ایمن‌سازی شبکه‌های بی‌سیم خانگی و سازمانی

چگونه از شبکه وای‌فای در برابر یک حمله هکری محافظت کنیم؟

اگر می‌خواهید امنیت زیرساخت ارتباطی خود را ارزیابی کنید، هیچ تکنیکی بهتر از آن نیست که پیش‌قدم شده و شبکه ارتباطی خود را به شکل عملی ارزیابی کنید تا آسیب‌پذیری‌های احتمالی درون شبکه کشف شوند. در ادامه یاد خواهید گرفت که چگونه مشکلات امنیتی مستتر درون شبکه وای‌فای خانگی یا سازمانی‌تان را پیدا کنید.

ابزارهای کشف آسیب‌پذیری‌های وای‌فای به شکل رایگان یا تقریبا رایگان در شناسایی مشکلات امنیتی بالقوه و پیدا کردن راه‌حل‌هایی برای محافظت از شبکه در برابر مشکلات کمک می‌کنند. یکی از بهترین راهکارهایی که دید روشنی نسبت به سطح ایمنی شبکه وای‌فای در اختیارتان قرار می‌دهد، ارزیابی عملی امنیت شبکه وای‌فای است. در حالت عادی نمی‌توانید به سراغ شبکه سازمانی رفته و آن را هک کرده یا به سوءاستفاده از شبکه وای‌فای همسایه‌تان بپردازید، حتی اگر به‌طور شفاهی اجازه انجام چنین کاری داشته باشید. باید در قالب یک قرارداد معتبر و با ذکر تاریخ و زمان به دنبال انجام هک اخلاقی و انجام آزمایش‌هایی در چهارچوب قانون باشید و در صورت تمایل شرکت‌ها، با آن‌ها در زمینه ایمن‌سازی زیرساخت‌های ارتباطی‌شان قرارداد منعقد کنید. هرچه میزان شناخت و درک‌تان از مشکلات احتمالی وای‌فای بیشتر باشد، به همان نسبت بیشتر می‌توانید از مکانیزم‌های حفاظتی بهتر برای ایمن‌سازی شبکه وای‌فای استفاده کرده و ارتباطات امن‌تری را برای سایر دستگاه‌های بی‌سیم رقم بزنید.

Wi-Fi Stumbler ابزاری مناسب برای تشخیص مشکلات

این ابزارها برای تست ساده یک شبکه وای‌فای در دسترس قرار دارند و این امکان را می‌دهند تا اکسس‌پوینت‌ها و جزئیات مربوط به آن‌ها را همچون سطح و کیفیت سیگنال و مک آدرس‌ها مشاهده کنید. یک ابزار تحلیل‌گر شبکه‌های وای‌فای به شما در تشخیص مشکلات امنیتی شبکه‌ها همچون به‌کارگیری پروتکل‌های امنیتی ضعیف مانند WEP یا نسخه‌های اولیه WPA کمک کرده و اجازه می‌دهد، اکسس‌پوینت‌های غیرمجازی را که توسط کارمندان یا سایر افراد در یک سازمان ایجاد شده‌اند و می‌توانند راه را برای حمله به زیرساخت‌های ارتباطی سازمان هموار کنند، پیدا کنید. استامبلرها می‌توانند اکسس‌پوینت‌های پنهان را به‌سرعت پیدا کرده و به شما نشان دهند.
Vistumbler، یکی از معروف‌ترین ابزارهای تحلیل شبکه‌های وای‌فای ویژه سیستم‌عامل ویندوز است که به شکل متن‌باز در اختیار متخصصان قرار دارد و قادر است جزئیات اصلی اکسس‌پوینت‌ها را همچون روش‌های رمزنگاری و احراز هویت، سطح سیگنال و SSID نشان دهد. این ابزار از کیفیت و سطح سیگنال‌ها و کانال‌هایی که استفاده شده‌اند، نمودارهایی ارائه می‌کند تا فرآیند اشکال‌زدایی شبکه‌های وای‌فای به‌سادگی امکان‌پذیر باشد. Vistumbler کاملا سفارشی بوده و گزینه‌های متعددی برای پیکربندی در اختیارتان قرار می‌دهد. این ابزار با پشتیبانی از Google Earth و با استفاده از نقشه اجازه می‌دهد به‌صورت زنده شبکه‌ها را روی یک نقشه پیدا کنید. با توجه به این‌که Vistumbler از فرمان Netsh استفاده می‌کند، به‌راحتی می‌تواند کارت‌های شبکه را از یکدیگر تفکیک کند. برای آن گروه از افرادی که سیستم‌عامل مورد استفاده آن‌ها iOS یا اندروید است، ابزار دیگری به نام AirPort وجود دارد که

