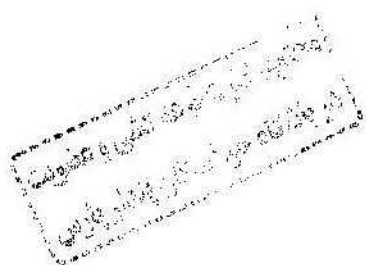


راهنمای پویش آسیب‌پذیری و تست نفوذ با

Nessus



www.ketab.ir

مهندس احسان نیک‌آور
مهندس سید سعید حسینی
انتشارات پندار پارس

سرشناسه : نیک‌آور، احسان، ۱۳۶۶ -
 عنوان و نام پدیدآور : راهنمای پویش آسیب‌پذیری و تست نفوذ با Nessus
 مشخصات نشر : تهران : پندار پارس ۱۳۹۴
 مشخصات ظاهری : ۱۹۲ ص.؛ مصور، جدول .
 شابک : ۹۷۸-۶۰۰-۶۵۲۹-۸۴-۴ : ۱۵۰۰۰۰ ریال
 وضعیت فهرست نویسی : فیهای مختصر
 یادداشت : فهرست‌نویسی کامل این اثر در نشانی: <http://opac.nlia.ir> قابل دسترسی است
 یادداشت : کتابنامه .
 شناسه افزوده : حسینی، سید سعید، ۱۳۶۰
 شماره کتابشناسی ملی : ۲۸۷۲۰۶۳

انتشارات پندار پارس



دفتر فروش: انقلاب، ابتدای کارگر جنوبی، کوی رشتچی، شماره ۱۴، واحد ۱۶ www.pendarepars.com
 تلفن: ۶۶۵۷۲۳۳۵ - تلفکس: ۶۶۹۲۶۵۷۸ همراه: ۰۹۲۱۴۳۷۱۹۶۴ info@pendarepars.com

نام کتاب : راهنمای پویش آسیب‌پذیری و تست نفوذ با Nessus
 ناشر : انتشارات پندار پارس
 ترجمه و تالیف : احسان نیک‌آور، سید سعید حسینی
 چاپ نخست : مرداد ۹۴
 شمارگان : ۵۰۰ نسخه
 طرح جلد و صفحه‌آرایی : سارا یعسوبی
 چاپ، صحافی : روز

قیمت : ۱۵۰۰۰ تومان شابک : ۹۷۸-۶۰۰-۶۵۲۹-۸۴-۴

* هرگونه کپی برداری، تکثیر و چاپ کاغذی یا الکترونیکی از این کتاب بدون اجازه ناشر تخلف بوده و پیگرد قانونی دارد *

فهرست

۳	فصل ۱- آشنایی با مفاهیم و محیط Nessus
۴	مفاهیم
۵	نمای کلی از واسط کاربری Nessus
۶	Installation
۱۹	فصل ۲- آشنایی با ساختار POLICY و مدیریت آن در Nessus
۱۹	سیاست‌ها (Policies)
۲۹	سرویس‌های Cloud
۳۲	Database
۳۴	Host
۳۴	الف- Windows
۴۲	Unix
۴۴	SNMPv3
۴۶	Settings
۴۸	تنظیمات Discovery
۵۸	تنظیمات Assessment
۶۲	Web Applications
۶۹	Report
۷۱	Advanced
۷۴	Mobile Device Management
۷۶	ایجاد یک Scan
۷۶	Plugins and Policy Preferences
۷۷	مدیریت اعتبار در دستگاه‌های تلفن همراه

۸۳	مدیریت وصله (Patch Management)
۸۴	IBM Tivoli Endpoint Manager (BigFix)
۸۸	WSUS
۹۰	SCCM
۹۱	Red Hat Network Satellite
۹۱	Dell KACE K1000
۹۲	Symantec Altiris
۹۶	اسکن با چندین مدیریت وصله
۹۷	مجازی‌سازی
۹۷	VMware
۹۹	Red Hat Enterprise Virtualization (RHEV)
۹۹	احراز هویت‌های متفرقه (Miscellaneous Authentication)
۱۰۲	احراز هویت پروتکل‌های Plaintext
۱۰۴	اسکن برنامه‌های تحت وب
۱۱۱	Plugins
۱۱۴	Compliance Audit Policies
۱۱۷	Offline Configuration Audit Policies
۱۱۸	PCI Policies
۱۱۹	الزامات استاندارد PCI DSS
۱۲۱	SCAP Policies
۱۲۵	فصل ۳ - اجرای عملیات اسکن
۱۲۵	Scan
۱۲۸	مثال‌هایی برای فایل میزبان
۱۳۷	فصل ۴ - نتایج اسکن و گزارش‌ها

