" امنیت شبکه های وایرلس "

Wireless security

مطابق دیگر مقاله های اینجانب همیشه سعی بر این بوده که بدور از تئوریات به اصل مطالب بپردازم ولی در این مقاله نیاز می باشد تئوریات زیادی بیان کنم که فهم مطالب روان تر شکل گیرد ، فعالیت چند ساله من در زمینه نفوذ به شبکه های وایرلس و تجارب مختلف به برآیندی در زمینه امنیت رسیده که بتوان امنیت قابل قبولی را در یک شبکه وایرلس اعمال کرد چرا که همیشه عقیده ام بر این بوده که " یک امنیت کار زمانی خوب است ، که با اخرین متدهای هکینگ آشنا باشد یا به اصطلاح یک هکر خوب باشد "

در ابتدا لازم است که تعریفی از شبکه های وایرلس داشته باشیم

شبکه وایرلس به کاربر اجازه می دهد که به یک شبکه محلی یا اینترنت وصل شود در واقع بسته های اطلاعات بوسیله امواج الکترو مغناطیس پراکنده شده و با استفاده از هوا بعنوان واسط انتقال ، منتقل می شوند

پس قابلیت اتصال به داده ها و رد و بدل کردن اطلاعات بدون نیاز به روند پرهزینه کابل کشی با کیفیت مشابه انتقال دیتا در شبکه های کابلی عواملی هستند که باعث گسترش و تکامل این نوع شبکه ها (وایرلس) گردید.

بنابراین اگر این ابزار بتواند به طور فیزیکی در یک شبکه ناحیه محلی (LAN) و یا شبکه ناحیه گسترده (WAN) بدون نیاز به هر گونه ارتباطات فیزیکی اطلاعات دیتا را جابه جا کند وایرلس است

استفاده هر روزه توسط افراد مختلف در کل دنیا باعث نیاز ها و مشکلاتی گردیده که در اولویت آنها امنیت این نوع شبکه ها دیده می شود در همین خصوص و در جهت بهبود امنیت این شبکه ها قدم های بسیاری برداشته شده و ابزارهای امنیتی چشم گیری هم روانه بازار شد که امنیت این نوع شبکه ها را بیش از پیش افزایش داده است.

- اما در این لحظه یک سوال پیش می آید که آیا همین ابزارها و انتخاب یک پروتکل امن برای امنیت یک شبکه وایرلس کفایت میکند یا خود کاربر هم باید محدودیت هایی اعمال کند؟

جواب این سوال رو یقینا با خواندن ادامه مباحث خواهید یافت

پروتکل امنیت در شبکه های wlan بر سه نوع می باشند :

Wired Equivalent Privacy (**WEP**)

Wi-fi Protected Access (**WPA**)

Wi-fi Protected Access II (**WPA2**)

که یقینا شبکه وایرلس ما از یکی ، از این پروتکل ها استفاده میکند ، راحترین روش برای اینکه متوجه شویم از چه پروتکل امنیتی در حال استفاده هستیم کافی است موس خود را روی شبکه وایرلس مورد نظر نگه داریم بدون هیچگونه واکنش کلیکی از موس ، نوع پروتکل برای ما مشخص خواهد شد همانند تصویر زیر :

برای اینکه متوجه شویم کدام پروتکل امنیت بالاتری دارد

لازم است در ابتدا پروتکل ها رو بشناسیم

پروتکل امنیت WEP :

به جرات میتوان گفت ضعیف ترین پروتکلی که از نظر امنیتی که در شبکه های وایرلس وجود دارد پروتکل WEP می باشد. کدها در این پروتکل بر دو اندازه می باشند ۴۰ بیت و ۱۰۴ بیت

در ابتدا همیشه از ٤٠ بیت استفاده میشد و تولید کنندگان هم معمولا کدهای ٤٠ بیتی را فراهم میکردند با پیشرفت و استاندارد های حاکم کدهای ٤٠ بیتی این نوع پروتکل بطور مسخره ای کوچک بودن و همین عامل باعث افزایش کدهای ١٠٤ بیتی گشت .

