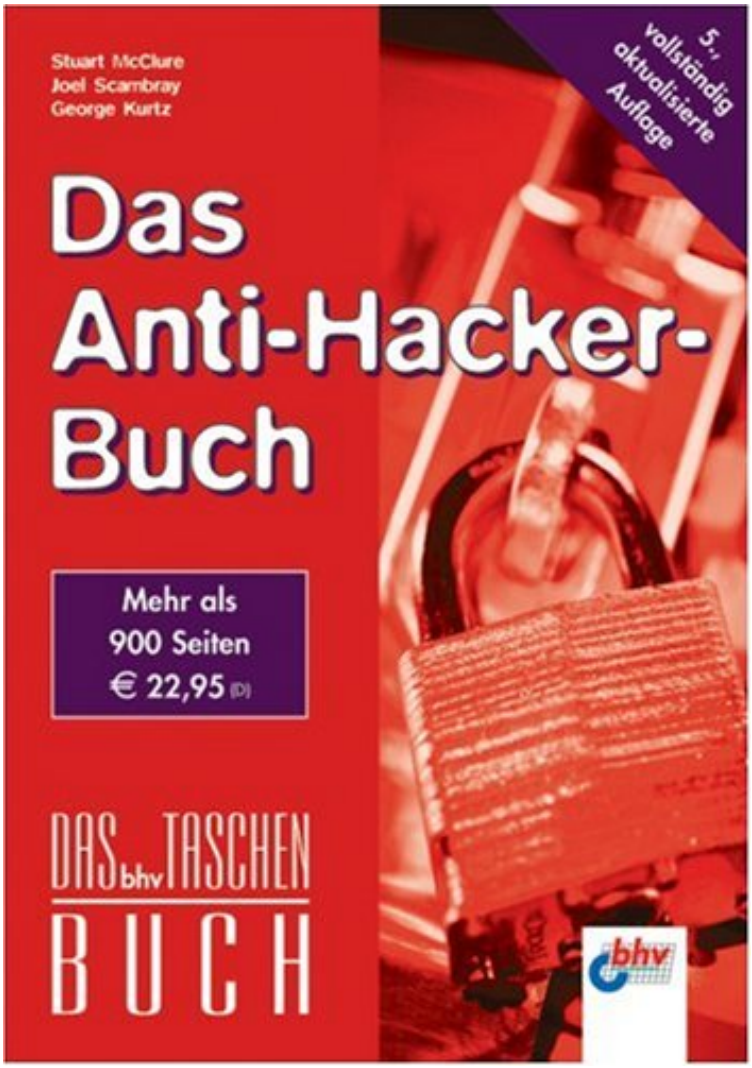
Das Anti-Hacker-Buch

Von Stuart McClure, Joel Scambray, George Kurtz
*DOC | *audiobook | ebooks | Download PDF | ePub*



Produktinformation -Verkaufsrang: #1521566 in BcherVerffentlicht am: 2005-11-01Abmessungen: 8.86 x 1.85b x 5.83l, Einband: Taschenbuch912 Seiten | File size: 61.Mb

Von Stuart McClure, Joel Scambray, George Kurtz : Das Anti-Hacker-Buch before purchasing it in order to gage whether or not it would be worth my time, and all praised Das Anti-Hacker-Buch:

KundenrezensionenHilfreichste Kundenrezensionen18 von 20 Kunden fanden die folgende Rezension hilfreich. Spionagethriller oder technisches Handbuch?Von Ein KundeKennen Sie die Lcher in Ihrer IT Infrastruktur? Sind Sie sicher, dass Ihr Netz sicher ist? Nur derjenige, der das Handwerk des Hackers versteht und durchschaut kann sich vor Angriffen schtzen. In der zweiten Auflage erschienen zeigt das Buch die aktuellen Sicherheitslcken und die neuesten Angriffstechniken in IT Systemen auf. Anschliessend werden die geeigenten Sicherheitsmassnahmen vorgestellt.In einem einfhrenden Kapitel gehen die Autoren auf einige Techniken ein, die zum Durchleuchten von potentiellen Angriffszielen von Crashern bzw. bswilligen Hackern angewandt werden. Es wird insbesondere die hohe Kunst des

