تست نفوذپذیری شبکه‌های بی‌سیم با

BACK TRACK 5

راهنمای مبتدی‌ها

ویوک راماچاندران

ترجمه:
دکترسید عنایت‌اله علوی
مهندس احسان محمدزاده

انتشارات پندار پارس

سرشناسه : راماچاندران، ویوک
Vivek ,Ramachandran
عنوان و نام پدیدآور : تست نفوذپذیری شبکه‌های بی‌سیم با BackTrack5 (راهنمای مبتدی‌ها)/ ویوک راماچاندران؛ ترجمه سیدعنایت اله علوی، احسان محمدزاده.
مشخصات نشر : تهران : پندار پارس ، ۱۳۹۲.
مشخصات ظاهری : ۱۸۴ ص.
شابک : 978-600-6529-59-2
وضعیت فهرست نویسی : فیپا
یادداشت : عنوان اصلی: Backtrack 5 wireless penetration testing: beginner's guide ,2011
موضوع : ارتباطات بی‌سیم -- تدابیر ایمنی-- دستنامه‌ها
موضوع : آزمایش نفوذ (ایمن‌سازی کامپیوتر)
شناسه افزوده : علوی، عنایت‌اله، ۱۳۴۶ -، مترجم
شناسه افزوده : محمدزاده، احسان، ۱۳۶۰ -، مترجم
رده بندی کنگره : ۱۳۹۲/۵۱۰۳TK /ر۲ت۵
رده بندی دیویی : ۸/۰۰۵
شماره کتابشناسی ملی : ۳۴۶۴۲۵۶

انتشارات پندارپارس

دفتر فروش: انقلاب، ابتدای کارگرجنوبی، کوچه [illegible]، شماره ۱۴، واحد ۱۶ www.pendarepars.com

تلفن: ۶۶۵۷۲۳۳۵ - تلفکس: ۶۶۹۲۶۵۷۸ همراه: ۰۹۱۲۲۳۲۳۴۸ info@pendarepars.com

نام کتاب : تست نفوذپذیری شبکه‌های بی‌سیم با Back Track

ناشر : انتشارات پندار پارس

تألیف : ویوک راماچاندران

ترجمه : سید عنایت‌اله علوی، احسان محمدزاده

چاپ نخست : اردیبهشت ۹۳

شمارگان : ۵۰۰ نسخه

لیتوگرافی : ترام‌سنج

چاپ، صحافی : فرشیوه، خیام

قیمت : ۱۳۰۰۰ تومان

شابک : ۹۷۸-۶۰۰-۶۵۲۹-۵۹-۲

فهرست

درباره‌ی نویسنده

وی‌وک راماچاندران[1] از سال ۲۰۰۳ روی امنیت وای‌فای کار کرده است. او حمله‌ی کافه‌لاته[2] را کشف کرد و همچن
WEP Cloaking را شکست، که یک الگوی حفاظتی عام WEP در سال ۲۰۰۷ در اجلاس Defcon است. وی‌وک
سال ۲۰۱۱، برای نخستین با ر نشان داد که نرم‌افزارهای مخرب چگونه از وای‌فای برای ساختن راه‌های پنهان
کرم‌ها و حتی بات‌نت[4]ها استفاده می‌کنند.

در اوایل او یکی از برنامه‌نویسان پروتکل 802.1x و امنیت درگاه[5] در سوئیچ‌های ۶۵۰۰ سری Catalyst سیسکو
همچنین یکی از برندگان مسابقه‌ی امنیتی ماکروسافت بود که در هند و در میان ۶۵۰۰۰ شرکت‌کننده برگزار شد. او
عنوان بنیانگذار سایت http://www.SecurityTube. net در جامعه‌ی هکرها شناخته شده است، جایی که به
معمول ویدئوهایی روی امنیت وای‌فای، زبان اسمبلی، فن‌های بهره‌برداری و غیره ارائه می‌شود. سا
SecurityTube.net ماهانه بیش از ۱۰۰۰۰۰ بازدیدکننده‌ی پروپاقرص دارد.

کار وی‌وک در زمینه‌ی امنیت شبکه‌های بی‌سیم در بی‌بی‌سی آنلاین، Info World، Mac World، The Register،
World Canada و ... مورد توجه قرار گرفته و درباره‌ی او صحبت شده است. امسال او در شماری از اجلاس‌های امنی
سخنرانی نموده و آموزش می‌دهد. این اجلاس‌ها شامل BlackHat، Defcon، Hacktivity، 44con، HITB-ML، rucon
Derbycon، HashDays، SecurityZone، SecurityByte و غیره هستند.

