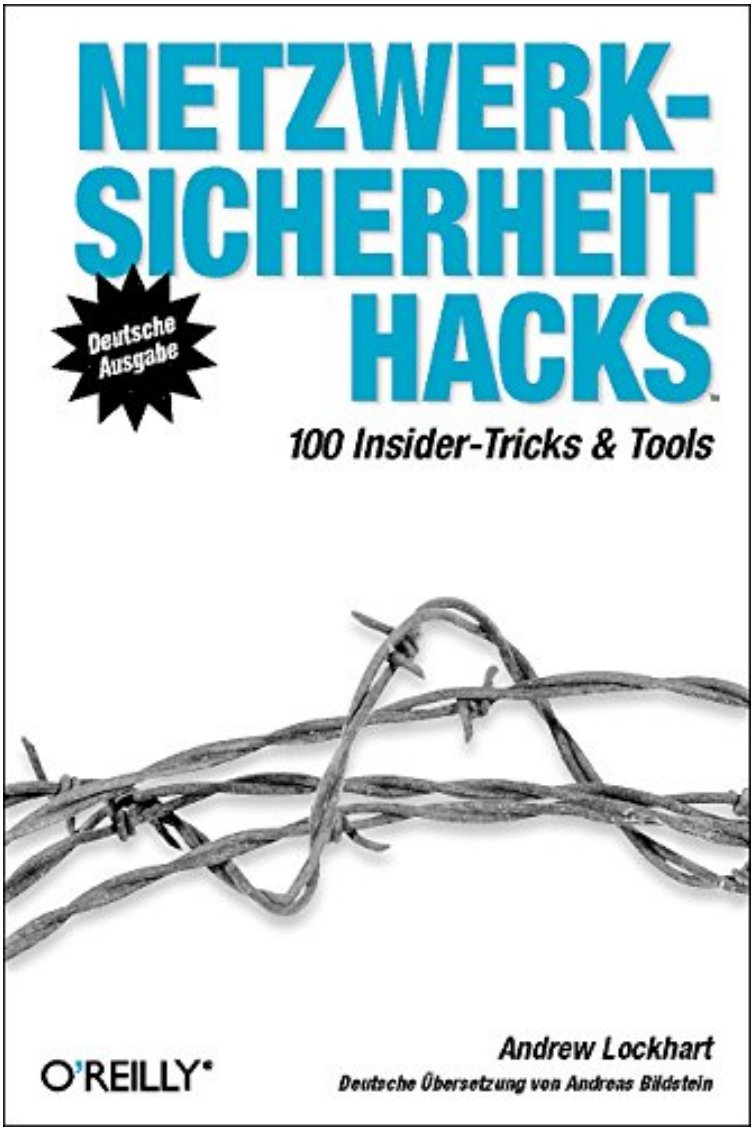
Netzwerksicherheit Hacks: 100 Insider-Tricks und Tools

Von Andrew Lockhart
*ePub | *DOC | audiobook | ebooks | Download PDF*



Produktinformation -Verkaufsrang: #1379747 in BcherMarke: O'reillyVerffentlicht am: 2004-09-01Einband: Taschenbuch362 Seiten | File size: 39.Mb

Von Andrew Lockhart : Netzwerksicherheit Hacks: 100 Insider-Tricks und Tools before purchasing it in order to gage whether or not it would be worth my time, and all praised Netzwerksicherheit Hacks: 100 Insider-Tricks und Tools:

KundenrezensionenHilfreichste Kundenrezensionen0 von 0 Kunden fanden die folgende Rezension hilfreich. ...;)Von KundeNa der Verlag spricht fr sich und der Autor ebenfalls. Der Windows oder Mac Nutzer hat vielleicht etwas weniger Spa an der Ausgabe als die mit Linux. Doch denke ich das es fr jeden sehr informativ ist.0 von 0 Kunden fanden die folgende Rezension hilfreich. Praxisorientierter berblick, leicht und gut verstndlich geschriebenVon

