



اصول تست نفوذ

با Kali Linux

ترجمه و تألیف: مهندس فریدالدین تواب مستندی

با همکاری: مهندس حامد زندی



۱۳۹۶

شابک	9786009467921 :
شماره کتابشناسی ملی	۴۷۱۸۰۰۱ :
عنوان و نام پدیدآور	اصول تست نفوذ با kali linux / ترجمه و تالیف فریدالدین تراب مستعدی، 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 (ایمن سازی کامپیوتر)
موضوع	Penetration testing (Computer security) :
موضوع	۰۰۵/۴ :
رده بندی دیویی	۱۳۹۶ ۴۷۱۸/۷۶QA س/ ۴۷۱۸
رده بندی کنگره	تراب مستعدی، فریدالدین، ۱۳۶۴ -
سرشناسه	زندی، حامد، ۱۳۸۸ -
شناسه افزوده	
وضعیت فهرست نویسی	

تماس با انتشارات: ۰۹۱۲۶۱۰۱۸۵۵ و ۰۲۱-۶۶۱۹۵۳۴۵

Email: paygahdanesh@gmail.com



نام کتاب	اصول تست نفوذ با Kali Linux :
ترجمه و تألیف	فریدالدین تراب مستعدی - حامد زندی
ناشر	پایگاه دانش
صفحه آرای	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 پایه دانش با بهره‌گیری از ظرفیت و توان اساتید، دانش‌آموختگان و متخصصین و باهدف ارائه کتب دانشگاهی و کاربردی در زمینه‌های فناوری اطلاعات، مدیریت و شاخه‌های مرتبط با آن کار خود را آغاز نموده است. با توجه به راهبرد 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 ستاد 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 ایدئولوژی 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 payghadhanesh@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 علاقه مناس به یادگیری و مطالعه در زمینه 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 بود. مانند اکثر کتاب‌فروشی‌ها طبقات زیادی را به کتاب‌های مرتبط با موضوع هک اختصاص داده‌اند، که شامل کتاب‌هایی در رابطه برنامه‌نویسی امنیت، امنیت نرم‌افزارهای وب، روت‌کیت‌ها و بدافزارها، تست نفوذ و همچنین هک کردن است. در نظر اول، اکثر این کتاب‌ها از نظر 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 هک این ابزارها چگونه در کنار هم قرار می‌گیرند، صحبتی نکرده‌اند و برخی دیگر بر روی یک موضوع خاص و رشته‌ای 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 هک 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 در زمینه هکینگ خسته و ناامید شده‌اند و یا قصد افزایش دانش در زمینه امنیت را دارند.

به‌طور خلاصه این کتاب برای کسانی نوشته شده 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 Entry 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 را می‌بخشد. ما این مفهوم "Zero Entry" این امکان را به شناگر می‌دهد، که بدون توجه به سن و توانایی شنا کردن از استخر استفاده نمایند. در این کتاب هم از مفهوم مشابهی استفاده شده است. ZEH به‌دفعه‌ای از کمر مفاهیم پایه‌ای بدون سردرگم کردن شما طراحی شده است. کامل کردن ZEH شما را برای کتاب‌ها به بحث می‌دهد و آماده می‌کند.

این کتاب با دیگر کتاب‌ها چه تفاوتی دارد؟

کتاب‌های زیادی در زمینه هکینگ و تست نفوذ موجود است. برخی از این کتاب‌ها آن‌قدر خوب هستند که بارها و بارها مورد استفاده قرار می‌گیرند، تا حدی که جلد و سرزده آن‌ها در حال خراب شدن است، اما بقیه آن‌ها نو و دست‌نخورده باقی‌مانده‌اند. کتابی که کارش را به درستی انجام دهد و جزئیات را بدون اتلاف وقت خواننده در اختیار او قرار دهد، بسیار ارزشمند است. کتاب‌هایی که در دسترس قرار می‌دهد، بسیار طولانی (بیشتر از ۵۰۰ صفحه) و یا بسیار متمرکز (یک راهنمای کامل در مورد یک موضوع خاص) می‌باشند، هیچ‌کدام از این دو حالت روش بدی برای ارائه مطالب نیست، برعکس نشان‌دهنده سطح پایین‌تری از جزئیات و وضوح بالای توضیحات نویسنده می‌باشند، که باعث می‌شود این کتاب‌ها ارزش زیادی داشته باشند. اما از طرفی، جزئیات زیاد در زمینه 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 نوشته شده است و دوم اینکه از مفهوم Zero Entry پیروی می‌کند. در صورتی که شما تاکنون هیچ کاری در زمینه هکینگ انجام نداده‌اید و یا از برخی از ابزارها استفاده

کرده‌اید، اما نمی‌دانید بعد از آن چه کاری 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.

در عین حال این کتاب ابزارهای اصلی مورد نیاز، جهت تکمیل هر کدام از مراحل تست نفوذپذیری را مورد بررسی 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، شما را سردرگم نماییم.

