Hardware requirements	11	Role of regulatory domains in wireless	55	Summary	118	Time for action – Man-in-the-Middle attack	173	Compromising Clients	230
Software requirements	12	Time for action – experimenting with your Alfa card	55	Chapter 5 . Attacks on the WLAN Infrastructure	119	Wireless Eavesdropping using MITM	180	Reporting	232
Installing BackTrack	12	Summary	59	Introduction	120	Time for action – wireless eavesdropping	180	Summary	233
Time for action – installing BackTrack	12	Chapter 3 . Bypassing WLAN Authentication	61	Default accounts and credentials on the access point	121	Session Hijacking over wireless	186	Conclusion	235
Setting up the access point	16	Introduction	62	Time for action – cracking default accounts on the access points	121	Time for action – session hijacking over wireless	186	Introduction	236
Time for action – configuring the access point	16	Hidden SSIDs	62	Denial of service attacks	124	Finding security configurations on the client	191	Wrapping up	236
Setting up the wireless card	20	Time for action – uncovering hidden SSIDs	63	Time for action – De-Authentication DoS attack	124	Time for action – enumerating wireless security profiles	192	Building an advanced Wi-Fi lab	237
Time for action – configuring your wireless card	20	MAC filters	69	Evil twin and access point MAC spoofing	128	Summary	196	Staying up-to-date	240
Connecting to the access point	22	Time for action – beating MAC filters	69	Time for action –evil twin with MAC spoofing	129	Chapter 8 . Attacking WPA-Enterprise and RADIUS	197	Conclusion	242
Time for action – configuring your wireless card	22	Open Authentication	74	Rogue access point	134	Introduction	198	Introduction	236
Summary	27	Time for action – bypassing Open Authentication	74	Time for action – Rogue access point	135	Setting up FreeRadius-WPE	198	Wrapping up	236
Chapter 2 . WLAN and Its Inherent Insecurities	29	Shared Key Authentication	75	Summary	139	Time for action – setting up the AP with FreeRadius-WPE	199	Building an advanced Wi-Fi lab	237
Introduction	29	Time for action – bypassing Shared Authentication	77	Chapter 6 . Attacking the Client	141	Attacking PEAP	205	Staying up-to-date	240
WLAN encryption	29	Summary	85	Introduction	142	Time for action – cracking PEAP	206	Conclusion	242
WEP encryption	89	Chapter 4 . WLAN Encryption Flaws	87	HoneyPot and Mis-Association attacks	143	Attacking EAP-TTLS	211		
Time for action – cracking WEP	90	Introduction	88	Time for action – orchestrating a Mis-Association attack	144	Time for action – cracking EAP-TTLS	212		
		WLAN encryption	89	Caffe Latte attack	150	Security best practices for Enterprises	214		
		WEP encryption	89	Time for action – conducting the Caffe Latte attack	151	Summary	215		
		Time for action – cracking WEP	90	De-Authentication and Dis-Association attacks	156	Chapter 9 . WLAN Penetration Testing Methodology	217		
						Introduction	217		