می‌خواهم از همسر دوست‌داشتنی‌ام برای تمام کمک‌ها و پشتیبانی‌هایش در طول نوشتن این کتاب تشکر کنم. و همچنین از پدر و مادرم، پدربزرگ و مادربزرگم و خواهرم برای اینکه مرا در طول این سال‌ها باور نموده و مشوق من بوده‌اند و در آخر، می‌خواهم از تمام کاربران سایت SecurityTube.net تشکر کنم که همیشه در کنار من بوده و حمایت خود را نسبت به کارهای من نشان داده‌اند. شما بچه‌ها خیلی با حالید!

Vivek Ramachandran
Caffe Latte
backdoors
botnet
port

درباره‌ی ویراستار

دانیل.و.دایترل[1] بیش از ۲۰ سال در زمینه فن‌آوری اطلاعات تجربه دارد. او سطوح گوناگون پشتیبانی را برای سرویس‌گیرنده‌ها، از مشاغل کوچک گرفته تا کمپانی‌های ثروتمند مهیا کرده است. دانیل از امنیت رایانه لذت می‌برد. وب‌نوشت امنیتی CyberArms (http://cyberarms.wordpress.com/) را راه‌اندازی نموده و در سایت https://Infosecisland.com/ به عنوان امنیت نویس مهمان حضور دارد.

می‌خواهم از همسر و بچه‌های زیبایم تشکر کنم که با از خود گذشتگی، زمان مورد نیاز برای پیشبرد این کتاب را به من دادند. بدون از خود گذشتگی آن‌ها، قادر نبودم بخشی از این پروژه‌ی هیجان‌انگیز باشم.

---

[1] Daniel W Dieterle

پیش‌گفتار

شبکه‌های بی‌سیم در جهان امروز در همه جا حاضر هستند. میلیون‌ها نفر از مردم در سرتاسر جهان هر روز در خانه، ادارات و مکان‌های عمومی، برای ورود به اینترنت و برای انجام کار شخصی و حرفه‌ای خود، از این شبکه‌ها استفاده می‌کنند. اگرچه بی‌سیم باعث می‌شود که زندگی فوق‌العاده آسان شود و به ما قدرت تحرک بالایی می‌دهد، خطرهایی هم به همراه دارد. اخیرا شبکه‌های ناامن بی‌سیم برای ورود غیرمجاز به شرکت‌ها، بانک‌ها و سازمان‌های دولتی، مورد سوء استفاده قرارگرفته‌اند. بسامد این حملات شدیدتر شده است، درحالی‌که مدیران شبکه هنوز برای چگونگی ایمن‌سازی شبکه‌ی بی‌سیم به شکلی قوی و بدون اشتباه سردرگم هستند.

کتاب **بک‌ترک ۵ تست نفوذپذیری شبکه‌های بی‌سیم: راهنمای مبتدی‌ها** با هدف کمک به خواننده برای درک ناامنی‌های مرتبط به شبکه‌های بی‌سیم و چگونگی هدایت تست‌های نفوذ برای یافتن و جلوگیری از آن‌ها نوشته شده است. این کتاب برای کسانی که تمایل به بررسی‌های امنیتی شبکه‌های بی‌سیم دارند و همیشه خواستار راهنمایی عملی گام به گام بوده‌اند مناسب و ضروری است. از آنجایی که هر حمله‌ی بی‌سیم توضیح داده‌شده در این کتاب بی‌درنگ با یک نمونه‌ی نمایشی همراه شده است، یادگیری را بسیار کامل می‌کند.

ما در این کتاب **بک‌ترک ۵** را به عنوان یک ابزار برای تست تمام حملات بی‌سیم انتخاب کرده‌ایم. بک‌ترک، همان گونه که شاید با آن آشنا باشید، مشهورترین توزیع تست نفوذپذیری در دنیا است. بک‌ترک شامل صدها ابزار هک امنیت است که برخی از آن‌ها را در این کتاب بکار خواهیم برد.

این کتاب چه مطالبی را دربر می‌گیرد

فصل ۱، راه‌اندازی آزمایشگاه بی‌سیم، تمرینات زیادی را که در این کتاب انجام خواهیم داد معرفی می‌کند. به منظور تلاش برای اجرای آن‌ها، خواننده نیاز دارد که یک آزمایشگاه بی‌سیم راه‌اندازی کند. تمرکز این فصل روی چگونگی ساختن یک آزمایشگاه بی‌سیم با استفاده از سخت‌افزارهای در دسترس و نرم‌افزارهای منبع باز است. ما در آغاز روی سخت‌افزار مورد نیاز شامل کارت‌های بی‌سیم، آنتن‌ها، اکسس‌پوینت‌ها و دیگر تجهیزات با قابلیت وای‌فای[1] متمرکز می‌شویم، و سپس تمرکزمان را روی نرم‌افزار مورد نیاز شامل سیستم‌عامل، درایورهای کارت‌ها و ابزارهای امنیتی قرار می‌دهیم. در پایان، یک بستر آزمایشی برای آزمایش‌هایمان خواهیم ساخت و پیکربندی‌های گوناگون شبکه‌ی بی‌سیم را روی آن نشان خواهیم داد.

