

به نام خدا

۱۴۰۱/۱۱/۲۴
۴۵/۵۴

مؤسسه فرهنگی هنری
دییگران تهران

ارزیابی نفوذپذیری در شبکه‌های بی‌سیم

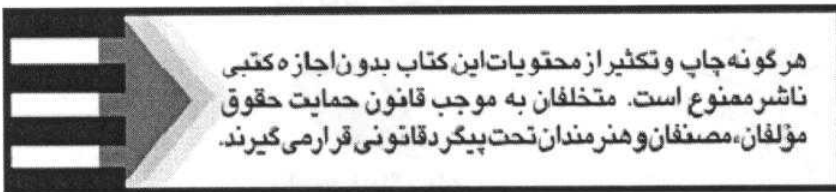
ویژه: متخصصان امنیت فناوری اطلاعات و تست نفوذ

اولین مرجع فارسی تست و آزمایش نفوذپذیری به وسیله Kali

مترجمان

مهندس رضا مقدم

مهندس فرزانه فرخی



عنوان کتاب اصلی: Backtrack5 Wireless Penetration Testing

ارزیابی نفوذپذیری در شبکه های بی سیم

مؤلف: Vivek Ramachandran

مترجمان: ههندس رضا مقدم

ههندس فرزانه فرخی

ناشر: مؤسسه فرهنگی هنری دیباگران تهران

حروفچینی و طراحی: مؤسسه فرهنگی هنری دیباگران تهران

طرح روی جلد: مجید بازاری

چاپ: نگین

نوبت چاپ: اول

تاریخ نشر: ۱۳۹۵

تیراژ: ۳۰۰ جلد

قیمت: ۲۳۰۰۰ ریال

شابک: ۹۷۸-۶۰۰-۱۲۴-۴۳۱-۵

ISBN: 978-600-124-431-5



نشانی واحد فروش: تهران، میدان انقلاب، خ کارگر جنوبی، روبروی پاساژ مهستان، پلاک ۱۲۵۱

کد پستی: ۱۳۱۴۹۸۳۱۸۵

تلفن: ۱۲-۰۲۲۰۸۵۱۱۱-۴۶۴۱۰۰۴۶

فروش اینترنتی: www.mftshop.com

پست الکترونیکی: bookmarket@mftmail.com

www.mftbook.ir

فهرست مطالب

۱۱	مقدمه ناشر
۱۲	مقدمه مترجم
۱۳	پیشگفتار
۱۳	آنچه در این کتاب می آموزید
۱۵	ابزارهای مورد نیاز برای برریر ها کتاب
۱۶	این کتاب برای چه کسانی مناسب است؟
۱۶	قراردادها
۱۷	فصل اول: آماده سازی آزمایشگاه بی سیم
۱۸	سخت افزار مورد نیاز
۱۸	سیستم های عامل مورد نیاز
۱۹	نصب Kali
۱۹	وقت کار است: نصب Kali
۲۱	چه اتفاقی افتاد؟
۲۲	شما هم امتحان کنید: نصب Kali روی ماشین مجازی
۲۲	راه اندازی اکسس پوینت
۲۲	وقت کار است: تنظیمات اکسس پوینت
۲۴	چه اتفاقی افتاد؟
۲۵	شما هم امتحان کنید: تنظیم اکسس پوینت برای استفاده از WEP و WPA
۲۵	راه اندازی کارت بی سیم
۲۵	وقت کار است: تنظیم کارت بی سیم
۲۶	چه اتفاقی افتاد؟
۲۶	اتصال به اکسس پوینت
۲۷	وقت کار است: تنظیم کارت بی سیم
۳۱	چه اتفاقی افتاد؟
۳۱	شما هم امتحان کنید: ایجاد اتصال با تنظیمات WEP

- سؤالات: درک مفاهیم پایه‌ای ۳۱
- خلاصه فصل ۳۱
- دستورات و کدهای مورد استفاده در فصل اول ۳۲

