هک‌های
Oracle

مؤلف: جان ویلی

مترجم: مرتضی کریمی

انتشارات ناقوس

سرشناسه : لیچفیلد، دیوید، ۱۹۷۵ - م. Litchfield, David
عنوان و نام پدیدآور : هک‌های Oracle/ مؤلف جان‌ویلی؛ مترجم مرتضی کریمی.
مشخصات نشر : تهران: انتشارات ناقوس، ۱۳۸۹.
مشخصات ظاهری : ۱۷۶ ص.: مصور، جدول.
شابک : ۹۷۸ -۹۶۴-۳۷۷-۱۹۶-۶ بها: ۵۰۰۰۰ ریال
وضعیت فهرست‌نویسی : فیپا
یادداشت : عنوان اصلی: Hacking and Defending Oracle.
موضوع : اوراکل (فایل کامپیوتر)
موضوع : پایگاه‌های اطلاعاتی— امنیت
شناسه افزوده : کریمی، مرتضی، ۱۳۶۴ - ، مترجم
رده بندی کنگره : QA۷۶/۹/ک۹ل ۱۳۸۹
رده بندی دیویی : ۰۰۵/۸
شمارهٔ کتابشناسی ملی : ۲۱۲۹۴۴۵

چاپ اول

نام کتاب : هک‌های Oracle
ناشر : انتشارات ناقوس
ناشر همکار : انتشارات الیاس
مؤلف : جان ویلی
مترجم : مرتضی کریمی
چاپ اول : ۱۳۸۹
تیراژ : ۱۰۰۰ جلد
لیتوگرافی : علامه
چاپ : علامه
صحافی : علامه
حروف‌نگار و صفحه‌آرا : مریم رضائی
قیمت : ۵۰۰۰۰ ریال
شابک : ۹۷۸ -۹۶۴-۳۷۷-۱۹۶-۶
ISBN : 978-964-377-196-6

مراکز پخش:
۱- انتشارات ناقوس: میدان انقلاب، خیابان کارگرجنوبی، خیابان روانمهر، کوچه دولتشاهی، پلاک ۲
تلفن و فاکس: ۶۶۴۰۸۵۲۰ - ۶۶۴۰۱۷۹۸ - ۶۶۴۱۷۰۷۲ - ۶۶۴۶۶۷۹۳
۲- کتابفروشی الیاس: خیابان انقلاب، نبش فروردین تلفن: ۶۶۴۰۵۰۸۴

فهرست مطالب

سرآغاز

از زمان تولید اولین کامپیوترها تاکنون مدت زیادی نمی‌گذرد و شاید انتظار نمی‌رفت که اینگونه کامپیوترها، جهان پیرامون انسان را احاطه کنند. امروزه جهان بدون کامپیوتر قابل تصور نیست و روز به روز این علم نوپا رو به پیشرفت است و بقیه علوم هم از این علم در حیطه کاری خود استفاده می‌کنند. یکی از رکن‌های اصلی در این علم ذخیره اطلاعات می‌باشد. در گذشته انسان مجبور بود اطلاعات مهم خود را روی کاغذ بنویسد و با آمدن کامپیوتر بشر به این فکر افتاد که از کامپیوتر به جای کاغذ استفاده کند. اما سوال این بود که چگونه باید این کار را انجام می‌داد؟ به همین منظور نرم‌افزارهای پایگاه داده ایجاد شدند. در این نرم‌افزارها کاربر می‌توانست اطلاعات خود را در جداولی منظم قرار دهد و از آنها استفاده نماید. کم کم این نرم‌افزارها توسعه پیدا کردند و توانستند در دیگر عرصه‌های کاربرد کامپیوتر نیز به کار روند. یکی از این نرم‌افزارها Oracle می‌باشد که از لحاظ امنیت از بقیه نرم‌افزارهای موجود در رتبه بالاتری قرار دارد. در این کتاب، مشکلات امنیتی این نرم‌افزار بیان شده است و یک مدیر پایگاه داده می‌تواند با شناخت آنها از آشکار شدن اطلاعات خود در مقابل مهاجمان جلوگیری نماید. هر چند از این مشکلات می‌توان بلعکس نیز استفاده و از آنها برای حمله به پایگاه داده استفاده کرد اما هدف اصلی این کتاب معرفی روش‌های لازم جهت ممانعت از انجام چنین اعمالیست. امیدوارم این کتاب راهنمای مناسبی برای خوانندگان عزیز بوده و بدین ترتیب توانسته باشم گامی هر چند کوچک در تعالی و پیشرفت این مرز و بوم داشته باشم.

