تست نفوذپذیری شبکه‌های بی‌سیم با

BACK TRACK 5

راهنمای مبتدی‌ها

ویوک راماچاندران

ترجمه:
دکترسید عنایت‌اله علوی
مهندس احسان محمدزاده
انتشارات پندار پارس

انتشارات پندارپارس

دفتر فروش: انقلاب، ابتدای کارگرجنوبی، کوی رشتچی، شماره ١٤، واحد ١٦ **www.pendarepars.com**

تلفن: ٦٦٥٧٢٣٣٥ - تلفکس: ٦٦٩٢٦٥٧٨همراه: ٠٩١٢٢٤٥٢٣٤٨ **info@pendarepars.com**

نام کتاب : **تست نفوذپذیری شبکه‌های بی‌سیم با Back Track 5**

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 : **۱۱۰۰۰ تومان** **شابک : ۲-۵۹-۶۵۲۹-۶۰۰-۹۷۸**

فهرست

درباره‌ی نویسنده

وی‌وک راماچاندران[1] از سال ۲۰۰۳ روی امنیت وای‌فای کار کرده است. او حمله‌ی کافه‌لاته[2] را کشف کرد و همچنین WEP Cloaking را شکست، که یک الگوی حفاظتی عام WEP در سال ۲۰۰۷ در اجلاس Defcon است. وی‌وک در سال ۲۰۱۱، برای نخستین بار نشان داد که نرم‌افزارهای مخرب چگونه از وای‌فای برای ساختن راه‌های پنهانی[3]، 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 و همچنین یکی از برندگان مسابقه‌ی امنیتی ماکروسافت بود که در هند و در میان ۶۵۰۰۰ شرکت‌کننده برگزار شد. او به عنوان بنیان‌گذار سایت http://www.SecurityTube.net در جامعه‌ی هکرها شناخته شده است، جایی که به طور معمول ویدئوهایی درباره‌ی امنیت وای‌فای، زبان اسمبلی، فن‌های بهره‌برداری و غیره ارائه می‌شود. سایت 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، IT World Canada و ... مورد توجه قرارگرفته و درباره‌ی او صحبت شده است. امسال او در شماری از اجلاس‌های امنیتی سخنرانی نموده و آموزش می‌دهد. این اجلاس‌ها شامل BlackHat، Defcon، Hacktivity، 44con، HITB-ML، Brucon، 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!

---

[1] Vivek Ramachandran
[2] Caffe Latte
[3] backdoors
[4] botnet
[5] 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 و 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 خانه‌ها، 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 راهنمای عملی گام به گام بوده‌اند مطلبی لازم 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 پلتفرم 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 و 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 دستگاه‌های با قابلیت وای‌فای[1] متمرکز می‌شویم، و سپس تمرکزمان را روی نرم‌افزار مورد نیاز شامل سیستم‌عامل، درایورهای وای‌فای 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 و داده می‌بینیم که چگونه اکسس‌پوینت و سرویس‌گیرنده در سطح بستک[1] با هم ارتباط دارند. سپس درباره‌ی تزریق و 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 محلی بی‌سیم صحبت می‌کند! ما قدم به قدم پیش خواهیم رفت و چگونگی بی‌اعتبار کردن احراز هویت‌های باز و کلید مشترک را بررسی خواهیم کرد. در این فصل، چگونگی آنالیز بستک‌های شبکه‌ی بی‌سیم و کشف مکانیزم احراز هویت شبکه را خواهید آموخت. همچنین نگاهی خواهیم انداخت به چگونگی ورود غیرمجاز به شبکه‌هایی با SSID پنهان و فیلتر مک. این‌ها دو مکانیزم مشهور هستند که توسط مدیران شبکه به‌کار گرفته می‌شوند تا نفوذ به شبکه‌های بی‌سیم را مشکل‌تر 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 بی‌سیم را شرح می‌دهد. این بخش الگوهای رمزنگاری WEP، WPA و WPA2 است. در طول دهه‌ی گذشته، هکرها معایب فراوانی در این الگوها پیداکرده‌اند و نرم‌افزاری را که به طور عمومی در دسترس باشد برای شکستن آن‌ها و رمزگشایی داده، نوشته‌اند. اگرچه WPA2/WPA طراحی امنی دارند، پیکربندی نادرست آن‌ها، راه را برای آسیب‌پذیری‌های امنیتی باز می‌کند و منجر به آسان شدن سوءاستفاده از آن‌ها می‌شود. در این فصل، ناامنی‌های موجود در هر یک از این الگوها را درک خواهیم کرد و نمونه‌های نمایشی عملی را برای شکستن آن‌ها انجام خواهیم داد.

فصل ۵، حمله به زیربنای شبکه‌ی محلی بی‌سیم، تمرکز ما را به آسیب‌های زیربنای شبکه‌ی محلی بی‌سیم تغییر می‌دهد. در این فصل به آسیب‌های به وجود آمده توسط مشکلات پیکربندی و طراحی نگاهی خواهیم انداخت. همچنین نمونه‌های عملی حمله‌ها را انجام خواهیم داد، حملاتی مانند: جعل مک اکسس‌پوینت، تغییر بیت و حملات بازپخش، اکسس‌پوینت‌های متجاوز[2]، فازینگ و انکار سرویس. این فصل به خواننده درکی قوی از چگونگی انجام 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 شما ایجاد نمی‌کند این فصل چشم و گوش شما را باز می‌کند! بیشتر کسانی که امنیت شبکه محلی بی‌سیم را مد نظر دارند سرویس‌گیرنده را از لیست خود حذف می‌کنند. این فصل اثبات خواهد کرد که برخلاف حدس و گمان، در هنگام تست نفوذپذیری یک شبکه‌ی محلی بی‌سیم، سرویس‌گیرنده نیز به اندازه‌ی اکسس‌پوینت مهم است. ما نگاهی خواهیم انداخت به چگونگی به خطر انداختن امنیت با استفاده از حمله به سرویس‌گیرنده مانند حملات: اتصال اشتباهی[3]، کافه‌لاته ، جداسازی[4]، اتصالات فی‌البداهه[5]، فازینگ[6]، هانی‌پات[1]ها و حملات دیگری از این دست.

---

[1] packet
[2] rogue access points
[3] mis-association
[4] disassociation
[5] ad-hoc connections
[6] fuzzing

فصل ۷، حملات پیشرفته‌ی شبکه‌ی محلی بی‌سیم، نگاهی به حملات پیشرفته‌تری می‌اندازد چرا که پیش از این بیشتر حملات ابتدایی به زیربنا و سرویس‌گیرنده را پوشش داده‌ایم. این حملات معمولا شامل ترکیب پیوسته‌ای از حملات ابتدایی فراوان است و برای شکستن امنیت در سناریوهای چالش‌برانگیز بیشتری کاربرد دارد. برخی از حملاتی که خواهیم آموخت شامل این موارد هستند: انگشت‌نگاری دستگاه بی‌سیم، مرد میانی[۲] روی شبکه‌ی بی‌سیم، فرار از سیستم‌های تشخیص نفوذپذیری شبکه‌ی بی‌سیم و سیستم‌های پیشگیری، عامل اکسس‌پوینت متجاوز با استفاده از پروتکل مرسوم، و شماری دیگر. این فصل چیزی کاملا جدید را درباره‌ی حملات بی‌سیم در دنیای واقعی ارائه می‌دهد.

فصل ۸، حمله به WPA–سازمانی و سرویس‌دهنده‌ی ردیوس[۳]، با معرفی حملات پیشرفته به WPA–سازمانی و راه‌اندازی سرویس‌دهنده‌ی ردیوس به کاربر، او را به سطح بعدی سوق می‌دهد. این حملات زمانی کارایی خواهند داشت که خواننده مجبور باشد تستی را روی شبکه‌های بزرگ اجرا کند که آن‌ها خود برای فراهم کردن امنیت، وابسته به احراز هویت[۴] WPA–سازمانی و رادیوس هستند. این حملات احتمالا به اندازه‌ی حملات وای‌فایی که می‌توان در دنیای واقعی انجام داد، پیشرفته‌اند.

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

پیوست الف، کلام آخر و مسیر پیش رو، جمع‌بندی کتاب و رها کردن 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 دارای کارت وای‌فای، یک آداپتور بی‌سیم وای‌فای نمونه آلفا AWUS036H USB، بک‌ترک ۵ و چند سخت‌افزار و نرم‌افزار دیگر نیاز دارید. این نیازمندی‌ها را در *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 کارت را با واسط USB به آن وصل کنید. این کار به شما کمک می‌کند تا با سرعت بیشتری شروع به استفاده از این کتاب کنید، ولی پیشنهاد ما این است که از دستگاهی اختصاصی که بک‌ترک ۵ را اجرا می‌کند برای ارزیابی‌های واقعی در این باره استفاده کنید.

---

[1] honeypot
[2] man-in-the-middle
[3] Radius
[4] authentication

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

مخاطب این کتاب

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

قراردادها

در این کتاب، عناوین گوناگونی را خواهید یافت که پی‌درپی به چشم می‌خورند.

برای ارائه‌ی دستورکارهای روشنی از چگونگی تکمیل یک 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.