فصل دوم: شبکه‌های بی‌سیم و ریسک‌های ذاتی آن ۳۳

- بازبینی فریم‌های شبکه‌های بی‌سیم ۳۳
- وقت کار است: ایجاد اینترفیس برای رصد کردن دیتا ۳۷
- چه اتفاقی افتاد؟ ۴۰
- شما هم امتحان کنید: ساخت چندین اینترفیس حالت نظارت ۴۰
- وقت کار است: شنود بسته‌های بی‌سیم ۴۱
- چه اتفاقی افتاد؟ ۴۲
- شما هم امتحان کنید: یافتن دستگاه‌های مختلف ۴۳
- وقت کار است: دیدن فریم‌های مدیریت، کنترل و دیتا ۴۳
- چه اتفاقی افتاد؟ ۴۶
- شما هم امتحان کنید: بازی با فیلترها ۴۷
- وقت کار است: شنود بسته‌های دیتا برای شبکه ما ۴۷
- چه اتفاقی افتاد؟ ۴۹
- شما هم امتحان کنید: تحلیل بسته‌های دیتا ۵۰
- وقت کار است: تزریق بسته ۵۰
- چه اتفاقی افتاد؟ ۵۱
- شما هم امتحان کنید: نصب Kali روی ماشین مجازی ۵۱
- نکته مهم در مورد شنود و تزریق در شبکه‌های بی‌سیم ۵۲
- وقت کار است: با کارت آلفای خود تمرین کنید ۵۲
- چه اتفاقی افتاد؟ ۵۴
- شما هم امتحان کنید: شنود چند کانال همزمان ۵۴
- نقش حوزه‌های مقرراتی در شبکه بی‌سیم ۵۴
- وقت کار است: با کارت آلفای خود تمرین کنید ۵۵
- چه اتفاقی افتاد؟ ۵۸
- شما هم امتحان کنید: حوزه‌های مقرراتی را بررسی کنید ۵۸
- سؤالات: تزریق و شنود بسته ۵۸
- خلاصه فصل ۵۹
- دستورات و کدهای مورد استفاده در فصل دوم ۵۹

فصل سوم: عبور از احراز هویت شبکه‌های بی‌سیم ۶۱

- SSIDهای مخفی ۶۲

۶۴	وقت کار است: کشف SSID مخفی
۶۸	چه اتفاقی افتاد؟
۶۹	شما هم امتحان کنید: لغو احراز هویت انتخابی
۶۹	فیلتر کردن مک
۶۹	مک فیلترینگ
۷۰	وقت کار است: شکست دادن مک فیلترینگ
۷۳	چه اتفاقی افتاد؟
۷۳	حراز هویت باز
۷۳	امنیت قدیمی شبکه بی سیم
۷۳	احراز هویت قدیمی
۷۵	وقت کار است: عبور از احراز هویت باز
۷۶	چه اتفاق افتاد؟
۷۶	احراز هویت کلید اشتراکی
۷۷	وقت کار است: عبور از احراز هویت اشتراکی
۸۳	چه اتفاقی افتاد؟
۸۳	شما هم امتحان کنید: پر کردن جدول اکسس پوینت
۸۳	سوالات: احراز هویت شبکه‌های بی سیم
۸۴	خلاصه فصل
۸۴	دستورات و کدهای مورد استفاده در فصل سوم
۸۷	فصل چهارم: معایب رمزگذاری در شبکه‌های بی سیم
۸۸	رمزگذاری شبکه‌های بی سیم
۸۸	رمزگذاری WEP
۸۸	رمزگذاری استاتیک WEP
۹۲	وقت کار است: شکستن WEP
۹۹	چه اتفاقی افتاد؟
۹۹	شما هم امتحان کنید: جعل هویت با شکستن کلید WEP
۱۰۰	رمزگذاری WPA و WPA2
۱۰۲	مکانیزم WPA و WPA2
۱۰۳	مکانیزم TKIP
۱۰۴	مکانیزم CCMP
۱۰۴	وقت کار است: شکستن کلمه عبور ضعیف در WPA-PSK
۱۰۸	چه اتفاقی افتاد؟
۱۰۹	شما هم امتحان کنید: سعی کنید WPA-PSK را با استفاده از Cowpatty بشکنید
۱۰۹	سرعت بخشیدن به فرایند شکستن کلمه عبور WPA و WPA2