MAAlso gleich vorneweg, dieses Buch ist ein Lesegenuss, weil es A.Lockhart geschafft hat eine sehr komplexe Thematik leicht und verstndlich zu formulieren.Ich selbst sehe mich als interessierten Einsteiger auf dem Gebiet Netzwerke, habe manches vor Jahren auf der Uni im Rahmen des Elektrotechnik-Studiums mal gehrt,ohne es jedoch in der Tiefe zu verstehen. Ich kenne mich mit Unix aus der User-Perspektive und Linux als Administrator eines Heim-PCs aus.Das Buch ist in sinnvolle Kapitel unterteilt die sich den verschiedenen Sicherheitsaspekten widmen (Linux und Windows Server, Privatsphre, Firewalls etc.).In den Kapiteln finden sich dann die eigentlichen Hacks, das heisst, umfangreiche Tipps, wie man im Detail bestimmte Tools oder Programme einsetzen kann,um die Sicherheit zu erhhen oder Systemeinbrche festzustellen.Manchmal gibt es bei den Hacks Hintergrundinfos, doch meist bestehen sie aus einem Leitfaden, wie man z.B. ein Tool auf seinem Rechner einsetzen kann,wie es arbeitet, wozu es geeignet ist, wo man es bekommt, wie es installiert wird etc.Super finde ich, dass der Autor Hinweise und Lsungen fr Probleme mit der Installation gibt, falls es welche geben sollte.Wie gesagt, es geht nie besonders in die Tiefe zu jedem Hack, doch dafr kann man sich mit diesem Buch an den PC setzen und die Hacks ausprobieren.Deshalb sehe ich es als Praxis-Leitfaden und man sollte schon mal auf Shell-Ebene ein Programm unter Linux installiert haben, bzw. wissen wie man make benutzt.Und eben, weil es nicht so sehr in die Tiefe geht kann man es so leicht, Hack fr Hack lesen, auch wenn man es nicht am PC ausprobiert.Um einen konzeptuellen berblick von Netzwerk-Sicherheit zu bekommen halte ich es eher fr ungeeignet, ebenso wie frMenschen, die noch nie einen Befehl in einer Unix-Shell eingegeben haben.Viele der Hacks machen eigentlich nur im Zusammenhang der Server-Administration Sinn, und sind daher fr kleine Heimnetzwerke(Laptop PC ber LAN/WLAN an DSL) weniger hilfreich und anwendbar.Mir hat es einen guten Einblick verschafft, was Administratoren zu tun haben, um ein Netzwerk zuverlssig und sicher zu betreiben.Ebenso hab ich ein gutes Verstndnis der Sicherheits-Probleme in Netzwerken bekommen und meine Befrchtungen verloren,dass mein Heimnetzwerk eine leichte Beute fr Internet-Attacken ist.Es hat mir Spass gemacht dieses Buch zu lesen und sehr bereichert, deshalb 5 Sterne :)8 von 10 Kunden fanden die folgende Rezension hilfreich. Informative Vorstellung verschiedener Mglichkeiten (Hacks).Von SebastianIn acht Kapiteln und 100 "Hacks" ist beschrieben, wie man seinen Rechner, Server oder seine Netzwerke (besser) schtzen oder berwachen kann. Obwohl das Buch "Netzwerksicherheit Hacks" heit, reicht es nicht aus, nur das Netzwerk sicher zu machen. Daher gibt es im Buch neben Kapitel 3 ("Netzwerksicherheit") noch viele andere vorgestellte Sicherheitstechniken und Mglichkeiten.Das Buch beschrnkt sich nicht auf Linux oder BSD. Auch Windows wird behandelt. Trotzdem berwiegt der Unix-Bereich doch deutlich."Netzwerksicherheit Hacks" ist vielleicht nicht das im Vorwort erwhnte Zauberbuch - aber meiner Meinung nach eine sehr informative Zusammenstellung von einzelnen Mglichkeiten (Hacks). Das Buch beschreibt und stellt viele Programme vor, mit denen man die Sicherheit seines Netzwerkes verbessern kann. Es ist locker zu lesen, da es viele kleine Hacks enthlt, die je nach Interesse einzeln und grtenteils unabhngig voneinander gelesen werden knnen.Ich finde, "Netzwerksicherheit Hacks" hat einen Platz in "Armreichweite" verdient.