همچنین شکل‌های گوناگونی از متن را خواهید یافت که میان انواع گوناگون اطلاعات تمایز می‌گذارند. در اینجا 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 می‌شوند: "به منظور دیدن بستک‌های داده برای اکسس‌پوینتمان، عبارت زیر را به فیلتر اضافه می‌کنیم **(wlan.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

فصل ۱

راه‌اندازی آزمایشگاه بی‌سیم

"اگر من هشت ساعت برای قطعه‌قطعه کردن یک درخت فرصت داشتم، شش ساعت تبرم را تیز می‌کردم."

آبراهام لینکلن، شانزدهمین رئیس‌جمهور آمریکا

پشت هر عمل موفقی ساعت‌ها یا روزها آماده‌سازی وجود دارد، و تست نفوذپذیری شبکه‌ی بی‌سیم هم از این قاعده مستثنا نیست. در این فصل ما یک آزمایشگاه بی‌سیم ایجاد کرده و از آن برای آزمایش‌های خود استفاده خواهیم کرد. این آزمایشگاه را پیش از اینکه به دنیای واقعی تست نفوذپذیری شیرجه بزنید میدان آمادگی بدانید!

تست نفوذپذیری شبکه‌ی بی‌سیم موضوعی عملی است و مهم است که در آغاز آزمایشگاهی راه‌اندازی کنیم تا بتوانیم تمام آزمایش‌های گوناگون این کتاب را در یک محیط امن و کنترل شده امتحان کنیم. بهتر است پیش از ادامه‌ی پیشروی در مطالب کتاب، ابتدا این آزمایشگاه را راه‌اندازی کنید.

در این فصل باید به موارد زیر نگاهی بیندازیم:

- سخت‌افزار و نرم‌افزار مورد نیاز
- نصب بک‌ترک ۵
- راه‌اندازی یک اکسس‌پوینت و پیکربندی آن
- نصب کارت شبکه‌ی بی‌سیم
- تست اتصال میان لپ‌تاپ و اکسس‌پوینت

پس بگذارید بازی شروع شود!

سخت‌افزار مورد نیاز

برای راه‌اندازی آزمایشگاه بی‌سیم به سخت‌افزار زیر نیاز داریم:

- **دو لپ‌تاپ با کارت‌های داخلی وای‌فای:** در آزمایشگاه‌مان، یکی از لپ‌تاپ‌ها را به عنوان قربانی و دیگری را به عنوان لپ‌تاپ تست‌کننده نفوذپذیری استفاده خواهیم کرد. اگرچه تقریبا هر لپ‌تاپی برای این کار مناسب است، لپ‌تاپی با دست‌کم ۳ گیگابایت رم عالی است. چرا که ممکن است شمار زیادی نرم‌افزار که حافظه اشغال می‌کنند را در آزمایش‌های خود اجرا کنیم.

- **یک آداپتور بی‌سیم آلفا:** به یک کارت USB وای‌فای نیاز داریم که تزریق بستک[1] و شنود بستک[2] را پشتیبانی نموده و توسط بک‌ترک پشتیبانی شود. به نظر می‌رسد بهترین انتخاب، کارت Alfa AWUS036H از شبکه‌های آلفا باشد زیرا بک‌ترک از این استاندارد پشتیبانی می‌کند. این کارت در سایت Amazon.com با قیمت جزئی ۳۴ دلار در زمان نوشتن این کتاب موجود است.

- **یک اکسس‌پوینت:** هر اکسس‌پوینتی که استانداردهای رمزگذاری WPA2/WPA/WEP را پشتیبانی کند برای ما مناسب است. من از یک روتر بی‌سیم D-LINK DIR-615 سری N به عنوان نمونه در سرتاسر کتاب استفاده خواهم کرد. شما می‌توانید آن را از سایت Amazon.com خریداری کنید که در زمان نوشتن کتاب با قیمت حدود ۳۵ دلار فروخته می‌شد.

- **یک اتصال اینترنت:** که برای جست‌وجو کردن، دانلود نرم‌افزار و برخی از آزمایش‌ها مفید خواهد بود.

نرم‌افزار مورد نیاز

- **بک‌ترک ۵**: بک‌ترک را می‌توان از سایت رسمی آن واقع در http://www.backtrack-linux.org دانلود کرد. این نرم‌افزار منبع باز است و باید بتوانید مستقیما آن را از وب سایت دانلود کنید.

- **7/Vista/Windows XP**: به یکی از ویندوزهای XP، ویستا یا ۷ نصب‌شده روی یکی از لپ‌تاپ‌ها احتیاج دارید. از این لپ‌تاپ به عنوان ماشین قربانی در ادامه کتاب استفاده خواهد شد.

مهم است که توجه داشته باشید اگرچه از یک سیستم‌عامل مبتنی بر ویندوز برای تست‌هایمان استفاده می‌کنیم، تکنیک‌های آموخته‌شده را می‌توان به هر دستگاهی که قابلیت وای‌فای دارد، مانند تلفن‌های هوشمند و تبلت‌ها، تعمیم داد.

---

[1] packet injection
[2] packet sniffing

نصب بک‌ترک

اینک بیایید به چگونگی آماده‌سازی و اجرای بک‌ترک نگاه سریعی بیاندازیم.

بک‌ترک روی لپ‌تاپی نصب خواهد شد که به عنوان ماشین تست‌کننده‌ی نفوذپذیری در ادامه کتاب عمل می‌کند.

آغاز کار: نصب بک‌ترک

نصب کردن بک‌ترک نسبتا ساده است. بک‌ترک را با بوت کردن از طریق DVD و سپس نصب آن روی هارد درایو اجرا خواهیم کرد. عملیات زیر را قدم به قدم انجام دهید:

۱. BackTrack ISO (ما از نسخه‌ی BackTrack 5 KDE 32-Bit استفاده می‌کنیم) را که دانلود کرده‌اید روی یک DVD قابل بوت شدن رایت کنید.

۲. لپ‌تاپ را با این DVD بوت کنید و گزینه‌ی BackTrack Text – Default Boot Text Mode را از منوی بوت انتخاب کنید.

۳. اگر عمل بوت شدن موفقیت‌آمیز باشد باید صفحه‌ی آشنای بک‌ترک را ببینید:

۴. با واردکردن دستور **startx** در خط فرمان می‌توانید در مد گرافیکی، بوت شوید. از موزیک بوت لذت ببرید! زمانی که در محیط گرافیکی هستید، صفحه‌ی شما باید به صورت زیر باشد:

۵. اینک روی آیکن **Install BackTrack** در سمت چپ دسکتاپ کلیک کنید. این کار همان گونه که در ادامه نشان داده شده است نصب کننده‌ی بک‌ترک را اجرا می‌کند.

۶. این نصب کننده مشابه نصب کننده‌های مبتنی بر محیط گرافیکی بیشتر سیستم‌های لینوکس بوده و دنبال کردن آن ساده است. گزینه‌های مناسب را در هر صفحه انتخاب و فرآیند نصب را شروع کنید. وقتی عملیات نصب انجام شد، همان گونه که سیستم اعلان می‌کند ماشین را ریستارت کرده و DVD را بردارید.

۷. وقتی ماشین ریستارت شد، یک صفحه‌ی ورود به شما نمایش می‌دهد. در بخش ورودی، کلمه‌ی "root" و در بخش گذرواژه، واژه‌ی "toor" را تایپ کنید. اکنون باید به نسخه‌ی نصب‌شده‌ی بک‌ترک خود وارد شوید. تبریک میگم!

من تم دسکتاپ و برخی از تنظیمات را برای این کتاب تغییر خواهم داد. شما برای استفاده از تم‌ها و تنظیمات رنگ دلخواهتان مختارید!

چه اتفاقی افتاد؟

در این بخش بک‌ترک را با موفقیت روی لپ‌تاپ نصب کردیم! از این لپ‌تاپ به عنوان لپ‌تاپ تست‌کننده‌ی نفوذپذیری همه‌ی آزمایش‌های کتاب استفاده خواهیم کرد.

خودتان آزمایش کنید: نصب بک‌ترک در Virtual Box

ما همچنین می‌توانیم بک‌ترک را درون نرم‌افزارهای مجازی‌ساز مانند Virtual Box نصب کنیم. این بهترین گزینه برای خوانندگانی است که نخواهند لپ‌تاپی را کاملا به بک‌ترک اختصاص دهند. مراحل نصب بک‌ترک در Virtual Box نیز دقیقا مانند مراحل گفته شده است. تنها تفاوت آن راه‌انداز اولیه است که باید در Virtual Box ایجاد کنید. امتحانش کنید! می‌توانید Virtual Box را از http://www.virtualbox.org دانلود کنید.

یکی دیگر از راه‌های نصب و استفاده از بک‌ترک، نصب آن روی درایوهای USB است. این روش هنگامی که نمی‌خواهید بک‌ترک را روی هارد درایو نصب کنید اما هنوز می‌خواهید داده‌های پایدارتان، مانند اسکریپ‌ها و ابزارهای جدید را روی نمونه‌ی بک‌ترک خودتان ذخیره کنید، قطعا مفید خواهد بود. شما را تشویق می‌کنیم که این کار را هم امتحان کنید.