۱۱۰	وقت کار است: سرعت بخشیدن به فرایند شکستن کلید
۱۱۴	چه اتفاقی افتاد؟
۱۱۴	رمزگشایی بسته‌های WEP و WPA
۱۱۴	وقت کار است: رمزگشایی بسته‌های WEP و WPA
۱۱۵	چه اتفاقی افتاد؟
۱۱۶	وصل شدن به شبکه‌های WEP و WPA
۱۱۶	وقت کار است: وصل شدن به شبکه WEP
۱۱۶	چه اتفاقی افتاد؟
۱۱۶	وقت کار است: وصل شدن به شبکه WPA
۱۱۸	چه اتفاقی افتاد؟
۱۱۸	سوالات: معایب رمزگذاری در شبکه‌های بی‌سیم
۱۱۸	خلاصه فصل
۱۱۹	دستورات کدهای مورد استفاده در فصل چهارم

فصل پنجم: حمله روی زیرساخت شبکه‌های بی‌سیم

۱۲۲	حساب‌های کاربری: اعتبارنامه‌های پیش‌فرض اکسس پوینت
۱۲۲	وقت کار است: شکستن حساب‌های پیش‌فرض روی اکسس پوینت
۱۲۳	چه اتفاقی افتاد؟
۱۲۳	شما هم امتحان کنید: شکستن حساب‌های کاربری با استفاده از حمله Bruteforce
۱۲۳	حمله منع سرویس‌دهی
۱۲۴	وقت کار است: حمله لغو احراز هویت
۱۲۷	چه اتفاقی افتاد؟
۱۲۷	شما هم امتحان کنید: حمله قطع اتصال از شبکه
۱۲۷	دوقلوی شیطانی و جعل آدرس مک
۱۲۸	وقت کار است: دوقلوی شیطانی با جعل آدرس MAC
۱۳۱	چه اتفاقی افتاد؟
۱۳۱	شما هم امتحان کنید: دوقلوی شیطانی و پرش کانال
۱۳۱	اکسس پوینت غیرمجاز
۱۳۲	وقت کار است: اکسس پوینت غیرمجاز
۱۳۵	چه اتفاقی افتاد؟
۱۳۵	شما هم امتحان کنید: چالش اکسس پوینت غیرمجاز
۱۳۵	سوالات: حمله روی زیرساخت شبکه‌های بی‌سیم
۱۳۶	خلاصه فصل
۱۳۶	اکسس پوینت غیرمجاز در شبکه
۱۳۶	دستورات و کدهای مورد استفاده در فصل پنجم

فصل ششم: حمله به کلاینت ۱۳۹

- ۱۴۰ حمله‌های Honeypot و Mis-Association
- ۱۴۰ وقت کار است: سازمان‌دهی یک حمله اتصال اشتباه
- ۱۴۵ چه اتفاقی افتاد؟
- ۱۴۵ شما هم امتحان کنید: وادار کردن کلاینت به وصل شدن به Honeypot
- ۱۴۵ حمله CafeLatte
- ۱۴۶ وقت کار است: حمله Cafe Latte
- ۱۴۹ چه اتفاقی افتاد؟
- ۱۵۰ شما هم امتحان کنید: تمرین کردن شما را موفق می‌کند
- ۱۵۰ حمله‌های لغز احراز هویت و قطع اتصال از شبکه
- ۱۵۰ وقت کار است: لغز احراز هویت از سمت کلاینت
- ۱۵۳ چه اتفاقی افتاد؟
- ۱۵۴ حمله Hirte
- ۱۵۴ وقت کار است: شستن WPA با استفاده از حمله Hirte
- ۱۵۶ چه اتفاقی افتاد؟
- ۱۵۶ شما هم امتحان کنید: تمرین کنید
- ۱۵۶ شکستن WPA-Personal بدون اکسپوینت
- ۱۵۷ وقت کار است: شکستن WPA بدون اکسپوینت
- ۱۵۹ چه اتفاقی افتاد؟
- ۱۵۹ شما هم امتحان کنید: شکستن WPA بدون اکسپوینت
- ۱۵۹ سوالات: حمله به کلاینت
- ۱۶۰ خلاصه فصل
- ۱۶۱ دستورات و کدهای مورد استفاده در فصل ششم

