اصول تست نفوذ

با Kali Linux

ترجمه و تألیف: مهندس فریدالدین ترابی هستادی

با همکاری: مهندس حامد زندی

پایگاه دانش

۱۳۹۶

شابک	: 9786009467921
شماره کتابشناسی ملی	: ۴۷۱۸۰۰۱
عنوان و نام پدیدآور	: اصول تست نفوذ با kali linux/ ترجمه و تالیف فریدالدین تراب‌مستعدی، با همکاری حامد زندی.
مشخصات نشر	: تهران: پایگاه دانش، ۱۳۹۶.
مشخصات ظاهری	: ۲۷۳ ص.
موضوع	: سیستم عامل لینوکس
موضوع	: Linux
موضوع	: سیستم‌های عامل (کامپیوتر)
موضوع	: Operating systems (Computers)
موضوع	: آزمایش نفوذ (ایمن‌سازی کامپیوتر)
موضوع	: Penetration testing (Computer security)
رده بندی دیویی	: ۰۰۵/۴[illegible]
رده بندی کنگره	: QA۷۶/۷۶ /س۹۴ت۴ ۱۳۹۶
سرشناسه	: تراب مستعدی، فریدالدین، ۱۳۶۴ -
شناسه افزوده	: زندی، حامد، ۱۳۸۸ -
وضعیت فهرست نویسی	:

تماس با انتشارات: ۰۹۱۲۶۱۰۱۸۵۵ و ۶۶۱۹۵۳۴۵-۰۲۱

Email: paygahdanesh@gmail.com

نام کتاب	: اصول تست نفوذ با Kali Linux
ترجمه و تألیف	: فریدالدین تراب مستعدی- حامد زندی
ناشر	: پایگاه دانش
صفحه آرایی	: واحد تولید انتشارات پایگاه دانش
نوبت چاپ	: اول- ۱۳۹۶
شمارگان	: ۵۰۰ جلد
قیمت	: ۳۲۰۰۰ تومان
شابک	: ۹۷۸-۶۰۰-۹۴۶۷۹-۲-۱
ISBN	978-600-94679-2-1:

سخن ناشر

با توجه به گسترش فناوری‌های نوین اطلاعاتی و افزایش خیل مشتاقان و دانش‌پژوهان حوزه فناوری اطلاعات و ارتباطات در صنایع و دانشگاه‌های کشور، لزوم تولید آثار غنی و پربار علمی که نیازمندی جامعه دانشگاهی را پوشش دهد و همچنین آثار کاربردی که برآورنده نیاز صنایع بازار کار در کشور باشد ضروری به نظر می‌رسد.

انتشارات پایگاه دانش با بهره‌گیری از ظرفیت و توان اساتید، دانش‌آموختگان و متخصصین و باهدف ارائه کتب دانشگاهی و کاربردی در زمینه های فناوری اطلاعات، مدیریت و شاخه‌های مرتبط با آن کار خود را آغاز نموده است. با توجه به اهداف انتشارات پایگاه دانش که همانا تولید آثار وزین، پربار و جامع دانشگاهی و کاربردی است، این انتشارات همواره تلاش خواهد نمود تا آثاری را به دست خواننده برساند که به لحاظ علمی، محتوایی و نگارشی از سطح بالایی برخوردار باشد و بتواند رضایت خوانندگان را به خود جلب نماید.

امید داریم که راهکارها و پیشنهادهای شما عزیزان اساتید و دانش‌پژوهان گران‌قدر بتواند ما را پیشبرد اهداف عالیه و نشر آثار پربار علمی یاری دهد تا انشاء الله شاهد ارتقای سطح دانشی دانش‌پژوهان ساعی و در پی آن افزایش رتبه علمی کشور عزیزمان باشیم. ضمن اینکه انتشارات پایگاه دانش، آمادگی لازم جهت همکاری با کلیه اساتید و مؤلفین عزیز جهت ارائه آثار ارزشمند علمی و تخصصی را دارد. خواهشمند است نظرات، راهکارها و پیشنهادهای خود را جهت پربارتر کردن آثار منتشرشده به آدرس paygahdanesh@gmail.com ارسال نمایید.