نفوذ به این نوع پروتکل ها در کمترین زمان ممکن امکان پذیر می باشد چرا که هیچگونه کریپت (رمزنگاری) قوی روی پکت ارسالی در فضا اعمال نشده و براحتی میتوان با شنود ترافیک در زمانی حتی کمتر از پنج دقیقه به پسورد دسترسی پیدا کرد که این فاجعه ای بزرگ محسوب می شود فقط کافی است IV به تعداد کافی برسد تا هکر پسورد را درون آن پیدا کند.

براحتی میتوان با ابزارهایی همچون airodumping عملیات تزریق ترافیک رو انجام داد و از aireplaying برای افزایش میزان دیتا جهت بدست آوردن پسورد استفاده کرد البته airecrack هم جزو ابزارهای مهم این زمینه است معمولا فراهم کنندگان خدمات اینترنت (ISP) از این پروتکل بیشتر استفاده میکنند زیرا نمیتوانند از WPA پشتیبانی کنند.

به هیچ عنوان حتی اگر تمامی ابزارهای امنیتی برای شبکه های وایرلس تان را هم اعمال کردید از این پروتکل استفاده نکنید بدلیل اینکه امنیت بسیار بسیار ضعیفی دارد و لو رفتن پسورد نه تنها ضرر مالی میرساند بلکه موجب ضرر های فاجعه آمیز دیگری از جمله از دست دادن اطلاعات و پسورد های شخصی و سوء استفاده با اینترنتی که به مالکیت شما ثبت گردیده است می شود.

در تصویر زیر عملیات نفوذ به دو شبکه وایرلس که از پروتکل امنیت WEP استفاده میکند مشخص گردیده که در زمان کمتر از ٣ دقیقه و ٨ دقیقه توانست پسورد آن شبکه را بدست آور

پروتکل امنیت WPA/WPA2 :

این نوع پروتکل امنیت شبکه های وایرلس را بسیار بهبود بخشیده و WPA2 فناوری امنیتی بسیار بالاتری نسبت به WPA دارد که در ادامه بررسی خواهیم کرد.

معمولا حملات به پروتکل های WPA به چهار صورت انجام میپذیرد

۱-هندشیک چهار طرفه (four-way handshake)

۲- بافراورفلو (buffer over flow)

۳-برات فورس (brut force)

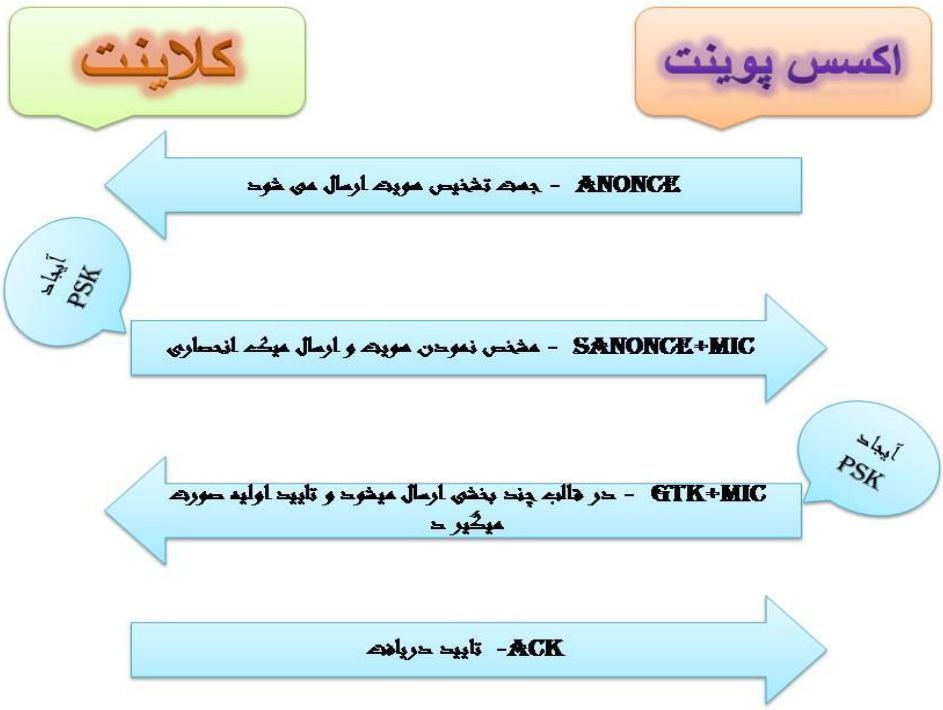
٤-شنود ترافیک (packet sniffer)

