کانون نشر علوم

شماره درخواست ۳۳

مرجع کاربردی ابزارهای تکمیلی هک برای کالی لینوکس

مؤلف:
مهندس مجید داوری دولت آبادی
عضو گروه امنیت GrayHat Hackers
Security Information Assets

ناشر:
کانون نشر علوم

کانون نشرعلوم
www.nashreoloom.com
پیشگام در نشر آثار برگزیده علوم کاربردی کامپیوتر و الکترونیک

سرشناسه: داوری دولت‌آبادی، مجید، ۱۳۵۹ -
عنوان و نام پدیدآور: مرجع کاربردی ابزارهای تکمیلی هک برای کالی لینوکس/ مولف مجید داوری‌دولت‌آبادی.
مشخصات نشر: تهران:کانون نشر علوم: کاتوزی، ۱۳۹۵.
مشخصات ظاهری: ۳۶۰ص.: مصور ،جدول ،نمودار.
شابک: ۹۷۸۹۶۴۳۲۷۱۵۹۶
وضعیت فهرست‌نویسی: فیپا
یادداشت: کتابنامه:ص. ۳۵۹.
موضوع: سیستم عامل لینوکس
موضوع: Linux
موضوع: سیستم‌های عامل (کامپیوتر)
موضوع: Operating systems (Computers)
رده‌بندی کنگره: ۱۳۹۵ ۲۸۴ ۱ س/QA۷۶/۷۶
رده‌بندی دیویی: ۰۰۵/۴۳۲
شماره کتابشناسی ملی: ۴۲۷۷۷۸

نام کتاب: مرجع کاربردی ابزارهای تکمیلی هک برای کالی لینوکس
ناشر: کانون نشرعلوم
ناشر همکار: کاتوزی
مؤلف: مهندس مجید داوری دولت آبادی
صفحه‌آرا: فاطمه آدیگوزل‌پور اردبیلی
طرح جلد: زهرا سلطان‌آبادی
چاپ اول: پاییز ۱۳۹۵
تیراژ: ۱۰۰۰
چاپ و صحافی: کانون نشرعلوم
قیمت: ۳۵۰۰۰ تومان
شابک: ۹۷۸۹۶۴۳۲۷۱۵۹۶

دفتر مرکزی پخش: خیابان انقلاب، خیابان فخررازی، خیابان وحید نظری شرقی، پلاک ۶۵، واحد۱
تلفن: ۶۶۴۹۴۹۱۱-۶۶۹۶۱۵۶۸

سخن ناشر

به نام خداوند بخشنده و مهربان

دستره دانش بشری در برابر علم بی‌پایان و نامتناهی حضرت حق (جلّ جلاله) بسیار ناچیز است؛ همچنان که در قرآن کریمه « و ما عطا نکردیم به شما علم را جز اندکی» شاهدی است بر ضعف معرفت انسان نسبت به حکمت صَمَدانی. با این حال چه نیکو سفارش فرموده است خاتم انبیاء، حضرت محمد مصطفی (ص)، که « بجویید علم را اگر چه به سرزمین چین». این توصیه، تمامی پیروان راستین دین حنیف اسلام را به فراگیری و اکتساب علوم و فنون مختلف در همه زمان‌ها و همه مکان‌ها فرا می‌خوانند.

تلاش کانون نشر علوم، همواره معطوف به تولید آثار شایسته و بایسته در زمینه فنی و مهندسی بوده است؛ اگرچه که در این راه مشکلات و دشواری‌های فراوانی حادث شده و خواهد شد. این امر تا حدّی بسیار، تابعی از ماهیت رشته‌های فنی و مهندسی و معارف مربوط به آنهاست؛ چرا که این رشته‌ها به‌سرعت و بی‌وقفه در حال نو به نو شدن می‌باشند. این امر رسالت کانون نشر علوم را در نشر آثار مربوطه، اعم از تألیف یا ترجمه، صحت‌برانگیخته و می‌کند. در این ارتباط دغدغه اصلی کانون نشر علوم این بوده و هست که اولاً، از قافله علم فنی و مهندسی عقب نماند؛ و ثانیاً، آثاری را به زیور طبع بیاراید که ضمن داشتن وجاهت علمی و برخوردار شأن مخاطبین اندیشمند و فاضل نیز باشد. امید است که خداوند منّان در این مهم مساعدت نماید.

پایان سخن اینکه، کانون نشر علوم دست یاری و همّت تمامی مؤلفین و مترجمین علاقه‌مند در زمینه علوم فنی و مهندسی را به‌گرمی می‌فشارد و تمامی ایشان را خاضعانه و خاشعانه به همکاری فرا می‌خواند. همچنین این مجموعه از تمامی مخاطبین استدعا دارد که با نظرات صائب و راهگشای خود، در بهبود شکلی و محتوایی آثار منتشر شده مساعدت فرمایند؛ و صد البته که تمامی کاستی‌ها از این رهگذر تنها و تنها متوجه این مجموعه بوده و هست.

