

به نام خدا



تست نفوذ با کایلی لینوکس

KALI LINUX

مؤلفان

مهندس حمیدرضا قنبری

مهندس آلاله هاشمی نیا

مهندس سجاد محمدزاده

با همکاری گروه فنی و مهندسی ذوق

فهرست مطالب

۹	فصل ۱
۹	آشنا شدن با کابلی لینوکس
۱۰	منو کالی لینوکس
۱۲	مدیریت سرویس های کالی لینوکس
۱۲	سرویس SSH
۱۴	سرویس HTTP
۱۵	محیط بش
۲۳	فصل ۲
۲۳	ابزارهای ضروری
۲۴	ابزار نت کت NETCAT
۲۶	انتقال فایل بوسیله ابزار نت کت
۲۸	مدیریت ریموت با ابزار نت کت NETCAT
۳۳	واپرشارک
۴۱	فصل ۳
۴۱	جمع آوری منفعل اطلاعات
۴۲	جمع آوری منفعل اطلاعات
۴۲	جمع آوری باز اطلاعات وب

۴۳ سرشماری با گوگل
۴۴ گوگل هکینگ
۴۹ NETCRAFT نت کرفت
۴۹ سرشماری هویز

فصل ۴..... ۶۴

جمع آوری فعال اطلاعات ۶۵

۶۶ سرشماری DNS
۶۶ اتوماسیون لوکاپ سرور
۶۷ پروت فورس لوکاپ
۶۸ انتقال ناحیه DNS
۷۱ ابزارهای دیگر در کالی لینوکس
۷۳ اسکن پورت
۷۴ اسکن UDP
۷۴ مشکلات رایج اسکن پورت
۸۱ بنرگرینگ و سرشماری سرویس ها
۸۳ سرشماری SMB
۸۳ اسکن برای سرویس نت بایوس
۸۴ سرشماری نشست نال
۸۶ سرشماری SMTP
۸۸ سرشماری SNMP
۸۸ درخت MIB
۸۹ اسکن SNMP

فصل ۵..... ۹۳

اسکن آسیب پذیری..... ۹۳

۹۴ اسکن آسیب پذیری
۹۵ اسکنر آسیب پذیری OPENVAS

فصل ۶..... ۱۰۵.....

سرریز بافر..... ۱۰۵.....

سرریز بافر (BUFFER OVERFLOWS)..... ۱۰۶.....

فازینگ (FUZZING)..... ۱۰۶.....

تاریخچه آسیب پذیری..... ۱۰۶.....

تعامل با پروتکل POP3..... ۱۰۷.....

فصل ۷..... ۱۱۳.....

بکارگیری سرریز بافر WIN32..... ۱۱۳.....

بازنویسی شکست..... ۱۱۴.....

کنترل EIP..... ۱۱۴.....

آنالیز درخت باینری..... ۱۱۴.....

بررسی کاراکترهای بد..... ۱۲۰.....

دسترسی به شل..... ۱۲۹.....

بهینه سازی اکسپلویت..... ۱۳۰.....

خط‌مشی کیفیت انتشارات مؤسسه فرهنگی هنری دیباگران تهران در عرصه کتاب‌هایی است که بتواند خواسته‌هایی به روز جامعه فرهنگی و علمی کشور را تا حد امکان پوشش دهد.

حمد و سپاس ایزد منان را که با الطاف بیکران خود این توفیق را به ما ارزانی داشت تا بتوانیم در راه ارتقای دانش عمومی و فرهنگی این مرز و بوم در زمینه چاپ و نشر کتب علمی دانشگاهی، علوم پایه و به ویژه علوم کامپیوتر و انفورماتیک گام‌هایی هرچند کوچک برداشته و در انجام رسالتی که بر عهده داریم، مؤثر واقع شویم.

گسترده‌گی علوم و توسعه روزافزون آن، شرایطی را به وجود آورده که هر روز شاهد تحولات اساسی چشمگیری در سطح جهان هستیم. این گسترش و توسعه نیاز به منابع مختلف از جمله کتاب را به عنوان قدیمی‌ترین و راحت‌ترین راه دستیابی به اطلاعات و اطلاع‌رسانی، بیش از پیش روشن می‌نماید.

در این راستا، واحد انتشارات مؤسسه فرهنگی هنری دیباگران تهران با همکاری جمعی از اساتید، مؤلفان، مترجمان، متخصصان، پژوهشگران، محققان و نیز پرسنل ورزیده و ماهر در زمینه امور نشر درصدد هستند تا با تلاش‌های مستمر خود برای رفع کمبودها و نیازهای موجود، منابعی پُر بار، معتبر و با کیفیت مناسب در اختیار علاقمندان قرار دهند.

کتابی که در دست دارید با همت "جناب آقایان حمیدرضا قنبری-سجاد محمدزاده -و سرکار خانم‌ها آلاله هاشمی نیا -مهرنوش آذرنیا و با همکاری گروه فنی و مهندسی ذوق" و تلاش جمعی از همکاران انتشارات میسر گشته که شایسته است از یکایک این گرامیان تشکر و قدردانی کنیم.

کارشناسی و نظارت بر محتوا: زهره قزلباش

در خاتمه ضمن سپاسگزاری از شما دانش‌پژوه گرامی درخواست می‌نماید با مراجعه به آدرس dibagaran.mft.info (ارتباط با مشتری) فرم نظرسنجی را برای کتابی که در دست دارید تکمیل و ارسال نموده، انتشارات دیباگران تهران را که جلب رضایت و وفاداری مشتریان را هدف خود می‌داند، یاری فرمایید.

امیدواریم همواره بهتر از گذشته خدمات و محصولات خود را تقدیم حضورتان نماییم.

مدیر انتشارات

مؤسسه فرهنگی هنری دیباگران تهران
Publishing@mftmail.com

مقدمه مولفان

هوالحکیم

آنچه در این کتاب می خوانید نگاهی است با رویکرد آموزشی بر سیستم کایلی لینوکس با محوریت نفوذ و پیشگیری و ارتقای سطح امنیتی شبکه ها و سیستم های کامپیوتری ، امید است مطالعه این کتاب گامی کوچک در ارتقای سطح دانش علمی مخاطبین گرامی به همراه داشته باشد .

زمستان ۱۳۹۶

گروه مولفان