



هک با کالی

تکنیکهای عملی تست نفوذ

نویسندگان:

James Broad
Andrew Bindner

مترجمین:

دکتر محمد رحمانی منش
(عضو هیأت علمی دانشگاه سمنان)
مهندس افشین امینی
علیرضا حسینی الهاشمی

سرشناسه	برود، جیمز Broad, James
عنوان و نام پدیدآور	هک با کالی: تکنیک‌های عملی تست نفوذ/نویسندگان [جیمز برود، اندرو بایندر]؛ مترجمین محمد رحمانی منش، افشین امینی، علیرضا حسینی الهاشمی.
مشخصات نشر	سمنان: دانشگاه سمنان، ۱۳۹۶.
مشخصات ظاهری	۲۹۸ص. شابک: 978-600-8424-51-2
وضعیت فهرست نویسی	فیا
یادداشت	عنوان اصلی: Hacking with Kali : practical penetration testing techniques, 2005.
موضوع	کالی لینوکس: موضوع: Kali Linux
موضوع	آزمایش نفوذ (ایمن سازی کامپیوتر) موضوع: Penetration testing (Computer security)
موضوع	هکرها: موضوع: Hackers
شناسه افزوده	Bindner, Andrew: رده بندی دیویی: ۰۰۵/۸
شناسه افزوده	حمزه منش، محمد، ۱۳۵۸ - مترجم: شناسه افزوده: امینی، افشین، ۱۳۷۱ - مترجم
شناسه افزوده	حسینی الهاشمی، علیرضا، ۱۳۷۱ - مترجم
شناسه افزوده	دانشگاه سمنان: شناسه افزوده: Semnan University
رده بندی کنگره	۱۳۹۶: ۷۶/۹/ک۹: شماره کتابشناسی ملی: ۴۹۴۹۸۱



هک با کالی تکنیکهای عملی تست نفوذ

مترجمان: دکتر محمد رحمانی منش - مهندس افشین امینی - علیرضا حسینی الهاشمی

نوبت چاپ: اول - پائیز ۱۳۹۶

ناشر: انتشارات دانشگاه سمنان

شمارگان: ۲۰۰ جلد

قیمت: ۳۲۰۰۰۰ ریال

ISBN: 978-600-8424-51-2



شابک:

حق چاپ محفوظ و متعلق به انتشارات دانشگاه سمنان می باشد.

مراکز پخش: سمنان: روبروی پارک سوکان - پردیس شماره ۱ - انتشارات دانشگاه سمنان - تلفن: ۰۲۳۳۳۶۵۴۱۴۲ و ۰۲۳۳۱۵۳۳۲۷۰

وب سایت: www.press.semnan.ac.ir

تهران: میدان انقلاب - ابتدای خیابان ۱۲ فروردین - پلاک ۹ - تلفن: ۰۲۱۶۶۹۶۶۱۱۴-۱۵ - انتشارات سیمای دانش

فصل اول : مقدمه

۱	۱-۱- نگاهی بر مطالب و نکات کلیدی کتاب.....	۱
۲	۲-۱- مخاطبان کتاب.....	۲
۴	۳-۱- نمودارها، شکل ها و اسکرین شات ها.....	۴
۵	۴-۱- اصطلاحات رایج.....	۵
۱۰	۵-۱- تاریخچه کالی لینوکس.....	۱۰

فصل دوم : داندلود و نصب کالی لینوکس

۱۳	۱-۲- کالی لینوکس.....	۱۳
۱۶	۲-۲- دریافت کالی لینوکس.....	۱۶
۱۷	۳-۲- نصب بر روی دیسک سخت.....	۱۷
۲۹	۴-۲- نصب بر روی فلش مموری.....	۲۹
۳۲	۵-۲- نصب بر روی کارتهای SD.....	۳۲

فصل سوم : نرم افزارها، پچها و بروزرسانیها

۳۳	۱-۳- ابزار مدیریت بسته APT.....	۳۳
۳۹	۲-۳- مدیریت بستههای دیبیا.....	۳۹
۴۱	۳-۳- آرشیوسازی با Tarballs.....	۴۱
۴۵	۴-۳- راهنمای عملی نصب برنامه Nessus.....	۴۵

فصل چهارم : پیکربندی کالی لینوکس

۵۰	۱-۴- مبانی شبکه.....	۵۰
۵۷	۲-۴- استفاده از رابط کاربری گرافیکی برای پیکربندی کارتهای شبکه سیمی.....	۵۷
۶۱	۳-۴- استفاده از دستورات نوشتاری در خط فرمان برای پیکربندی کارتهای شبکه سیمی.....	۶۱
۶۵	۴-۴- استفاده از GUI برای پیکربندی کارت شبکه بی سیم.....	۶۵
۷۲	۵-۴- استفاده از GUI برای راه اندازی، توقف و راه اندازی مجدد سرور آپاچی.....	۷۲
۷۴	۶-۴- سرور FTP.....	۷۴

۷۷	SSH سرور
۷۶	۸-۴ پیکربندی و دسترسی به رسانه‌های خارجی
۸۰	۹-۴ بروزرسانی کالی
۸۱	۱۰-۴ ارتقای کالی
۸۲	۱۱-۴ افزودن یک مخزن

فصل پنجم : ساخت یک آزمایشگاه تست نفوذ

۸۶	۱-۵ ساخت یک آزمایشگاه کوچک
۱۰۰	۲-۵ ماشین مجازی METASPLOITABLE2
۱۰۸	۳-۵ آزمایشگاه خود را گسترش دهید
۱۱۱	۴-۵ مجموعه رمزهای MAGICAL CODE INJECTION RAINBOW

فصل ششم : معرفی مراحل تست نفوذ

۱۱۹	۱-۶ مقدمه ای بر چرخه حیات
-----	--------------------------------

فصل هفتم : شناسایی

۱۲۶	۱-۷ مقدمه
۱۲۸	۲-۷ نمونه گیری از وب سایت
۱۳۰	۳-۷ جستجوهای گوگل
۱۳۶	۴-۷ گوگل هک
۱۳۸	۵-۷ شبکه‌های اجتماعی
۱۳۹	۶-۷ سایتهای کاربایی
۱۴۰	۷-۷ DNS و حمله DNS

فصل هشتم : اسکن

۱۴۶	۱-۸ مقدمه‌ای بر فاز اسکن
۱۴۸	۲-۸ درک پروتکل‌های بر مبنای IP
۱۵۵	۳-۸ Nmap پادشاه پوشگرها
۱۷۱	۴-۸ HPING3
۱۷۲	۵-۸ NESSUS

فصل نهم : اکسپلویت

۱۸۳	 ۱-۹- مقدمه
۱۸۹	 ۲-۹- نمای کلی از فریم ورک متاسپلویت
۱۹۷	 ۳-۹- دسترسی به متاسپلویت
۲۱۶	 ۴-۹- اکسپلویت وب سرورها و نرم افزارهای تحت وب

فصل دهم : تثبیت دسترسی

۲۳۶	 ۱-۱۰- مقدمه
۲۳۷	 ۲-۱۰- اصطلاحات و مفاهیم اصلی
۲۴۲	 ۳-۱۰- درآپشتی
۲۵۱	 ۴-۱۰- کی‌لرها

فصل یازدهم : * ارزش‌ها - هالب‌ها

۲۵۵	 ۱-۱۱- گزارش دهی
-----	-----------------------