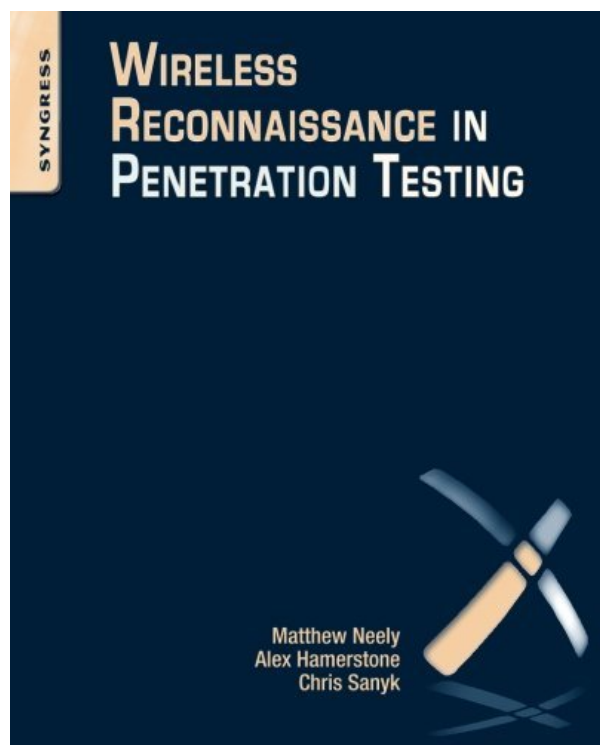
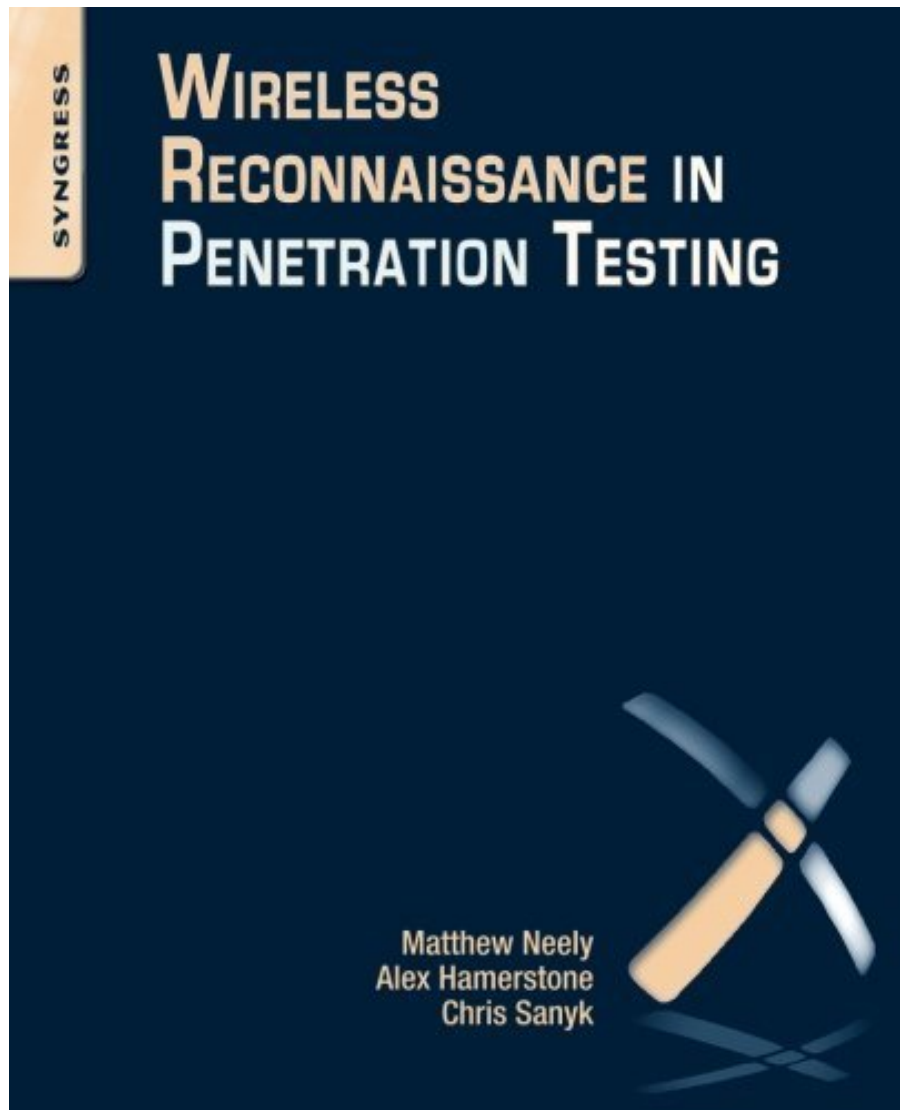


**WIRELESS RECONNAISSANCE IN
PENETRATION TESTING BY MATTHEW
NEELY, ALEX HAMERSTONE, CHRIS
SANYK**



**DOWNLOAD EBOOK : WIRELESS RECONNAISSANCE IN PENETRATION
TESTING BY MATTHEW NEELY, ALEX HAMERSTONE, CHRIS SANYK PDF**





Click link bellow and free register to download ebook:

**WIRELESS RECONNAISSANCE IN PENETRATION TESTING BY MATTHEW NEELY, ALEX
HAMERSTONE, CHRIS SANYK**

[DOWNLOAD FROM OUR ONLINE LIBRARY](#)

WIRELESS RECONNAISSANCE IN PENETRATION TESTING BY MATTHEW NEELY, ALEX HAMERSTONE, CHRIS SANYK PDF

Yet, just how is the means to obtain this publication Wireless Reconnaissance In Penetration Testing By Matthew Neely, Alex Hamerstone, Chris Sanyk Still puzzled? It does not matter. You could appreciate reviewing this e-book Wireless Reconnaissance In Penetration Testing By Matthew Neely, Alex Hamerstone, Chris Sanyk by online or soft data. Just download the publication Wireless Reconnaissance In Penetration Testing By Matthew Neely, Alex Hamerstone, Chris Sanyk in the link offered to visit. You will get this Wireless Reconnaissance In Penetration Testing By Matthew Neely, Alex Hamerstone, Chris Sanyk by online. After downloading and install, you could conserve the soft documents in your computer or gizmo. So, it will reduce you to review this publication Wireless Reconnaissance In Penetration Testing By Matthew Neely, Alex Hamerstone, Chris Sanyk in particular time or place. It could be uncertain to delight in reviewing this publication [Wireless Reconnaissance In Penetration Testing By Matthew Neely, Alex Hamerstone, Chris Sanyk](#), since you have bunches of work. Yet, with this soft documents, you could delight in checking out in the extra time even in the gaps of your works in office.

Review

"Despite the increasingly number of wireless devices, these security and information technology professionals contend that physical penetration tests for defending computer systems and companies neglect wireless traffic outside of Bluetooth and 802.11 devices and thus, often miss testing other wireless devices such as guard radios, wireless headsets, and cordless phones."--Reference and Research Book News, August 2013

From the Back Cover

In many penetration tests, there is a lot of useful information to be gathered from the radios used by organizations. These radios can include two-way radios used by guards, wireless headsets, cordless phones and wireless cameras. Wireless Reconnaissance in Penetration Testing describes the many ways that a penetration tester can gather and apply the information available from radio traffic. Stopping attacks means thinking like an attacker, and understanding all the ways that attackers gather information, or in industry terms profile, specific targets. With information from what equipment to use and how to find frequency information, to tips for reducing radio information leakage, to actual case studies describing how this information can be used to attack computer systems, this book is the go-to resource for penetration testing and radio profiling.

About the Author

Matthew Neely (CISSP, CTGA, GCIH, GCWN) is the Profiling Team Manager at SecureState, a Cleveland,

Ohio-based security consulting company.

Alex Hamerstone, CTGA - Security Consultant, Risk Management.

Chris Sanyk is a journeyman IT professional with over twelve years of experience with everything from desktop publishing and web design, to user support, to system administration, to software development. In his spare time, he blogs and develops video games at his website, csanyk.com.

WIRELESS RECONNAISSANCE IN PENETRATION TESTING BY MATTHEW NEELY, ALEX HAMERSTONE, CHRIS SANYK PDF

[Download: WIRELESS RECONNAISSANCE IN PENETRATION TESTING BY MATTHEW NEELY, ALEX HAMERSTONE, CHRIS SANYK PDF](#)

Why should wait for some days to obtain or get the book **Wireless Reconnaissance In Penetration Testing By Matthew Neely, Alex Hamerstone, Chris Sanyk** that you order? Why must you take it if you could get Wireless Reconnaissance In Penetration Testing By Matthew Neely, Alex Hamerstone, Chris Sanyk the faster one? You could discover the very same book that you buy here. This is it the book Wireless Reconnaissance In Penetration Testing By Matthew Neely, Alex Hamerstone, Chris Sanyk that you could get straight after purchasing. This Wireless Reconnaissance In Penetration Testing By Matthew Neely, Alex Hamerstone, Chris Sanyk is well known book around the world, naturally many individuals will aim to own it. Why don't you end up being the initial? Still perplexed with the means?

