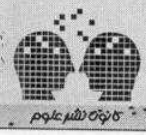

لینوکس، سیستم‌عامل نفوذگران

مؤلف:
مهندس مجید داوری دولت‌آبادی

ناشر:
کانون نشر علوم

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

سرشناسه: داوری دولت‌آبادی، مجید، ۱۳۵۹-
عنوان و نام پدیدآور: لینوکس، سیستم‌عامل نفوذگران/ مؤلف مجید داوری دولت‌آبادی.
مشخصات نشر: تهران:کانون نشر علوم: انتشارات آترا، ۱۳۹۴.
مشخصات ظاهری: ۶۴۰ ص.: مصور، جدول، نمودار.
شابک: ۹۷۸۹۶۴۳۲۷۱۱۷۶
وضعیت فهرست‌نویسی: فیپا
موضوع: سیستم‌عامل لینوکس
موضوع: سیستم‌های عامل (کامپیوتر)
رده‌بندی کنگره: ۱۳۹۳ ۲۸۳د۹۴س/QA ۷۶/۷۶
رده‌بندی دیویی: ۰۰۵/۴۳۲
شماره کتابشناسی ملی: ۳۷۰۰۰۰۵

نام کتاب: لینوکس، سیستم‌عامل نفوذگران
ناشر: کانون نشرعلوم
ناشر همکار: انتشارات آترا
مؤلف: مهندس مجید داوری دولت‌آبادی
ویراستار ادبی: کانون نشر علوم
صفحه‌آرا: فاطمه سلطان‌آبادی
طرح جلد: شیما نجفی
چاپ اول: بهار ۱۳۹۴
تیراژ: ۱۰۰۰
چاپ و صحافی: کانون نشر علوم
قیمت: ۴۰۰۰۰ تومان
شابک: ۹۷۸۹۶۴۳۲۷۱۱۷۶

مراکز پخش:
پخش علوم: خیابان انقلاب، خیابان فخررازی، خیابان وحید نظری شرقی، پلاک ۶۵، واحد۱
تلفن: ۶۶۴۹۴۹۱۱-۶۶۹۶۱۵۶۸
نشر و پخش آترا: میدان انقلاب، خیابان جمالزاده جنوبی، کوچه شهید آقاصبوری، پلاک ۱۳
تلفن: ۶۶۹۲۲۰۸۲

سخن ناشر

به نام خداوند بخشنده و مهربان

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

امروزه در دنیای هک و نفوذ، استفاده از سیستم‌عامل لینوکس امری بدیهی و ابزاری لازم و ضروری است. در واقع سیستم‌عامل لینوکس برای یک نفوذگر واقعی حکم عصای دست وی را دارد و نبود آن می‌تواند در روند عملیات نفوذ یا آزمایش‌نفوذ ایجاد اختلال کند. در این میان توزیع‌های لینوکس قدرتمندی نیز متخص انجام عملیات آزمایش‌نفوذ و هک ارائه شده‌اند که در آن‌ها تمامی ابزارهایی که یک نفوذگر ویا متخصص درحین انجام عملیات به آن‌ها نیاز دارد، به‌طور پیش‌فرض بر روی این نوع توزیع‌ها نصب و راه‌اندازی شده است که می‌توان از آن‌ها استفاده کرد. سیستم‌عامل لینوکس چه از دیدگاه ابزارهای موجود برای نفوذ و بهره‌برداری در جهت حمله و چه از نظر کدنویسی در این خصوص از توانایی بالایی برخوردار است. یک نفوذگر یا متخصص امنیت هر چقدر که آزمایشات خود را با سیستم‌عامل ویندوز انجام دهد، زمانی فرا می‌رسد که مجبور می‌شود تا از سیستم‌عامل لینوکس استفاده کند، زیرا ویندوز جوابگوی پیاده‌سازی تمامی آزمایشات در شاخه نفوذ نمی‌باشد.

