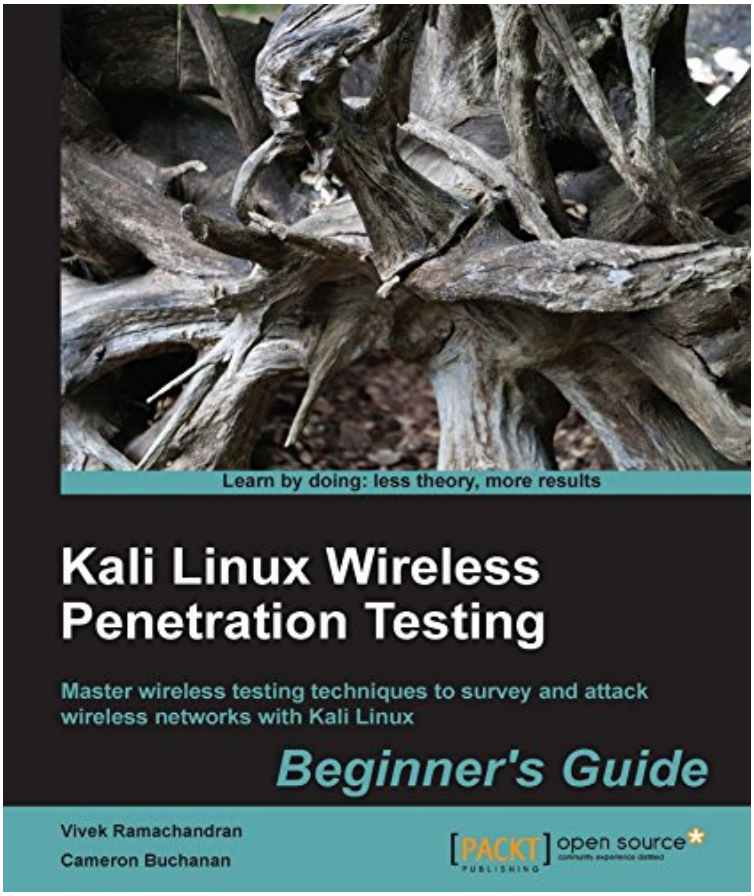
Kali Linux Wireless Penetration Testing: Beginner's Guide

Von Vivek Ramachandran, Cameron Buchanan
**Download PDF | ePub | DOC | audiobook | ebooks*



Produktinformation -Verkaufsrang: #420809 in eBooksVerffentlicht am: 2015-03-30Erscheinungsdatum: 2015-03-30File Name: B00VGE6ABC | File size: 63.Mb

Von Vivek Ramachandran, Cameron Buchanan : Kali Linux Wireless Penetration Testing: Beginner's Guide before purchasing it in order to gage whether or not it would be worth my time, and all praised Kali Linux Wireless Penetration Testing: Beginner's Guide:

KundenrezensionenHilfreichste Kundenrezensionen1 von 1 Kunden fanden die folgende Rezension hilfreich. Etwas oberflchlichVon jayrockIch habe das Buch als Kindle Edition gekauft mit dem Ziel, die Wireless-Tools von Kali besser kennen zu lernen. Das Buch liefert eine strukturierte Anleitung zum Aufbau eines WLAN-Testbeds und eine gute Einfhrung in die aircrack-ng-Suite.Leider ist das dann auch alles. Weitere Tools, wie z.B. Wireshark oder reaver werden nur kurz angesprochen und der Leser aufgefordert, die entsprechende Dokumentation zu lesen. Andere Tools wie wifihoney oder wifite werden gar nicht behandelt. Insgesamt wird Kali auf die Platform zur Durchfhrung der Beispiele reduziert. Mit anderen Linux-Distros lsst sich dies genauso durchfhren. M.E. wre "Introduction to aircrack-ng" ein treffenderer Titel.Ich habe das Buch in etwa zwei Stunden durchgelesen, fr den aufgerufenen Preis finde es das etwas dnn.0 von 0 Kunden fanden die folgende Rezension hilfreich. Nachfolger vom gleichen Backtrack-BuchVon Herbert AppelMan merkt, dass im Vorgngerbuch einfach nur das Wort "Backtrack" durch "Kali" ersetzt wurde -

meistens :-)Viele Unstimmigkeiten im Buch.

KurzbeschreibungKey FeaturesLearn wireless penetration testing with Kali Linux, the latest iteration of BacktrackDetect hidden wireless networks and discover their namesExplore advanced Wi-Fi hacking techniques including rogue access point hosting and probe sniffingDevelop your encryption cracking skills and gain an insight into the methods used by attackers and the underlying technologies that facilitate these attacksBook Description As wireless networks become ubiquitous in our lives, wireless penetration testing has become a key skill in the repertoire of the professional penetration tester. The Kali Linux security distribution comes with a myriad of tools used for networking attacks and detecting security loopholes.Kali Linux Wireless Penetration Testing Beginner's Guide presents wireless pentesting from the ground up, introducing all elements of penetration testing with each new technology. Learn various wireless testing methodologies by example, from the basics of wireless routing and encryption through to detailed coverage of hacking methods and attacks such as the Hirte and Caffe Latte.What you will learnCreate a wireless lab for your experimentsSniff out wireless packets and hidden networksCapture and crack WPA-2 keysDiscover hidden SSIDsExplore the ins and outs of wireless technologiesSniff probe requests and track users through SSID historyAttack radius authentication systemsSniff wireless traffic and collect interesting dataDecrypt encrypted traffic with stolen keysAbout the AuthorsVivek Ramachandran has been working in Wireless Security since 2003. He discovered the Caffe Latte attack and also broke WEP Cloaking, a WEP protection schema, publicly in 2007 at DEF CON. In 2011, he was the first to demonstrate how malware could use Wi-Fi to create backdoors, worms, and even botnets. Earlier, he was one of the programmers of the 802.1x protocol and Port Security in Cisco's 6500 Catalyst series of switches and was also one of the winners of the Microsoft Security Shootout contest held in India among a reported 65,000 participants. He is best known in the hacker community as the founder of SecurityTube.net, where he routinely posts videos on Wi-Fi Security and exploitation techniques.Cameron Buchanan is an experienced penetration tester, having worked in a huge range of industries. He is also the author of Packt's Kali Linux CTF Blueprints.Table of ContentsWireless Lab SetupWLAN and its Inherent InsecuritiesBypassing WLAN AuthenticationWLAN Encryption FlawsAttacks on the WLAN InfrastructureAttacking the ClientAdvanced WLAN AttacksAttacking WPA-Enterprise and RadiusWLAN Penetration Testing MethodologyWPS and ProbesKurzbeschreibungKey FeaturesLearn wireless penetration testing with Kali Linux, the latest iteration of BacktrackDetect hidden wireless networks and discover their namesExplore advanced Wi-Fi hacking techniques including rogue access point hosting and probe sniffingDevelop your encryption cracking skills and gain an insight into the methods used by attackers and the underlying technologies that facilitate these attacksBook Description As wireless networks become ubiquitous in our lives, wireless penetration testing has become a key skill in the repertoire of the professional penetration tester. The Kali Linux security distribution comes with a myriad of tools used for networking attacks and detecting security loopholes.Kali Linux Wireless Penetration Testing Beginner's Guide presents wireless pentesting from the ground up, introducing all elements of penetration testing with each new technology. Learn various wireless testing methodologies by example, from the basics of wireless routing and encryption through to detailed coverage of hacking methods and attacks such as the Hirte and Caffe Latte.What you will learnCreate a wireless lab for your experimentsSniff out wireless packets and hidden networksCapture and crack WPA-2 keysDiscover hidden SSIDsExplore the ins and outs of wireless technologiesSniff probe requests and track users through SSID historyAttack radius authentication systemsSniff wireless traffic and collect interesting dataDecrypt encrypted traffic with stolen keysAbout the AuthorsVivek Ramachandran has been working in Wireless Security since 2003. He discovered the Caffe Latte attack and also broke WEP Cloaking, a WEP protection schema, publicly in 2007 at DEF CON. In 2011, he was the first to demonstrate how malware could use Wi-Fi to create backdoors, worms, and even botnets. Earlier, he was one of the programmers of the 802.1x protocol and Port Security in Cisco's 6500 Catalyst series of switches and was also one of the winners of the Microsoft Security Shootout contest held in India among a reported 65,000 participants. He is best known in the hacker community as the founder of SecurityTube.net, where he routinely posts videos on Wi-Fi Security and exploitation techniques.Cameron Buchanan is an experienced penetration tester, having worked in a huge range of industries. He is also the author of Packt's Kali Linux CTF Blueprints.Table of ContentsWireless Lab SetupWLAN and its Inherent InsecuritiesBypassing WLAN AuthenticationWLAN Encryption FlawsAttacks on the WLAN InfrastructureAttacking the ClientAdvanced WLAN AttacksAttacking WPA-Enterprise and RadiusWLAN Penetration Testing MethodologyWPS and Probesber den Autor und weitere MitwirkendeVivek Ramachandran Vivek Ramachandran has been working on Wi-Fi Security since 2003. He discovered the Caffe Latte attack and also broke WEP Cloaking, a WEP protection schema, publicly in 2007 at DEF CON. In 2011, he was the first to demonstrate how malware could use Wi-Fi to create backdoors, worms, and even botnets. Earlier, he was one of the programmers of the 802.1x protocol and Port Security in Cisco's 6500 Catalyst series of switches and was also one of the winners of the Microsoft Security Shootout contest held in India among a reported 65,000 participants. He is best known in the hacker community as the founder of SecurityTube.net, where he

routinely posts videos on Wi-Fi Security, assembly language, exploitation techniques, and so on. SecurityTube.net receives over 100,000 unique visitors a month. Vivek's work on wireless security has been quoted in BBC Online, InfoWorld, MacWorld, The Register, IT World Canada, and so on. This year, he will speak or train at a number of security conferences, including Blackhat, Defcon, Hacktivity, 44con, HITB-ML, BruCON Derbycon, Hashdays, SecurityZone, SecurityByte, and so on.Cameron Buchanan Cameron Buchanan is a penetration tester by trade and a writer in his spare time. He has performed penetration tests around the world for a variety of clients across many industries. Previously, he was a member of the RAF. He enjoys doing stupid things, such as trying to make things fly, getting electrocuted, and dunking himself in freezing cold water in his spare time. He is married and lives in London.