فصل ۲، شبکه‌ی محلی بی‌سیم[2] (WLAN) و ناامنی‌های ذاتی آن، روی معایب طراحی ذاتی در شبکه‌های بی‌سیم متمرکز می‌شود که این معایب منجر به ناامنی آن‌ها در هنگام استفاده می‌شود. در آغاز با استفاده از یک تحلیل‌گر شبکه به نام وایرشارک[3] نگاهی اجمالی به پروتکل‌های شبکه‌ی محلی بی‌سیم 802.11 خواهیم انداخت. این کار درک

---

1. Wi-Fi
2. Wireless Local Area Netwoke
3. Wireshark

عملی درباره‌ی چگونگی کارکرد این پروتکل‌ها را به ما می‌دهد. از همه مهم‌تر، با آنالیز فریم‌های مدیریت، کنترل
داده می‌بینیم که چگونه اکسس‌پوینت و سرویس‌گیرنده در سطح بستک[1] با هم ارتباط دارند. سپس درباره‌ی تزریق
شنود بستک در شبکه‌های بی‌سیم خواهیم آموخت و ابزارهایی را خواهیم دید که ما را قادر به انجام این کار می‌کنند

فصل ۳، دور زدن احراز هویت شبکه‌ی محلی بی‌سیم، درباره‌ی چگونگی شکستن مکانیزم احراز هویت شبکه‌ی مح
بی‌سیم صحبت می‌کند! ما قدم به قدم پیش خواهیم رفت و چگونگی بی‌اعتبار کردن احراز هویت‌های باز و ک
مشترک را بررسی خواهیم کرد. در این فصل، چگونگی آنالیز بستک‌های شبکه‌ی بی‌سیم و کشف مکانیزم احراز هو
شبکه را خواهید آموخت. همچنین نگاهی خواهیم انداخت به چگونگی ورود غیرمجاز به شبکه‌هایی با SSID پنهان
فیلترینگ. این‌ها دو مکانیزم مشهور هستند که توسط مدیران شبکه به‌کار گرفته می‌شوند تا نفوذ به شبکه‌های بی‌س
را مشکل کنند. به هر روی، این سازوکارها بسیار ساده دور زده می‌شوند.

فصل ۴، معایب رمزنگاری شبکه‌ی محلی بی‌سیم، یکی از آسیب‌پذیرترین بخش‌های پروتکل شبکه‌ی محلی بی‌سی
شرح می‌دهد. این بخش الگوریتم‌های رمزنگاری WEP، WPA و WPA2 است. در طول دهه‌ی گذشته، هکرها معا
فراوانی در این الگوها پیدا کرده‌اند و نرم‌افزارهایی را که به طور عمومی در دسترس باشد برای شکستن آن‌ها و رمزگش
داده، نوشته‌اند. اگرچه WPA/WPA2 طراحی امنی دارند، پیکربندی نادرست آن‌ها، راه را برای آسیب‌پذیری‌های امن
باز می‌کند و منجر به آسان شدن سوءاستفاده از آن‌ها می‌شود. در این فصل، ناامنی‌های موجود در هر یک از این الگ
را درک خواهیم کرد و نمونه‌های نمایشی عملی برای شکستن آن‌ها انجام خواهیم داد.

فصل ۵، حمله به زیربنای شبکه‌ی محلی بی‌سیم، ما را به آسیب‌های زیربنای شبکه‌ی محلی بی‌سیم آ
می‌دهد. در این فصل به آسیب‌های به وجود آمده توسط مشکلات پیکربندی و طراحی نگاهی خواهیم انداخ
همچنین نمونه‌های عملی حمله‌ها را انجام خواهیم داد. حملاتی مانند: جعل مک اکسس‌پوینت، تغییر بیت و حما
بازپخش، اکسس‌پوینت‌های متجاوز[2]، فازینگ و انکار سرویس. در این فصل به خواننده درکی قوی از چگونگی ان
تست نفوذپذیری زیربنای شبکه‌ی محلی بی‌سیم را می‌دهد.