سید محمدحسین منوّری
کانون نشر علوم

مقدمه مؤلف

توزیع لینوکس Kali، یکی از توزیع‌های قدرتمندی است که امروزه به دلیل پشتیبانی مستمر و دقیق بسیار مورد توجه نفوذگران، متخصصان آزمایش نفوذ و حتی کاربران حوزه شبکه و امنیت قرار دارد. در واقع این توزیع لینوکس به نوعی عصای دست متخصصان حوزه امنیت و شبکه به‌حساب می‌آید که در آن تمامی ابزارهای مورد نیاز یک آزمایش‌کننده نفوذ ویا نفوذگر برای رسیدن به اهدافشان به‌صورت پیش‌فرض وجود دارد. هر کدام از این ابزارها به نوبه خود جزو ابزارهای حوزه هک می‌باشند و در روند انجام عملیات نفوذ ویا آزمایش به کمک آزمایش‌کننده ویا نفوذگر می‌آیند و کار را برای آن‌ها ساده‌تر و سریع‌تر می‌کنند. البته برخی از ابزارهای تکمیلی مورد نیاز جهت پیاده‌سازی حملات حرفه‌ای‌تر هک و آزمایش نفوذ به‌صورت پیش‌فرض بر روی این توزیع موجود نمی‌باشند. این ابزارها و Frameworkها می‌توانند توسط فرد ویا گروه هکری خاصی طراحی و ارائه شده باشند. لازم به‌ذکر است که توزیع لینوکس Kali در زمینه نصب و اضافه این ابزارها به مجموعه ابزارهای خود از انعطاف‌پذیری بالایی برخوردار است و به‌راحتی می‌توان آن‌ها را بر روی هر نسخه‌ای از این توزیع نصب کرد. همچنین توسعه‌دهندگان این ابزارها نیز، نرم‌افزارها و Frameworkهای خود را مخصوص توزیع لینوکس Kali طراحی و پیاده‌سازی کرده‌اند، درنتیجه به‌راحتی بر روی این توزیع قابل نصب و راه‌اندازی می‌باشند.

در این کتاب سعی شده است تا به بررسی و تحلیل ابزارها و Frameworkهای تکمیلی و حرفه‌ای توسعه داده شده برای توزیع لینوکس Kali پرداخته شود و آن‌ها در جهت پیاده‌سازی یک حمله و خط‌مشی حملات هکری استفاده گردد. در این کتاب با کمک این ابزارهای تکمیلی قدرتمند، انواع حملات مطرح در حوزه نفوذگری مورد بررسی و پیاده‌سازی قرار گرفته است. البته لازم به‌ذکر است که در کنار این ابزارها در روند پیاده‌سازی حملات از ابزارهای پیش‌فرض توزیع Kali نیز بهره گرفته شده است. در این کتاب از تمامی منابع معتبر و پایه‌ای مربوط به توزیع لینوکس Kali و علم هک استفاده شده است که البته با تجزیبات ناچیز اینجانب آمیخته گردیده است تا کتابی جامع و مفید ایجاد شود.

اینجانب به‌عنوان عضو کوچکی از خانواده بزرگ امنیت و شبکه درصدد گردآوری و تألیف کتابی مرجع به‌منظور افزایش آگاهی متخصصین، دانشجویان و مدیران شبکه در زمینه نحوه

استفاده از ابزارهای توسعه داده شده برای توزیع لینوکس Kali که به‌صورت پیش‌فرض بر روی این توزیع نصب نمی‌باشند، اما توسط نفوذگران حرفه‌ای برای این نوع توزیع نوشته شده‌اند بودم تا آن‌ها را با اصول فنّی آزمایشات نفوذ با کمک این ابزارها آشنا و آگاه سازم و بتوانند از آن‌ها در فرآیندها و پروژه‌های آزمایش‌نفوذ استفاده کنند (گرچه مدیران و متخصصین امنیت شبکه حُکم اساتید اینجانب را دارند، امّا به حُکم وظیفه برخود لازم دانستم که این آگاه سازی را انجام دهم.) همان‌طور که گفته شد، شیرازه اصلی کتاب حاضر برگرفته از کتاب‌ها و منابع معتبر در حوزه توزیع لینوکس Kali می‌باشد که با تجربیات اینجانب در این خصوص آمیخته شده است، که به‌فرم کاملاً آزاد از مطالب و تجربیات گردآوری، و دخل و تصرفی نیز با آن صورت گرفته است. پیشاپیش تمام کاستی‌های آن را می‌پذیرم و ضمن پوزش از اساتید، متخصصان، دانشجویان و مدیران عزیز، انتقادات و راهنمایی‌های دلسوزانه آن‌ها را به دیده منّت پذیرا هستم.

(m_Davari@TOP-co.ir)
(m_Davary@Parshack.zzn.com)

پس از سپاس و ستایش به درگاه پروردگار از تمام دوستان و اساتید عزیزی که مهربانانه دست مرا در انجام اینکار ناچیز فشردند، تشکر می‌کنم. بخصوص لازم می دانم از زحمات بی‌دریغ سرکار خانم مهندس سیده پونه مرتضویان تشکر و قدردانی نمایم. زحمات خاضعانه ایشان سهم بزرگی در تهیه و تدوین این کتاب داشته است.

در پایان از مدیریت فرزانه انتشارات کانون نشر علوم جناب آقای منوری و تمامی همکارانشان که زحمت چاپ کتاب را متقبل شده‌اند، صمیمانه قدردانی می‌نمایم.

خدایا نام تو در دل عیان است کنار محفلم یادت نهان است

به راه راست بر دل را، که تنها تو را دارم، چه حاجت بر بیان است

(مجید داوری دولت آبادی - پاییز ۱۳۹۵)

فهرست مطالب