بهترین روش برای بدست آوردن پسورد در این پروتکل ها استفاده از روش "بافراورفلو" می باشد ولی بدلیل اینکه به سختی میتوان ابزارهایی پیدا کرد که از روش بافر پسورد را بگیرند از روش های "هندشیک" و "برات فورس" به مراتب بیشتر استفاده میشود از روش "شنود ترافیک" دقیقا عکس پروتکل WEP بسیار کمتر استفاده میشود چرا که در این پروتکل پکت ها و ترافیک بصورت بسیار قوی کریپت (رمزنگاری) شده اند.

در ادامه مباحث برای بهتر متوجه شدن مفهوم به توضیحاتی در خصوص چهار روش فوق میپردازیم

دست دادن چهار طرفه : (four-way handshake)

این روش بیشتر ارتباط بین کلاینت و اکسس پوینت رو میرساند ، یک تصویر طراحی کردم که برای درک بهتر مفهوم کمک شایانی میکند



در زیر هم یک نمونه حمله به شبکه های وایرلس به روش هندشیک مشخص شده

خب همانطور که در تصویر مشخص است نوع حمله بروش هندشیک است که در آن کلاینت و مک انحصاری به تایید میرسد در این نوع حمله اگر تعداد کلاینت ها بیشتر یافت شود احتمال موفقیت بیشتر می شود.

۲- بافراورفلو (buffer over flow)

این روش یک روش تضمینی است که تقریبا می شود گفت که میتواند یک شبکه وایرلس با هر امنیتی را مورد تهدید قرار دهد چرا که از روش بافر کردن مودم پسورد را بدست می آورد

در این روش ابتدا هکر با استفاده از ارسال پکت های زیاد به سمت مودم هدف باعث می شود بافر یا حافظه جانبی مودم پر شود و به مرحله سر ریز برسید "over flow" و مودم در عرض چند ثانیه در این حالت گیج می شود و هکر از همین زمان نهایت استفاده را میبرد و از مودم درخواست میکند که پسورد خود را در اختیارش قرار دهد و از آنجایی که مودم در آن حالت نمی تواند تشخیص دهد که این دستور از طرف ادمین می باشد یا یک غریبه (هکر) دستور را بدون هیچ محدودیتی اجرا میکند و هکر پسورد آن شبکه را بدست می آورد .

معمولا این روش یک پروسه زمانی چند ساعته است ولی احتمال موفقیت را در حد قابل توجهی بالا میبرد

در تصاویر زیر دو حمله بروش بافر اور فلو برایتان تهیه کردم که ساعات مختلفی برای بدست آوردن پسورد زمان برد

۳-برات فورس (brut force)

این روش بر اساس حدس و گمان عمل میکند به این منظور که شما در ابتدا رمز عبورهایی که حدس میزنید شاید بعنوان پسورد انتخاب شود را در یک فایل (دیکشنری لیست) نگه داری میکنید و بوسیله ابزارهایی که در این زمینه هستند تک تک آن رمزهای عبور احتمالی شما روی آن شبکه وایرلس تست میگردد خب همانطور که از روش مذکور مشخص هست احتمال موفقیت به مراتب پایین تر از دو روش فوق می باشد.

یکی از قدرتمندترین ابزارها در زمینه برات فورس airecrack می باشد.

٤-شنود ترافیک (packet sniffer)

نوع حمله در این روش همانند حمله به پروتکل WEP می باشد ولی بدلیل اینکه در پروتکل های WPA پکت ها بصورت حفاظت شده ای ارسال می شوند و کریپت (رمزنگاری) قوی را در خود می بینند به مراتب موفقیت را پایین تر می آورد آنقدر پایین که روش برات فورس به آن ترجیح داده می شود.

