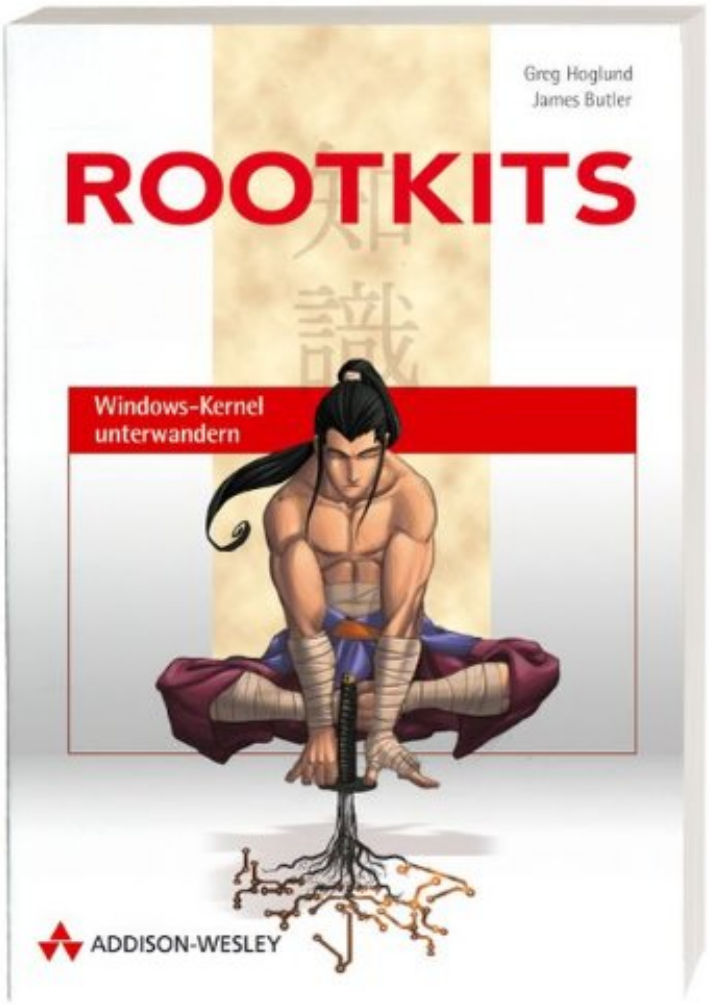
Rootkits. Das Standardwerk zu Funktionsweise, Entwicklung und Entdeckung von Rootkits fr Windows 2000/XP.

Von James Butler, Greg Hoglund
**Download PDF | ePub | DOC | audiobook | ebooks*



Produktinformation -Verkaufsrang: #55370 in BcherVerffentlicht am: 2005-12-01Einband: Taschenbuch360 Seiten | File size: 40.Mb

Von James Butler, Greg Hoglund : Rootkits. Das Standardwerk zu Funktionsweise, Entwicklung und Entdeckung von Rootkits fr Windows 2000/XP. before purchasing it in order to gage whether or not it would be worth my time, and all praised Rootkits. Das Standardwerk zu Funktionsweise, Entwicklung und Entdeckung von Rootkits fr Windows 2000/XP.:

KundenrezensionenHilfreichste Kundenrezensionen3 von 3 Kunden fanden die folgende Rezension hilfreich. StandardwerkVon LegasthenikerBei dem Buch handelt es sicherlich um ein Standardwerk was Rootkits unter

Windows angeht.Sieht man einmal von den neusten Rootkits ab die auf Virtualisierungs-Ebene arbeiten, gibt das Buch eine sehr gute Einfhrung in das Thema. Besonders erwhnenswert ist meines Erachtens, dass die Codebeispiele so aufgebaut sind, dass sie jedermann/frau nachvollziehen kann.Fazit: Ein muss fr jeden den das Thema interessiert1 von 1 Kunden fanden die folgende Rezension hilfreich. Rootkits - alte Tols in neuem GlanzVon Frank SolinskeHier fhren die Autoren Windows so richtig vor. Nahezu spielerrisch wird gezeigt, wie man jedes System untergrbt und dabei nicht einmal entdeckt werden kann. Die Codebeispiele zeigen, dass man, mit dem entsprechenden Wissen, alles im Netz machen kann, wenn man loakle Adminrechte misbraucht. Natrlich wird auch gezeigt, welche Prventivmanahmen notwendig sind, um es den bsen Buben schwer zu machen.3 von 7 Kunden fanden die folgende Rezension hilfreich. Die Stille Kriegskunst,...schn!Von plusbitOhne als Schmalhans verbraten zum werden, legt in aller Ruhe dieses Buch wichtige Grundsteine oder poliert jene, lngst vergessenen wieder auf.Der unergrndliche Fundus an Wissen, ber den Aufbau der Betriebssysteme und die khle Art dieses zu vermitteln, verschmelzen zu einer besserwisserlosen Lektre der wertvolleren Natur! So manches Kapitel zeigt ein eigenes Defizit auf, was man schon lnger beseitigen wollte! An unscharfen Stellen kommt von dem Autoren Team genug Futter fr die eigene Recherche.Die Stille Kriegskunst; an dem Gegner ist nicht Spott sondern Achtung, ohne die eigene Freude am Sieg zu Missachten!

