آموزش جلوگیری از هک وایرلس و شناسایی و جلوگیری از هک شبکه WiFi (نسخه چاپی)

همانطور که سـری مباحث را دنبال میکنید، تا اینجا درباره مفاهیم شبکه های وایرلس، رمزنگاری در وایرلس، حملات محتمل در شبکه های وایرلس، روش شناسی هک وایرلس و بحث هک در تکنولوژی بلوتوث صحبت کردیم. تمام این مفاهیم هرکدام به نوعی مارا در هک کردن و همچنین تست نفوذ گرفتن از شـبکه های وایرلس کمک میکننـد و بماننـد تیکه های پازل برای نتیجه گرفتن نیازمند درک و اسـتفاده از همه آن ها هستیم .

حالاـ میخواهیم در مراحـل آخر روش هـای پیشـگیرانه ای که کمـک میکننـد تـا حفره هـای امنیـتی موجود در بحث وایرلس و بلوتوث را بشناسـیم و پوشـش دهیم، را بشما معرفی میکنیم. پیشگیری، تمرینی در استفاده از چندین سیستم یا تکنولوژی امنیتی برای جلوگیری از تصادم در شـبکه است.این بخش به دوقسـمت روش های پیشگیری و تمرین هایی تقسیم میشود که میتوانند در برابر روش ها و تکنیک های مختلف هک از شبکه شما محافظت کنند.

چگونه در برابر هک بلوتوث، دفاع کنیم؟

بطور معمول نقائص و مشـکلات امنیتی در دوره های زمانی خاصـی توسط شـرکت های سازنده و متخصصان برطرف میشوند اما در اینجا قصد داریم راه هایی که یک کاربر عادی برای محافظت از ارتباط بلوتوث خود در برابر یک هکر آماتور میتواند انجام دهد را بیان کنیم:

- در حالت عادی، بلوتوث خود را خاموش نگه داریـد و فقط زمانی آن را روشن کنید که نیاز است و پس از آن بلافاصـله آن را خاموش نمایید.
- دیوایس خود را از جستجو مخفی نگه دارید (non-discoverable /hidden mode)
- هر درخواست غیرمنتظره و ناشناس را برای برقراری ارتباط بلوتوث قرارگیری یک دیوایس در لیست دیوایس های مورد اعتماد، قبول نکنید.
- از عبارت های غیرمنظم و پیچیده برای کلید پین جهت قراردادن یک دستگاه در لیست دیوایس های مورد اعتماد استفاده کنید.
- در بـازه های زمانی مختلف لیست دیوایس های مورد اطمینان (که بـدون کلیـد پین ارتباط برقرار میکننـد) را چک کرده و نام های مشکوک و یا ان هایی را که درباره ان ها مطمئن نیستید، پاک نمایید.
- همیشه هنگامی که ارتباط بلوتوث با کامپیوتر برقرار میکنید، از رمزنگاری (Encrypt) استفاده کنید.

چگـونه میتوان اکسـس پوینت غیر مجـاز را شـناسایی کرد و جلوی آن را گرفت؟

شناسـایی اکسـس پوینت های غیر مجازو جلوی فعالیت آن را گرفتن، از جمله وظایف مهمی است که در تامین امنیت یک شـبکه وایرلس باید اجرایی شود.

شناسایی اکسس پوینت غیر مجاز

اساسـا اکسـس پوینت غیرمجاز به آن اینترفیسـی اطلاق میشود که برای فعالیتش از سوی مـدیر شـبکه مجاز شـناخته نشود. مشـکلی که اینگونه اکسـس پوینت ها ایجاد میکنند این است که این دیوایس ها با سـیاست های امنیتی موجود در شبکه تناقض دارند. این موضوع باعث وجود یک اینترفیس ناامن در یک شبکه امن میشود. تکنیک های مختلفی برای شناسایی اکسس پوینت غیر مجاز وجود دارد که در زیر به آن ها اشاره خواهیم کرد:

- **اسکن فرکانس رادیویی:** برای انجام این اسـکن،هـدف از پیش تعین شده اکسـس پوینت ها که فقط بسـته های داده را رکورد کرده و بـا سـنسورهای فرکـانس رادیویی خود آن هـا را تحلیـل می کننـد، این قرار داده میشود که از طریق اتصال به شـبکه کابلی، هرگونه دیوایس وایرلس را که در محیط فعالیت میکنـد، شـناسایی کرده و به مـدیر شـبکه اطلاع دهد. این سـنسورها در نواحی به اصطلاح مرده (dead zone, dead spot) بدرستی کار نمیکنند و آن ها را پوشش نمیدهند. نواحی مرده به مناطقی اطلاق میشود که فرکانس های رادیویی در آنجا با هم تـداخل داشـته یا بر اثر وجود مانعی نمیتواننـد به آن جا نفوذ کنند. اگر میخواهیم که اکسـس پوینت ها نواحی مرده را نیز شناسایی کرده و تحت پوشش خود قرار دهند، نیاز به سنسورهای بیشتری داریم.