فصل ۶، حمله به سرویس‌گیرنده، اگر همیشه بر این باور بوده‌اید که امنیت سرویس‌گیرنده‌ی بی‌سیم نگرانی برای
ایجاد نمی‌کند این فصل چشم و گوش شما را باز می‌کند! بیشتر کسانی که امنیت شبکه‌ی محلی بی‌سیم را مد نظر د
سرویس‌گیرنده را از لیست خود حذف می‌کنند. این فصل اثبات خواهد کرد که برخلاف تصور و گمان، در هنگام تـ
نفوذپذیری یک شبکه‌ی محلی بی‌سیم، سرویس‌گیرنده نیز به اندازه‌ی اکسس‌پوینت مهم است. ما نگاهی خوا
انداخت به چگونگی به خطر انداختن امنیت با استفاده از حمله به سرویس‌گیرنده مانند حملات: اتصال اشتباه
کافه‌لاته ، جداسازی[4]، اتصالات فی‌البداهه[5]، فازینگ[6]، هانی‌پات[7]ها و حملات دیگری از این دست.

---

1. cket
2. ue access points
3. -association
4. association
5. hoc connections
6. zing

پیش‌گفتار

فصل ۷، حملات پیشرفته‌ی شبکه‌ی محلی بی‌سیم، نگاهی به حملات پیشرفته‌تری می‌اندازد چرا که پیش از ا
بیشتر حملات ابتدایی به زیربنا و سر ویس‌گیرنده را پوشش داده‌ایم. این حملات معمولا شامل ترکیب پیوسته‌ای
حملات ابتدایی فراوان است و برای شکستن امنیت در سناریوهای چالش‌برانگیز بیشتری کاربرد دارد. برخی از حملا
که خواهیم آموخت شامل این موارد هستند: انگشت‌نگاری دستگاه بی‌سیم، مرد میانی[2] روی شبکه‌ی بی‌سیم، فرار
سیستم‌های تشخیص نفوذپذیری شبکه‌ی بی‌سیم و سیستم‌های پیشگیری، عامل اکسس‌پوینت متجاوز با استفاده
پروتکل مرسوم، و شماری دیگر. این فصل چیزی کاملا جدید را درباره‌ی حملات بی‌سیم در دنیای واقعی ارائه می‌د

فصل ۸، حمله به WPA–سازمانی و سرویس‌دهنده‌ی رادیوس[3]، با معرفی حملات پیشرفته به WPA–سازمانی
راه‌اندازی سرویس‌دهنده‌ی رادیوس به کاربر، او را به سطح بعدی سوق می‌دهد. این حملات زمانی کارایی خواه
داشت که نفوذکننده مجهز باشد تستی را روی شبکه‌های بزرگ اجرا کند که آن‌ها خود برای فراهم کردن امنیت، وابس
به احراز هویت WPA–سازمانی و رادیوس هستند. این حملات احتمالا به اندازه‌ی حملات وای‌فایی که می‌توان
دنیای واقعی انجام داد، پیشرفته‌اند.

فصل ۹، روش‌شناسی تست نفوذپذیری شبکه‌ی بی‌سیم، جایی است که تمام آموخته‌های فصل‌های پیشین در آنج
هم پیوند می‌خورند. همچنین چگونگی انجام یک تست بی‌سیم به طریق سامانمند و روشمند نگاهی خواه
انداخت. در این فصل فازهای گوناگون تست نفوذپذیری، از جمله: برنامه‌ریزی، کشف، حمله و گزارش را خواه
آموخت، و آن را در یک تست نفوذ اجرا خواهیم کرد. همچنین چگونگی ارائه‌ی پیشنهادها و بهترین عملکرد را پس
تست نفوذپذیری شبکه‌ی بی‌سیم خواهیم آموخت.

پیوست الف، کلام آخر و مسیر پیش رو، جمع‌بندی کتاب و راهنمایی کاربر با برخی از نشانه‌ها برای خواندن و پژوهش
بیشتر است.

آنچه برای خواندن این کتاب لازم است

برای دنبال کردن و دوباره‌سازی تمرینات عملی در این کتاب، به دو لپ‌تاپ، یک کارت وای‌فای، یک آداپتور بی‌س
وای‌فای نمونه آلفا AWUS036H USB، بک‌ترک ۵ و چند سخت‌افزار و نرم‌افزار دیگر نیاز دارید. این نیازمندی‌ها را
فصل ۱، راه‌اندازی آزمایشگاه بی‌سیم شرح خواهیم داد.