راه‌اندازی اکسس‌پوینت

اکنون اکسس‌پوینت را راه‌اندازی می‌کنیم. همان‌گونه که پیش‌تر گفتیم، برای همه‌ی آزمایش‌های کتاب از روتر بی‌سیم D-LINK DIR-61 استفاده خواهیم کرد اما شما برای استفاده از هر اکسس‌پوینت دیگری آزادید. اصول اساسی عملکرد و استفاده آن‌ها یکسان است.

آغاز کار: پیکربندی اکسس‌پوینت

بیایید شروع کنیم! اکسس‌پوینت را به گونه‌ای راه‌اندازی می‌کنیم تا از احراز هویت باز[1] و SSID "Wireless Lab" استفاده کند.

عملیات زیر را گام به گام دنبال کنید:

۱. اکسس‌پوینت را روشن کنید و از یک کابل اترنت برای اتصال لپ‌تاپ خود به یکی از درگاه‌های اترنت اکسس‌پوینت استفاده کنید.

۲. آدرس آی‌پی ترمینال پیکربندی اکسس‌پوینت را در مرورگر وارد کنید. برای DIR-615، در دفترچه راهنما این آدرس ۱۹۲.۱۶۸.۰.۱ داده شده است. باید به راهنمای راه‌انداز اکسس‌پوینت خود نگاه کنید تا آدرس آی‌پی آن را بیابید. اگر راهنمای اکسس‌پوینت را ندارید، می‌توانید با اجرای دستور route –n، آدرس آی‌پی را بیابید. معمولا آدرس آی‌پی مربوط به دروازه[2]، همان آدرس آی‌پی اکسس‌پوینت است. پس از اتصال، باید درگاه پیکربندی زیر را ببینید:

۳. پس از وارد شدن، تنظیمات گوناگون را در درگاه بررسی کنید و تنظیمات مربوط به پیکربندی یک SSID جدید را بیابید.

۴. شناسه‌ی **SSID** را به **Wireless Lab** تغییر دهید. بسته به اکسس‌پوینت، ممکن است لازم باشد برای تغییر تنظیمات، آن را راه‌اندازی مجدد[3] کنید.

---

[1] Open Authentication
[2] gateway
[3] reboot

۵. به طور مشابه، تنظیمات مربوط به **Authentication** را بیابید و آن را به **Open Authentication** تغییر دهید. در حالتی که من کار می‌کنم، **None** بودن پیکربندی **Security Mode** نشان‌دهنده‌ی این است که از حالت احراز هویت باز استفاده می‌کند.

۶. تغییرات را در اکسس‌پوینت ذخیره کرده و در صورت لزوم، آن را راه‌اندازی مجدد کنید. اکنون اکسس‌پوینت شما باید بالا آمده و با SSID، **Wireless Lab** در حال اجرا باشد.

یک راه آسان برای اطمینان از این مطلب، استفاده از امکانات پیکربندی شبکه‌ی بی‌سیم در ویندوز و مشاهده‌ی شبکه‌های موجود است. این کار با استفاده از لپ‌تاپی که ویندوز روی آن نصب‌شده، امکان‌پذیر است. باید **Wireless Lab** را به عنوان یکی از شبکه‌ها در لیست پیدا کنید.

چه اتفاقی افتاد؟

ما با موفقیت اکسس‌پوینتمان را با SSID، **Wireless Lab** راه‌اندازی کردیم. این اکسس‌پوینت حضورش را به همه‌ی دستگاه‌های در دسترس اعلام کرده و به‌وسیله‌ی لپ‌تاپ ما با سیستم‌عامل ویندوز و دستگاه‌های دیگری که در محدوده‌ی فرکانسی آن باشند دریافت می‌شود.

مهم است توجه داشته باشید اکسس‌پوینت را در مد باز که از امنیت کمتری برخوردار است پیکربندی کرده‌ایم. توصیه می‌شود آن را زمانی که روشن است به اینترنت وصل نکنید، چرا که تمام کسانی که در محدوده‌ی فرکانسی باشند، قادر به استفاده از آن برای دسترسی به اینترنت خواهند بود.

خودتان آزمایش کنید: پیکربندی اکسس‌پوینت برای استفاده از WEP و WPA

با گزینه‌های پیکربندی اکسس‌پوینت خود بازی کنید. سعی کنید ببینید می‌توانید آن را بالا آورده و با استفاده از طرح‌هایی مانند WEP و WPA2/WPA اجرا کنید. از این حالت‌ها در فصل‌های آینده برای نشان دادن حمله به آن‌ها استفاده خواهیم کرد.

راه‌اندازی کارت بی‌سیم

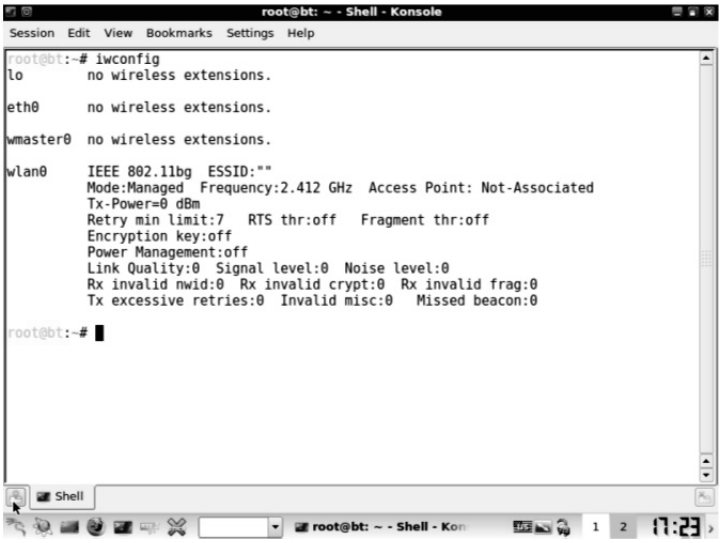
راه‌اندازی کارت بی‌سیم آلفا از اکسس‌پوینت بسیار آسان‌تر است. مزیت آن این است که بک‌ترک استاندارد این کارت را پشتیبانی می‌کند و با تمام درایورهای دستگاه‌های ملزوم برای فعال کردن تزریق و شنود بستک سازگار است.

آغاز کار: پیکربندی کارت بی‌سیم خود

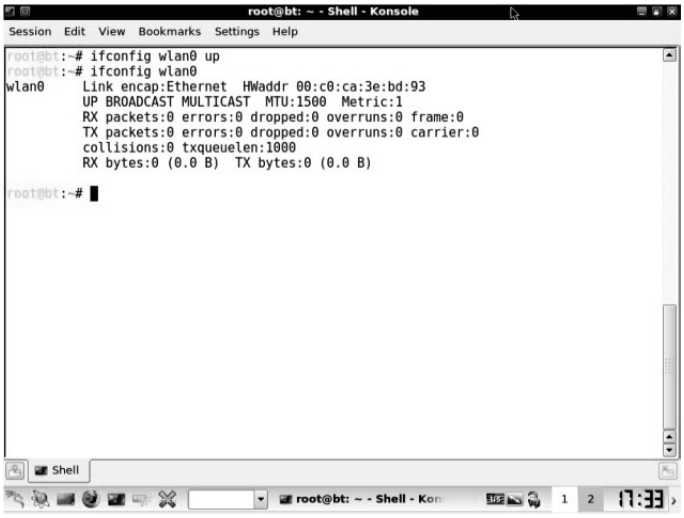
از کارت بی‌سیم آلفا با لپ‌تاپ تست‌کننده استفاده خواهیم کرد.

لطفا این عملیات را گام به گام برای راه‌اندازی کارت خود دنبال کنید:

۱. کارت را به یکی از درگاه‌های USB لپ‌تاپ بک‌ترک بزنید و آن را بوت کنید.
۲. وقتی وارد سیستم شدید یک کنسول ترمینال را بازکرده و iwconfig را در آن تایپ کنید. صفحه‌ی شما باید به شکل زیر در بیاید:



همان گونه که می‌توانید ببینید، wlan0 واسط بی‌سیم است که برای کارت بی‌سیم آلفا ساخته شده است. برای اینکه واسط را فعال کنید ifconfig wlan0 up را در آن تایپ کنید. سپس ifconfig wlan0 را برای مشاهده‌ی وضعیت کنونی واسط تایپ کنید:



۳. آدرس مک 00:c0:ca:3e:bd:93 باید با آدرس مک نوشته‌شده زیر کارت آلفای شما یکسان باشد. این طریقه‌ی چک کردن، یک راه سریع برای اطمینان از این است که شما واسط صحیح را فعال کرده‌اید.

چه اتفاقی افتاد؟

بک‌ترک با تمام درایورهای لازم برای کارت آلفا سازگار است. به محض اینکه ماشین بوت شد، کارت شناخته‌شده و به واسط شبکه‌ی wlan0 اختصاص داده شد. به طور پیش‌فرض، تمام واسط‌های شبکه در بک‌ترک به هنگام بوت غیرفعال می‌باشند. ما واسط را با استفاده از دستور ifconfig فعال کردیم. اکنون کارت آلفا آماده و قابل استفاده است!

