

۲۳۵۹۹۰

راهنمای جامع کالی لینوکس

کتاب مرجع برای تست نفوذ

www.ketab.ir
محمدعلی یاسر

سرشناسه	: الیاسی، محمدعلی، ۱۳۷۸-
عنوان و نام پدیدآور	: راهنمای جامع کالی لینوکس : کتاب مرجع برای تست نفوذ
مشخصات نشر	: تهران: آروین نگار، ۱۴۰۲.
مشخصات ظاهری	: ۶۲۵ ص.: مصور (بخشی رنگی)، جدول، نمودار
شابک	: 978-622-5756-32-8
عنوان دیگر	: کتاب مرجع برای تست نفوذ.
موضوع	: کالی لینوکس - Kali Linux
موضوع	: آزمایش نفوذ - (ایمن سازی کامپیوتر)
	: Penetration testing (Computer security)
	: هکرها - Hackers
رده بندی کنگره	: QA۷۶/۹
رده بندی دبیوی	: ۰۰۵/۸
شماره کتابشناسی ملی	: ۹۳۰۱۳۰۵
اطلاعات رکورد کتابشناسی	: فیبا

این اثر مشمول قانون حمایت مؤلفان و مصنفان و هنرمندان مصوب ۱۳۴۸ است. هرکس تمام یا قسمتی از این اثر را بدون اجازه ناشر) نشر یا پخش یا عرضه کند مورد پیگرد قانونی قرار خواهد گرفت.

تلفن: ۶۶۴۱۸۵۱۲



همراه: ۰۹۳۹۱۲۶۱۴۱۹

مرکز پخش: میدان انقلاب، خیابان انقلاب ترسیده به ۱۲ فروردین، پلاک ۱۳۱۴، طبقه سوم، واحد ۱۱

عنوان کتاب	راهنمای جامع کالی لینوکس، کتاب مرجع برای تست نفوذ
مؤلف	محمدعلی الیاسی
ناشر	انتشارات آروین نگار
نوبت و سال چاپ	اول / ۱۴۰۲
تیراژ	۱۰۰ نسخه
قیمت	۴۲۰۰۰۰ تومان
شابک	۹۷۸-۶۲۲-۵۷۵۶-۳۲-۸

مرکز پخش: فروشگاه اینترنتی کتاب آرتین www.artinbook.ir

فروشگاه اینترنتی گنبد نیلگون آسمان www.gnapub.ir

تلفن: ۰۹۱۲۴۱۶۱۹۰۹ - ۶۶۴۸۱۸۷۰

پست الکترونیکی arvinnegarpub@gmail.com

کلیه حقوق این کتاب برای آروین نگار محفوظ است.

مقدمه

کالی لینوکس یک توزیع لینوکس بسیار قدرتمند است که برای متخصصان امنیتی طراحی شده است. این توزیع شامل ابزارهایی است که برای تست نفوذ، تحلیل بسترهای شبکه و بررسی امنیت سیستم‌های مختلف مورد استفاده قرار می‌گیرند.

انگیزه خلق این کتاب، رویکرد مرحله به مرحله در کالی لینوکس است که درک آن برای همه آسان می‌باشد و به همه خوانندگان کمک می‌کند تا با استفاده از جدیدترین ابزارها و تکنیک‌ها پس از اتمام متخصصان ماهر شوند.

در این کتاب، سعی شده است به صورت جامع و کامل، ابزارهای موجود در کالی لینوکس را معرفی و توضیح داده شود. همچنین، در این استفاده از این ابزارها و تکنیک‌های مورد استفاده در حوزه امنیت شبکه و سیستم‌های کامپیوتری نیز به شما آموزش داده می‌شود.

