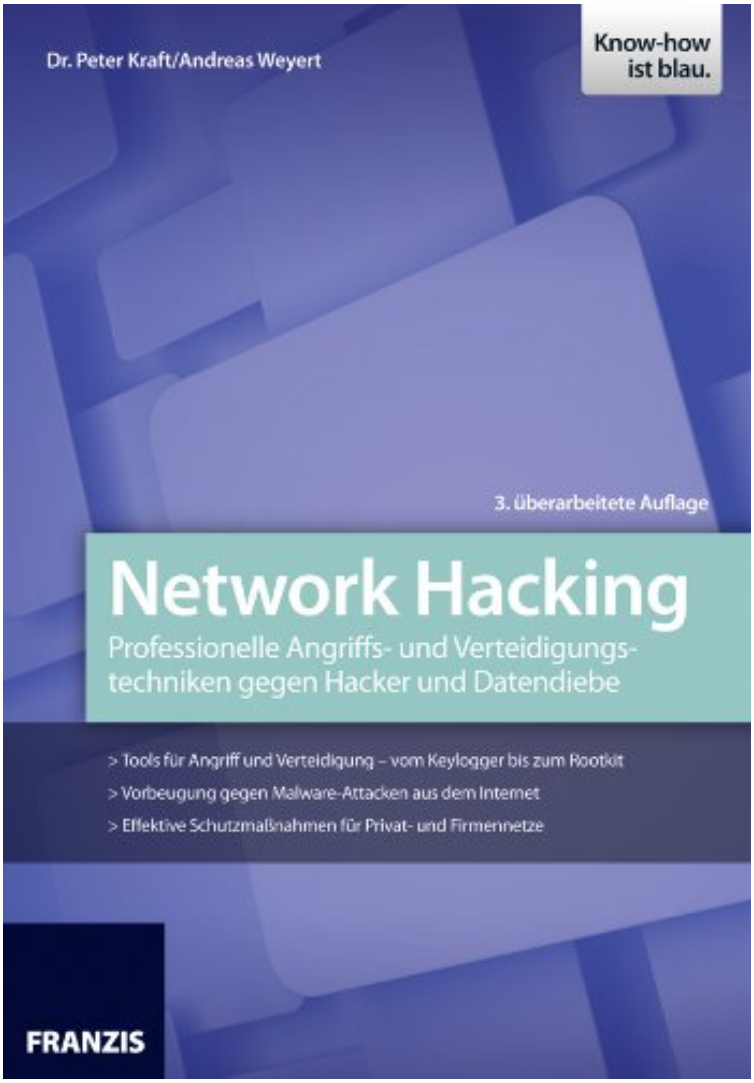
Network Hacking

Von Peter Kraft, Andreas Weyert
**Download PDF | ePub | DOC | audiobook | ebooks*



Produktinformation -Verkaufsrang: #862104 in BcherVerffentlicht am: 2012-09-24Abmessungen: 9.72 x 1.61b x 7.01l, Einband: Broschiert600 Seiten | File size: 64.Mb

Von Peter Kraft, Andreas Weyert : Network Hacking before purchasing it in order to gage whether or not it would be worth my time, and all praised Network Hacking:

KundenrezensionenHilfreichste Kundenrezensionen4 von 5 Kunden fanden die folgende Rezension hilfreich. Sehr praxisorientiertVon jmoorsEin sehr an der Praxis orientiertes Buch, das anschaulich aufzeigt, wie Netzwerke gehackt werden. Bitte nur im privaten Bereich ben!

KurzbeschreibungDie Daten eines Unternehmens sind viel wert - egal ob aus Entwicklung, Geschftsfhrung oder Personalbuchhaltung. Hacker wissen das, knacken Firmennetze und richten dort erheblichen Schaden an, hufig vllig unbemerkt. Dieses Buch zeigt die wichtigsten Hacking-Tools, konkrete Angriffs- und Abwehrszenarien und die effektivsten Vorsorgemanahmen. Lassen Sie Hackern keine Chance! Als Poweruser, Netzwerkadministrator oder Sicherheitsprofi bekommen Sie mit diesem Buch Gelegenheit, den Autoren u. a. beim Knacken von Logins, Ausspionieren von Firmendaten, berwinden von Sicherheitssperren sowie bei Lauschangriffen und Penetrationstests ber die Schulter zu schauen und von ihrem Know-how zu profitieren. Teil I - Hacking -Tools: Nur wer wei, wie Hacking-Tools funktionieren, kann auch die passenden Abwehrmanahmen und -strategien dagegenstellen. Hier finden Sie die wichtigsten Ausstattungsmerkmale und Anwendungszwecke bersichtlich zum Nachschlagen. Teil II - Angriff und Abwehr: Die Angriffsziele von Hackern reichen von ungesicherten WLANs ber Internetseiten bis hin zu gut gesicherten Firmennetzen. Hier finden Sie einige der am hufigsten vorkommenden Angriffsszenarien, in denen die in Teil I geschilderten Tools zum Einsatz kommen - samt den passenden Abwehrstrategien. Teil III - Vorsorge: Im dritten Teil geht es um Prvention und Prophylaxe. Durch proaktives Sicherheitsmanagement verhindern Sie, dass es berhaupt erst zu erfolgreichen Angriffen kommt. Dabei spielt es keine Rolle, ob Sie das heimische WLAN oder das Netzwerk eines Unternehmens absichern wollen.