- **اسکن اکسس پوینت:** اکسـس پوینت ها میتوانند اکسـس پوینت های همسایه و فعال در اطراف خود را شـناسایی کنند و داده هـای انتقالی آن ها را از طریق اینترفیس وب و MIB هابیینند. MIB یا همان Management Information Base، مرکز داده ایست برای مدیریت داده های ورودی در ارتباطات شـبکه. نقطه ضـعف این حالت این است که توانایی اکسس پوینت ها در شناسایی دیوایس های همسایه خوددر یک محیط مشخص، محدود است و صد در صدی نیست.
- **نرم افزار مدیریت شبکه:** از این تکنیک برای شناسایی اکسس پیونت های غیر مجاز استفاده میکنند. این نرم افزار دیوایس هایی را که از طرق مختلف مثـل SNMP، Telnet و CDP(پروتکل شـناسایی سیسـکو) و با استفاده از پروتکل های مختلف به شبکه محلی متصل هسـتند، شـناسایی میکند. صرفنظر از مکان فیزیکی، اکسس پوینت ها هرجای شبکه که باشند با این روش شناسایی خواهند شد.

جلوگیری از فعالیت اکسس پیونت غیرمجاز

اگر در اسـکن هـای خود هرگونه اکسـس پوینت غیرمجاز را پیـدا کردیـد، سـریعا بایـد قبل از ایجاد اختلال در ارتباط کاربران مجاز، جلوی فعالیت آن را بگیرید. این کار از دو روش میتواند انجام شود:

- با انجام حمله DoS جلوی ارائه سرویس وایرلس غیرمجاز به کلاینت ها را بگیرید.
- جلوی پورتی را که اکسـس پوینت به آن متصل است بگیرید و یا این که بصورت دستی و فیزیکی اکسـس پیونت را از شبکه خارج کنید.

چگونه باید در برابر حملات وایرلس، دفاع کرد؟

در کنار اسـتفاده از ابزار مانیتورینگ امنیت وشبکه وایرلس، کاربران میتوانند با بکارگیری برخی از راه کارها از شبکه شان در برابر تهدیدات و حملات مختلف دفاع کنند. در زیر به برخی از این راه کارها اشاره میکنیم:

- پس از پیکربندی شبکه وایرلس، SSID پیش فرض را عوض کنید.
- برای دسترسی به روتر یا اکسس پیونت رمز عبور بگذارید و برای حفاظت از آن، فایروال را فعال کنید.
- انتشار SSID را غیرفعال کنید.
- دسترسی ریموت به اکسس پوینت و مدیریت وایرلس را غیرفعال کنید.
- بر روی اکسس پوینت و یا روتر شبکه، مک فیلترینگ راه اندازی کنید.
- رمزنگاری را روی اکسس پوینت فعال کرده و پس از آن عبارت عبور را عوض کنید.

با تغیر تنظیمات SSID به حـداکثر مرحله امنیت، میتوان در برابر تهدیدات و حملات مختلف شـبکه را بیمه کرد. در زیر انحصارا به راه های بالا بردن امنیت SSID اشاره میکنیم:

- برای جلوگیری از انتشارSSID برای هرکسی، باید آن را پنهان کرد.
- برای تعیین نام SSID هرگز از نام های قابل حدس مانند نام شرکت، نام شبکه و غیره استفاده نکنید.
- در بین مسـیر اکسـس پوینت با ورودی اینترت به شبکه، از فایروال یا هرگونه دیوایسی که بسته ها را فیلتر میکنند (فیلتر به معنای بازرسی بسته ها) باید استفاده کرد.
- پوشـش سراسـری سـیگنال های وایرلس را بایـد به انـدازه محدوده شـرکت خود، محدود کنید تا کسـی نتواند از بیرون شـرکت به

وایرلس وصل شود.

- دیوایس های وایرلس را از لحاظ پیکربندی و تنظیمات درست بررسی کنید.
- از تکنیک های مختلف مقل IPSec برای رمزنگاری ترافیک استفاده کنید.

قراردادن احراز هویت قوی در دسترسـی به شبکه های وای-فای میتواند به عنوان یک راه پیشگیری در برابر تهدیدات و حملات مختلف در نظر گرفته شود:

- بجای استفاده از WEP از WPA استفاده کنید.
- در صورت امکان و در هرجایی که مقدور بود، WPA۲ را اجرایی کنید.
- در مواقعی که به شبکه نیاز ندارید، آن را غیرفعال کنید.
- دیوایس اکسس پوینت را در یک مکان امن قرار دهید.
- تمام درایورهای موجود را بر روی تجهیزات وایرلس، بروز نگه دارید.
- برای احراز هویت از سرور مرکزی مثل RADIUS استفاده کنید.