فصل هفتم: حمله‌های پیشرفته در شبکه‌های بی‌سیم ۱۶۳

- ۱۶۴ حمله واسط میانی MITM
- ۱۶۴ وقت کار است: حمله واسط میانی
- ۱۶۸ چه اتفاقی افتاد؟
- ۱۶۸ شما هم امتحان کنید: حمله واسط میانی روی شبکه بی‌سیم
- ۱۶۹ استراق سمع بی‌سیم با استفاده از MITM
- ۱۷۳ چه اتفاقی افتاد؟
- ۱۷۴ شما هم امتحان کنید: پیدا کردن جستجوهای گوگل
- ۱۷۴ ربودن ارتباط و جلسه روی شبکه بی‌سیم
- ۱۷۴ وقت کار است: ربودن ارتباط و جلسه روی شبکه بی‌سیم

۱۷۷.....	چه اتفاقی افتاد؟
۱۷۸.....	شما هم امتحان کنید: چالش ربودن لایه کاربرد
۱۷۸.....	پیدا کردن تنظیمات امنیتی روی کامپیوتر کلاینت
۱۷۸.....	وقت کار است: لیست گرفتن از پروفایل های امنیتی
۱۸۱.....	چه اتفاقی افتاد؟
۱۸۱.....	شما هم امتحان کنید: تله گذاشتن برای کلاینت
۱۸۲.....	سوالات: حمله های پیشرفته در شبکه های بی سیم
۱۸۳.....	خلاصه فصل
۱۸۳.....	دستورات و کدهای مورد استفاده در فصل هفتم

فصل هشتم: حمله به RADIUS و WPA-ENTERPRISE ۱۸۵

۱۸۶.....	تنظیمات WPA FreeRadius
۱۸۶.....	وقت کار است: تنظیمات AP با FreeRadius-WPE
۱۹۰.....	چه اتفاقی افتاد؟
۱۹۰.....	شما هم امتحان کنید: بازی با RADIUS
۱۹۰.....	حمله به PEAP
۱۹۰.....	وقت کار است: شکستن PEAP
۱۹۴.....	چه اتفاقی افتاد؟
۱۹۵.....	شما هم امتحان کنید: حمله های مختلف روی PEAP
۱۹۵.....	حمله به EAP-TTLS
۱۹۵.....	وقت کار است: حمله به EAP-TTLS
۱۹۷.....	چه اتفاقی افتاد؟
۱۹۷.....	شما هم امتحان کنید: EAP-TTLS
۱۹۷.....	بهترین نوع امنیت برای شرکت ها
۱۹۸.....	سوالات: حمله به WPA-Enterprise و RADIUS
۱۹۹.....	خلاصه فصل
۱۹۹.....	دستورات و کدهای مورد استفاده در فصل هشتم

فصل نهم: شناسایی روش تست نفوذ به شبکه های بی سیم ۲۰۱

۲۰۱.....	تست نفوذ شبکه بی سیم
۲۰۲.....	فاز برنامه ریزی
۲۰۳.....	فاز اکتشاف
۲۰۳.....	وقت کار است: کشف دستگاه های بی سیم
۲۰۵.....	چه اتفاقی افتاد؟
۲۰۵.....	فاز حمله