Footprinting und des Scanning detailliert beschrieben.Die Autoren beschreiben im Detail, welche Angriffe auf Windows 95/98/ME, Windows NT, Windows 2000, Novell NetWare bzw. UNIX Systeme mglich sind. In den einzelnen Kapiteln werden konkrete Beispiele aufgezeigt und verschiedene Angreifer-Tools vorgestellt, so dass der Leser die mglichen Schwachstellen in seinem System bzw. Netzwerk leichter erkennen kann.Ein separate dritter Teil des Buch beschreibt die Besonderheiten bei Netzwerken, speziell bezglich Angriffen auf DF Netzwerke, VPN und Netzwerkgerte. Die Besonderheiten von Firewalls werden auf 27 Seiten beschrieben. Die Autoren gehen auch auf die Beweggrnde eines Denial-of-Service (DoS) Angreifers sowie die verschiedenen DoS-Angriffstypen ein. In einem vierten Teil werden Angriffe gegen Software, Remote-Control-Lsungen, Session-Hijacking, Backdoors und Trojaner detailliert beschrieben. Der Hacker-Angriff auf das Internet, d.h. Web-Hacking sowie der Angriff auf den Internet-User schliessen das Buch ab.In einem Anhang werden hilfreiche Internetressourcen und Links angegeben.Das Buch ist sehr locker geschrieben und erinnert in manchen Kapiteln eher an einen Spionagethriller als an ein technisches Handbuch. Das Buch ist sowohl fr den Netzwerk-Administrator, den IT-Sicherheitsverantwortlichen als auch den interessierten Laien geeignet. (Romeike/RiskNet)10 von 11 Kunden fanden die folgende Rezension hilfreich. sehr empfehlenswert fr Netzwerk-AdminsVon Ein KundeDas Buch ist fesselnd wie ein sehr guter Roman und gleichzeitig eine ernchternde Darstellung der Angreifbarkeit der eigenen Systeme. Die Autoren haben sich umfassend mit dem Thema Hacking auseinandergesetzt. Im Prinzip ist es eine Step by Step Anleitung zum Hacken aber ich bin auch der Meinung, Das Thema kann nur so bearbeitet werden. Man lernt zu Denken wie ein Hacker und die Info-Quellen eines Hackers zu benutzen. Mir hat das Buch sehr viel gegeben. Ich habe neue Strategien zur Sicherung eines Firmennetzes erlernt und mir bekannte im konkreten Fall weiterentwickelt. Die Denkanste, die dieses Buch gibt, sind jede Mark wert, die es kostet! Das einzig negative ist die Website der Autoren. Angeblich gibt es dort eine Mailinglist zum Thema. Ich habe es bis heute nicht geschafft, mich dort einzutragen. Permanente Fehlermeldungen!!!8 von 9 Kunden fanden die folgende Rezension hilfreich. Admin JA, Hacker NEIN!Von Ein KundeSicherlich ein ntzliches Buch fr Administratoren, die sich auch noch mit den Problemen der Netzwerk- ,Daten- Informationssicherheit rumschlagen mssen. Das Buch gibt einen berblick ber die gebruchlichsten Sicherheitstools, Sicherheitslcken und ber Abwehrmassnahmen, ohne wirklich ins Detail gehen zu knnen. Wer sich die empfohlenen Ratschlge zu herzen nimmt und bei gengend Erfahrung auf diesem Gebiet umsetzt,kann davon ausgehen, dass er ein Netzwerk hat, dass zumindest die gebruchlichsten Attacken abwehren kann. Um Firmennetzwerke abzusichern oder Sicherheitsmassnahmen auf dem aktuellen Stand der Technik aufzubauen, muss sich der geneigte Leser unbedingt tiefer mit der Materie befassen.Es ist sicherlich kein Buch fr Einsteiger in dieses Gebiet, aber auch nicht das Werk, welches die letzten Geheimnisse der Hacker oder der Abwehr von Netzwerkangriffen beschreibt.Die Beispiele sind nochvollziebar, jedoch nur auf strflich ungeschtzten Rechnern oder Netzwerken, die kaum noch so wie beschrieben anzutreffen sind.Hier sei noch einmal davor gewarnt, mit voller Absicht die Beispiele mit "Google" nochzuvollziehen. Das Datenschutzgesetz in Deutschland stellt diese Vorgehensweisen unter Strafe!!! im Gegensatz zu anderen Lndern!!!