همچنین به عنوان جایگزینی برای راه‌اندازی دو لپ‌تاپ، می‌توانید یک ماشین مجازی برای بک‌ترک ۵ ساخته، و کار
را با واسط USB به آن وصل کنید. این کار به شما کمک می‌کند تا با سرعت بیشتری شروع به استفاده از این کتا
کنید، ولی پیشنهاد ما این است که از دستگاهی اختصاصی که بک‌ترک ۵ را اجرا می‌کند برای ارزیابی‌های واقعی
این باره استفاده کنید.

---

oneypot
nan-in-the-middle
adius
uthentication

به عنوان پیش‌نیاز، خوانندگان باید از اصول اولیه شبکه‌های بی‌سیم آگاه باشند. این آگاهی شامل دانش پیشین دربارد
اصول اولیه‌ی پروتکل 802.11 و ارتباطات سرویس‌گیرنده-اکسس‌پوینت است. اگر چه در هنگام راه‌اندازی آزمایشگ
به طور چکیده اشاره‌ای به برخی از این موارد خواهیم کرد، ولی انتظار می‌رود که کاربر پیشاپیش نسبت به این مفاه
آگاهی داشته باشد.

مخاطب این کتاب

اگرچه این کتاب مجموعه‌ای مبتدی است، اما برای تمام سطوح کاربران از غیرحرفه‌ای تا متخصصان امنیت شبکه
بی‌سیم برای تمام اقشار علاقمند مطلب دارد. این کتاب با حملات ساده شروع کرده و به سمت توضیح مو
پیچیده‌تری پیش می‌رود و در نهایت حملات یکتا و تحقیقات جدید را شرح می‌دهد. از آنجایی که تمام حملات
استفاده از مثال‌های [illegible] توضیح داده می‌شوند، خوانندگان در هر سطحی که باشند برایشان آسان است که به‌دس
خودشان و به سرعت این حملات را انجام دهند. لطفا توجه داشته باشید اگر چه این کتاب حملات گوناگونی را
می‌توان بر ضد شبکه‌ی بی‌سیم انداخت را مشخص می‌کند، هدف واقعی آن آموزش کاربر برای تبدیل شدن به ی
تست‌کننده‌ی نفوذپذیری بی‌سیم است تست‌کننده‌ای ماهر که تمام حملات را درک کرده و اگر سرویس‌گیرند
بخواهد، قادر است به آسانی آن را به انجام پیش بگذارد.

قراردادها

در این کتاب، عناوین گوناگونی را خواهید یافت که [illegible] چشم می‌خورند.

برای ارائه‌ی دستورکارهای روشنی از چگونگی تکمیل [illegible] رویه و یا کار، از موارد زیر استفاده می‌کنیم:

آغاز کار: "عنوان مطلب"

روند موضوع به‌صورت گام به گام، بررسی می‌شود.

دستورکارها اغلب به توضیحات بیشتری نیاز دارند تا محسوس باشند، بنابراین همراه می‌شوند با:

چه اتفاقی افتاد؟

این عنوان نحوه‌ی اجرای کارها یا دستورکارهایی که کمی پیش کامل کردید را نشان می‌دهد.

همچنین در این کتاب، برخی دیگر از کمک‌های آموزشی را پیدا خواهید کرد، از جمله موارد زیر:

آزمون: "عنوان آزمون"

این‌ها پرسش‌های مفهومی چندگزینه‌ای کوتاهی هستند که به شما کمک می‌کنند تا آموخته‌های خود را بسنجید.

خودتان آزمایش کنید: "عنوان مطلب"

این‌ها چالش‌های عملی و ایده‌هایی را برای آزمایش آنچه که آموخته‌اید ارائه می‌دهند.

پیش‌گفتار /

همچنین شکل‌های گوناگونی از متن را خواهید یافت که میان انواع گوناگون اطلاعات تمایز می‌گذارند. در این
نمونه‌هایی از این سبک‌ها و توضیح معنای آن‌ها، آمده است.

کلمات کد در متن به این صورت نشان داده‌شده است: " ما واسط را با استفاده از فرمان ifconfig فعال کردیم."

کلماتی که روی صفحه می‌بینید، برای مثال در منوها یا در جعبه‌های گفتگو[1]، در متنی مانند این نشان داده می‌شو
"به منظور دیدن بستک‌های داده برای اکسس‌پوینتمان، عبارت زیر را به فیلتر اضافه می‌کنیم **(== lan.bssid**
(00:21:91:d2:8e:25) && (wlan.fc.type_subtype == 0x20".


هشدارها و نکات مهم در یک جعبه مانند این نشان داده می‌شوند.


نکات و ترفندها در جعبه‌ای مانند این نشان داده می‌شوند

[1] dialog boxes