# برترین ابزارها و چهارچوب‌های هک در 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: برترین ابزارها و چهارچوب‌های هک در کالی‌لینوکس/ مولف مجید داوری‌دولت‌آبادی.
مشخصات نشر: تهران : کانون نشر علوم: کاتوزی، ۱۳۹۵.
مشخصات ظاهری: ۴۵۶ ص.: مصور (بخشی رنگی).
شابک: ۹۷۸۹۶۴۳۲۷۱۵۷۲
وضعیت فهرست‌نویسی: فیپا
یادداشت: کتابنامه: ص. ۴۵۶.
موضوع: سیستم عامل لینوکس
موضوع: Linux
موضوع: سیستم‌های عامل (کامپیوتر)
موضوع: Operating systems (Computers)
رده‌بندی کنگره: ۱۳۹۵ ۷ د۹۴ص/QA۷۶/۷۶
رده‌بندی دیویی: ۰۰۵/۴۴۲
شماره کتابشناسی ملی: ۴۲۱۰۷۶۵

نام کتاب: برترین ابزارها و چهارچوب‌های هک در کالی لینوکس
ناشر: کانون نشرعلوم
ناشر همکار: کاتوزی
مؤلف: مهندس مجید داوری دولت‌آبادی
صفحه‌آرا: فاطمه آدیگوزل‌پور اردبیلی
طرح جلد: زهرا سلطان‌آبادی
چاپ اول: پاییز ۱۳۹۵
تیراژ: ۱۰۰۰
چاپ و صحافی: کانون نشرعلوم
قیمت: ۴۰۰۰۰ تومان
شابک: ۹۷۸۹۶۴۳۲۷۱۵۷۲

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

گستره دانش بشر در برابر علم بی‌پایان و نامتناهی حضرت حق (جلّ جلاله) بسیار ناچیز است؛ همچنان که آیه « و ما عطا نکردیم به شما علم را جز اندکی» شاهدی است بر ضعف معرفت انسانی در مقابل عظمت 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 می‌خواند.

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، خطیرتر کرده و می‌کند. در این ارتباط دغدغه اصلی کانون نشر علوم این بوده و هست که اولاً، از قافله علوم فنی و مهندسی عقب نماند؛ و ثانیاً، آثاری را به زیور طبع بیاراید که ضمن داشتن وجاهت علمی در خور شأن مخاطبین اندیشمند و فاضل نیز باشد. امید است که خداوند منّان در این مهم مساعدت فرماید.

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

در حال حاضر یکی از توزیع‌های قدرتمندی که مورد توجه نفوذگران، متخصصان آزمایش نفوذ و حتی کاربران حوزه شبکه و امنیت قرار دارد، توزیع لینوکس Kali می‌باشد که پشتیبانی کامل و دقیقی از آن به‌عمل می‌آید. 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، برترین‌های 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. از این میان ابزارهای حرفه‌ای‌تری نیز وجود دارند که درقالب Frameworkها تحت توزیع ارائه شده‌اند که از قابلیت‌ها و امکانات فوق‌العاده‌ای برخوردار هستند.

در این کتاب سعی شده است تا به بررسی و تحلیل ابزارها و Frameworkهای حرفه‌ای و برتر موجود در توزیع لینوکس Kali پرداخته شود و از آن‌ها در جهت پیاده‌سازی یک حمله و خط‌مشی حملات هکری استفاده گردد. در واقع در این کتاب با کمک این ابزارهای قدرتمند انواع حملات مطرح در حوزه نفوذگری مورد بررسی و پیاده‌سازی قرار گرفته است. لازم به‌ذکر است که تمامی حملات و مدل‌های حمله‌ای که در این کتاب ارائه شده است با کمک ابزارهای موجود در توزیع لینوکس Kali انجام گرفته است. البته برای حرفه‌ای هک نیز نیازمند ابزارها و Frameworkهای تکمیلی هک می‌باشند که به‌صورت پیش‌فرض بر روی توزیع لینوکس Kali نصب نمی‌باشند و باید بر روی این توزیع نصب گردند. نحوه استفاده و خط‌مشی پیاده‌سازی حملات نفوذگری با کمک ابزارهای تکمیلی در توزیع لینوکس Kali درقالب کتاب دیگری ارائه شده است که می‌توان از آن برای پیاده‌سازی آزمایشات نفوذ و انجام حملات هکری با کمک ابزارهای تکمیلی استفاده کرد. در این کتاب از تمامی منابع معتبر و پایه‌ای مربوط به توزیع لینوکس Kali و علم هک استفاده شده است که البته با تجزیات 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 ابزارها و Frameworkهای برتر پیش‌فرض در توزیع لینوکس Kali به‌منظور پیاده‌سازی آزمایش نفوذ بودم تا آن‌ها را با اصول فنّی آزمایشات نفوذ با کمک این ابزارها آشنا و آگاه سازم و بتوان از آن‌ها در فرآیندها و پروژه‌های آزمایش‌نفوذ استفاده نمود (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، دخل و تصرفی نیز با آن همراه بوده است. پیشاپیش تمام کاستی‌های آن را می‌پذیرم و سمنم پوزش از اساتید، متخصصان، دانشجویان و مدیران عزیز، انتقادات و راهنمایی‌های دلسوزانه آن‌ها را دیده منّت پذیرا هستم.

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

پس از سپاس و ستایش به درگاه پروردگار انام دوستان و اساتید عزیزی که مهربانانه دست مرا در انجام اینکار ناچیز فشردند، تشکر می کنم. برخود 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 مهندس نوری و تمامی همکارانشان که زحمت چاپ کتاب را متقبل شده‌اند، صمیمانه قدردانی می‌نمایم.

**یارب ز گناه زشت خود منفعلم — وز قول بد و فعل بد خود خجلم**

**فیضی به دلم ز عالم قدس رسان — تا محو شود خیال باطل ز دلم**

(مجید داوری دولت آبادی - پاییز ۱۳۹۵)

# فهرست مطالب