- ۲۰۵..... پیدا کردن نقاط دسترسی غیرمجاز
- ۲۰۶..... وقت کار است: پیدا کردن اکسس پوینت غیرمجاز
- ۲۰۷..... چه اتفاقی افتاد؟
- ۲۰۷..... پیدا کردن کلاینت‌های غیرمجاز
- ۲۰۷..... وقت کار است: کلاینت‌های غیرمجاز
- ۲۰۸..... چه اتفاقی افتاد؟
- ۲۰۸..... شکستن رمزگذاری
- ۲۰۹..... وقت کار است: شکستن WPA
- ۲۱۱..... چه اتفاقی افتاد؟
- ۲۱۱..... هک کردن کلاینت‌ها
- ۲۱۱..... وقت کار است: هک کردن کلاینت‌ها
- ۲۱۲..... چه اتفاقی افتاد؟
- ۲۱۳..... فاز گزارش
- ۲۱۳..... سوالات: تست خود شبکه
- ۲۱۴..... خلاصه فصل
- ۲۱۴..... دستورات و کدهای مورد نیاز برای فصل نهم

خط مشی کیفیت انتشارات مؤسسه فرهنگی دیباگران تهران در عرصه کتاب الکترونیک است که بتواند خواره‌های 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.

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 راست‌ترین دسترسی به اطلاعات و اطلاع‌رسانی، بیش از پیش روشن می‌نماید. در این راستا، واحد انتشارات مؤسسه فرهنگی 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 و دایم برافراشته، رفع کمبودها و نیازهای موجود، منابعی پربار، معتبر و با کیفیت مناسب در اختیار علاقمندان قرار دهند.

کتابی که در دست دارید با همت "آقای مهندس رضا مقدم، سرکار خانم مهندس فرزانه فرخی" و تلاش جمعی از همکاران انتشارات میسر گشته که شاید علت انتخاب از یکایک این گرامیان تشکر و قدردانی کنیم.

کارشناسی و نظارت بر محتوا: زهره قزلباش

در خانمه ضمن سپاسگزاری از شما دانش‌پژوه گرامی درخواست می‌نماید تا 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 مترجم

امروزه شبکه‌های بی‌سیم در همه جهان رایج شده است. هر روز میلیون‌ها نفر از سراسر جهان در خانه‌ها، دفاتر کار و مکان‌های عمومی از آن استفاده می‌کنند تا برای انجام کارهای شخصی و حرفه‌ای خود به اینترنت وصل شوند. با وجود این که فناوری بی‌سیم زندگی را بسیار ساده‌تر کرده است و به ما اجازه جابه‌جایی می‌دهد، خطراتی را هم به همراه دارد. در سال‌های اخیر شبکه‌های بی‌سیم ناامن روی سیستم‌های شرکت‌ها، بانک‌ها و سازمان‌های دولتی، مورد سوء استفاده افرادی قرار می‌گیرد که قصد ورود به سیستم‌ها و دسترسی غیرمجاز به اطلاعات را دارند. به تازگی میزان این حمله‌ها رو به افزایش است و بسیاری از مدیران شبکه‌ها هنوز نمی‌دانند چگونه شبکه‌های خود را قابل اطمینان، امن و غیرقابل نفوذ کنند.

این کتاب قصه دارد به خواننده کمک کند تا بتواند نقاط ضعف شبکه بی‌سیم را بشناسد، آزمون نفوذپذیری را روی شبکه انجام دهد و در پایان نقاط ضعف به دست آمده را رفع کند. خواندن این کتاب برای کسانی که می‌خواهند روی شبکه‌های بی‌سیم، سنجش امنیتی انجام دهند و خود را نیازمند یک راهنمای قدم به قدم به قدم به قدم می‌داند ضروری است، زیرا هر کدام از حمله‌های بی‌سیم شرح داده شده در کتاب، یک مثال کاربردی به دنبال دارد. یادگیری به صورت کامل انجام می‌شود.

ما Kali را به عنوان بستر نرم‌افزاری برای تست همه حمله‌های این کتاب انتخاب کرده‌ایم؛ زیرا Kali که احتمالاً بسیاری از شما با آن آشنایی دارید، محبوب‌ترین توزیع¹ تست و آزمایش شبکه بی‌سیم در دنیاست. Kali شامل صدها ابزار هک و ابزار امنیتی است که برخی از آن‌ها را در این کتاب مورد استفاده قرار خواهیم داد.

پیشنهاد می‌شود برای آزمایش نفوذ شبکه‌های کامپیوتری خود در کتاب آزمون نفوذپذیری پیشرفته در شبکه‌های بسیار ایمن و کتاب آشنایی با Kali و پیاده‌سازی آزمایشگاه تست نفوذ را تهیه و از محتویات آموزشی آن‌ها استفاده کنید.