۱۳۷	نتایج و گزارش‌های اسکن
۱۳۸	Dashboard
۱۴۵	نتایج انطباق
۱۴۷	محدودسازی‌های گزارش
۱۵۴	CPE چیست؟
۱۵۵	CVSS چیست؟
۱۵۶	CVE چیست؟
۱۵۶	Bugtraq ID چیست؟
۱۵۶	CERT Advisory ID
۱۵۷	OSVDB ID
۱۵۷	Secunia ID
۱۵۷	Exploit Database ID
۱۵۷	Metasploit Name and Framework
۱۵۸	Screenshot های گزارش
۱۵۹	Knowledge Base اسکن یا KB مربوط به اسکن
۱۶۲	بارگذاری کردن (Upload) و استخراج (Export) گزارش‌ها
۱۶۳	سفارشی کردن فرمت‌های HTML و PDF
۱۶۴	حذف نتایج اسکن
۱۶۷	پیوست ۱- نصب Nessus بر روی سیستم‌عامل ویندوز
۱۶۷	نصب Nessus در ویندوز (با دسترسی مستقیم به اینترنت)
۱۷۴	نصب Nessus در ویندوز (بدون دسترسی مستقیم به اینترنت)
۱۷۷	پیوست ۲- نمونه‌ای از اسکن در محیط واقعی

پیش‌گفتار

امروزه فناوری اطلاعات در تمامی سازمان‌ها و شرکت‌ها رشد چشمگیری را به خود دیده است. استفاده از این فناوری و استفاده از شبکه‌های رایانه‌ای در بخش‌های گوناگون سازمان موجب پیشرفت قابل توجه سازمان در نحوه ارائه خدمات و همچنین افزایش کارایی سازمان گردیده است. استفاده از این امکانات بدون رعایت نکات امنیتی و استفاده شایسته از ابزارهای موجود، همواره با مخاطرات بسیاری همراه می‌باشد. امنیت، یکی از مهمترین اجزای مرتبط با فناوری اطلاعات می‌باشد و عدم رعایت موارد امنیت می‌تواند صدمات جبران ناپذیری را به سازمان مطبوع شما وارد نماید.

در این کتاب قصد ما بر این است که شما را با ابزاری به نام Nessus آشنا کنیم که این ابزار قادر به کشف آسیب‌پذیری‌های موجود در سیستم‌های موجود در سازمان یا شرکت شما خواهد بود. با استفاده از این ابزار می‌توانید امنیت خود را به چالش کشیده و همچنین آن را مورد ارزیابی قرار دهید. گفتنی است، مطالب موجود در این کتاب برگرفته از منابع اصلی این ابزار و شرکت ارائه دهنده‌ی آن یعنی Tenable می‌باشد.

مدیران، کارشناسان امنیت و همچنین تمامی علاقمندان حوزه‌ی امنیت شبکه و اطلاعات می‌توانند از این کتاب استفاده کنند و با توجه به اینکه کتاب پیش رو توسط اعضای کوچکی از کارشناسان امنیت فراهم گردیده است لذا خالی از اشکال نیست. به همین منظور از تمامی عزیزانی که در حوزه‌ی امنیت مشغول هستند، صمیمانه خواهشمندیم تا انتقادهای، نظرها و پیشنهادهای خود را به آدرس info@esecurity.ir ارسال نمایند. البته دوستان عزیز که پس از مطالعه‌ی این کتاب پرسشی در باره‌ی موضوعات آن دارند نیز می‌توانند با همین آدرس پست الکترونیکی ارتباط برقرار نمایند. در پایان نیز امیدوارم مطالب موجود در این کتاب برای شما خواننده‌ی عزیز مفید واقع گردد.

احسان نیک‌آور

تابستان ۹۴