RezensionZurckgehackt: Andrew Lockhart geht mit seinem Netzwerksicherheit Hacks in die zweite Runde und hat diesmal mithilfe zahlreicher Sicherheitsprofis 125 Insider-Tricks und Tools auf den neusten Stand der Hackertechnik gebracht -- Abwehren, Erkennen und Verstehen lautet Lockharts Devise und liefert dafr die perfekte Vorlage. Jedes Kapitel beginnt mit einer kurzen Einfhrung, dann folgen die Hacks: eine kurze Darstellung des Problems und die entsprechende Herangehensweise bzw. Lsung. Tipps, Code und Erklrungen schildern dann die mglichen Patches fr Kernel, Tools wie Tor oder Verschlsselungssysteme. Lockhart beginnt mit der Unix-Host-Sicherheit, berhaupt liegt der Schwerpunkt auf auf der Unix-Welt, aber das ist angesichts der Mehrheit der Unix-Netzwerkstrukturen kein Wunder. Hier zeigt er die Hrtung von Linux-, FreeBSD- oder OpenBSD-Servern. Als nchstes Windows-Host-Sicherheit: Sicherheitslcken beseitigen und bekannte Angriffsflchen absichern. Darauf folgen Kapitel zu Privatsphre und Anonymitt, Firewalls, Verschlsseln und sichern von Diensten, Netzwerksicherheit sowie die Sicherheit von Drahtlossystemen, die Protokollierung, Monitoring und Trending, Tunnel, Netzwerk-Intrusion-Detection und schlielich zum Abschluss die Wiederherstellung und Reaktion auf Vorflle. Dazu am Buchende zum Schnellauffinden ein Index. Mit der 2. Ausgabe seine Netzwerksicherheit Hacks-Buchs fasst Lockart alles zusammen, was man als Admin wissen muss, um gegen die neusten Hack-Angriffe von auen gewappnet zu sein -- wer von diesem Erfahrungsschatz profitiert, vermeidet es, alles selbst durch schlechte Erfahrung erlernen zu mssen. --Wolfgang TreKurzbeschreibungWir htten dieses Buch auch Hacker gegen Cracker nennen knnen: Hier zeigen die guten Jungs mit cleveren Insider-Tricks, wie man den bsen Jungs auf die Schliche kommt und Schaden fr die eigenen Systeme abwehrt oder begrenzt. Mit seinen fortgeschrittenen Hacks fr Unix- und Windows-Server (einschlielich 2003) beschftigt sich dieses Buch vor allem mit dem Absichern von TCP/IP-basierten Diensten. Daneben bietet es aber auch eine ganze Reihe von raffinierten hostbasierten Sicherheitstechniken. Systemadministratoren, die schnelle Lsungen fr reale Sicherheitsprobleme bentigen, finden hier prgnante Beispiele fr Systemhrtung, angewandte Verschlsselung, Intrusion Detection, sicheres Tunneling, Logging und Monitoring, Incident Response und vieles mehr. Jeder Hack kann in wenigen Minuten gelesen werden, erspart Ihnen aber mglicherweise viele Stunden fr Nachforschungen nach

einem Einbruch, Nachtschichten zur Wiederherstellung des Systems und jede Menge grauer Haare. Die 100 Hacks behandeln unter anderem diese Sicherheitstechniken: * Hrten von Linux-, BSD- und Windows-Systemen gegenber Angriffen * Netzwerke und Dienste mit Intrusion-Detection-Systemen wie Snort und Spade berwachen * Einrichtung von virtuellen Netzwerken (Honeypots), um Angreifer zu tuschen und zu verwirren * E-Mail und andere entscheidende Dienste mit starker Verschlsselung schtzen * Netzwerk-Scanner abblocken, die Betriebssystem-Identitten erkennen und vortuschen * Mit VPN-Lsungen (inkl. IPSec, OpenVPN, PPTP, VTun und SSH) entfernte Sites sicher ber das Internet verbinden * Vorgehensweise nach Einbrchenber den Autor und weitere MitwirkendeAndrew Lockhart stammt ursprnglich aus South Carolina, hat seinen Wohnsitz jetzt aber im Norden von Colorado, wo er seine Zeit mit dem Versuch verbringt, die schwarze Kunst der berprfung von disassemblierten Binrdateien zu erlernen, und sich davor zu bewahren, sich zu Tode zu frieren. Er besitzt einen Abschluss in Informatik der Colorado State University und hat in dieser Gegend Sicherheitsberatungen fr kleine Unternehmen durchgefhrt. Wenn er nicht gerade schreibt, arbeitet er derzeit bei einem der Fortune 100-Unternehmen. In seiner Freizeit arbeitet er an Snort-Wireless (http://snort-wireless.org), einem Projekt, das darauf abzielt, mit dem populren Open Source-IDS-System Snort auch drahtlose Intrusion Detection zu untersttzen.