لازم به ذکر است تمامی تست‌ها و آزمایش‌ها قابلیت اجرا در سیستم عامل Kali و Backtrack را دارا می‌باشد.

تقدیم به همسر عزیزم که همواره مشوق و پشتیبانم بوده است.

رضا مقدم

R.Moghadam@Hotmail.com

www.IPEXPerts.ir

آنچه در این کتاب بی‌آموزید

فصل اول، آماده‌سازی آزمایشگاه بی‌سیم: این فصل شما را با ده‌ها تمرینی که در این کتاب می‌خوانید، آشنا می‌کند. خواننده برای انجام این تمرین‌ها باید آزمایشگاه شخصی بی‌سیم برپا کند. تمرکز این فصل روی آموزش چگونگی ساخت یک آزمایشگاه تست شبکه بی‌سیم با استفاده از سخت‌افزارهای موجود در بازار و نرم‌افزارهای متن باز است. در ابتدا، ابزارهای مورد نیاز شامل کارت شبکه، آنتن، اکسس پوینت و سایر دستگاه‌های مربوط به فناوری Wi-Fi¹ آشنا می‌شویم. سپس روی نرم‌افزارهای مورد نیاز تمرکز می‌کنیم که شامل سیستم‌عامل، درایورهای Wi-Fi، ابزارهای امنیتی هستند. با رعایت همه این موارد بستری مناسب برای تست و انجام آزمایش‌ها و پیاده‌سازی انواع تنظیمات و **پیرس**² ایجاد می‌کنیم.

فصل دوم، شبکه‌های بی‌سیم و ریسک‌های ذاتی آن: هدف این فصل، تمرکز روی خطاهای طراحی ذاتی در شبکه‌های بی‌سیم است. خطاهایی که آن‌ها را از ابتدای شروع به کار ناامن می‌داند. با یک مرور کلی و سریع روی پروتکل‌های بی‌سیم 802.11 با استفاده از Wireshark³ شروع می‌کنیم. این کار باعث می‌شود درک عمیقی از عملکرد این پروتکل‌ها پیدا کنید. مهم‌تر از همه، می‌بینیم که رابطه بین اکسس پوینت بی‌سیم و کامپیوتر کاربر در سطح بسته‌های اطلاعاتی چگونه است و برای این کار فریم‌های مدیریت، کنترل و دیتا را آنالیز می‌کنیم. در مرحله بعد معنی **تزریق بسته**² و **شنود بسته**³ در شبکه‌های بی‌سیم را یاد می‌گیریم و نگاهی به ابزارهای انجام این دو کار می‌اندازیم.

1. Wireless

2. Packet Injection

3. Packet Sniffing

فصل سوم، عبور از احراز هویت شبکه‌های بی‌سیم: شکست دادن مکانیسم احراز هویت در شبکه‌های بی‌سیم را بررسی می‌کند. قدم به قدم عبور از احراز هویت در روش‌های **کلید اشتراکی**^۱ یا باز را به شما نشان می‌دهیم و با این کار شما چگونگی تحلیل بسته‌های بی‌سیم و نحوه تشخیص مکانیسم احراز هویت را می‌آموزید. همچنین یاد می‌گیرید چگونه وارد شبکه‌هایی با SSID مخفی یا دارای فیلترکننده آدرس مک شوید. فعال کردن ویژگی مک فیلترینگ و مخفی کردن SSID دو شیوه رایج در بین مدیران شبکه‌های بی‌سیم برای بالا بردن امنیت و پایین آوردن احتمال نفوذ به شبکه است که متأسفانه به راحتی قابل دور زدن هستند.