هک‌های اخلاقی و آزمونگرهای نفوذ باید به جدیدترین دانش، مهارت‌ها و ابزارها برای کشف و بهره‌برداری مؤثر از آسیب‌پذیری‌های امنیتی پنهان در سیستم‌ها و شبکه‌های هدف خود مجهز شوند. در طول فرآیند نگارش این کتاب، از رویکرد ویژه‌ای پسند استفاده کرده‌ام، که به شما کمک می‌کند پیچیده‌ترین موضوعات، اصطلاحات، و چرایی نیاز به آزمایش نقص‌های امنیتی در یک سیستم و شبکه را به راحتی درک کنید.

این کتاب با آشنایی شما با طرز فکر یک بازیگر تهدید مانند هکر و مقایسه طرز فکر هکرها با آزمونگرهای نفوذ آغاز می‌شود. این مهم است که بفهمیم یک بازیگر تهدید چگونه فکر می‌کند و چه چیزی برای آنها ارزشمندتر است. در حالی که آزمونگرهای نفوذ

ممکن است طرز فکر مشابهی داشته باشند، هدف آنها کشف و کمک به رفع آسیب پذیری های امنیتی قبل از وقوع یک حمله سایبری واقعی به یک سازمان است.

علاوه بر این، نحوه ایجاد یک محیط آزمایشگاهی با استفاده از فناوری های مجازی سازی برای کاهش هزینه خرید تجهیزات را یاد خواهید گرفت. محیط آزمایشگاه یک شبکه با سیستم های آسیب پذیر و سرورهای وب اپلیکیشن را تقلید می کند. علاوه بر این، یک آزمایشگاه اکتیو دایرکتوری ویندوز کاملاً اصلاح شده برای نشان دادن آسیب پذیری های امنیتی موجود در دامنه ویندوز ایجاد شده است.

به زودی خواهید آموخت که چگونه با استفاده از ابزارها و استراتژی های رایج برای شناسایی و جمع آوری اطلاعات، جمع آوری اطلاعات در دنیای واقعی را در سازمان ها انجام دهید. یادگیری هک اخلاقی و تست نفوذ بدون یادگیری نحوه انجام ارزیابی آسیب پذیری با استفاده از ابزارهای استاندارد صنعت کامل نخواهد بود. علاوه بر این، مدتی را صرف یادگیری نحوه بهره برداری از آسیب پذیری های امنیتی رایج خواهید کرد. پس از مرحله بهره برداری، در معرض تکنیک های پس از بهره برداری قرار خواهید گرفت و نحوه راه اندازی عملیات فرماندهی و کنترل (C2) برای حفظ دسترسی در یک شبکه در معرض خطر را یاد خواهید گرفت.

با تکمیل این کتاب، به عنوان یک حرفه ای مشتاق امنیت سایبری در صنعت، از یک مبتدی تا متخصص از نظر یادگیری، درک و توسعه مهارت های خود در زمینه هک اخلاقی و تست نفوذ، سفری شگفت انگیز را طی خواهید کرد.

پس از تکمیل این کتاب با خلاقیت و مهارت های جدید خود، سعی کنید سناریوهای آزمایشگاهی اضافی بسازید و حتی محیط آزمایشگاه خود را با اضافه کردن ماشین های مجازی اضافی برای بهبود مجموعه مهارت خود گسترش دهید. این به شما کمک می کند تا به یادگیری ادامه دهید و مهارت های خود را به عنوان یک هکر قانونمند مشتاق و آزمونگر نفوذ توسعه دهید.

فهرست مطالب

فصل ۱. مقدمه ای بر هک

۱۶

- ۱-۱. شناسایی عوامل تهدید و هدف آنها..... ۱۸
- درک آنچه برای بازیگران تهدید مهم است..... ۲۲
- ۱-۱-۱. زمان..... ۲۲
- ۱-۲. منابع..... ۲۳
- ۱-۲-۱. عوامل مالی..... ۲۳
- ۱-۳. ارزش هک..... ۲۴
- ۱-۴. کاوش اصطلاحات امنیت سایبری..... ۲۴
- بررسی نیاز به تست نفوذ و مراحل آن..... ۲۸
- ۱-۵. ایجاد یک طرح نبرد تست نفوذ..... ۲۹
- مدل سازی تهدید..... ۳۲
- ۱-۶. تجزیه و تحلیل آسیب پذیری..... ۳۳
- بهره برداری..... ۳۳
- ۱-۷. درک رویکردهای تست نفوذ..... ۳۵
- انواع تست نفوذ..... ۳۶
- ۱-۸. بررسی مراحل هک..... ۳۹
- درک چارچوب زنجیره کشتار سایبری..... ۴۳
- ۱-۹. خلاصه..... ۵۰