قادر است اطلاعاتی مشابه با Vistumbler را ارائه کند.
Wifi Analyzer، ابزار متن‌باز و رایگان دیگری است که ویژه پلتفرم اندروید ارائه شده است. این برنامه به شما در پیدا کردن اکسس‌پوینت‌های مبتنی بر گوشی‌ها یا تبلت‌های اندرویدی کمک می‌کند. این برنامه جزئیات اصلی مرتبط با اکسس‌پوینت‌ها را روی هر دو باند 2.4 و 5 گیگاهرتز به شکل فهرست شده ارائه کرده و اجازه می‌دهد فهرست اکسس‌پوینت‌ها را در فرمت XML برای برنامه ایمیلی خود یا سایر برنامه‌ها ارسال کرده یا اسکرین‌شاتی از فهرست ارائه شده، تهیه کنید. از دیگر امکانات این برنامه کاربردی می‌توان به ارائه نموداری که سیگنال‌ها را بر اساس کانال‌ها نشان می‌دهد و قابلیت اندازه‌گیری کیفیت و قدرت سیگنال‌ها به‌منظور پیدا کردن اکسس‌پوینت‌ها اشاره کرد.
دقت کنید، برای یک سازمان هیچ‌چیز بدتر از آن نیست که کارمندی یک هات‌اسپات شخصی ایجاد کند و دستگاه‌های مهم سازمان را به هات‌اسپات شخصی خود متصل کند.

ابزارهای بررسی وضعیت وای‌فای

این ابزارها فراتر از استامبلرها عمل می‌کنند و به‌جای آن‌که فقط جزئیات شبکه را جمع‌آوری کنند، جزئیات را ضبط و نمایش داده یا به تجزیه‌وتحلیل بسته‌های خامی می‌پردازند که از طریق امواج رادیویی ارسال شده‌اند. این ابزارها به شما اجازه می‌دهند ترافیک ضبط شده را برای ابزارهای تحلیل‌گر پیشرفته‌تر ارسال کنید تا اطلاعات دقیق‌تری به دست آورید. البته برخی از ابزارهای بررسی وضعیت به قابلیت‌هایی در ارتباط با تجزیه‌وتحلیل بسته‌های اطلاعاتی تجهیز هستند. برخی از نمونه‌های پیشرفته این ابزارها فقط برای نظارت بر ترافیک خاصی از شبکه استفاده می‌شوند. به‌عنوان مثال، زمانی که اطلاعاتی شبیه گذرواژه‌ها در قالب یک متن خام ارسال می‌شود، این ابزارها اطلاعات فوق را دریافت کرده و در قالب گزارشی در اختیار متخصصان قرار می‌دهند.
CommView یک ابزار بررسی وضعیت وای‌فای و تحلیل‌گری قدرتمند و محبوب است که به‌صورت تجاری عرضه شده و نسخه 30 روزه آن به شکل آزمایشی در دسترس متخصصان قرار دارد. ابزار فوق به قابلیت نشان دادن جزئیات شبکه، کانال‌های استفاده شده و ارائه نموداری برای این اطلاعات تجهیز شده است. این ابزار می‌تواند ارتباطات آی‌پی را بررسی کرده، جزئیات مربوط به هر نشست VoIP را ضبط کرده و همچنین گزینه‌هایی برای ضبط و مشاهده بسته‌های خام اطلاعاتی در اختیارتان قرار دهد.

مطلب پیشنهادی

یک استاندارد جامع و پرسرعت
مزایای وای‌فای 6 خرید یک روتر جدید را توجیه‌پذیر می‌کنند؟

اگر به یک شبکه وای‌فای متصل شوید و عبارت عبور PSK را درون برنامه وارد کنید، در ادامه، برنامه بسته‌های ارزیابی شده را به شما نشان می‌دهد. همچنین می‌توانید قواعدی را برای فیلتر کردن داده‌هایی که قصد مشاهده آن‌ها را دارید و هشدارهایی را برای زمانی‌که به دنبال دستگاه‌های غیرمجاز هستید، تنظیم کنید. Kismet، یکی دیگر از ابزارهای محبوبی است که به قابلیت ارزیابی بسته‌ها، سامانه تشخیص نفوذ و استامبلر شبکه مجهز است.
برنامه‌ای چندسکویی که روی پلتفرم‌های ویندوز (از طریق چهارچوب WSL)، سیستم‌عامل Mac OS X، لینوکس و BSD قابل اجرا است. ابزار فوق جزئیات دقیق یک اکسس‌پوینت و مواردی همچون SSIDهای پنهان شبکه را نشان می‌دهد. این ابزار اجازه می‌دهد بسته‌های بی‌سیم خام را ضبط کرده و در ادامه برنامه‌هایی همچون وایرشارک، TCPdump یا سایر ابزارهای مشابه را وارد کنید. Kismet، در ویندوز فقط با آداپتورهای بی‌سیم CACE AirPcap به دلیل محدودیت درایورهای ویندوز کار می‌کند. بااین‌حال، از انواع مختلف آداپتورهای بی‌سیم در Mac OS X و لینوکس پشتیبانی می‌کند.

ابزارهایی برای مشاهده جزئیات وای‌فای

WirelessKeyView، از شرکت NirSoft یک ابزار ساده اما کاربردی است که فهرستی از کلیدهای WEP، WPA و WPA2 یا عبارات عبور ذخیره شده در کامپیوتر ویندوزی را که از آن استفاده می‌کنید، نشان می‌دهد. درست است که کلیدهای ذخیره شده در سیستم‌عامل ویندوز 7 و نسخه‌های قبل از این سیستم‌عامل به‌سادگی قابل‌مشاهده بودند، اما مایکروسافت در ویندوز 10

فرآیند نمایش این اطلاعات را پیچیده‌تر کرده است. WirelessKeyView فهرستی از اطلاعات کاربردی مرتبط با شبکه‌ها را فارغ از سیستم‌عاملی که از آن استفاده می‌کنید، نشان می‌دهد. ابزارهایی شبیه WirelessKeyView می‌توانند نشان دهند که چگونه یک دستگاه به سرقت رفته یا چگونه هک شده و ممکن است اطلاعاتی به‌مراتب حساس‌تر از افشای اسناد را فاش کند. ابزار فوق به‌خوبی اهمیت استفاده از مکانیزم احراز هویت 802.1x را نشان می‌دهد، جایی‌که کاربران برای دسترسی به وای‌فای مجبور هستند، اطلاعات لاگین را به‌درستی وارد کنند. گزینه دیگری که در این زمینه در اختیارتان قرار دارد، Aircrack-ng است که در اصل مجموعه‌ای از ابزارهای منبع باز بوده که برای دریافت اطلاعاتی در ارتباط با WEP و WPA/WPA2-Key crack cracking استفاده می‌شود. این برنامه در ویندوز، مک OS X، لینوکس و OpenBSD قابل اجرا بوده و برای مشاهده شبکه‌های وای‌فای پیرامون‌تان، SSIDهای پنهان یا غیرپخشی و ضبط بسته‌های خام قابل استفاده است. ابزار فوق را می‌توان در قالب یک ایمیج VMware دانلود کرده و استفاده کرد.

توزیع‌های کاربردی لینوکس برای انجام ارزیابی‌های امنیتی

یکی از پرطرفدارترین توزیع‌های لینوکسی که برای انجام آزمایش‌های امنیتی از آن استفاده می‌شود، توزیع کالی است. توزیع فوق را می‌توان روی یک کامپیوتر نصب و از آن استفاده کرد یا یک دیسک قابل بوت از آن ایجاد کرده و استفاده کرد یا ایمیج‌های VMware یا VirtualBox آن را استفاده کرد. توزیع فوق شامل طیف بسیار گسترده‌ای از ابزارهای امنیتی و قانونی است که برخی از آن‌ها در زمینه آزمایش وای‌فای کاربرد دارند. به‌عنوان مثال، ابزارهای Kismet و Aircrack-ng و ابزارهای وای‌فای قدرتمند دیگری درون این توزیع قرار گرفته‌اند که از آن جمله می‌توان به Reaver برای بررسی شبکه‌هایی که از پین‌کدهای غیرایمن WPS استفاده می‌کنند، FreeRadius-WPE که توانایی یک شبکه را در برابر حملات مرد میانی و احراز هویت مبتنی بر 802.1X ارزیابی می‌کند و Wifi Honey که برای ساخت یک ظرف عسل برای به دام انداختن هکرها به‌منظور اتصال به یک اکسس‌پوینت جعلی از آن‌ها استفاده می‌شود، اشاره کرد.

مطلب پیشنهادی

نتورک‌پلاس دروازه ورود به دنیای شبکه
دانلود کتاب الکترونیکی Network+ راهنمای شبکه‌ها

از ابزارهای سخت‌افزاری غافل نشوید

اگر در مورد امنیت بی‌سیم و آسیب‌پذیری‌های مستتر در شبکه‌های وای‌فای سازمانی خود نگران هستید نباید از ابزارهایی همچون Wifi pineapple Tetra غافل شوید.
Wifi pineapple Tetra یک راه‌حل مبتنی بر سخت‌افزار است که به‌طور خاص برای بررسی وای‌فای و انجام آزمایش‌های مربوط طراحی شده است. ابزار فوق به‌منظور پویش، ردیابی، بررسی و گزارش‌گیری در ارتباط با تهدیدات و ضعف‌های شبکه استفاده می‌شود. WiFi Pineapple ظاهری شبیه یک روتر داشته و از یک رابط کاربری مبتنی بر وب استفاده می‌کند. ابزار فوق برای مشاهده جزئیات مربوط به دستگاه‌های کلاینت متصل به هر اکسس‌پوینت، ساخت اکسس‌پوینت‌های جعلی با هدف ارزیابی آسیب‌پذیری دستگاه‌های کلاینت در ارتباط با حملات مرد میانی یا رمزگشایی بسته‌های احرازهویت قابل استفاده است. ابزار فوق به شما کمک می‌کند تا میزان آسیب‌پذیری کاربران و دستگاه‌های کلاینت را در برابر حمله مسموم‌سازی سامانه نام دامنه با ایجاد یک DNS جعلی بررسی کنید.
Wifi pineapple، در حال حاضر دو گزینه سخت‌افزاری را در اندازه جیبی و تک‌بانده NANO به قیمت 99 دلار و یک نوع دو بانده را که ظاهری شبیه به یک روتر دارد، با قیمت 199 دلار عرضه کرده است.
لازم به توضیح است که Wifi pineapple Tetra به قیمت یک میلیون تومان در زمان نگارش این مقاله در فروشگاه‌های اینترنتی کشور عرضه شده است

تاریخ انتشار:

23 شهریور 1398

نشانی منبع:
https://www.shabakeh-mag.com/network-tricks/internet-tricks/16009/%DA%86%DA%AF%D9%88%D9%86%D9%87-%D8%A7%D8%B2-%D8%B4%D8%A8%DA%A9%D9%87-%D9%88%D8%A7%DB%8C%E2%80%8C%D9%81%D8%A7%DB%8C-%D8%AF%D8%B1-%D8%A8%D8%B1%D8%A7%D8%A8%D8%B1-%DB%8C%DA%A9-%D8%AD%D9%85%D9%84%D9%87-%D9%87%DA%A9%D8%B1%DB%8C-%D9%85%D8%AD%D8%A7%D9%81%D8%B8%D8%AA-%DA%A9%D9%86%DB%8C%D9%85%D8%9F