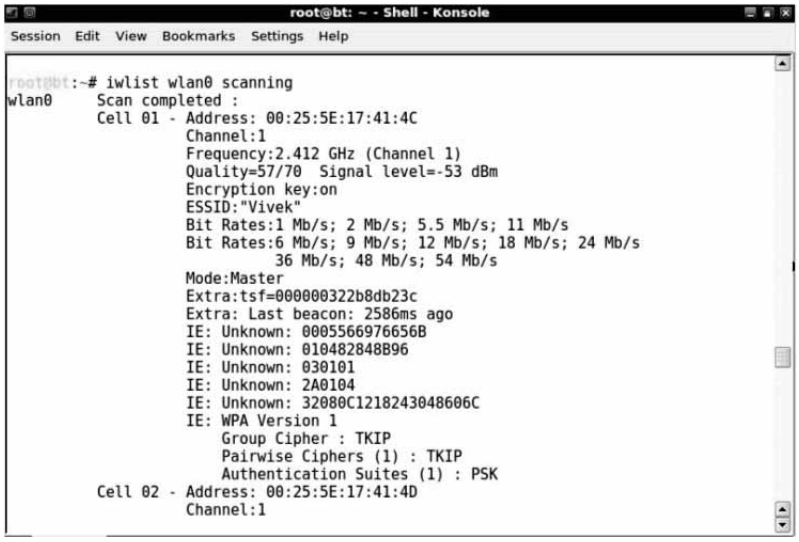
اتصال به اکسس‌پوینت

در این بخش نگاهی خواهیم انداخت به چگونگی اتصال به اکسس‌پوینت با استفاده از کارت بی‌سیم آلفا. اکسس‌پوینت ما یک SSID، **Wireless Lab** دارد و از هیچ‌گونه احراز هویتی استفاده نمی‌کند.

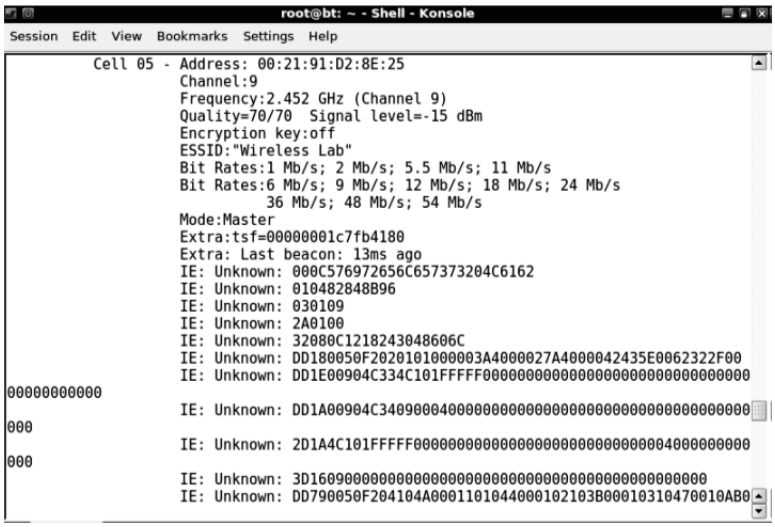
آغاز کار: پیکربندی کارت بی‌سیم خود

ادامه می‌دهیم! مراحل زیر را برای اتصال کارت بی‌سیم به اکسس‌پوینت دنبال کنید:

۱. ابتدا اجازه دهید ببینیم چه شبکه‌های بی‌سیمی را کارت آلفای ما پیدا می‌کند. دستور iwlist wlan0 scanning را وارد کنید و لیستی از شبکه‌ها را در نزدیکی‌تان خواهید یافت:

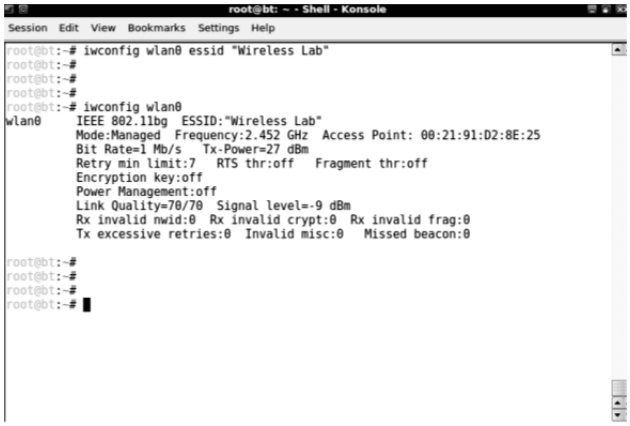


۲. با پایین کشیدن اسکرول باید شبکه‌ی Wireless Lab را در لیست پیدا کنید. در تنظیمات من این شبکه با عنوان Cell 05 مشخص شده است، در این مورد در تنظیمات شما ممکن است متفاوت باشد. فیلد ESSID حاوی نام شبکه است:



۳. از آنجایی که چند اکسس‌پوینت می‌توانند SSID یکسانی داشته باشند، مطمئن شوید مک آدرسی که در فیلد آدرس بالا قید شده است با مک اکسس‌پوینت شما همخوانی دارد. یک راه سریع و آسان برای فهمیدن مک آدرس، استفاده از اطلاعات نوشته‌شده در پشت اکسس‌پوینت یا استفاده از تنظیمات گرافیکی مبتنی بر وب است.

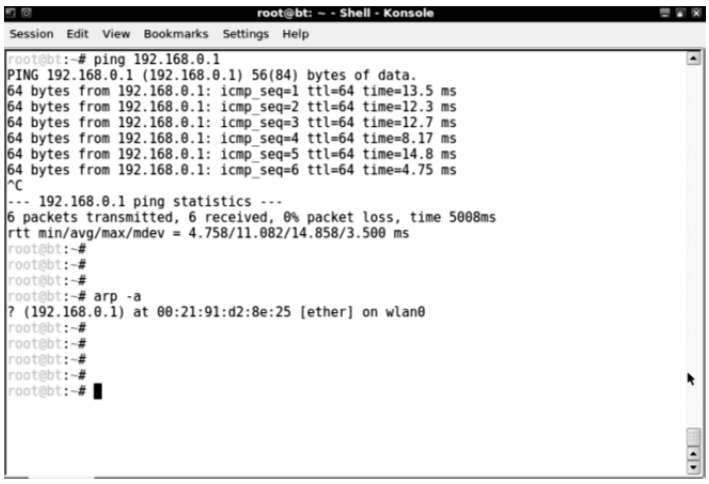
۴. اینک دستور iwconfig wlan0 essid "Wireless Lab" و سپس iwconfig wlan0 را برای چک کردن وضعیت وارد کنید. همان گونه که در تصویر نشان داده‌شده است اگر با موفقیت به اکسس‌پوینت متصل شده‌اید، باید مک آدرس اکسس‌پوینت را در فیلد :Access Point در خروجی دستور iwconfig ببینید:



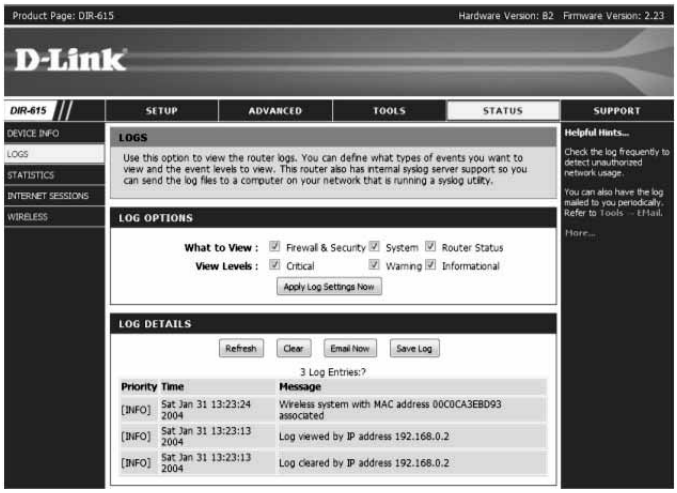
۵. می‌دانیم که اکسس‌پوینت یک آدرس آی‌پی واسط مدیریتی "۱۹۲.۱۶۸.۰.۱" دارد که در راهنمای آن اکسس‌پوینت قرار دارد. به عنوان یک جایگزین، وقتی که دستور route –n را اجرا می‌کنیم این همان آدرس آی‌پی پیش‌فرض روتر است. بیایید آدرس آی‌پی خود را با استفاده از دستور ifconfig wlan0 192.168.0.2 netmask 255.255.255.0 up در همین زیر شبکه تنظیم کنیم. با واردکردن ifconfig wlan0 و بررسی خروجی مطمئن شوید که دستور موفقیت‌آمیز بوده است:

۶. اکنون بیایید اکسس‌پوینت را با استفاده از دستور ping 192.168.0.1، پینگ کنیم. اگر اتصال شبکه به درستی تنظیم شده باشد، می‌بایست پاسخ‌های اکسس‌پوینت را ببینید. همچنین می‌توانید دستور arp –a را برای اطمینان از اینکه پاسخ‌ها از اکسس‌پوینت می‌آیند وارد کنید. باید ببینید که مک آدرس آی‌پی ۱۹۲.۱۶۸.۰.۱ همان مک آدرسی است که ما پیش‌تر ذکر کرده بودیم. لازم به ذکر است که بسیاری از اکسس‌پوینت‌های اخیر ممکن است

در پاسخ به بستک‌های درخواست ICMP Echo ناتوان باشند. این کار معمولا انجام می‌شود تا استاندارد امنیت اکسس‌پوینت تنها با کمترین تنظیمات پیکربندی قابل انجام باشد. در چنین موردی می‌توانید یک مرورگر را باز نموده و برای بررسی برقراری و فعال بودن اتصال، به واسط وب آن سری بزنید.