بسـیاری از تکنیک های دفاع در شـبکه وایرلس به نسـبت انواع حملاتی که ممکن است بر علیه شبکه وایرلس انجام میشود، طراحی شده اند. بنابراین استفاده از مکانیزم های امنیتی در جای درست خودمیتواند بخوبی در برابر حملات از شبکه شما محافظت کنند.

خوب دوسـتان عزیز. در این ایسـتگاه هم با روش های گرچه بعضا ساده ولی کارای محافظت از شـبکه وایرلس، آشـنا شدیـد. تا پایان این فصل از سرفصل های دوره CEH چیزی نمانده است که امیدوارم با همراهی شما دوستان عزیز، آن را نیز به پایان برسانیم.

سربلند و مانا باشید

پایان

نویسنده: احسان امجدی

منبع: انجمن تخصصی فناوری اطلاعات ایران

مهران سیفعلی نیا

ممنون از مطالبتون.

من شـنیدم که رمزهایی که با الگوی WEP رمزگـذاری میشن رو میشه در عرض چند ثانیه،نهایت چند ساعت هک کرد،بدون نیاز به نرم افزارها و تجهیزات خاص.

ولی الگوی WPA/WPA۲ رو میشه از چند ساعت تا چند روز هک کرد،اون هم با نرم افزار ها و تجهیزات خاص.

سوالی که من داشتم اینه:

میگن اگه در الگوی WPA//WPA۲ از کلماتی که در فرهنگ لغت انگلیسی موجود هست(Apple,Hello,Killer) و یا از اسامی(John) و یا از الگوی‌تو‌های یک نواخت(۱۲۳۴۵۶۷۸۹ یا ۲۴۶۸ یا ۱۱۱۱۱۱۱۱) استفاده بشه میشه در عرض چند ثانیه رمز تجهیزات به رمز درست برسد یا

الگوریتمهای یک نواخت(۱۲۳۴۵۶۷۸۹ یا ۱۱۲۲۸ یا ۱۱۰۰۱۱۰۰۱۱۰) استفاده بشه،میشه در عرض چندثانیه بدون تجهیزات به رمز دست پیدا کرد که به عنوان عیبب روش رمزگذاری WPA/WPA۲ شناسایی شده.

میخواستم بپرسم که شما در این مورد چیزی میدونید و اینکه دلیل این اتفاق چیه؟

احسان امجدی

ممنون مهران جان بابت سوالت. خوب برای پیـدا کردن مقـدار (ارزش)یک کلیـد رمز، دو روش کلی وجود داره.. یا باید مقدار کلید رمز بعـدی رو از روی قبلی حدس زد (کاملا شانسـی)و یا بر اساس مشاهداتی، پیش بینی کرد. یکی از ابتدایی ترین روش های پیش بینی یک عبارت روش Brute force هستش که با روش دیکشنری انجام میشه. یعنی این که هکر میاد بر اساس یک دیکشنری جامع از انواع ارزش ها و مقادیری که بر طبق الگوریتم های خاصـی وجود دارند، یکی یکی اونا رو به عنوان پسورد و یا کلید رمز تست میکنه تا ببینه کدوم جواب میده. (دقیقا مثل شاه کلید)

خوب همونطور هم که گفتی کلمات و عبارات واضـحی مثل اون چیزی که شـما مثال زدی، جزو بدیهیات یک دیکشـنری هستش و در عرض صدم ثانیه ممکنه پیش بینی بشه...

واسه همینم هست که توصیه میشه همیشه پسوردها رو از عبارات ترکیبی غیر مرتبط و بی ربط و همچنین پیچیده انتخاب کرد.

درباره کلید رمز هم باید بگم که در WEP چون از یک الگوریتم برای رمزنگاری همه بسته ها استفاده میشه، براحتی میشه با مانیتورینگ یک سری از بسته های رمز شده به الگوریتم اون پی برد.

اما در WPA و WPA۲ اینطوری نیست و کلیـد رمز با اسـتفاده از الگوریتم و پارامترهای مختلف و متغیر (تصادفی)ایجاد میشه. یعنی با مانیتورینـگ و کپچر یـک سـری از بسـته ها نمیتونی به ترتیب و الگوریتم قطعی تولیـد کلیـد رمز پی ببری چون هیـچ ربطی بینشون نیست.

پس زمانی پروتکل WPA و WPA۲ بهتر از WEP هستند که شما از تمام قابلیت هاشون استفاده کنی. در ضمن تمام این پروتکل ها برای رمزکردن بسته /فریم داده هاست و ربطی به پسورد SSID ندارند.

مطلب اصلی