1. Record Nr. UNINA9910781707903321

Autore	Ramachandran Vivek
Titolo	BackTrack 5 wireless penetration testing [[electronic resource]] : beginner's guide : master bleeding edge wireless testing techniques with BackTrack 5 / / Vivek Ramachandran
Pubbl/distr/stampa	Birmingham [U.K.], : Packt Pub. Ltd., 2011
ISBN	1-62198-900-3 1-283-30827-4 9786613308276 1-84951-559-X
Descrizione fisica	1 online resource (220 p.)
Disciplina	005.8
Soggetti	Computers - Access control Penetration testing (Computer security) Computer networks - Security measures - Testing
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	"Learn by doing: less theory, more results"--Cover. Includes index.
Nota di bibliografia	Includes index.
Nota di contenuto	Cover; Copyright; Credits; About the Author; About the Reviewer; www.PacktPub.com; Table of Contents; Preface; Chapter 1:Wireless Lab Setup; Hardware requirements; Software requirements; Installing BackTrack; Time for action - installing BackTrack; Setting up the access point; Time for action - configuring the access point; Setting up the wireless card; Time for action - configuring your wireless card; Connecting to the access point; Time for action - configuring your wireless card; Summary; Chapter 2:WLAN and ItsInherent Insecurities; Revisiting WLAN frames Time for action - creating a monitor mode interfaceTime for action - sniffing wireless packets; Time for action - viewing Management, Control, And Data frames; Time for action - sniffing data packets for our network; Time for action - packet injection; Important note on WLAN sniffing and injection; Time for action - experimenting with your Alfa card; Role of regulatory domains in wireless; Time for action - experimenting with your Alfa card; Summary; Chapter 3:Bypassing

WLAN Authentication; Hidden SSIDs; Time for action - uncovering hidden SSIDs; MAC filters
Time for action - beating MAC filtersOpen Authentication; Time for action - bypassing Open Authentication; Shared Key Authentication; Time for action - bypassing Shared Authentication; Summary; Chapter 4:WLAN Encryption Flaws; WLAN encryption; WEP encryption; Time for action - cracking WEP; WPA/WPA2; Time for action - cracking WPA-PSK weak passphrase; Speeding up WPA/WPA2 PSK cracking; Time for action - speeding up the cracking process; Decrypting WEP and WPA packets; Time for action - decrypting WEP and WPA packets; Connecting to WEP and WPA networks
Time for action - connecting to a WEP networkTime for action - connecting to a WPA network; Summary; Chapter 5:Attacks on the WLANInfrastructure; Default accounts and credentials on the access point; Time for action - cracking default accounts on the access; points; Denial of service attacks; Time for action - De-Authentication DoS attack; Evil twin and access point MAC spoofing; Time for action - evil twin with MAC spoofing; Rogue access point; Time for action - Rogue access point; Summary; Chapter 6:Attacking the Client; Honeypot and Mis-Association attacks
Time for action - orchestrating a Mis-Association attackCaffe Latte attack; Time for action - conducting the Caffe Latte attack; De-Authentication and Dis-Association Attacks; Time for action - De-Authenticating the client; Hirte attack; Time for action - cracking WEP with the Hirte attack; AP-less WPA-Personal cracking; Time for action - AP-less WPA cracking; Summary; Chapter 7:Advanced WLAN Attacks; Man-in-the-Middle attack; Time for action - Man-in-the-Middle attack; Wireless Eavesdropping using MITM; Time for action - Wireless Eavesdropping; Session Hijacking over wireless
Time for action - Session hijacking over wireless

Sommario/riassunto

Master bleeding edge wireless testing techniques with BackTrack 5.