در پایان این کتاب را به پدر و مادر عزیزم تقدیم کرده و از زحمات تمامی کسانی که مرا در نگارش این کتاب یاری نموده‌اند تشکر می‌نمایم.

مرتضی کریمی

مقدمه

امنیت نرم‌افزار همیشه یکی از مسائل مهم برای تولیدکنندگان و استفاده‌کنندگان آن به شمار می‌آید. در پایگاه داده این فاکتور از دیگر مسائل مهم‌تر است و همیشه بر آن تاکید می‌شود. امنیت نرم‌افزار تا به حال، هیچگاه به طور کامل برای تولیدکنندگان و استفاده‌کنندگان بدست نیامده و Oracle نیز که در جهان امروز یکی از بهترین نرم‌افزارهای پایگاه داده بشمار می‌آید خالی از این نقیصه نیست. در این کتاب سعی شده است حفره‌های امنیتی Oracle برای شما عزیزان بازگو شود و با مثال‌ها و کدهایی که در آن ارائه شده است آن را به شما نشان دهد. حفره‌هایی که در این کتاب آمده است معمولاً برای نسخه‌های Oracle 10g Release 2، Oracle 10g Release 1، Oracle 9i و ویرایش‌های قبل‌تر از آن کاربرد دارد.

در فصل اول این کتاب، ابتدا نگاهی اجمالی بر معماری Oracle داریم و بعد از آن به فرآیندها، سیستم فایل و Patching در Oracle خواهیم پرداخت.

در فصل دوم به معماری شبکه Oracle و مسائل پیرامون آن می‌پردازیم.

در فصل سوم نحوه حمله به TNS Listener و Dispatcherها را بررسی می‌کنیم.

در فصل چهارم چگونگی حمله به سندیت فرآیندها و همچنین چگونگی استفاده از نام‌های کاربری و رمزهای عبوری که به طور پیش‌فرض در Oracle وجود دارد را بررسی می‌کنیم.

در فصل‌های پنجم و ششم به ترتیب PL/SQL و Triggerها را بررسی می‌کنیم. همچنین چگونگی وارد کردن SQL در Oracle , معرفی Triggerها و نحوه استفاده از آنها را نیز تشریح خواهیم کرد.

در فصل هفتم با تکیه بر مطالب فصل‌های پنجم و ششم به چگونگی افزایش امتیازات از طریق Triggerها می‌پردازیم.

در فصل هشتم به VPD یا (Virtual Private Databases) خواهیم پرداخت.

در فصل نهم به چگونگی بهره‌برداری از برنامه‌های وب PL/SQL می‌پردازیم.

در فصل دهم به چگونگی اجرای فرمان‌های OS اشاره می‌کنیم.

در فصل یازدهم به چگونگی دسترسی به سیستم فایل خواهیم پرداخت.

در فصل دوازدهم نحوه دسترسی به شبکه را بررسی می‌کنیم.

در سه فصل آخر کتاب به ترکیب PL/SQL و Java را اشاره کرده و با تکیه بر این دو فاکتور نحوه نفوذ در Oracle را بررسی می‌کنیم.

در ضمیمه کتاب نیز تمامی نام‌های کاربری و رمزهای عبور پیش‌فرض در Oracle 10g ارائه شده است و از تمامی شما دوستان عزیز توصیه می‌کنم از این ضمیمه براحتی نگذشته و حتما آن را مطالعه فرمایید

زیرا یکی از رکن‌های اساسی نفوذ در Oracle بر چگونگی استفاده از این نام‌های کاربری و رمزهای عبور تکیه دارد. بدیهی است این کتاب فقط به مسائل پایه می‌پردازد و برای تسلط بیشتر در این زمینه، شما دوستان عزیز باید زمان و انرژی بیشتری را صرف نمایید.

مخاطبان

این کتاب برای مخاطبان در سطح متوسط و پیشرفته می‌باشد و برای استفاده هر چه بهتر از آن لازم است کاربران عزیز، آشنایی لازم با محیط Oracle و زبان‌های SQL، C و Java را داشته باشند.

نظرات، انتقادات و پیشنهادت

تمامی خوانندگان عزیز می‌توانند نظرات، انتقادات و پیشنهادات خود را به پست الکترونیکی Morteza_karimi_64@yahoo.com ارسال نمایند.