فصل چهارم، معایب رمزگذاری شبکه‌های بی‌سیم: این فصل به یکی از آسیب‌پذیرترین قسمت‌های پروتکل شبکه‌های بی‌سیم یعنی الگوهای رمزگذاری^۲ (WPA، WEP و WPA2) می‌پردازد. طی دهه گذشته هکرها ایرادات^۳ این الگوها یافته و در قالب نرم‌افزار ارائه کرده‌اند تا برای دستیابی به اطلاعات و رمزگشایی^۴ مورد استفاده قرار گیرند. با وجود این که WPA و WPA2 طراحی قابل اطمینانی دارند، تنظیمات نادرست آن‌ها را آسیب‌پذیر می‌کند و این گونه سهل‌انگاری‌ها می‌توانند به سادگی مورد سوءاستفاده هکرها قرار گیرند. در این فصل به بررسی نقاط ضعف در هر یک از این الگوهای رمزگذاری می‌پردازیم و مثال‌هایی از شیوه‌های دسترسی غیرمجاز^۵ ارائه می‌کنیم.

فصل پنجم، حمله به زیرساخت شبکه‌های بی‌سیم: در این فصل روی نقاط ضعف زیرساخت شبکه‌های بی‌سیم تمرکز می‌کنیم. نگاهی به مشکلات زیربنایی و همچنین تنظیمات خواهیم داشت و مثال‌هایی عملی از حمله به اکسس پوینت به روش جعل آدرس مک^۶ دست‌کاری بیت^۷، حمله ارسال مجدد^۸، اکسس پوینت غیرمجاز^۹، فایزینگ و منع سرویس دهی^{۱۰} ارائه خواهیم کرد. این فصل تست زیرساخت شبکه‌های بی‌سیم را به خواننده می‌آموزد.

فصل ششم، حمله به کلاینت: اگر تا به حال تصور می‌کردید که نگرانی از امنیت کلاینت در شبکه بی‌سیم وجود ندارد، این فصل چشمان شما را به مسائل جدیدی باز خواهد کرد. اکثر افراد، کلاینت را از لیست مشکلات امنیتی شبکه‌های بی‌سیم حذف می‌کنند، بدون شک این دلیل به شما ثابت می‌کند که هنگام انجام تست نفوذ کامپیوتر سرویس‌گیرنده هم به اندازه اکسس پوینت مهم است. در این فصل

1. Shared Key

2. Encryption

3. Decryption

4. Mac Spoof

5. Bit Flip

6. Replay Attack

7. Rogue Access Point

8. Denial of Service

یاد می‌گیریم که چگونه از طریق حمله‌های سمت کلاینت امنیت شبکه را مورد آزمایش قرار دهیم. حمله‌هایی مثل **اتصال اشتباه**^۱، CafeLatte، رد اتصال، اتصال‌های ad-hoc، فایزینگ، هانی پات و بسیاری دیگر.

فصل هفتم، حمله‌های پیشرفته شبکه‌های بی‌سیم: این فصل، حمله‌های پیشرفته‌تر از فصل‌های قبل را بررسی می‌کند. حمله‌های روی زیرساخت‌های شبکه و کلاینت. این حمله‌ها معمولاً شامل استفاده از چندین حمله ابتدایی همزمان برای شکستن سد امنیتی در سناریوهای چالشی و پیچیده می‌شود. بعضی از این حمله‌ها شامل **ذخیره اثر انگشت**^۲، **حمله واسط میانی**^۳ بی‌سیم، فرار از تشخیص نفوذ و سیستم‌های پد خیر، کسب پوینت غیرمجاز با پروتکل‌های تغییر یافته و چند حمله دیگر هستند. این فصل جدیدترین حمله‌های بی‌سیم دنیا را ارائه می‌کند.

فصل هشتم، حمله به WPA Enterprise و RADIUS: دانش کاربر را به سطح بالاتری از مراحل حمله به شبکه بی‌سیم ارتقا می‌دهد. این حمله‌ها زمانی که کاربر باید تست نفوذ را روی شبکه‌های بزرگ تجاری انجام دهد، کاربرد دارد که برای حفظ امنیت به احراز هویت WPA Enterprise و RADIUS^۴ تکیه می‌کند. این احتمالاً پیشرفته‌ترین حمله ممکن در Wi-Fi است.

