به نام خدا

مؤسسه فرهنگی هنری
دیباگران 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

مولف : Vivek Ramachandran

مترجمان : مهندس رضا مقدم

مهندس فرزانه فرخی

ناشر: مؤسسه فرهنگی هنری دیباگران تهران

حروفچینی و صفحه آرایی: مؤسسه فرهنگی هنری دیباگران تهران

طرح روی جلد: مجید [illegible] بازی

چاپ: نگین

نوبت چاپ: اول

تاریخ نشر: ۱۳۹۵

تیراژ:۳۰۰ جلد

قیمت:۲۳۰۰۰۰ ریال

سرشناسه: راماچاندارن-ویوک

عنوان و نام پدید آور :ارزیابی نفوذپذیری در شبکه های بی سیم /ویژه ...مولف: ویوک راما چاندارن؛مترجمان :رضا مقدم- فرزانه فرخی

مشخصات نشر: تهران- دیباگران تهران -۱۳۹۵

مشخصات ظاهری: ۲۱۶ ص – مصور

شابک: ۹۷۸-۶۰۰-۱۲۴-۴۳۱-۵

وضعیت فهرست نویسی: فیپا

یادداشت: عنوان اصلی: Backtrack5 wireless penetration testing :beginner's guide

یادداشت: کتاب حاضر ... عنوان "تست نفوذپذیری شبکه های بی سیم با back track5 راهنمای مبتدی ها " با ترجمه ی سید عنایت الله موسوی-احسان محمد زاده توسط انتشارات پندار پارس در ۱۳۹۳ منتشر شده است.

عنوان دیگر :تست نفوذپذیری شبکه های بی سیم با back track5 راهنمای مبتدی ها.

موضوع :ارتباطات بی سیم-ایمنی سیستم ها

موضوع :wireless communication systems-security measures-handbooks-manuals-etc

موضوع :آزمایش نفوذ (ایمن سازی کامپیوتر)

موضوع :penetration testing (computer security)

شناسه افزوده:مقدم-رضا-۱۳۶۹-مترجم

شناسه افزوده فرخی فرزانه -۱۳۶۵ مترجم

رده بندی کنگره: ۱۳۹۵ ۵ ت ۲ ر ۲/ ۵۱۰۳ TK

رده بندی دیویی : ۰۰۵/۸

شماره کتابشناسی ملی: ۴۲۸۲۳۲۴

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

تلفن: ۱۲-۶۶۴۱۰۰۴۶-۲۲۰۸۵۱۱۱ کد پستی: ۱۳۱۴۹۸۳۱۸۵

پست الکترونیکی: **bookmarket@mftmail.com** فروش اینترنتی: **www.mftshop.com**

www.mftbook.ir

فهرست مطالب

مقدمه ناشر

خط مشی کیفیت انتشارات مؤسسه فرهنگی هنری دیباگران تهران در عرصه کتاب‌هایی 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، مؤثر واقع شویم.

گستردگی 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 راحت‌ترین 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 پُربار، معتبر و با کیفیت مناسب در اختیار علاقمندان قرار دهند.

کتابی که در دست دارید با همت **"آقای مهندس رضا مقدم"** و **سرکار خانم مهندس فرزانه فرخی"** 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 می‌نماید 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 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 این‌که 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 قصد دارد به خواننده کمک کند تا بتواند نقاط ضعف شبکه بی‌سیم را بشناسد، آزمون نفوذپذیری را روی شبکه انجام دهد و درپایان نقاط ضعف به‌دست 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 می‌دانند ضروری است، زیرا هرکدام از حمله‌های بی‌سیم شرح داده‌شده در کتاب، یک مثال کاربردی به دنبال خود دارد و 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 **توزیع**[1] 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، 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 Backtrack و Kali را دارا می‌باشد.

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

رضا مقدم

R.Moghadam@Hotmail.com

www. IPExPerts.ir

1. Distribution

پیشگفتار

آنچه در این کتاب می‌آموزید

فصل اول، آماده‌سازی آزمایشگاه می‌دهیم: 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 سخت‌افزارهای مورد نیاز شامل کارت شبکه، آنتن، **اکسس پوینت** و سایر دستگاه‌های مربوط به فناوری **Wi-Fi** آشنا می‌شویم. سپس روی نرم‌افزارهای مورد نیاز تمرکز می‌کنیم که شامل سیستم‌عامل، درایورهای Wi-Fi و ابزارهای امنیتی هستند. با رعایت همه این موارد بستری مناسب برای تست و انجام آزمایش‌ها و پیاده‌سازی انواع تنظیمات ***وایرلس***[1] 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 می‌کند. با یک مرور کلی و سریع روی پروتکل‌های بی‌سیم 802.11 با استفاده از **Wireshark** 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***[1] 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***[2] (WEP، WPA و WPA2) می‌پردازد. طی دهه گذشته هکرها ایراداتی در این الگوها یافته و در قالب نرم‌افزار ارائه کرده‌اند تا برای دستیابی به اطلاعات و ***رمزگشایی***[3] مورد استفاده قرار گیرند. با وجود این‌که WPA و WPA2 طراحی قابل اطمینانی دارند، تنظیمات نادرست آن‌ها را آسیب‌پذیر می‌کند و این‌گونه 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 شیوه شکستن آن‌ها ارائه می‌کنیم.

فصل پنجم، حمله به زیرساخت شبکه‌های بی‌سیم: در این فصل روی نقاط ضعف زیرساخت شبکه‌های بی‌سیم تمرکز می‌کنیم. نگاهی به مشکلات زیرساختی و همچنین تنظیمات خواهیم داشت و مثال‌هایی عملی از حمله به **اکسس پوینت** به روش جعل ***آدرس مک***[4]، ***دست‌کاری بیت***[5]، ***حمله ارسال مجدد***[6]، ***اکسس پوینت غیرمجاز***[7]، ***فازینگ*** و ***منع سرویس‌دهی***[8] 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 نظر 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 فصل 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***[1]، CafeLatte، رد اتصال، اتصال‌های ad-hoc، فازینگ، 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***[2]، ***حمله واسط میانی***[3] بی‌سیم، فرار از تشخیص نفوذ و سیستم‌های پیشگیری، اکسس پوینت غیرمجاز با پروتکل‌های تغییریافته 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***[4] 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 جامع تست 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 آزمایش شبکه 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 فصل‌اول، 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 طورکلی 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 آغاز 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. توصیه کنیم 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 به‌راحتی اجرا کند.

قراردادها

در ادامه کتاب، عنوان‌هایی هستند که تکرار می‌شوند. برای نوشتن دستورالعمل انجام دقیق کارهای مختلف از تیتر «وقت کار است: عنوان» استفاده می‌کنیم. در صورتی که بعد از انجام دستورالعمل‌ها نیاز به توضیح اضافی باشد از تیتر «چه اتفاقی افتاد؟» استفاده می‌شود.

همچنین برای کاربرانی که تمایل دارند مطالعه دقیق‌تر و بیشتری داشته باشند از قسمت‌های مخصوصی با عنوان «سؤالات: عنوان» و «شما هم امتحان کنید:عنوان» استفاده می‌کنیم.