This is why we suggest you to constantly see this web page when you need such book *Wireless Reconnaissance In Penetration Testing By Matthew Neely, Alex Hamerstone, Chris Sanyk*, every book. By online, you may not go to get guide shop in your city. By this on-line library, you can discover the book that you truly wish to read after for very long time. This Wireless Reconnaissance In Penetration Testing By Matthew Neely, Alex Hamerstone, Chris Sanyk, as one of the recommended readings, has the tendency to remain in soft documents, as all of book collections here. So, you could likewise not get ready for couple of days later to get as well as read guide Wireless Reconnaissance In Penetration Testing By Matthew Neely, Alex Hamerstone, Chris Sanyk.

The soft file means that you have to go to the web link for downloading and after that conserve Wireless Reconnaissance In Penetration Testing By Matthew Neely, Alex Hamerstone, Chris Sanyk You have actually possessed guide to check out, you have actually posed this Wireless Reconnaissance In Penetration Testing By Matthew Neely, Alex Hamerstone, Chris Sanyk It is simple as visiting the book shops, is it? After getting this quick description, with any luck you can download one and start to check out Wireless Reconnaissance In Penetration Testing By Matthew Neely, Alex Hamerstone, Chris Sanyk This book is extremely simple to read every single time you have the spare time.

WIRELESS RECONNAISSANCE IN PENETRATION TESTING BY MATTHEW NEELY, ALEX HAMERSTONE, CHRIS SANYK PDF

In many penetration tests, there is a lot of useful information to be gathered from the radios used by organizations. These radios can include two-way radios used by guards, wireless headsets, cordless phones and wireless cameras. *Wireless Reconnaissance in Penetration Testing* describes the many ways that a penetration tester can gather and apply the information available from radio traffic. Stopping attacks means thinking like an attacker, and understanding all the ways that attackers gather information, or in industry terms profile, specific targets. With information from what equipment to use and how to find frequency information, to tips for reducing radio information leakage, to actual case studies describing how this information can be used to attack computer systems, this book is the go-to resource for penetration testing and radio profiling.

- Author Matthew Neely is a respected and well-known expert and speaker on radio reconnaissance and penetration testing
- Includes real-world case studies of actual penetration tests using radio profiling
- Covers data leakage, frequency, attacks, and information gathering

- Sales Rank: #2203303 in Books
- Brand: Brand: Syngress
- Published on: 2012-11-12
- Released on: 2012-10-29
- Original language: English
- Number of items: 1
- Dimensions: 9.25" h x .42" w x 7.50" l, .85 pounds
- Binding: Paperback
- 226 pages

Features

- Used Book in Good Condition

Review

"Despite the increasingly number of wireless devices, these security and information technology professionals contend that physical penetration tests for defending computer systems and companies neglect wireless traffic outside of Bluetooth and 802.11 devices and thus, often miss testing other wireless devices such as guard radios, wireless headsets, and cordless phones."--Reference and Research Book News, August 2013

From the Back Cover

In many penetration tests, there is a lot of useful information to be gathered from the radios used by organizations. These radios can include two-way radios used by guards, wireless headsets, cordless phones and wireless cameras. *Wireless Reconnaissance in Penetration Testing* describes the many ways that a penetration tester can gather and apply the information available from radio traffic. Stopping attacks means thinking like an attacker, and understanding all the ways that attackers gather information, or in industry terms profile, specific targets. With information from what equipment to use and how to find frequency information, to tips for reducing radio information leakage, to actual case studies describing how this information can be used to attack computer systems, this book is the go-to resource for penetration testing and radio profiling.

About the Author

Matthew Neely (CISSP, CTGA, GCIH, GCWN) is the Profiling Team Manager at SecureState, a Cleveland, Ohio-based security consulting company.

Alex Hamerstone, CTGA - Security Consultant, Risk Management.

Chris Sanyk is a journeyman IT professional with over twelve years of experience with everything from desktop publishing and web design, to user support, to system administration, to software development. In his spare time, he blogs and develops video games at his website, csanyk.com.

Most helpful customer reviews

3 of 3 people found the following review helpful.

Great wireless book for wireless that isn't 802.11 & Bluetooth!

By Edward J. Smiley

Let me preface this review with this: I am a penetration tester, but I am a complete newbie when it comes to radio and radio theory. What was very helpful for me is that this book has a whole chapter (Chapter 2) on radio systems and theory, which really helped me learn everything I needed to know in order to add radio reconnaissance to my penetration testing arsenal.

There are two things that really stick out about this book:

1. The authors do an excellent job of applying the theory presented in the book with case studies of real life penetration tests. While there are case studies at the end of many chapters, there is a whole chapter (Chapter 8) dedicated to a penetration test on a casino. Yes, plenty of other books have case studies, but where this one stands out is that it includes additional sections on remediation and lessons learned. This was a welcome addition to the excellent case studies given. Many testers have to face this after the test: "I just broke it, how do I fix it!". This book gives you some help with the remediation process.

