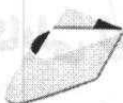


۱۴۰۵۵۵۵
۹۷/۲/۱۹

به نام خدا



مؤسسه فرهنگی هنری
دیباگران تهران

تست نفوذ با کایلی لینوکس

مؤلفان

مهندس حمیدرضا قنبری

مهندس آلاله هاشمی نیا

مهندس سجاد محمدزاده

مهندس مهرنوش آذرنیا

هرگونه چاپ و تکثیر از محتویات این کتاب بدون اجازه کتبی ناشر ممنوع است. متخلفان به موجب قانون حمایت حقوق مؤلفان، مصنفان و هنرمندان تحت پیگرد قانونی قرار می گیرند.

عنوان کتاب: تست نفوذ با کالی لینوکس ۲

KALI LINUX

مؤلفان: مهندس حمیدرضا قنبری

مهندس آلاله هاشمی نیا

مهندس سجاد محمدزاده

مهندس مهرداد آذر نیا

ناشر: موسسه نشری دیباگران تهران

صفحه آرای: فرنوش عادلهم

طراح جلد: داریوش فرسای

نوبت چاپ: اول

تاریخ نشر: ۱۳۹۷

چاپ و صحافی: دانشجو

تیراژ: ۱۰۰ جلد

قیمت: ۳۰۰۰۰۰ ریال

شابک: ۹۷۸-۶۰۰-۱۲۴-۸۲۱-۴

نشانی واحد فروش: تهران، میدان انقلاب،

خ کارگر جنوبی، روبروی پاساژ مهستان،

پلاک ۱۲۵۱

تلفن: ۰۲۰۸۵۱۱۱-۶۶۴۱۰۰۴۶

کد پستی: ۱۳۱۴۹۸۳۱۸۵

فروشگاههای اینترنتی دیباگران تهران :

عنوان و نام پدیدآور: تست نفوذ با کالی لینوکس ۲/مؤلفان: حمیدرضا قنبری.....و دیگران.

مشخصات نشر: تهران: دیباگران تهران: ۱۳۹۷

مشخصات ظاهری: ۱۶۲ ص:مصور.

شابک: ۹۷۸-۶۰۰-۱۲۴-۸۲۱-۴

وضعیت فهرست نویسی: فیبا

یادداشت: مؤلفان: حمیدرضا قنبری، آلاله هاشمی

نیا، سجاد محمدزاده، مهرنوش آذر نیا.

یادداشت: عنوان دیگر: تست نفوذ با کالی لینوکس ۲

kali linux

موضوع: سیستم عامل لینوکس

منبع: linux

موضوع: سیستم های عامل (کامپیوتر)

موضوع: operating systems (computer)

موضوع: آشنایی (تست نفوذ) (ایمن سازی کامپیوتر)

موضوع: penetration testing (computer security)

شناسه افزوده: قنبری، حمیدرضا، ۱۳۶۸-

رده بندی کنگره: ۱۳۹۷ ۹۱۰/۷۶/۷۶ QA

رده بندی دیویی: ۰۰۵/۴۳۲

شماره کتابشناسی ملی: ۵۱۳۶۴۶۲

www.mftbook.ir / www.dibagaran-tehran.com/ www.mftdibagaran.ir

لینک ربات دیباگران: @dibagaran-tehranbot

نشانی تلگرام: @mftbook

اپلیکشین دیباگران را از سایت های فروشگاههای ما دریافت و نصب نمایید.

فهرست مطالب

فصل ۱.....	۹
بکارگیری سرور بافر لینوکس.....	۹
بکارگیری سرور بافر ویندوز.....	۱۰
شکست کراس فایل.....	۱۱
فصل ۲.....	۲۳
کار کردن با اکسلویتیته ها.....	۲۳
کار کردن با اکسلویتیته ها.....	۲۴
فصل ۳.....	۳۱
انتقال فایل.....	۳۱
انتقال فایل.....	۳۲
آپلود فایل ها.....	۳۳
استفاده از DEBUG.EXE برای انتقال فایل ها.....	۳۷
فصل ۴.....	۴۱
ارتقاء مجوزهای دسترسی.....	۴۱
مثال اکسلویتیته ارتقا مجوزهای دسترسی در لینوکس.....	۴۲
مثال اکسلویتیته ارتقا مجوزهای دسترسی در ویندوز.....	۴۳

فصل ۵ ۵۱

حملات سمت کلاینت ۵۱

حملات سمت مشتری ۵۲

شبکه خود را بشناسید ۵۲

حمله جاوا اپلت ۵۷

فصل ۶ ۶۱

حملات اسکریپشن وب ۶۱

حملات اسکریپت نویسی کراس سایت (XSS) ۶۲

حملات تزریق اسکریپت، کورانه ۶۹

حملات تزریق اسکریپت (نظری) ۷۶

فصل ۷ ۸۵

حملات پسورد ۸۵

آماده سازی برای پروت فورس ۸۶

فایل های دیکشنری (DICTIONARY FILES) ۸۶

ابزارهای PWDUMP و FGDUMP ۸۸

ایجاد پروفایل پسورد ۹۱

تغییر پسوردها ۹۲

پروت فورس HTTP ۹۴

ابزار JHON THE RIPPER ۹۷

فصل ۸ ۱۰۱

تغییر مسیر پورت ۱۰۱

تغییر مسیر پورت و تانلینگ ((PORT REDIRECTION AND TUNNELING) ۱۰۲

تانلینگ HTTP ۱۰۷

فصل ۹..... ۱۱۱

فریم ورک متاسپلویت ۱۱۱

ماژول های اگزپلوری ۱۱۴

پیلودهای متاسپلویت ۱۲۰

فصل ۱۰..... ۱۲۹

عبور از آنتی ویروس ۱۲۹

عبور از نرم افزار آنتی ویروس ۱۳۰

انکودینگ با پیلودهای متاسپلویت ۱۳۰

فصل ۱۱..... ۱۳۵

آزمایشگاه ۱۳۵

ابلیکیشن آسیب پذیر DVWA ۱۳۶

نصب کالی لینوکس ۱۳۹

پایه سازی متاسپلویتیل METASPLOITABLE ۱۵۱

سیستم آسیب پذیر OWASPBWA ۱۵۶

منابع ۱۶۲

خط‌مشی کیفیت انتشارات مؤسسه فرهنگی هنری دیباگران تهران در عرصه کتاب ملی است که بتواند خواسته‌های 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، دیرتر واقع شویم.

گسترده‌ی 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 محتمل‌ترین 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 پربار، معتبر و با کیفیت مناسب در اختیار علاقمندان قرار دهند.

کتابی که در دست دارید با همت و مساعدت همکاران حمیدرضا قنبری-آلاله هاشمی-نیا-سجاد محمدزاده-مهرنوش آذرینیا" 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 درنماید 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 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 دالاله این کتاب گامی کوچک در ارتقای سطح دانش علمی مخاطبین گرامی به همراه داشته باشد .

زمستان ۱۳۹۶

گروه مولفان

www.ketab.ir