مقدمه مؤلف

قبل از هر چیز لازم است که توضیحاتی در رابطه با این کتاب و ساختار آن خدمت شما خوانندگان عزیز ارائه نمایم، چراکه می‌دانم سؤالات زیادی در رابطه با این کتاب در ذهن شما مطرح خواهد شد، سؤالاتی از قبیل اینکه:

مخاطب این کتاب چه کسانی هستند؟

این کتاب با دیگر کتاب‌ها چه تفاوتی دارد؟

برای کسی که علاقه‌مند به یادگیری و مطالعه درزمینه هک و تست نفوذپذیری است، جستجو در یک کتاب‌فروشی بزرگ، برای پیدا کردن کتاب در مورد هک و تست نفوذ، کاری سخت و سردرگم کننده است. زیرا گزینه‌های زیادی جهت انتخاب وجود دارند. اکثر کتاب‌فروشی‌ها طبقات زیادی را به کتاب‌های مرتبط با موضوع هک اختصاص داده‌اند، که شامل کتاب‌هایی در رابطه برنامه‌نویسی امنیت، امنیت نرم‌افزارهای وب، روت کیت‌ها و بدافزارها، تست نفوذ و همچنین هک کردن است. در نظر اول، اکثر این کتاب‌ها ازنظر محتویات و موضوع باهم متفاوت می‌باشند، اما با بررسی و مطالعه آن‌ها متوجه خواهید شد، که تعدادی از آن‌ها بر روی استفاده از ابزارها تمرکز کرده و در رابطه با اینکه این ابزارها چگونه در کنار هم قرار می‌گیرند، صحبتی نکرده‌اند و برخی دیگر بر روی یک موضوع خاص و یک رشته از هکینگ تمرکز کرده و دید کلی در رابطه با کل پروسه تست نفوذ ارائه نمی‌کنند.

هدف کتاب حاضر حل این مشکل است، لذا باهدف ایجاد یک نقطه شروع برای تمام افرادی که به موضوع هکینگ و تست نفوذ علاقه‌مند هستند، طراحی شده است. این کتاب متدولوژی کلی در رابطه با کل پروسه تست نفوذ ارائه می‌کند و سپس به بررسی ابزارهای مرتبط با هریک از این فازها می‌پردازد، تا خواننده علاوه بر به دست آوردن یک دید کلی از پروسه تست نفوذ، با ابزارهای کاربردی هر فاز نیز آشنا شود.

مخاطبان این کتاب چه کسانی هستند؟

این کتاب یک راهنمای مناسب جهت ورود به دنیای هک و تست نفوذپذیری است. هدف این کتاب کمک به شما جهت یادگیری قدم‌های ابتدایی موردنیاز جهت انجام یک هک کامل بدون ایجاد سردرگمی است. بعد از اتمام این کتاب شما دانش کاملی در رابطه با پروسه‌ی تست نفوذ خواهید داشت و با ابزارهای اولیه‌ای که

جهت انجام این کار استفاده می‌شوند، آشنا می‌شوید. هدف این کتاب به‌طور ویژه افرادی است که به‌تازگی وارد دنیای هک و تست نفوذ شده‌اند و دارای تجربه کم و یا بدون تجربه هستند یا کسانی که از نداشتن یک دید کامل درزمینه هکینگ خسته و ناامید شده‌اند و یا قصد افزایش دانش درزمینه امنیت رادارند.

به‌طور خلاصه این کتاب برای کسانی نوشته‌شده است که به امنیت کامپیوتر، هکینگ یا تست نفوذپذیری علاقه‌مند هستند، اما تجربه‌ای در این زمینه ندارند و نمی‌دانند که از کجا باید شروع کنند. ما این مفهوم را "Zero Entery Hacking" یا ZEH می‌نامیم. که شباهت بسیار زیادی به استخرهایی دارد، که در ابتدا دارای عمق کم می‌باشند و کم‌کم عمقشان زیاد می‌شود. این مسئله به شناگر امکان راه رفتن در آب را بدون تحمل فشار و ترس از غرق شدن می‌دهد. مفهوم"Zero Entery" این امکان را به شناگر می‌دهد، که بدون توجه به سن و یا توانایی شنا کردن از استخر استفاده نمایند. در این کتاب هم از مفهوم مشابهی استفاده‌شده است. ZEH به هدف آشنا کردن شما با مفاهیم پایه‌ای بدون سردرگم کردن شما طراحی‌شده است. کامل کردن ZEH شمارا برای کتاب‌های پیچیده‌تر آماده می‌کند.

این کتاب با دیگر کتاب‌ها چه تفاوتی دارد؟

کتاب‌های زیادی درزمینه هکینگ و تست نفوذ وجود است برخی از این کتاب‌ها آن‌قدر خوب هستند که بارها و بارها مورداستفاده قرار می‌گیرند، تا حدی که جلد و شیرازه آن‌ها در حال خراب شدن است، اما بقیه آن‌ها نو و دست‌نخورده باقی‌مانده‌اند. کتابی که کارش را به‌درستی انجام دهد و جزئیات را بدون اتلاف وقت خواننده در اختیار او قرار دهد، بسیار ارزشمند است. کتاب‌هایی که مورد دوم هستند می‌باشند، بسیار طولانی (بیشتر از ۵۰۰ صفحه) و یا بسیار متمرکز (یک‌راهنمای کامل در مورد یک موضوع خاص) می‌باشند، هیچ‌کدام از این دو حالت روش بدی برای ارائه مطالب نیست، برعکس نشان‌دهنده‌ی سطح بالایی از جزئیات و وضوح‌بالای توضیحات نویسنده می‌باشند، که باعث می‌شود این کتاب‌ها ارزش زیادی داشته باشند. اما از طرفی، جزئیات زیاد درزمینه امنیت می‌تواند باعث سردرگم شدن افراد تازه‌وارد شود.

متأسفانه به‌عنوان یک فرد تازه‌کار که می‌خواهد وارد حوزه امنیت شود و مبانی هکینگ را یاد بگیرد، مطالعه یکی از این کتاب‌های قطور می‌تواند هراس‌انگیز و گیج‌کننده باشد. این کتاب از دو جهت با دیگر کتاب‌ها تفاوت دارد، اول اینکه برای افراد مبتدی نوشته‌شده است و دوم اینکه از مفهوم Zero Entry پیروی می‌کند. درصورتی‌که شما تاکنون هیچ کاری درزمینه هکینگ انجام نداده‌اید و یا از برخی از ابزارها استفاده

کرده‌اید، اما نمی‌دانید بعدازآن چه‌کاری باید انجام دهید، این کتاب برای شما مناسب است. هدف این کتاب دفن کردن شما در زیر کوهی از جزئیات نیست و تنها می‌خواهد یک دید کلی از فیلد هکینگ ارائه نماید.

درعین‌حال این کتاب ابزارهای اصلی موردنیاز، جهت تکمیل هرکدام از مراحل تست نفوذپذیری را موردبررسی قرار می‌دهد، اما برای بررسی دقیق و کامل آن نرم‌افزارها متوقف نمی‌شود. زیرا این کتاب بر روی جزئیات تمرکز نمی‌کند. بنابراین نمی‌خواهیم با تمرکز بر روی خصوصیات پیشرفته و تفاوت‌های اندک میان نسخه‌های مختلف، شمارا سردرگم نماییم.

برای مثال، زمانی که در رابطه با اسکن پورت‌ها صحبت می‌کنیم، در همان فصل چگونگی انجام اسکن‌های پایه‌ای را توسط پورت اسکنر محبوب Nmap بررسی می‌نماییم. ازآنجایی‌که ما بر روی مطالب پایه‌ای تمرکز می‌کنیم، نسخه‌ای که کاربر برای انجام این تست‌ها از آن استفاده می‌کند، اهمیتی ندارد. به‌عنوان‌مثال انجام TCP SYN Scan در Nmap نسخه‌ی ۲ و ۵ کاملاً مشابه هم است. تا حد امکان ازاین‌روش استفاده‌شده است، تا خواننده بتواند بدون نگرانی از تغییراتی که در عملکرد نسخه‌های مختلف ایجاد می‌شود، طریقه کار کردن با ابزارهای مختلف را یاد بگیرد.

هدف این کتاب فراهم کردن دانش عمومی است، که به شما امکان درگیر شدن با مباحث و کتاب‌های پیشرفته را می‌دهد. به خاطر داشته باشید که اگر شما دانش کلی در رابطه با مبانی داشته باشید، هر زمان‌که اراده کنید، می‌توانید به عقب برگشته و دانش خود را در رابطه با جزئیات خاص و یا قابلیت‌های پیشرفته‌ی یک ابزار کامل نمایید. علاوه بر این، هر فصل از این کتاب با یک لیست از ابزارها و مباحث پیشرفته پایان می‌پذیرد، که خارج از حوزه این کتاب می‌باشند، اما می‌توانند جهت مطالعه بیشتر و تکمیل کردن دانش شما مورداستفاده قرار گیرند.

این کتاب اطلاعات را با روش کاملاً منحصربه‌فردی به خواننده ارائه می‌کند. تمامی روش‌ها و ابزارهای استفاده‌شده در این کتاب با ترتیب خاصی بر روی اهداف مختلف مرتبط مورداستفاده قرار می‌گیرند(مثلاً تمامی ماشین‌های هدف به یک Subnet مشابه تعلق دارند، لذا خواننده می‌تواند به‌راحتی شبکه هدف را بازسازی کرده و از ابزارها استفاده نماید). در این کتاب خواننده یاد می‌گیرد که چگونه خروجی یک ابزار را ترجمه کرده و از آن برای ادامه‌ی حمله و حرکت از یک‌فاز به فاز بعدی استفاده نماید.

استفاده از مثال‌های مختلف در این کتاب، به خواننده این امکان را می‌دهد، که تصویر کامل و بهتری را از طریقه کار کردن با ابزارها و فازهای مختلف آن، در کنار هم به دست آورد. این موضوع باعث تمایز این کتاب از دیگر کتاب‌ها می‌شود، که حملات مختلف را شرح می‌دهند، اما نمی‌توانند ارتباط میان آن‌ها را برای خواننده بیان نمایند. نمایش اطلاعات با روشی که به کاربر آموزش دهد چگونه از یک‌فاز به فاز دیگر حرکت کند، تجربه‌ی ارزشمندی را به او می‌دهد، که با استفاده از آن می‌تواند تمامی مراحل پروسه تست نفوذپذیری را با کمک مثال‌های کتاب کامل نماید. این موضوع به خواننده این امکان را می‌دهد که فهم کاملی از مطالب پایه‌ای به دست آورده و بداند که ابزارها و فازهای مختلف چگونه به هم مرتبط می‌شوند.

هشدار:

این کتاب صرفاً برای افزایش آگاهی و رشد علمی متخصصین امنیت کشور تالیف گردیده است. در نتیجه عواقب ناشی از هرگونه سوءاستفاده احتمالی از مطالب عنوان شده در این کتاب بر عهده شخص خاطی بوده و مؤلف و ناشر هیچ مسئولیتی در این مورد ندارند.

فهرست مطالب