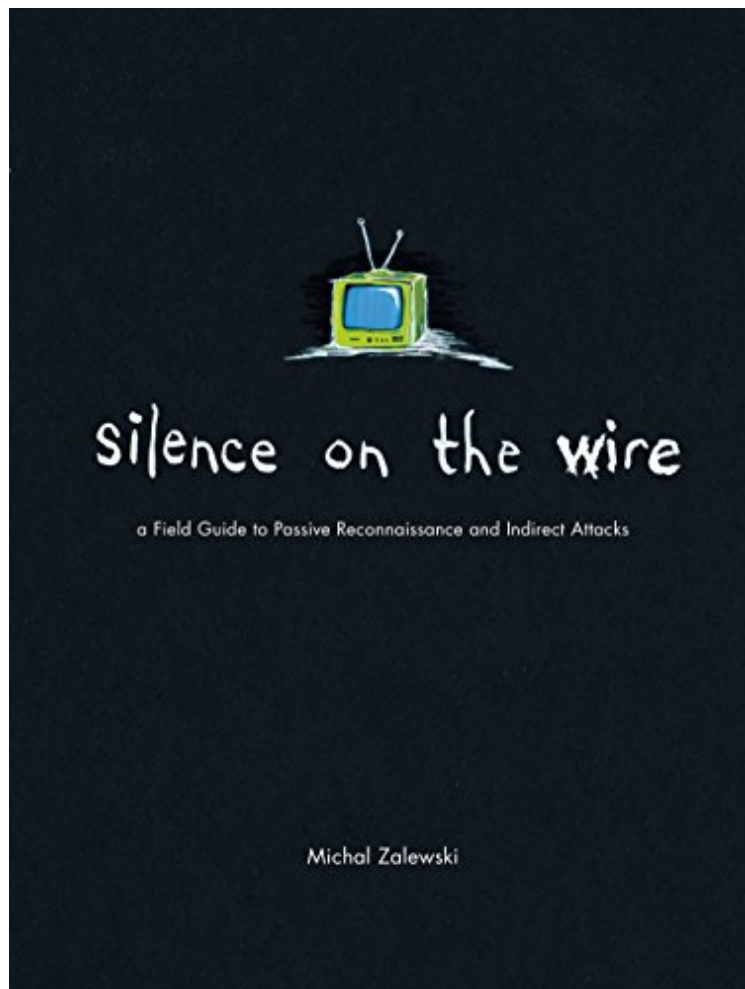


Silence on the Wire: A Field Guide to Passive Reconnaissance and Indirect Attacks

Von Michal Zalewski

DOC | *audiobook | ebooks | Download PDF | ePub



 Download

 Read Online

Produktinformation -Verkaufsrang: #90907 in eBooksVerffentlicht am: 2005-04-05Erscheinungsdatum: 2005-04-05File Name: B008FRNHVY | File size: 65.Mb

Von Michal Zalewski : Silence on the Wire: A Field Guide to Passive Reconnaissance and Indirect Attacks
before purchasing it in order to gage whether or not it would be worth my time, and all praised Silence on the Wire: A Field Guide to Passive Reconnaissance and Indirect Attacks:

KundenrezensionenHilfreichste Kundenrezensionen0 von 0 Kunden fanden die folgende Rezension hilfreich. Sehr informativ und kurzweiligVon T. W.Habe das Buch aus allgemeinem Interesse am Thema gekauft und war begeistert davon, wie der Autor das Buch inhaltlich aufgebaut hat und wie kurzweilig die teils sehr detaillierten technischen Ausfhrungen zu lesen sind.Neben dem, was man zum Thema Daten'lecks' lernt, nimmt man als Leser quasi "im Vorbeigehen" auch eine Menge an technischem Detailwissen ber einzelne Stellen in Computern und Netzwerkgeräten auf, was ich als einen groen Pluspunkt sehe.Alle behandelten Themen werden ausreichend ausgefñrt, so dass ein

grundlegendes Verständnis dafür da ist, was hier eigentlich das Problem ist und warum es sich ausnutzen und nicht "einfach" lösen lässt. Es schadet sicher nichts, ein bisschen Vorkenntnisse über den Aufbau von Computern und Netzwerken zu haben, ganz ohne dieses wird man während dem Lesen weiter inne halten und Wikipedia befragen müssen. 0 von 0 Kunden fanden die folgende Rezension hilfreich. Interessantes Buch Von nuklear86 Interessant geschriebenes Buch. Trotz englischer Sprache gut zu verstehen. Wer am Thema Interesse hat macht mit dem Buch nichts falsch.

Kurzbeschreibung Author Michal Zalewski has long been known and respected in the hacking and security communities for his intelligence, curiosity and creativity, and this book is truly unlike anything else out there. In *Silence on the Wire: A Field Guide to Passive Reconnaissance and Indirect Attacks*, Zalewski shares his expertise and experience to explain how computers and networks work, how information is processed and delivered, and what security threats lurk in the shadows. No humdrum technical white paper or how-to manual for protecting one's network, this book is a fascinating narrative that explores a variety of unique, uncommon and often quite elegant security challenges that defy classification and eschew the traditional attacker-victim model.

Kurzbeschreibung Author Michal Zalewski has long been known and respected in the hacking and security communities for his intelligence, curiosity and creativity, and this book is truly unlike anything else out there. In *Silence on the Wire: A Field Guide to Passive Reconnaissance and Indirect Attacks*, Zalewski shares his expertise and experience to explain how computers and networks work, how information is processed and delivered, and what security threats lurk in the shadows. No humdrum technical white paper or how-to manual for protecting one's network, this book is a fascinating narrative that explores a variety of unique, uncommon and often quite elegant security challenges that defy classification and eschew the traditional attacker-victim model.

Synopsis There are many ways that a potential attacker can intercept information, or learn more about the sender, as the information travels over a network. *Silence on the Wire* uncovers these silent attacks so that system administrators can defend against them, as well as better understand and monitor their systems. *Silence on the Wire* dissects several unique and fascinating security and privacy problems associated with the technologies and protocols used in everyday computing, and shows how to use this knowledge to learn more about others or to better defend systems. By taking an in-depth look at modern computing, from hardware on up, the book helps the system administrator to better understand security issues, and to approach networking from a new, more creative perspective. The sys admin can apply this knowledge to network monitoring, policy enforcement, evidence analysis, IDS, honeypots, firewalls, and forensics.