برای مثال، زمانی که با اسکن پورت‌ها صحبت می‌کنیم، در همان فصل چگونگی انجام اسکن‌های پایه‌ای را توسط پورت اسکنر محبوب Nmap بررسی می‌نماییم. از آنجایی که ما بر روی مطالب پایه‌ای تمرکز می‌کنیم، نسخه‌ای که کاربر برای انجام این تست‌ها از آن استفاده می‌کند، اهمیتی ندارد. به عنوان مثال انجام Nmap Scan در نسخه ۲ و ۵ کاملاً مشابه هم است. تا حد امکان از این روش استفاده شده است، تا خواننده بتواند بدون نگرانی، 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 عمومی در رابطه با مبانی داشته باشید، هر زمان که 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 نیست از ابزارها و مباحث پیشرفته پایان می‌پذیرد، که خارج از حوزه این کتاب می‌باشند، اما می‌توانند جهت مطالعه بیشتر به کمک کردن دانش شما مورد استفاده قرار گیرند.

این کتاب اطلاعات را با روش کاملاً منحصربه‌فردی به خواننده ارائه می‌کند. تمامی روش‌ها و ابزارهای استفاده شده در این کتاب با ترتیب خاصی بر روی اهداف مختلف مرتبط مورد استفاده قرار می‌گیرند (مثلاً تمامی ماشین‌های هدف به یک Subnet مشابه تعلق دارند، لذا خواننده می‌تواند به راحتی 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 یک فاز 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 یک فاز 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 داشته باشد و بداند که ابزارها و فازهای مختلف چگونه به هم مرتبط می‌شوند.

هشدار:

این کتاب صرفاً برای عزایندگان 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

۱۵	فصل اول - تست نفوذ چیست؟
۱۶	مقدمه
۱۶	آماده‌سازی صحنه کاری
۱۸	مقدمه‌ای در رابطه با KALI
۲۳	آشنایی با لینوکس KALI
۲۵	ایجاد و استفاده از آزمایشگاه تست نفوذ
۲۷	فازهای تست نفوذ
۳۱	قدم بعدی چیست
۳۳	خلاصه فصل
۳۴	نمونه سؤالات تشریحی فصل اول
۳۵	نمونه سؤالات تستی فصل اول
۳۹	فصل دوم - فاز اکتشاف یا RECONNAISSANCE
۴۰	مقدمه
۴۴	کپی وبسایت با HTTrack
۴۷	بهبود مهارت‌های استفاده از گوگل با Google Directives
۵۱	عضای جادویی SHODAN
۵۲	پیدا کردن آدرس‌های ایمیل با Harvester
۵۵	دستور WHOIS
۵۷	وبسایت Netcraft
۵۸	دستور Host
۵۹	دستور Dmitry
۶۱	استخراج اطلاعات از سرور DNS
۶۲	دستور Nslookup
۶۴	دستور Dig
۶۴	دستور Fierce
۶۵	دستور dnsenum
۶۵	واکشی اطلاعات از سرورهای ایمیل

۶۶	ابزار Metagoofil
۶۷	جمع‌آوری اطلاعات با ابزار حرفه‌ای Maltego
۷۱	مقدمه‌ای در رابطه با مهندسی اجتماعی
۷۳	بررسی اطلاعات جهت یافتن اهداف مناسب حمله
۷۴	قدم بعدی چیست؟
۷۵	خلاصه فصل
۷۶	سؤالات تشریحی فصل دوم
۷۷	سؤالات تست فصل دوم

فصل سوم - فاز اسکن ۸۱

۸۲	مقدمه
۸۶	انجام Ping sweep با Fping
۸۸	اسکن پورت‌ها و تشخیص سرویس‌ها با Nmap
۸۹	توافق سه مرحله‌ای
۹۰	استفاده از Nmap جهت انجام یک اسکن TCP
۹۲	استفاده از Nmap جهت انجام اسکن SYN
۹۴	استفاده از Nmap جهت انجام اسکن UDP
۹۷	استفاده از nmap جهت انجام اسکن XMAS
۹۸	استفاده از Nmap جهت انجام اسکن Null
۹۹	گسترش قابلیت‌های Nmap با NSE
۱۰۱	خاتمه‌ی اسکن پورت‌ها

۱۰۲	اسکن آسیب‌پذیری‌ها
۱۰۷	چگونه این فصل را تمرین کنم؟
۱۰۸	قدم بعدی چیست؟
۱۰۹	خلاصه فصل