۷. در اکسس‌پوینت، می‌توانیم با نگاه انداختن به لاگ‌های اتصال، از وصل بودن مطمئن شویم. همان گونه که در لاگ زیر می‌بینید، مک آدرس کارت بی‌سیم 00:c0:ca:3a:bd:93 گزارش شده است:



چه اتفاقی افتاد؟

ما کمی پیش از بک‌ترک با موفقیت به اکسس‌پوینت خود متصل شدیم. این کار را با استفاده از کارت بی‌سیم آلفا به عنوان وسیله‌ی بی‌سیم انجام دادیم. همچنین آموختیم که چگونه می‌توان مطمئن شد که یک اتصال هم از طرف سرویس‌گیرنده‌ی بی‌سیم و هم از طرف اکسس‌پوینت برقرار شده است.

خودتان آزمایش کنید: برقراری اتصال در پیکربندی WEP

در اینجا یک تمرین چالش‌برانگیز برای شما داریم و آن تنظیم اکسس‌پوینت در پیکربندی WEP است. برای هر کدام از این‌ها، سعی کنید با استفاده از آداپتور بی‌سیم، یک اتصال به اکسس‌پوینت برقرار کنید.

توجه: با واردکردن man iwconfig، راهنما را برای دستور iwconfig بررسی کنید تا ببینید پیکربندی کارت برای اتصال به WEP چگونه است.

آزمون: درک مفاهیم اساسی

۱. پس از واردکردن دستور ifconfig wlan0 up، چگونه مطمئن می‌شوید کارت بی‌سیم آماده و قابل استفاده است؟

۲. آیا می‌توانیم تمام آزمایش‌های خود را تنها با استفاده از CD بک‌ترک اجرا کنیم؟ و آن را روی هارد درایو نصب نکنیم؟

۳. دستور arp –a چه چیزی را نشان می‌دهد؟

۴. از چه ابزاری باید برای اتصال به شبکه‌های WPA/WPA2 در بک‌ترک استفاده کنیم؟

چکیده‌ی این فصل

این فصل با دستورهای جزء به جزء به شما می‌گوید که چگونه می‌توانید آزمایشگاه بی‌سیمتان را راه‌اندازی کنید. همچنین در این مرحله گام‌های اساسی زیر را آموخته‌اید:

- نصب بک‌ترک روی هارد درایو و مشاهده‌ی موارد دیگر مانند VMware و USB
- پیکربندی اکسس‌پوینت از طریق واسط وب
- آشنایی و استفاده از چندین دستور برای پیکربندی و استفاده از کارت بی‌سیم
- چگونگی اطمینان از وضعیت اتصال میان سرویس‌گیرنده‌ی بی‌سیم و اکسس‌پوینت

مهم است که در پیکربندی سیستم، به خود مطمئن شوید. وگرنه، توصیه می‌شود این مثال‌ها را چندین بار دیگر تکرار کنید. در فصل‌های آینده، سناریوهای پیچیده‌تری را طراحی خواهیم کرد.

در فصل آینده، درباره‌ی ناامنی‌های ذاتی ناشی از طراحی در شبکه‌های محلی بی‌سیم خواهیم آموخت. برای درک این مفاهیم به صورت عملی، از ابزار تحلیلگر شبکه وایرشارک استفاده خواهیم کرد.

فصل ۲

شبکه‌ی محلی بی‌سیم و ناامنی‌های ذاتی آن

"هر چه ساختمان بلندتر باشد، پی ریزی آن باید عمیق تر باشد."

توماس کمپیس، نویسنده

هیچ‌چیز بزرگی نمی‌تواند روی یک پی ضعیف بنا شود و در زمینه کار ما هم هیچ‌چیز امنی نمی‌تواند روی چیزی که ذاتا ناامن است بنا شود.

شبکه‌های محلی بی‌سیم به خاطر طراحی‌شان ناامنی‌های مشخصی دارند که نسبتا برای سوءاستفاده کردن آسان هستند؛ مانند جعل بستک[1]، تزریق بستک و شنود (که حتی می‌تواند از فاصله‌ی دور اتفاق بیفتد). این معایب را در این فصل بررسی خواهیم کرد.

در این فصل به موارد زیر نگاهی خواهیم انداخت:

- بازبینی فریم‌های شبکه‌ی محلی بی‌سیم
- انواع گوناگون فریم و زیر نوع‌ها
- استفاده از وایرشارک برای شنود فریم‌های مدیریت، کنترل و داده
- شنود بستک‌های داده برای یک شبکه‌ی بی‌سیم مشخص
- تزریق بستک‌ها به یک شبکه‌ی بی‌سیم مشخص

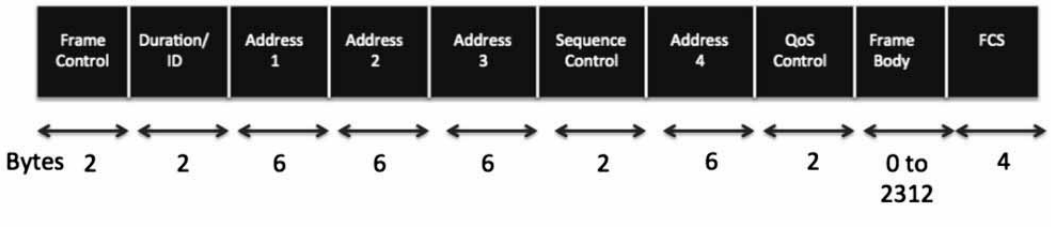
بیایید شروع کنیم!

[1] packet spoofing

بازبینی فریم‌های شبکه‌ی محلی بی‌سیم

از آنجایی که این کتاب با جنبه‌های امنیتی شبکه‌ی بی‌سیم سر و کار دارد، فرض می‌کنیم که هم‌اینک یک دانش اولیه از پروتکل و سرآیندهای بستک دارید. اگر چنین نیست یا اینکه از زمانی که با شبکه‌های بی‌سیم کارکرده‌اید مدتی گذشته است، فرصت خوبی است که آن را بازبینی کنید.

اجازه دهید سریعا برخی از مفاهیم اولیه‌ی شبکه‌های محلی بی‌سیم را که ممکن است بسیاری از شما آن‌ها را می‌دانید مرور کنیم. در شبکه‌های محلی بی‌سیم، ارتباطات از طریق فریم‌ها برقرار می‌شود. یک فریم باید ساختار سرآیند زیر را داشته باشد:



فیلد "Frame Control" به نوبه‌ی خود ساختار پیچیده‌تری دارد:

فیلد "Type" نوع فریم شبکه‌ی محلی بی‌سیم را تعریف می‌کند که سه حالت دارد:

۱. **فریم‌های مدیریت:** فریم‌های مدیریت مسئول نگهداری و حمایت از ارتباطات میان نقاط دسترسی و سرویس‌گیرنده‌های بی‌سیم هستند. فریم‌های مدیریت می‌توانند زیرنوع‌های زیر را داشته باشند:
   - احراز هویت
   - نفی احراز هویت[1]

[1] De-authentication

- درخواست پیوند[۱]
- پاسخ به درخواست پیوند[۲]
- درخواست پیوند مجدد
- پاسخ به درخواست پیوند مجدد
- گسست
- علامت[۳]
- درخواست کاوش[۴]
- پاسخ کاوش[۵]

۲. **فریم‌های کنترل:** فریم‌های کنترل، مسئول اطمینان از تبادل صحیح داده میان نقطه‌ی دسترسی و سرویس‌گیرنده‌های بی‌سیم هستند. فریم‌های کنترل می‌توانند زیرنوع‌های زیر را داشته باشند:
   - درخواست ارسال[۶] (RTS)
   - اجازه‌ی ارسال[۷] (CTS)
   - تصدیق[۸] (ACK)

۳. **فریم‌های داده:** فریم‌های داده، داده‌ی واقعی که در شبکه‌ی بی‌سیم ارسال می‌شود را حمل می‌کنند. زیر نوعی برای فریم‌های داده وجود ندارد.

معانی امنیتی هر کدام از این فریم‌ها را وقتی حملات گوناگون را در فصل‌های بعدی گفتیم، شرح خواهیم داد.

اکنون نگاهی می‌اندازیم به اینکه چگونه می‌توان با استفاده از وایرشارک، این فریم‌ها را روی یک شبکه‌ی بی‌سیم شنود کرد. ابزارهای دیگری نیز مانند Airodump-NG، Tcpdump یا Tshark وجود دارد که برای شنود استفاده می‌شوند. هر چند در بیشتر بخش‌های این کتاب از وایرشارک استفاده می‌کنیم، اما شما را تشویق می‌کنیم که ابزارهای دیگر را نیز امتحان کنید. نخستین گام برای انجام این کار، ساختن یک واسط در حالت پایش است. این کار برای کارت آلفای ما واسطی ایجاد می‌کند که به ما اجازه می‌دهد تا تمام فریم‌های شبکه‌ی بی‌سیم موجود در هوا را صرف‌نظر از اینکه برای ما ارسال‌شده‌اند یا نه، بخوانیم. در دنیای ارتباطات باسیمی، این حالت عموما حالت بی‌قاعده[۹] نامیده می‌شود.

