

۱۵۸۹۰۸۱
۹۷۷۷۷۷

به نام خدا



تست نفوذ نیا کایلی لینوکس

KALI LINUX

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

KALI LINUX

مؤلفان: مهندس حمیدرضا قنبری

خندس آلاله هاشمی نیا

خندس سجاد محمدزاده

مهندس ه. ر. ش. آرنیا

با همکاری گروه نی و خندس ذوق

ناشر: موسسه فرهنگی هنری دیباگران تهران

صفحه آرای: فرنوش عبدال

طراح جلد: داریوش فرسای

نوبت چاپ: اول

تاریخ نشر: ۱۳۹۷

چاپ و صحافی: دانشجو

تیراژ: ۱۰۰ جلد

قیمت: ۲۱۰۰۰۰ ریال

شابک: ۹۷۸-۶۰۰-۱۲۴-۸۵۸-۰

نشانی واحد فروش: تهران، میدان انقلاب،

خ کارگر جنوبی، روبروی پاساژ مهستان،

پلاک ۱۲۵۱

تلفن: ۲۲۰۸۵۱۱۱-۶۶۴۱۰۰۴۶

فروشگاههای اینترنتی:

www.mftbook.ir

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

نشانی تلگرام: @mftbook لینک ربات دیباگران: @dibagaran-tehranbot

سرشناسه: قنبری، حمیدرضا، ۱۳۶۸-

عنوان و نام پدیدآور: تست نفوذ با کالی لینوکس

KALI LINUX

مؤلفان: حمیدرضا قنبری، آلاله هاشمی نیا، سجاد محمدزاده،

با همکاری گروه فنی و مهندسی ذوق

مشخصات نشر: تهران: دیباگران تهران: ۱۳۹۶

مشخصات ظاهری: ۱۳۴-۸۵۸-۰۰-۶۰۰-۹۷۸ ص: مصور،

شابک: ۹۷۸-۶۰۰-۱۲۴-۸۵۸-۰۰

وضعیت فهرست نویسی: فیبا

موضوع: سیستم عامل لینوکس

موضوع: LINUX

موضوع: سیستم های عامل (کامپیوتر)

موضوع: Operating systems (computers)

موضوع: آرایش نفوذ (ایمن سازی کامپیوتر)

موضوع: penetration (computer security)

شناسه افزودن: ۱۳۷۰-۰۰-۱۲۴-۸۵۸-۰۰

شناسه افزوده: ۱۳۶۸-۰۰-۱۲۴-۸۵۸-۰۰

شناسه افزوده: گروه ایده پدیدآور: گروه فنی و مهندسی ذوق

رده بندی کنگره: ۹۱۳۹۷ ق ۷۶/۷۶ QA

رده بندی دیویی: ۰۰۵/۴۲۲

شماره کتابشناسی ملی: ۵۱۲۸۵۰۰

فهرست مطالب

۹	فصل ۱
۹	آشنا شدن با پای لینوکس
۱۰	منو کالی لینوکس
۱۲	مدیریت سرویس های پای ه کس
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	وایرشارک
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	 نت کرفت NETCRAFT
۴۹	 سرشماری هويز

فصل ۴ ۶۴

جمع آوری فعال اطلاعات ۶۵

۶۶	 سرشماری DNS
۶۶	 اتوما جیون لوکاپ سرور
۶۷	 پروت فورس اسکنر
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	 اسکن آسیب پذیری OPENVAS

فصل ۶..... ۱۰۵

سرریز بافر..... ۱۰۵

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

فازینگ (FUZZING)..... ۱۰۶

تاریخچه آسیب پذیری..... ۱۰۶

تعامل با روتکال POP..... ۱۰۷

فصل ۷..... ۱۱۳

بکارگیری سرریز بیت 32 بیت..... ۱۱۳

بازنویسی شکست..... ۱۱۴

کنترل EIP..... ۱۱۴

آنالیز درخت باینری..... ۱۱۴

بررسی کاراکترهای بد..... ۱۲۰

دسترسی به شل..... ۱۲۹

بهینه سازی اکسپلویت..... ۱۳۰

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