فصل ۲. راه اندازی برای تکنیک های هک پیشرفته

۵۱

- ۲-۱. ساخت آزمایشگاه تیم قرمز AD..... ۵۲

۵۴.....	قسمت ۱ - نصب ویندوز سرور ۲۰۱۹.....	۲-۲.
۶۵.....	قسمت ۳ - ارتقاء به DC.....	۲-۳.
۶۷.....	بخش ۴ - ایجاد کاربران دامنه و حساب های سرپرست.....	۲-۴.
۶۹.....	قسمت ۵ - غیرفعال کردن محافظت از ضد بدافزار و فایروال دامنه.....	۲-۵.
۷۵.....	راه اندازی آزمایشگاه تست نفوذ بی سیم.....	۲-۶.
۷۷.....	پیاده سازی سرور RADIUS.....	۲-۷.
۸۷.....	قسمت ۳ - پیکربندی روتر بی سیم با RADIUS.....	۲-۸.
۸۹.....	خلاصه.....	۲-۹.

فصل ۳. شناسایی فعال شبکه های خارجی و داخلی

۹۱.....	۳-۱. تکنیک های اسکن مخفی.....	۳-۱.
۹۳.....	۳-۱-۱. تنظیم بسته IP منبع و تنظیمات شناسایی ابزار.....	۳-۱-۱.
۹۵.....	۳-۱-۲. اصلاح پارامترهای بسته.....	۳-۱-۲.
۹۷.....	۳-۱-۳. استفاده از پروکسی با شبکه های ناشناس.....	۳-۱-۳.
۱۰۳.....	۳-۲. شناسایی DNS و route mapping.....	۳-۲.
۱۰۳.....	۳-۲-۱. فرمان whois (پس از GDPR).....	۳-۲-۱.
۱۰۴.....	۳-۳. بکارگیری برنامه های شناسایی جامع.....	۳-۳.
۱۰۵.....	۳-۴. فریم ورک recon-ng.....	۳-۴.
۱۱۸.....	۳-۵. شناسایی زیرساخت شبکه خارجی.....	۳-۵.
۱۲۰.....	۳-۶. نقشه برداری فراتر از فایروال.....	۳-۶.
۱۲۱.....	۳-۶-۱. شناسایی IDS/IPS.....	۳-۶-۱.
۱۲۲.....	۳-۷. کاوش هاست ها.....	۳-۷.
۱۲۴.....	۳-۸. کشف پورت، سیستم عامل و سرویس.....	۳-۸.
۱۲۵.....	۳-۹. نوشتن پورت اسکنر خود با استفاده از netcat.....	۳-۹.
۱۲۶.....	۳-۹-۱. فوت پرینتینگ سیستم عامل.....	۳-۹-۱.
۱۲۷.....	۳-۹-۲. تعیین سرویس های فعال.....	۳-۹-۲.
۱۲۹.....	۳-۱۰. اسکن در مقیاس بزرگ.....	۳-۱۰.