---

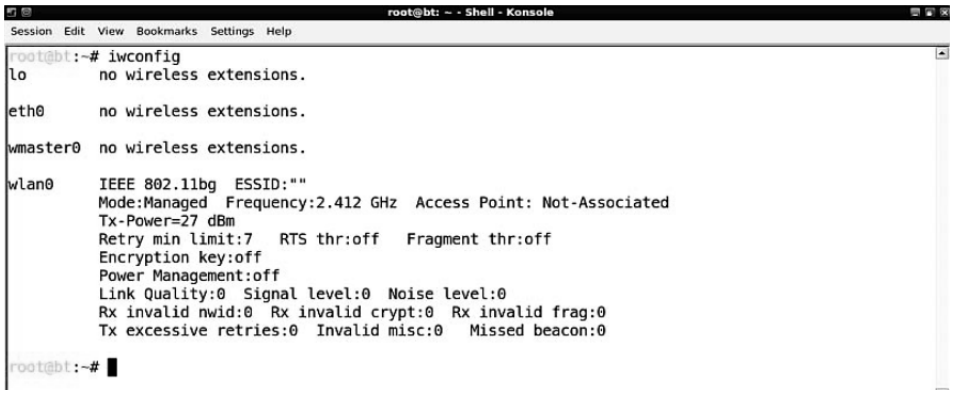
[1] Association Request
[2] Association Response
[3] Beacon
[4] Probe Request
[5] Probe Response
[6] Request To Send
[7] Clear To Send
[8] Acknowledge
[9] promiscuous mode

اکنون بیایید کارت آلفای خود را در حالت پایش قرار دهیم!

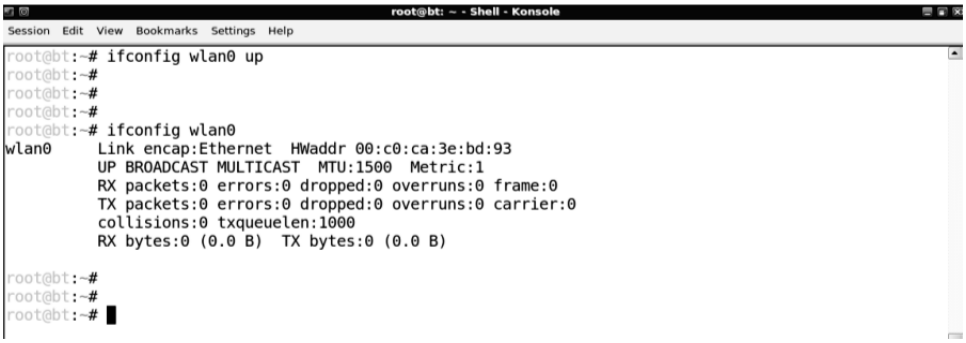
آغاز کار: ایجاد یک واسط در حالت پایش

برای شروع عملیات زیر را دنبال کنید:

۱. درحالی‌که کارت آلفا متصل است بک‌ترک را بوت کنید. در کنسول، دستور iwconfig را وارد کنید تا مطمئن شوید که کارت شما شناخته‌شده و درایور آن به درستی بارگذاری شده است:

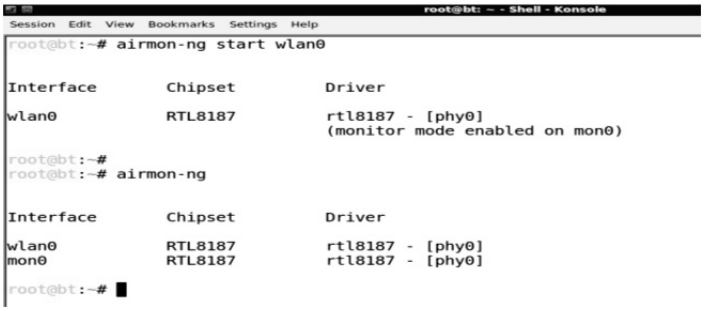


۲. از دستور ifconfig wlan0 up استفاده کنید تا کارت را بالا بیاورید. با اجرای iwconfig wlan0 مطمئن شوید که کارت آماده است. واژه‌ی UP را باید در خط دوم خروجی همان گونه که نشان داده‌شده ببینید:

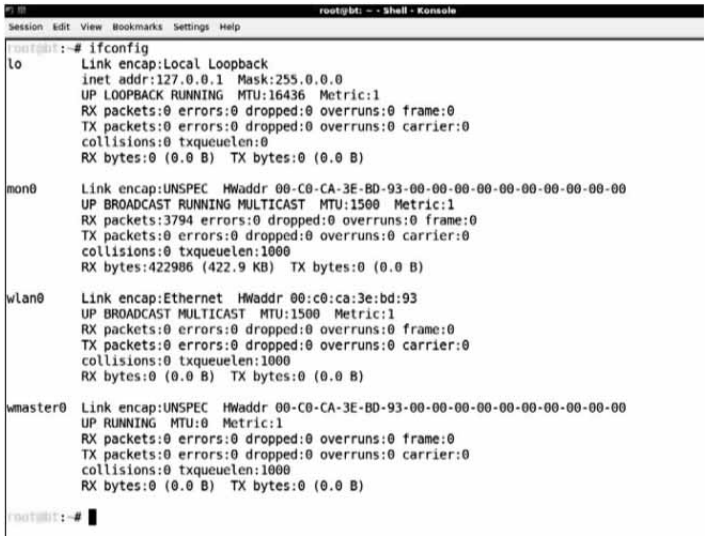


۳. برای اینکه کارتمان را در حالت پایش قرار دهیم، از ابزار airmon-ng که به طور پیش‌فرض در بک‌ترک موجود است، استفاده خواهیم کرد. ابتدا airmon-ng را اجرا کنید تا مطمئن شوید که کارت‌های موجود را می‌شناسد. باید واسط wlan0 را که در خروجی لیست شده است ببینید:

۴. اکنون airmon-ng start wlan0 را وارد کنید تا واسط حالت پایش مربوط به ابزار wlan0 را ایجاد کنید. این واسط حالت پایش جدید، mon0 نام خواهد گرفت. با اجرای دوباره‌ی airmon-ng بدون آرگومان، می‌توانید از ایجاد شدن آن مطمئن شوید:



۵. همچنین، اکنون اجرای ifconfig باید یک واسط جدید به نام mon0 به شما نشان بدهد:



چه اتفاقی افتاد؟

توانستیم با موفقیت، یک واسط حالت پایش mon0 بسازیم. این واسط برای شنود بستک‌های موجود در هوا استفاده خواهد شد. این واسط برای کارت آلفای بی‌سیم ما ساخته شده است.

خودتان آزمایش کنید: ایجاد واسط‌های حالت پایش چندگانه

می‌توان واسط‌های حالت پایش چندگانه را با استفاده از همین کارت فیزیکی ایجاد کرد. برای آگاهی از چگونگی انجام این کار می‌توان از ابزار airmon-ng استفاده کرد.

فوق‌العاده است! اینک یک واسط حالت پایش داریم که منتظر است بستک‌ها را از روی هوا بخواند.

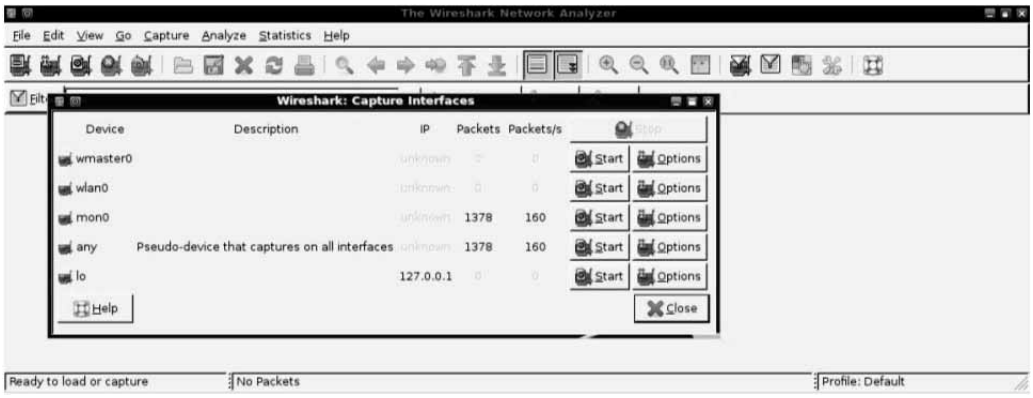
بنابراین بیایید شروع کنیم!
در تمرین بعدی، از وایرشارک برای شنود بستک‌ها در هوا با استفاده از واسط حالت پایش **mon0** که به تازگی ساخته‌ایم، استفاده خواهیم کرد.