Pressestimmen[...] Spannend und bedrohlich gleichzeitig: Rootkits. Das Standardwerk zu Funktionsweise, Entwicklung und Entdeckung von Rootkits fr Windows 2000/XP. ffnet eine Tr, von der viele bisher keine Ahnung hatten. Gut, beispielhaft und fundiert dargestellt und mit und ohne C-Kenntnisse verstndlich. Und last but not least: Eins der besten und coolsten Computer-Buch-Cover der letzten Jahre! --Wolfgang Tre, texteco - Januar 2006[...] Mit einem Rootkit erlangt ein Angreifer vollstndige Kontrolle ber ein System - und das unentdeckt. Mit diesem Buch haben zwei fhrende Experten den ersten umfassenden Leitfaden zur Funktionsweise, zur Entwicklung und zum Aufspren von Rootkits geschrieben. Greg Hoglund und James Butler enthllen unverffentlichte Informationen zu den offensiven Aspekten der Rootkit-Technologie. Sie zeigen detailliert, wie sich die Kernel von Windows XP und Windows 2000 bertragen lsst. (Dealers only, 1/06)RezensionRootkits? rootkit.com! Und wenn es deutsch sein muss? Rootkits. Das Standardwerk zu Funktionsweise, Entwicklung und Entdeckung von Rootkits fr Windows 2000/XP -- Greg Hoglund und James Butler sind Sicherheitsfreaks der ersten Stunde und waren mit die Ersten, die mit rootkit.com (Forum zum Reverse-Engineering und Rootkit-Entwicklung) auf Wirkungsweisen und mgliche Gefahren der Rootkits aufmerksam machten und Schutzmglichkeiten diskutierten. Ein Buch zu Rootkits aus ihrer Hand ist ein Versprechen mit Garantie. "Ein Rootkit ist ein Satz von Programmen und Code, der eine dauerhafte und nicht aufzusprende Prsenz auf einem Computer erlaubt." Aha. Klingt nicht gut. Zumindest fr den Computer-Besitzer. Wie schon erwhnt, Hoglund und Butler betreiben rootkit.com und geben Kurse (Black-Hat-Sicherheitskonverenz) zum Thema rootkit, aus denen dieses Buch entstanden ist. Kernthema sind Windows-Rootkits, genauer Kernel-Rootkits, nicht nur oder eben nicht speziell das Eindringen eines Angreifers in ein Computersystem, sondern was ein Eindringling anstellen kann, um sein Tun auf dem infiltrierten Rechner zu verbergen. C-Vorkenntnisse sind beim Verstndnis der Code-Beispiele von Nutzen, aber nicht zwingend notwendig. Los geht es mit einer Einfhrung in die rootkits: Motive der Angreifer, was rootkits sind, was nicht und was man mit ihnen machen kann. Dann klren die beiden Autoren die Frage,wie rootkits den Kernel unterwandern knnen, die Hardware-Connection, Hooking und Runtime-Patching. Weiter geht es dann mit geschichteten Treibern, der direkten Manipulation von Kernel-Objekten, Hardware-Manipulation, verborgene Kanle und zuletzt, als Perspektiven-Switch vom Angreifer zum Verteidiger: Wie sprt man rootkits auf? Den Code zu den Beispielen erhlt man ber rootkit.com, Links dazu sind im Buch an den entsprechenden Stellen. Spannend und bedrohlich gleichzeitig: Rootkits. Das Standardwerk zu Funktionsweise, Entwicklung und Entdeckung von Rootkits fr Windows 2000/XP. ffnet eine Tr, von der viele bisher keine Ahnung hatten. Gut, beispielhaft und fundiert dargestellt und mit und ohne C-Kenntnisse verstndlich. Und last but not least: Eins der besten und coolsten Computer-Buch-Cover der letzten Jahre! --Wolfgang TreAutorenkommentarHoglund und Butler erklren in ihrem Werk, was ein Eindringling anstellen kann, um seine Anwesenheit auf dem geknackten Rechner zu verbergen. Um unser Wissen ber Rootkits am besten zu vermitteln, haben wir den grten Teil aus der Sichtweise eines Angreifers geschrieben, kehren aber zum Schluss zum Standpunkt des Verteidigers zurck. Dadurch, dass Sie die Ziele und Techniken der Angreifer kennen lernen, beginnen Sie auch die Schwchen Ihres Systems zu verstehen und erfahren, wie Sie sie mildern knnen. Die Lektre dieses Buches hilft Ihnen, die Sicherheit Ihres Systems zu verstrken oder beim Erwerb von Sicherheitssoftware Entscheidungen auf einer sinnvollen Grundlage zu treffen. Greg Hoglund und James Butler, die Betreiber von rootkit.com glauben, dass die meisten Softwarehersteller Rootkits nicht ernst nehmen: Aus diesem Grund verffentlichen wir dieses Buch. Es ist fr Leser gedacht, die sich fr Computersicherheit interessieren und sich einen realistischen berblick ber die Bedrohungen verschaffen mchten. Es sollte Ihnen zeigen, dass Ihr Virenscanner und Ihre Desktop-Firewall nicht ausreichen und dass ein Rootkit auf Ihren Rechner gelangen und dort Jahre verbleiben kann, ohne dass Sie etwas davon mitbekommen. Aber was sind Rootkits? Unter einem Rootkit ist eine Sammlung von Softwarewerkzeugen zu verstehen, die nach dem Einbruch in ein

Computersystem installiert wird, um erneute Logins des Eindringlings zu verbergen, Prozesse zu verstecken und Daten mitzuschneiden. Mit einem Rootkit erlangt ein Angreifer also vollstndige Kontrolle ber ein System - und das unentdeckt. Deshalb ist ein Spyware-Rootkit Sicherheits-Risiko Nummer 1!.