"ما تا اینجا با شبکه وایرلس آشنا شدیم و متوجه شدیم که به چه روش هایی احتمال نفوذ به شبکه وایرلس ما وجود دارد و این نفوذ چه پیامدهایی فاجعه آفرینی برای ما میتواند داشته باشد حال به امنیت این شبکه ها میپردازیم و بصورت نکته به نکته شبکه خود را محدود و محدودتر میکنیم تا نفوذ برای هکر به مراتب سخت و سخت تر شود"

۱- تغییر به پروتکل امنیتی WPA2

۲- انتخاب رمزعبوری امن برای شبکه وایرلس

۳- تغییر پسورد Default مودم

٤- غیر فعال کردن WPS

٥- استفاده متداول از برنامه WHOIS ON MY WIFI

٦- فیلتر کردن اتصال به MAC

۷- استفاده از AES رمزنگاری شده بجای TKIP

۸- استفاده از Shieldeville

۹- SNIFF شبکه وایرلس بوسیله KISMET

- تغییر به پروتکل امنیتی WPA2

WP2 یکی از بهترین گزینه انتخابی برای ماست چرا که نسبت به دیگر پروتکل های امنیتی ، امنیت بالاتری دارد و زمان قابل توجه و چشم گیری را از مهاجم برای بدست آوردن پسورد میگیرد.

زمان ممکن برای بدست آوردن و نفوذ به این پروتکل ها بین ٦ ساعت تا چند روز متغیر است و دقیقا همین عامل باعث می شود که نفوذگر معولا از این پروتکل ها اجتناب می کند.

- انتخاب رمزعبوری امن برای شبکه وایرلس

همانگونه که در این مقاله بیان کردم ، یکی از روش های نفوذ برات فورس و حدس زدن پسورد است اگر پسورد شما امنیت لازم را نداشته باشد و براحتی قابل حدس زدن باشد یک هکر براحتی میتوانند پسورد شما را بدست آورد.

خیلی از افراد از پسوردهایی از قبیل شماره تلفن همراه و یا شماره ملی استفاده میکنند که تعداد قابل توجهی هم از آنها یافت میشود که با این تفکر که هیچکدام از افرادی که نزدیک به شبکه وایرلس من هستند شماره همراه من را ندارند یا به هر شکل به کد ملی من دسترسی ندارند یک حاشیه امن برای خودشان ایجاد میکنند در صورتی که یک هکر هیچ نیازی به دانستن شماره شما ندارد معمولا دیکشنری لیست هایی (پسورد لیست)که در اختیار هکر ها قرار دارند ، مجموع حجم عظیمی از اعداد هستند یعنی اعداد که از صفر شروع میشوند و تا ۱۵ رقم بصورت کامل ترتیبی و پشت سر هم ادامه پیدا میکنند و بخواهم واضح تر بیان کنم هیچ عددی که از صفر شروع شود و تا ۱۵ رقم ادامه داشته باشد وجود ندارد که درآن پسورد لیست هکر قرار نداشته باشد چه شماره تلفن ، چه تاریخ تولد و چه شماره ملی و ....

ضمن اینکه پسورد لیست تنها به شماره ها خلاصه نمیشود بلکه سرشار از اسامی و پسوردهای احتمالی گنجانده شده است پس امنیت پسورد شما همیشه در خطر است پیشنهاد من انتخاب پسوردی است که از حروف کوچک و بزرگ همراه با عدد و سمبل در پسورد موجود باشد و

لازم به ذکر است پسورد های بالاتر از ۱۵ کاراکتر در شبکه های وایرلس به سختی کرک میشوند پس سعی در این داشته باشید که پسوردی بالاتر از ۱۵ کاراکتر انتخاب کنید که پسوردی امن برای وایرلس خود ایجاد کنید.

نباید از این نکته هم گذشت که تغییر مرتب پسورد کمک شایانی در امنیت هر چه بیشتر میکند.