آغاز کار: شنود بسکت‌های بی‌سیم

عملیات زیر را برای شروع شنود بستک‌ها دنبال کنید:

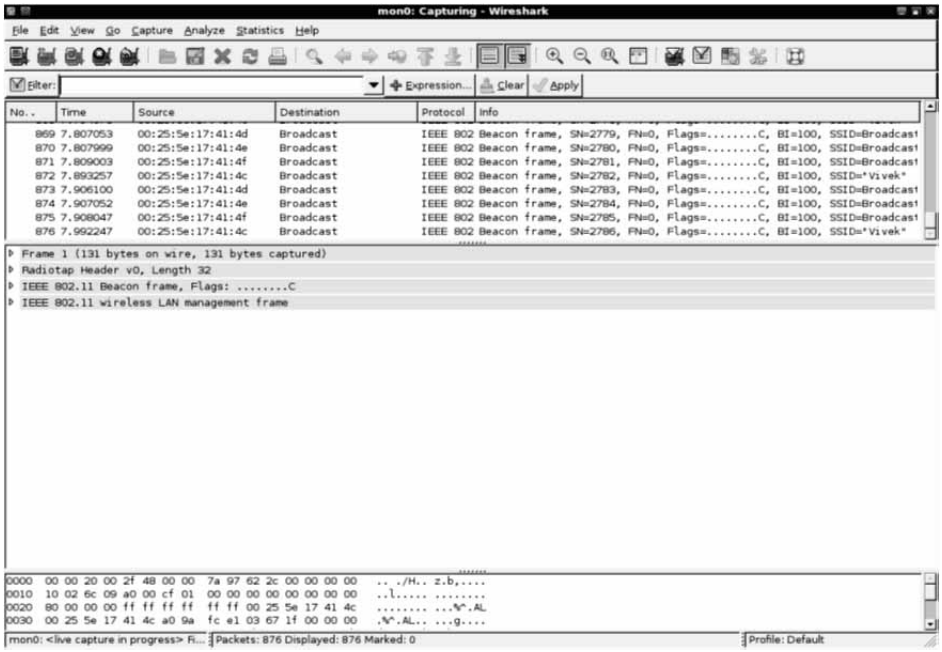
۱. اکسس‌پوینتمان Wireless Lab را که در فصل یک، راه‌اندازی آزمایشگاه بی‌سیم، پیکربندی کردیم روشن کنید.

۲. وایرشارک را با واردکردن دستور &Wireshark در کنسول اجرا کنید. درحالی‌که وایرشارک در حال اجراست، روی زیر منوی **Capture | Interfaces** کلیک کنید:

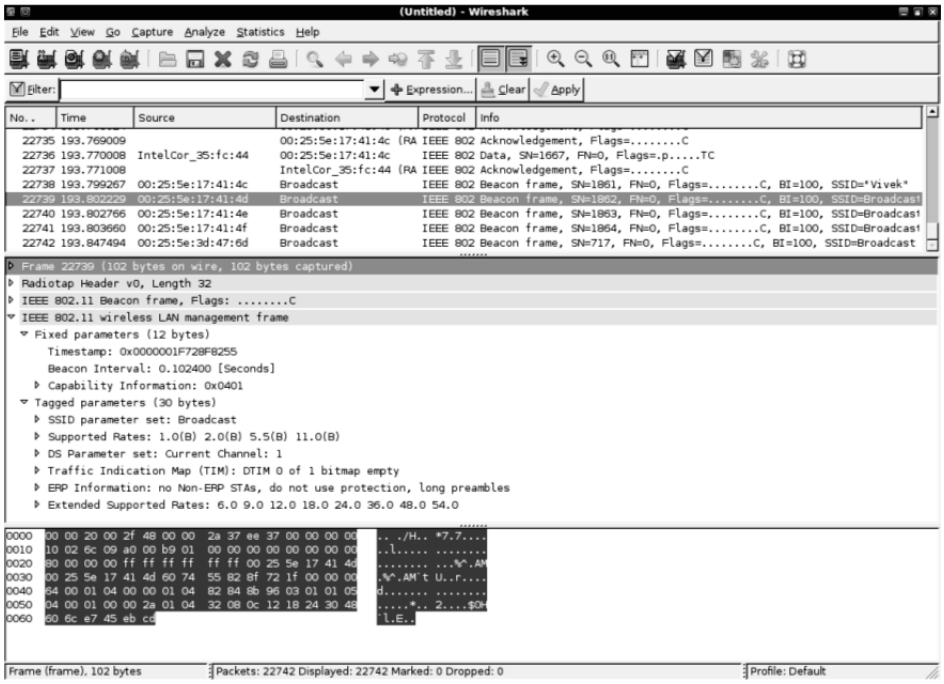


۳. با کلیک کردن روی دکمه‌ی **Start** در سمت راست واسط mon0، packet cap را از روی واسط mon0 همان گونه که در تصویر پیشین نشان داده شد انتخاب کنید. وایرشارک، دریافت[1] را شروع خواهد کرد و اینک باید بستک‌ها را در پنجره‌ی وایرشارک ببینید:

[1] capture



۴. این‌ها بستک‌هایی هستند که کارت بی‌سیم آلفای شما از هوا شنود می‌کند. برای اینکه هر بستکی را ببینید، آن را از پنجره‌ی بالا انتخاب کنید و کل بستک در پنجره‌ی میانی نشان داده خواهد شد:



۵. روی مثلث مقابل **IEEE 802.11 wireless LAN management frame** کلیک کنید تا باز شود و اطلاعات اضافی را ببینید.

۶. به فیلدهای سرآیند گوناگون در بستک نگاه کنید و با انواع فریم شبکه‌ی محلی بی‌سیم و زیر نوع‌های آن که پیش‌تر یاد گرفتید مطابقت دهید.

چه اتفاقی افتاد؟

نخستین مجموعه بستکمان را از هوا شنود کردیم! وایرشارک را راه انداختیم که از واسط حالت پایش **mon0**، که پیش‌تر ساختیم استفاده می‌کند. با نگاه کردن به بخش پایین وایرشارک متوجه سرعت دریافت و همچنین شمار بستک‌هایی که تا این لحظه دریافت شده‌اند می‌شویم.

خودتان آزمایش کنید: یافتن ابزارهای گوناگون

اثر[1]های وایرشارک ممکن است گاهی کمی ترسناک باشد و حتی برای یک شبکه‌ی بی‌سیم معمول، باید چندین هزار بستک را شنود کنید؛ بنابراین، مهم است که بتوانیم تنها روی بستک‌هایی که برایمان جالب هستند تمرکز کنیم. این امر با استفاده از فیلترها در وایرشارک امکان‌پذیر می‌شود. بررسی کنید که چگونه می‌توانید از این فیلترها برای شناسایی دستگاه‌های بی‌سیم خاص همچون اکسس‌پوینت‌ها و سرویس‌گیرنده‌ها در اثرها استفاده کنید.

اگر نتوانستید چنین کاری را انجام دهید، نگران نباشید چون این مطلب بعدی است که قرار است یاد بگیریم.

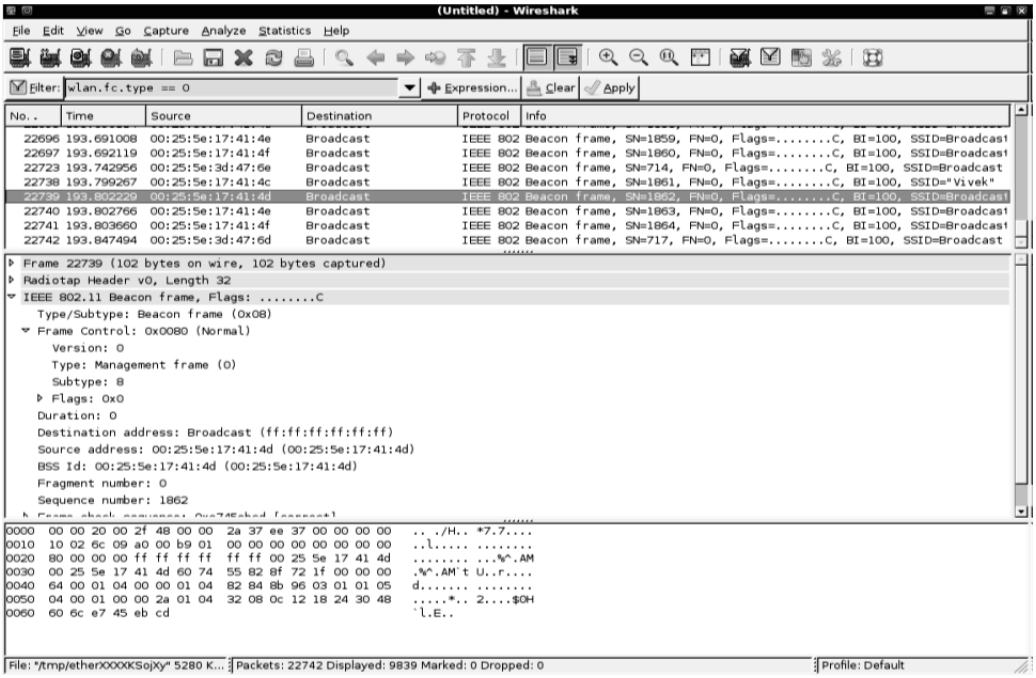
آغاز کار: مشاهده‌ی فریم‌های مدیریت، کنترل و داده

اکنون یاد خواهیم گرفت که چگونه در وایرشارک، فیلتر قرار دهیم تا فریم‌های داده، کنترل و مدیریت را ببینیم.