فصل نهم، شناسایی روش تست نفوذ بی‌سیم: در این فصل همه آنچه از فصل‌های قبل آموخته‌اید جمع‌آوری می‌شود و شیوه سیستماتیک و جاسج شده، نفوذ، بررسی و جمع‌بندی می‌شود. فازهای مختلف تست نفوذ (برنامه‌ریزی، کشف، حمله و گزارش) را می‌آموزیم و از آن برای تست نفوذ استفاده خواهیم کرد و همچنین می‌آموزیم بعد از انجام آزمایش‌ها چه پیشنهادهایی برای بهبود آن ارائه کنیم.

ابزارهای مورد نیاز برای تمرین‌های کتاب

برای دنبال کردن و انجام تمرین‌های عملی این کتاب به دو لپ‌تاپ دارای کارت شبکه بی‌سیم، یک آداپتور بی‌سیم‌آلفا مدل AWUS036H، Kali نسخه 5 و چند نرم‌افزار و سخت‌افزار دیگر نیاز دارید. این موارد را با جزئیات کامل در فصول، آماده‌سازی آزمایشگاه بی‌سیم، توضیح داده‌ایم.

به عنوان جایگزینی برای دو لپ‌تاپ می‌توانید یک ماشین مجازی ایجاد کرده و Kali را روی آن نصب کنید و کارت را از طریق USB به آن وصل کنید. به این شکل می‌توانید کار با کتاب را سریع‌تر شروع

1. Mis-Association
2. Device Fingerprinting
3. Man In The Middle Attack
4. Remote Access Dial In User Service

کنید؛ اما به شما پیشنهاد می‌کنیم در آینده برای تست نفوذ در شبکه‌های واقعی از یک کامپیوتر مختص این کار که Kali روی آن نصب‌شده استفاده کنید.

به عنوان پیش‌نیاز، خوانندگان باید با بحث‌های مقدماتی شبکه Wirelees آشنایی داشته باشند. این مقدمات شامل آشنایی با پروتکل 802.11 و ارتباط بین کلاینت و اکسس پوینت است. با این‌که در طول فصل اول بعضی از این مسائل را به طور کلی بیان خواهیم کرد، بهتر است خواننده از قبل اطلاعاتی در مورد شبکه بی‌سیم داشته باشد.

این کتاب برای چه کسانی مناسب است؟

با وجود این‌که این کتاب جزء کتاب‌های سطح مبتدی طبقه‌بندی شده است، برای همه نوع کاربری قابل استفاده است. افراد غیرحرفه‌ای و کارشناسان امنیت بی‌سیم، می‌توانند از این کتاب استفاده کنند چون با حمله‌های ساده آشنایی می‌شود و به مسائل پیچیده‌تر می‌رسد و در پایان تحقیق‌ها و حمله‌های جدید را بررسی می‌کند. حمله‌ها با مثال‌های عملی توضیح داده شده‌اند و کار یادگیری را برای خواننده‌ها ساده‌تر کرده‌اند. البته کتاب با وجود این‌که کتاب، حمله‌های مختلف به شبکه بی‌سیم را شرح می‌دهد اما هدف واقعی، آموزش کاربران برای تبدیل شدن به کارشناس تست نفوذ شبکه بی‌سیم است. یک کارشناس تست نفوذ خبره با همه حمله‌های ممکن آشنایی دارد و در صورت تمایل مشتری می‌تواند آن‌ها را به راحتی اجرا کند.

قراردادها

در ادامه کتاب، عنوان‌هایی هستند که تکرار می‌شوند. برای نشان دادن دستورالعمل انجام دقیق کارهای مختلف از تیتیر «وقت کار است: عنوان» استفاده می‌کنیم. در صورتی‌که بعد از انجام دستورالعمل‌ها نیاز به توضیح اضافی باشد از تیتیر «چه اتفاقی افتاد؟» استفاده می‌شود. همچنین برای کاربرانی که تمایل دارند مطالعه دقیق‌تر و بیشتری داشته باشند از قسمت‌های مخصوصی با عنوان «سوالات: عنوان» و «شما هم امتحان کنید: عنوان» استفاده می‌کنیم.