2. Many times throughout the book, the authors go the extra step to cover things that testers might forget about when performing the engagement, such as checking with local laws and making sure your scope and rules of engagement allow you perform that specific test. While you can find plenty of technical books, very few mention proper testing techniques beyond running the tool.

This book clearly reflects that the authors know their trade very well and is very well written and illustrated. *Wireless Reconnaissance in Penetration Testing* is great for someone just getting into radio (like me) or even the seasoned amateur radio operator. There is plenty of content outside the theory chapter, both on the radio side and the penetration test side. This is the first and only book I have seen combining radio theory with penetration testing and it should quickly become the standard read on this topic. Well done Matthew, Alex,

and Chris!

1 of 1 people found the following review helpful.

A great book for all levels - Highly recommended

By G.Reid

I bought this book to not only brush up on things that I already knew, but also to learn new tools and techniques that could help with performing penetration tests.

This book is great for people of all skill levels and should be read by all. The authors provided a nice blend of theory vs. real world in an easy-to-understand format. I would highly recommend this book to anyone that has an interest in the security field.

1 of 1 people found the following review helpful.

A great book

By John Leonardelli

Having been a radio nut for over 40 years i found the book to be well written. This area of a pen test would be easily overlooked.

See all 7 customer reviews...

WIRELESS RECONNAISSANCE IN PENETRATION TESTING BY MATTHEW NEELY, ALEX HAMERSTONE, CHRIS SANYK PDF

It's no any sort of faults when others with their phone on their hand, and you're as well. The difference might last on the material to open **Wireless Reconnaissance In Penetration Testing By Matthew Neely, Alex Hamerstone, Chris Sanyk** When others open up the phone for chatting and also talking all points, you can in some cases open up and also review the soft documents of the Wireless Reconnaissance In Penetration Testing By Matthew Neely, Alex Hamerstone, Chris Sanyk Certainly, it's unless your phone is available. You could additionally make or wait in your laptop or computer system that relieves you to read Wireless Reconnaissance In Penetration Testing By Matthew Neely, Alex Hamerstone, Chris Sanyk.

Review

"Despite the increasingly number of wireless devices, these security and information technology professionals contend that physical penetration tests for defending computer systems and companies neglect wireless traffic outside of Bluetooth and 802.11 devices and thus, often miss testing other wireless devices such as guard radios, wireless headsets, and cordless phones."--Reference and Research Book News, August 2013

From the Back Cover

In many penetration tests, there is a lot of useful information to be gathered from the radios used by organizations. These radios can include two-way radios used by guards, wireless headsets, cordless phones and wireless cameras. Wireless Reconnaissance in Penetration Testing describes the many ways that a penetration tester can gather and apply the information available from radio traffic. Stopping attacks means thinking like an attacker, and understanding all the ways that attackers gather information, or in industry terms profile, specific targets. With information from what equipment to use and how to find frequency information, to tips for reducing radio information leakage, to actual case studies describing how this information can be used to attack computer systems, this book is the go-to resource for penetration testing and radio profiling.

About the Author

Matthew Neely (CISSP, CTGA, GCIH, GCWN) is the Profiling Team Manager at SecureState, a Cleveland, Ohio-based security consulting company.

Alex Hamerstone, CTGA - Security Consultant, Risk Management.

Chris Sanyk is a journeyman IT professional with over twelve years of experience with everything from desktop publishing and web design, to user support, to system administration, to software development. In his spare time, he blogs and develops video games at his website, csanyk.com.

Yet, just how is the means to obtain this publication Wireless Reconnaissance In Penetration Testing By

Matthew Neely, Alex Hamerstone, Chris Sanyk Still puzzled? It does not matter. You could appreciate reviewing this e-book Wireless Reconnaissance In Penetration Testing By Matthew Neely, Alex Hamerstone, Chris Sanyk by online or soft data. Just download the publication Wireless Reconnaissance In Penetration Testing By Matthew Neely, Alex Hamerstone, Chris Sanyk in the link offered to visit. You will get this Wireless Reconnaissance In Penetration Testing By Matthew Neely, Alex Hamerstone, Chris Sanyk by online. After downloading and install, you could conserve the soft documents in your computer or gizmo. So, it will reduce you to review this publication Wireless Reconnaissance In Penetration Testing By Matthew Neely, Alex Hamerstone, Chris Sanyk in particular time or place. It could be uncertain to delight in reviewing this publication Wireless Reconnaissance In Penetration Testing By Matthew Neely, Alex Hamerstone, Chris Sanyk, since you have bunches of work. Yet, with this soft documents, you could delight in checking out in the extra time even in the gaps of your works in office.