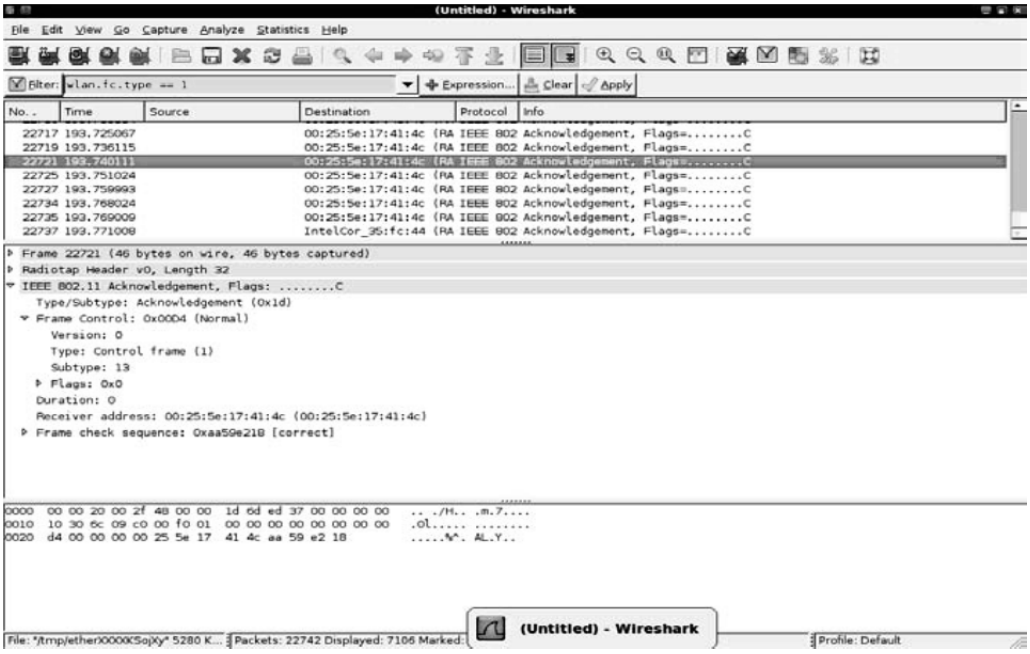
لطفا عملیات زیر را گام به گام دنبال کنید:

۱. برای نمایش همه‌ی فریم‌های مدیریت که در بستک‌های دریافت شده هستند، فیلتر **wlan.fc.type == 0** را در پنجره‌ی فیلتر وارد و روی **Apply** کلیک کنید. اگر می‌خواهید از حرکت سریع بستک‌ها به سمت پایین جلوگیری کنید، می‌توانید دریافت بستک‌ها را متوقف کنید.

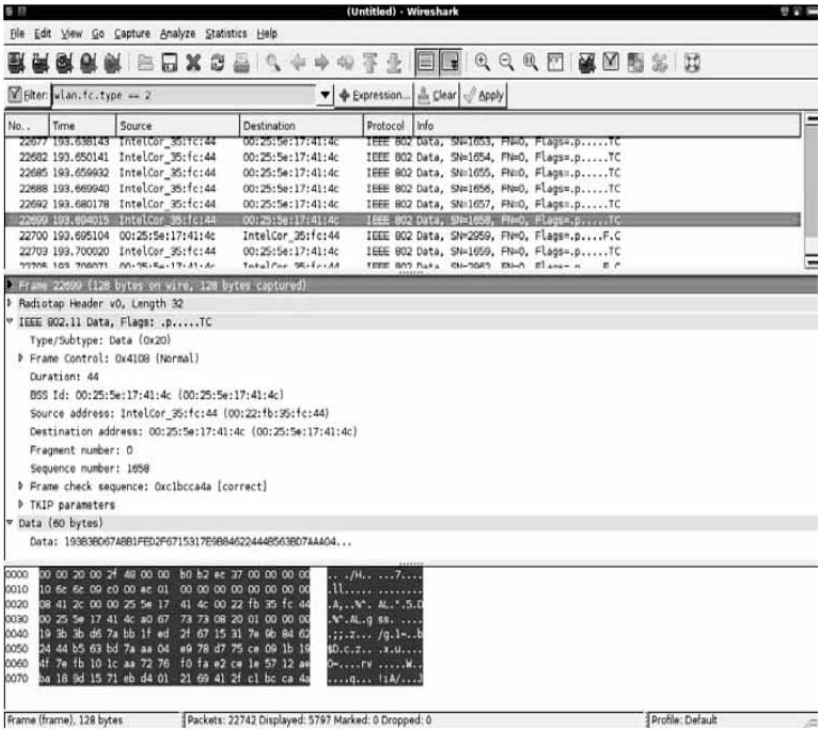
[1] trace



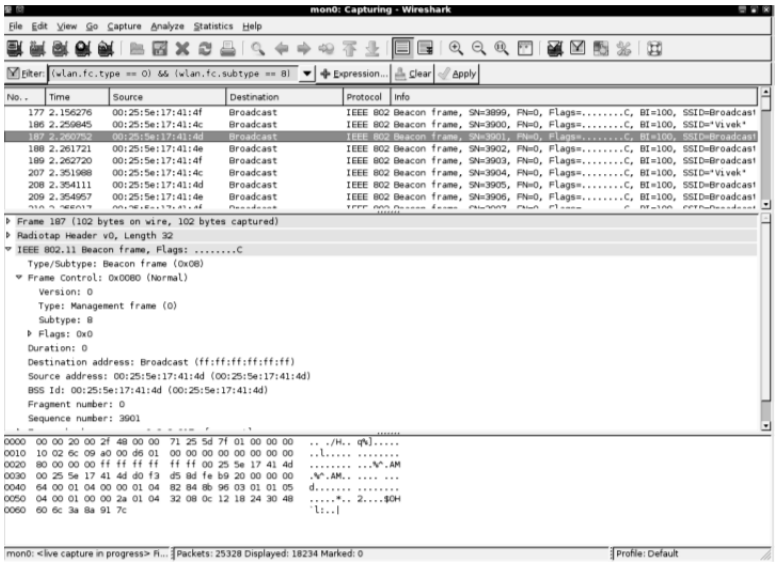
۲. برای مشاهده‌ی فریم‌های کنترل، عبارت فیلتر را به **wlan.fc.type == 1** تغییر دهید:



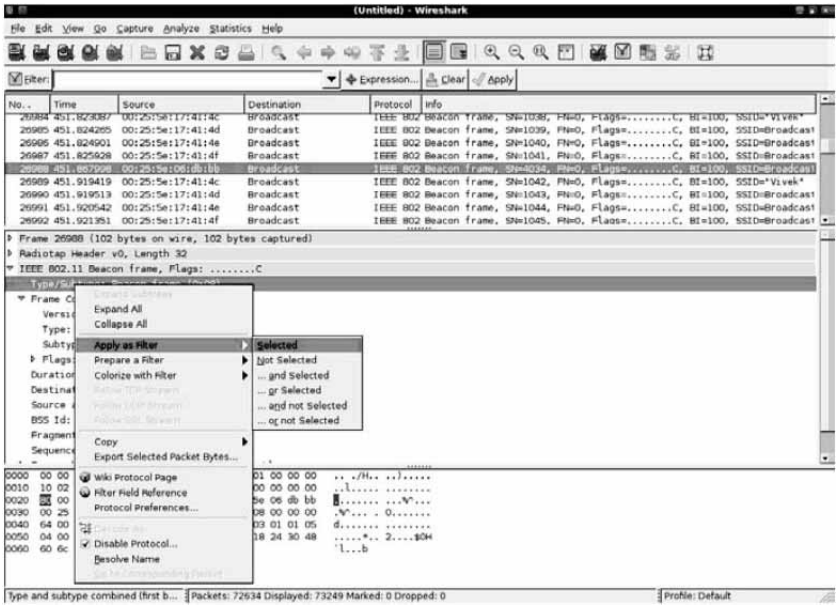
۳. برای مشاهده‌ی فریم‌های داده، عبارت فیلتر را به **wlan.fc.type == 2** تغییر دهید:



۴. افزون بر این، برای انتخاب یک زیر نوع، از فیلتر **wlan.fc.subtype** استفاده کنید. برای مثال، برای نمایش تمام فریم‌های Beacon در میان همه‌ی فریم‌های مدیریتی از فیلتر زیر استفاده کنید **(wlan.fc.type == 0) && (wlan.fc.subtype == 8)**.



۵. به جای آن، می‌توانید روی یکی از فیلدهای سرآیند در پنجره‌ی میانی، کلیک راست و سپس | **Apply as Filter** **Selected** را انتخاب کنید تا یک فیلتر به عنوان اضافه شود:



۶. همان‌گونه که نشان داده شده، این کار به طور خودکار عبارت فیلتر صحیح را برای شما در فیلد **Filter** اضافه می‌کند: