آموزش هک وایرلس : فاز شناسایی قدم ۱ : پیدا کردن شبکه های هدف حمله (نسخه PDF)

پس از سریال ۴ قسمتی پرداختن به انواع حملات در شبکه وایرلس لازم است در ادامه بحث به استانداردسازی هک وایرلس بپردازیم و این استانداردسازی جز با یاد گرفتن و درک مفاهیم مراحل روش شناسی، حاصل نمیشود. بی صحبت زیادی به موضوع میپردازیم،موضوعیت این فصل بخطر انداختن شبکه وای-فای به منظور بدست آوردن دسترسی غیرمجاز به منابع شبکه است.

هکرها معمولا- برای اطمینان از صحیح انجام دادن مراحل هک و پرهیز از اشتباه احتمالی، از روش شناسی هک برای انجام کار خود استفاده میکنند. پیدا کردن یک شبکه وای-فای و یا یک دیوایس وای-فای اولین قدمی است که هکر باید انجام دهد. در این مرحله معمولا از ابزاری چون NetSurveyor، WirelessMon، Vistumbler، Insider، Netstumbler و غیره استفاده میشود.

ردیابی (Footprint) شبکه وایرلس

حمله به یک شبکه وایرلس از جستجو و ردیابی یک شبکه وایرلس آغاز میشود. منظور از ردیابی پیدا کردن مکان و تحلیل(فهم) شبکه است. ردیابی شبکه وایرلس در به دو صورت میتواند انجام شود: روش پسیو و روش اکتیو ، برای ردیابی یک شبکه وایرلس اولین چیزی که مورد نیاز است، تشخیص BSS است که توسط اکسس پوینت ارائه میشود. BSS یا IBSS با کمک SSID شناسایی میشود. هکر از SSID استفاده میکند تا بتواند با اکسس پوینت ارتباط برقرار کند.

- **نکته: Basic Service Set** یا اختصارا BSS، بلوک ساختمانی یک شبکه محلی وایرلس بر مبنای استاندارد ۸۰۲.۱۱ را مشخص میکند. شاید برای شروع کار این جمله سنگین باشد. بسیار خوب تعریف را بر میگردانیم. در حالت ساختاری، یک اکسس پوینت به همراه تمام Station های مرتبط با آن(STA) را یک BSS مینامند. همانطور که در مقالات قبل گفته شد، Station هر نودی است که قابلیت وای- فای دارد و بصورت خاص میتواند هر دیوایسی باشد که شبکه وایرلس را Bridge میکند؛ مثل روتر. خوب به ادامه تعریف BSS بر میگردیم. باید دقت کرد که مفهوم BSS را با محدوده پوشش دهی اکسس پوینت (BSA) اشتباه نگرفت. در مفهوم BSS، اکسس پوینت به عنوان نقطه مرکزی عمل کرده و station ها را کنترل میکند. در ساده ترین مثالی که میتوان از BSS زد، میشود یک اکسس پوینت و یک Station را نام برد. در زیر بیشتر با دو روش ردیابی که در بالا به آن ها اشاره شد، میپردازیم:

روش غیرفعال(Passive)

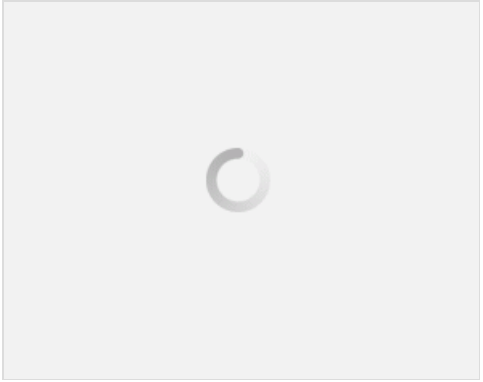
هکر از این روش برای تشخیص وجود یا عدم وجود اکسس پوینت استفاده میکند و برای اینکار راه شنود بسته های موجود در امواج معلق در فضا را پیش میگیرد که بخوبی اکسس پوینت، SSID و حتی دیوایس وایرلس هکر را که بصورت لایو (Live) درحال شنود است را نشان میدهد.

روش فعال (Active)

در این روش دستگاه وایرلس هکر یک درخواست کاوش به همراه یک SSID ارسال میکنند و منتظر میمانند تا ببینند که ایا اکسس پوینت عکس العمل نشان میدهد یا نه. در ابتدای کار دیوایس وایرلس هکر SSID را نداشته باشد، میتواند درخواست کاوش را با SSID خالی ارسال کند. در این حالت، اکثر اکسس پوینت ها درجواب با SSID خودشان پاسخ میدهند. بنابراین خالی گذاشتن جای SSID در درخواست کاوش در شناسایی SSID دیگر اکسس پوینت ها مفید و کارامد است. با این روش هکر میتواند BSS صحیح را متوجه شود. یک اکسس پوینت میتواند طوری پیکربندی شود تا درخواست های کاوش با SSID خالی را جواب ندهد.

پویش شبکه های وای-فای

هکرها میتوانند شبکه های وای-فای را بوسیله ابزارهای اسکن شبکه وایرلس مانند NetSurveyor، Retina Wi-Fi scanner و غیره پویش کنند. هدف از این پویش پیدا کردن SSID و متعاقب آن پیدا کردن BSS است. SSID در beacon، درخواست های کاوش و پاسخ های متناظرشان و در نهایت در درخواست های تشکلیل ارتباط و یا قطع ارتباط یافت میشود. هکر میتواند SSID شبکه را با استفاده از روش پسیو بدست آورد. وقتی که هکر توانست SSID را بدست آورد، میتواند به شبکه وایرلس وصل شود و حملات مختلفی را انجام دهد. پویش شبکه وایرلس، شنود را در کانال های مختلف رادیویی از دیوایس های مختلف مقدور میسازد.



پیدا کردن شبکه های وای-فای برای انجام حمله

اولین مرحله ای که هکر برای جستجوی هدف وای-فای خود انجام میدهد، بررسی شبکه های موجود در محدوده و انتخاب بهترین آن ها برای حمله است. برای پیدا کردن شبکه های وای-فای کافیست با یک لپ تاپ وای-فای روشن، در محدوده مورد نظر خودتان بگردید. توجه کنید که بر روی لپ تاپ مورد استفاده حتما باید ابزار جستجوی وایرلس نصب شده باشد. برای پیدا کردن شبکه های وای-فای، هکر به موارد زیر نیاز دارد:

- لپ تاپ با کارت شبکه وایرلس
- آنتن وای-فای اکسترنال
- برنامه های جستجو و کشف شبکه

بسیاری ابزار جستجو و کشف شبکه بصورت آنلاین وجود دارند که اطلاعات زیادی در رابطه با شبکه های وایرلس موجود در اطرافتان به شما میدهند. از جمله این ابزار میتوان به NetStumbler، NetSurveyor، inSSIDer و Vistumbler اشاره کرد.در ادامه این نکته قصد آشنایی بیشتر با ابزارهای معرفی شده و نحوه کار با آن ها را داشتیم که به علت تناقض با سیاست های سایت در رابطه با معرفی ابزارهای هک، از گذاشتن آن خودداری کردیم. در روزهای آینده با ادامه مراحل روش شناسی در هک وایرلس با ما همراه باشید. سربلند و مانا باشید

پایان

نویسنده: احسان امجدی

منبع: انجمن تخصصی فناوری اطلاعات ایران

محمد نصیری

لذت بردیم از مطلبت مهندس امجدی ، من فقط جثارتا برای تکمیل شدن موضوع یک نکته رو اضافه می کنم ، وقتی از حالت Passive در اسکن شبکه های وایرلس استفاده می کنید یعنی از امواج فقط شنود میگیرد و خودتون درخواستی رو به هیچ عنوان به Access Point ارسال نمی کنید ، اینکار باعث میشه هکر ناشناس باقی بمونه چون فقط شنود کرده ، در حالت Passive شنود کردن معمولا زیاد زمان می بره چون منتظر یک اتفاق هستیم که شاید و تاکید می کنم شاید یک IV درست رو بتونیم شنود کنیم ، اما Passive Scan خوبیش اینه که مهاجم ناشناس باقی می مونه چون هیچ Session ای با AP ایجاد نکرده ، برعکس این موضوع در Active Scan هست ، یعنی شما به AP سعی می کنید متصل بشید و بهش مرتب درخواست میدید و ازش جواب میخاید ، اینکار سرعت شنود شما رو بالا می برده از طرفی براحتی شما قابل شناسایی می شید ...

احسان امجدی

مهندس نصیری سپاس از نکته بجاتون. حق با شماست . در نکته بالا این موضوع رو زیاد بسط نداده بودم و فقط اشاره ای بهش شده بود. ممنون از این که مطالب رو مطالعه میکنید و در کامل شدن اون نهایت همکاری رو دارید.

مطلب اصلی