فصل چهارم - اکسپلویت سیستم هدف ۱۱۱

۱۱۲	مقدمه
۱۱۴	دسترسی به سرویس‌های راه دور با Medusa
۱۱۸	هک سیستم با Metasploit

۱۳۱	John the Ripper پادشاه کرک کننده‌های پسورد
۱۳۴	کرک کردن پسوردها به صورت محلی
۱۴۲	کرک کردن پسوردها از راه دور
۱۴۳	کرک کردن پسوردهای لینوکس
۱۴۴	Reset کردن پسورد
۱۴۷	حمله به سوئیچ ها با Macof و شنود ترافیک با Wireshark
۱۴۹	حمله به سوئیچ Macof
۱۵۰	شنود ترافیک شبکه با Wireshark
۱۵۳	ابزار Armitage
۱۶۱	چگونه مطالب فصل را تمرین کنیم؟
۱۶۳	قدم بعدی چیست؟
۱۶۶	خلاصه فصل
۱۶۷	نمونه سؤالات تشریحی فصل چهارم
۱۶۸	نمونه سؤالات تستی فصل چهارم
۱۷۳	فصل پنجم - مهندسی اجتماعی
۱۷۴	مقدمه
۱۷۵	مبانی SET
۱۷۷	روش های حمله با استفاده از وبسایت ها
۱۸۲	به دست آوردن حساب کاربری
۱۸۴	بررسی سایر گزینه های SET
۱۸۵	خلاصه فصل
۱۸۶	نمونه سؤالات تشریحی فصل پنجم
۱۸۷	نمونه سؤالات تستی فصل پنجم
۱۸۹	فصل ششم - اکسپلویت کردن وب (وب هکینگ)
۱۹۰	مقدمه
۱۹۳	بازجویی وب سرورها با Nikto

۱۹۴	بررسی ابزار قدرتمند W3af.....
۱۹۶	جمع آوری اطلاعات با خزیدن در اطراف وبسایت هدف.....
۲۰۱	حائل شدن در مسیر درخواست‌های کاربر با WebScarab.....
۲۰۳	حملات SQL Injection.....
۲۰۷	حملات Cross-Site Scripting.....
۲۱۰	بررسی ابزار ZAP.....
۲۱۱	حائل شدن توسط ZAP.....
۲۱۲	Ordering در ZAP.....
۲۱۳	اسکن کردن استفاده از ZAP.....
۲۱۵	چگونه مطالب این فصل را تمرین کنم؟.....
۲۱۶	قدم بعدی چیست.....
۲۱۷	خلاصه فصل.....
۲۱۸	نمونه سؤالات تشریحی فصل.....
۲۱۹	نمونه سؤالات تستی فصل ۶.....
۲۲۱	فصل هفتم - تثبیت دسترسی بعد از اکسپلویت.....
۲۲۲	مقدمه.....
۲۲۳	ابزار Netcat یا چاقوی نظامی سوئیسی.....
۲۲۹	Cryptcat نسخه رمز شده Netcat.....
۲۳۰	مفاهیم Rootkit.....
۲۳۱	Bandook.....
۲۳۴	کشف و مقابله با روت کیت‌ها.....
۲۳۵	به کار گیری Meterpreter Shell.....
۲۳۸	چگونه مطالب این فصل را تمرین کنم؟.....
۲۳۹	قدم بعدی چیست؟.....
۲۴۰	خلاصه فصل.....
۲۴۱	نمونه سؤالات تشریحی فصل هفتم.....
۲۴۲	نمونه سؤالات تستی فصل هفتم.....

فصل هشتم - ایجاد گزارش تست نفوذ..... ۲۴۵

۲۴۶		مقدمه
۲۴۶		نوشتن گزارش تست نفوذ
۲۴۷		خلاصه‌ی اجرایی
۲۴۸		گزارش جزئیات
۲۴۹		خروجی‌های خام
۲۵۰		چرخه‌ی حیات
۲۵۱		سخن پایانی
۲۵۲		نمونه سؤالات تشریحی فصل هشتم

فصل نهم - پاسخ سؤالات مطالعاتی در کتاب..... ۲۵۳

۲۵۴		پاسخ سؤالات تشریحی فصل اول
۲۵۶		پاسخ سؤالات تستی فصل اول
۲۵۷		پاسخ سؤالات تشریحی فصل دوم
۲۵۹		پاسخ سؤالات تستی فصل دوم
۲۶۰		پاسخ سؤالات تشریحی فصل سوم
۲۶۲		پاسخ سؤالات تستی فصل سوم
۲۶۳		پاسخ سؤالات تشریحی فصل چهارم
۲۶۶		پاسخ سؤالات تستی فصل چهارم
۲۶۷		پاسخ سؤالات تشریحی فصل پنجم
۲۶۸		پاسخ سؤالات تستی فصل پنجم
۲۶۹		پاسخ سؤالات تشریحی فصل ششم
۲۷۰		پاسخ سؤالات تستی فصل ششم
۲۷۱		پاسخ سؤالات تشریحی فصل هفتم
۲۷۳		پاسخ سؤالات تستی فصل هفتم
۲۷۴		پاسخ سؤالات تشریحی فصل هشتم