ProduktbeschreibungSIEHE MEIN FOTO

KurzbeschreibungMachen Sie sich nichts vor - ein Hacker im Internet braucht nicht einmal 30 Minuten, um Ihren Computer zu entdecken. Jede Sekunde eines jeden Tages durchforsten bsartige Hacker die digitale Landschaft auf der Suche nach leichter Beute. Wussten Sie, dass ber 819 Schwachstellen jedes Jahr verffentlicht werden? Wie viele davon kennen Sie? Dieses Buch enthlt keine Fiktionen, es geht um Techniken und authentische Geschichten aus dem Alltag des digitalen Schlachtfeldes, auf dem wir uns stndig behaupten mssen. Der Feind steht in der Tr, und er ist fr alle - ausgenommen ein paar Sicherheitsexperten - vllig unsichtbar. Beim Lesen und Durcharbeiten dieses Buches werden Sie sich ffnen mssen, sich mit der Denkart und Motivation Ihres Feindes auseinandersetzen mssen, nur so erfahren Sie, was ihn bewegt, und wie genau er vorgeht. Und nur so erfahren Sie, wie Sie diesen Feind schlagen knnen. Zu den Neuerungen der dritten deutschsprachigen Ausgabe des internationalen Bestsellers gehren: - Angriffe auf drahtlose 802.11-Netzwerke - Analyse des Code Red-Wurms - Neue Angriffe auf Windows, insbesondere auf Windows 2000 und Windows .NET Server - Neueste Tools und Tricks bei DDOS-Angriffen - Neue Schwachstellen des format-Strings von Windows und UNIX - Aktualisierte Fallstudien am Anfang jedes Abschnitts - Live-Links auf die neuesten Versionen der im Buch besprochenen Sicherheitstools - CD-ROM mit einer Auswahl der besten Sicherheitstools und Passwortdatenbank mit einer Liste der gngigsten Passwrter auf Routern, Switches etc.Der Verlag ber das BuchSpannende Hilfe anhand topaktuellem InsiderwissenIn der bewhrten Manier seines Vorgngers zeigt dieses Buch zunchst die neuesten Sicherheitslcken und Angriffstechniken in modernen Computersystemen auf, um im Anschluss daran die ntigen Gegenmanahmen durchzuspielen. Credo des Buches ist, dass nur derjenige den Hacker durchschaut und pariert, der dessen Handwerk selbst beherrscht. Das Buch ist in allen Teilen aktualisiert worden, vor allem Erkenntnisse, die die Sicherheit der neuen Betriebssystemversionen Windows Me und Windows 2000 professional (auf der Client-Seite) sowie Windows 2000 Server und Novell NetWare 5.x (auf der Server-Seite) betreffen, machten eine grndliche berarbeitung unumgnglich. Mit Hilfe des Insiderwissens der Autoren und anhand echter Fallbeispiele lernen Leser mgliche Schwach-stellen in Netzen und Systemen kennen und werden befhigt,

geeignete Gegenmanahmen zu ergreifen. Die Autoren sind allesamt ausgewiesene Experten auf den Gebieten der IT-Sicherheit, Netzwerktechnologien und Betriebsysteme mit langjhriger Berufserfahrung als Entwickler und Projektleiter.