" لینوکس، سیستم‌عامل نفوذگران "، کتابی است که سعی می‌کند کاربران و نفوذگران را با انواع روش‌های حمله و نفوذگری از طریق سیستم‌عامل لینوکس آشنا نماید. در این کتاب یک توزیع خاص سیستم‌عامل لینوکس مطرح نمی‌باشد بلکه ابزارهای موجود در انواع توزیع‌های سیستم عامل لینوکس جهت امور امنیتی و نفوذگری استفاده شده است. کتاب مذکور به کاربران تازه کار لینوکس توصیه نمی‌شود و بایستی ابتدا از طریق یک کتاب پایه و مرجع اصول و روش کار، استفاده و کار با محیط سیستم‌عامل لینوکس فراگرفته شود و سپس جهت پیاده‌سازی امور نفوذگری و امنیتی به این کتاب مراجعه کرد. این کتاب برای کارشناسان، دانشجویان، متخصصان شبکه و امنیت شبکه بسیار مفید می‌باشد و از طریق آن می‌توانند با اصول و روش‌های حمله و مقابله با آن از طریق مبداء های لینوکسی آشنا شوند و راه‌کارهای مقابله با آن را فرا گیرند. این کتاب قصد دارد کارشناسان و متخصصان شبکه را با اصول و قواعد حملات برعلیه شبکه‌های کامپیوتری آشنا نماید. درحال حاضر نسخه‌های لاتینی که در این خصوص نوشته شده است به‌صورت پراکنده به بررسی حملات پرداخته است، اما این کتاب قصد دارد با یک انسجام کامل به حملاتی که توسط سیستم‌های‌عامل لینوکس برعلیه تمامی سیستم‌های‌عامل انجام می‌شود بپردازد، زیرا همان‌طور که می‌دانید سیستم‌عامل لینوکس از ابزارهای اساسی و پایه‌ای نفوذگران و هکران برخوردار می‌باشد و یک هکر جهت انجام حملات هکری خود، شدیداً نیازمند این نوع سیستم‌عامل است. در این کتاب از تمامی منابع معتبر و پایه‌ای 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 آزمایشات نفوذ،

قوانین هکرهای بااخلاق و نحوه استفاده از ابزارهای موجود در توزیع‌های قدرتمند لینوکس در حوزه نفوذ بودم تا آن‌ها را با اصول فنّی آزمایشات نفوذ با کمک این توزیع‌ها آشنا و آگاه سازم و بتوان از آن 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 و استاندارد ساخه امنیت داده، اصول آزمایشات نفوذ، استانداردهای امنیت اطلاعات، نفوذگری (هک)، توزیع‌های استاندارد آزمایش‌نفوذ و هک می‌باشد که با تجربیات اینجانب در این خصوص آمیخته شده است، و به‌فرجام آزاد از مطالب و تجربیات گردآوری، و دخل و تصرفی نیز با آن همراه بوده 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)

این کتاب صرفاً برای افزایش آگاهی‌ها و رشد علمی متخصصین کامپیوتر تألیف گردیده است. در نتیجه عواقب ناشی از هرگونه سوءاستفاده از مطالب این کتاب برعهده شخص خاطی بوده و مؤلف و انتشارات هیچ گونه مسئولیتی در این مورد برعهده نخواهند گرفت.

پس از سپاس و ستایش به درگاه پروردگار از تمام دوستان و اساتیدی که مهربانانه دست مرا در انجام اینکار ناچیز فشردند، تشکر می‌کنم. برخود لازم می دانم از زحمات بی دریغ سرکار خانم مهندس سیده پونهٔ مرتضویان تشکر و قدردانی نمایم. زحمات خاضعانه ایشان سهم بزرگی در تهیه و تدوین این کتاب داشته است. همچنین از جناب آقای سعید بیکی نیز کمال تشکر را دارم. اکثر مطالب فصل چهارم این کتاب برگرفته از ترجمه کتاب هنر اکسپلویت‌نویسی می‌باشد که توسط ایشان ترجمه شده است.

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

یارب بگشا گره ز کار من زار — رحمی که ز عقل عاجزم در همه کار
جز درگه تو کی بودم درگاهی — محروم ازین درم مکن یا غفار

مجید داوری دولت آبادی - زمستان ۱۳۹۳

فهرست مطالب