۱۳۰.....	اطلاعات DHCP	۳-۱۰-۱
۱۳۱.....	شناسایی و کاوش میزبان های شبکه داخلی	۳-۱۰-۲
۱۳۳.....	دستورات نیتیو MS Windows	۳-۱۰-۳
۱۳۶.....	پخش ARP	۳-۱۰-۴
۱۳۷.....	پینگ سوئیپ	۳-۱۰-۵
	استفاده از اسکریپت ها برای ترکیب اسکن nmap و masscan	۳-۱۰-۶

۱۳۸

۱۴۰.....	استفاده از SNMP	۳-۱۰-۷
۱۴۳.....	اطلاعات اکانت ویندوز با نشست های SMB	۳-۱۰-۸
۱۴۴.....	مکان یابی اشتراک های شبکه	۳-۱۰-۹
۱۴۶.....	شناسایی سرورهای دامنه اکتیو دایرکتوری	۳-۱۰-۱۰
۱۴۷.....	کاوش محیط Microsoft Azure	۳-۱۰-۱۱
۱۵۰.....	استفاده از ابزار جامع (Legion)	۳-۱۰-۱۲
۱۵۱.....	استفاده از یادگیری ماشینی برای شناسایی	۳-۱۰-۱۳
۱۵۴.....	خلاصه	۳-۱۱

۱۵۵

فصل ۴. ارزیابی آسیب پذیری

۱۵۷.....	دیتابیس های آسیب پذیری محلی و آنلاین	۴-۱
۱۶۲.....	اسکن آسیب پذیری با Nmap	۴-۱-۱
۱۶۴.....	مقدمه ای بر اسکریپت نویسی Lua	۴-۱-۲
۱۶۶.....	سفارشی کردن اسکریپت های NSE	۴-۱-۳
۱۶۸.....	اسکنرهای آسیب پذیری وب اپلیکیشن ها	۴-۱-۴
۱۶۹.....	نیکتو	۴-۱-۵
۱۷۳.....	OWASP ZAP	4-1-6
۱۷۷.....	اسکنر آسیب پذیری برای برنامه های موبایل	۴-۲
۱۷۹.....	اسکنر آسیب پذیری شبکه OpenVAS	۴-۲-۱
۱۸۲.....	سفارشی کردن OpenVAS	۴-۲-۲

۱۸۲.....	اسکنرهای آسیب پذیری تجاری	۴-۳
۱۸۳.....	نسوس	۴-۳-۱
۱۸۵.....	Qualys	۴-۳-۲
۱۸۶.....	اسکنرهای تخصصی	۴-۴
۱۸۷.....	مدل سازی تهدید	۴-۵
۱۹۲.....	خلاصه	۴-۶

فصل ۵. مهندسی اجتماعی پیشرفته و امنیت فیزیکی

۱۹۵.....	متدولوژی فرمان و TTP	۵-۱
۱۹۶.....	فن آوری	۵-۱-۱
۲۰۰.....	حملات فیزیکی به کنسول	۵-۱-۲
۲۰۶.....	Sticky Keys	۵-۱-۳
۲۰۸.....	ایجاد یک دستگاه فیزیکی Rogue	۵-۱-۴
۲۰۹.....	عوامل حمله میکرو کامپیوتر یا USB	۵-۱-۵
۲۱۰.....	Raspberry Pi	۵-۱-۶
۲۱۲.....	MalDuino : BadUSB	5-1-7.
۲۱۶.....	مجموعه ابزار مهندسی اجتماعی (SET)	۵-۲
۲۲۰.....	حملات مهندسی اجتماعی	۵-۲-۱
۲۲۱.....	روش حمله وب Credential harvester	۵-۲-۲
۲۲۶.....	روش وب اتک چند حمله ای (Multi-attack web attack)	۵-۲-۳
۲۲۷.....	روش حمله به وب HTA	۵-۲-۴
۲۳۰.....	استفاده از حمله تزریق شل کد الفبایی PowerShell	۵-۲-۵
۲۳۱.....	مخفی کردن فایل های اجرایی و مبهم کردن URL مهاجم	۵-۲-۶
۲۳۳.....	تشدید حمله با استفاده از تغییر مسیر DNS	۵-۲-۷
۲۳۵.....	حمله Spear phishing	۵-۲-۸
۲۴۰.....	فیشینگ ایمیل با استفاده از Gophish	۵-۲-۹
۲۴۳.....	راه اندازی یک حمله فیشینگ با استفاده از Gophish	۵-۲-۱۰