- تغییر پسورد Default مودم

مودم ما دارای یک پسورد Default می باشد که ما با یوزر و پسورد admin میتوانیم به مودم خود لاگین کنیم هکر براحتی میتواند با بدست آوردن آی پی ولید شما و بوسیله پسورد دیفالت به مودم شما لاگین کند و براحتی به پسورد شبکه وایرلس شما دسترسی پیدا کند در اولین زمان ممکن حتما پسورد Default مودم خود را به پسوردی امن تغییر دهید

- غیر فعال کردن WPS

این گزینه معمولا برای امنیت شبکه های وایرلس هست اگر در تمامی سایت های اینترنتی هم جستجو کنید فقط چیزهای مختلف در خصوص امن کردن از این ابزار می شنوید بعنوان مثال یکی از تعاریف بدین صورت می باشد:

"Wi-Fi Protect Setup مکانیزمی است که به طور خودکار اطلاعات تبادلی میان دستگاه‌های وای‌فای را رمزنگاری و امن می‌کند. این مکانیزم شامل تعریف رمز عبور، انتخاب پروتکل رمزنگاری، اعتبارسنجی دستگاه‌های گیرنده و فرستنده اطلاعات و... است.در حقیقت، تمامی کارهایی که باید یک کاربر به طور دستی برای امنیت شبکه بی‌سیم انجام دهد، با زدن یک کلید انجام می‌گیرد. توجه کنید که تمامی دستگاه‌های درون شبکه شما باید از WPS پشتیبانی کنند. "

اما همین عوامل ، من را به گفتن مجدد این جمله ترغیت میکند که زمانی میتوانید یک امنیت کار خوب باشیدکه یک هکر خوب بوده باشید .

زمانی که شما از فناوری WPS استفاده میکنید ، آسیب پذیرهایی که این فناوری دارد زمینه مناسبی برای فعالیت هکر ایجاد میکند که کمک شایانی برای نفوذگر محسوب می شود و به جرات اعلام میکنم که هر شبکه ای که WPS را فعال کرده باشد براحتی توسط هکر در عرض چند ساعت مورد نفوذ قرار میگیرد.

این فناوری بیشتر در روش های های حمله Buffer Over Flow و Reaver مورد استفاده قرار میگیرد اگر در تصاویری که به روش بافر گذاشتم دقت کنید هر دو شبکه از طریق wps مورد نفوذ قرار گرفت

پس دقت داشته باشید که حتما wps در شبکه شما غیر فعال باشد معمولا فعال یا غیر فعال کردنش بوسیله یک دکمه که بروی مودم تعبیه شده انجام می شود

- استفاده متداول از برنامه WHOIS ON MY WIFI

این برنامه این امکان را به شما می دهد ، که شما متوجه شوید در همین لحظه چند نفر به شبکه وایرلس شما متصل هستند و براحتی میتوان متوجه شد که آیا کسی دیگری به جز خودتان به شبکه شما متصل می باشد یا خیر .

از قابلیت های دیگر این برنامه بی نظیر بدست آوردن Computer Name کلاینت های (کاربران) متصل به شبکه هست که قابلیت بی نظری محسوب می شود.

پس با بررسی روزانه این برنامه میتوان از هک نشدن شبکه وایرلس خود اطمینان حاصل کنیم و اگر متوجه شدیم شبکه وایرلس ما به هر نحوی مورد حمله واقع شد و هکر در حال استفاده از نت ما می باشد براحتی میتوانیم با عوض کردن پسورد دسترسی هکر را قطع کنیم

- فیلتر کردن اتصال به MAC

در مودم قابلیتی وجود دارد که شما را قادر می سازد اتصال به شبکه را به مک محدود کنید

در ابتدا از MAC یک تعریف ساده داشته باشیم ؛

مک یک کد منحصربه‌فرد مخصوص کارت‌های شبکه کابلی یا بی‌سیم یا هر دستگاه سخت‌افزاری در شبکه است و با دستور ipconfig /all در محیط کامنتی (cmd) میتوانیم مک دستگاه خود را بدست آوریم .

در تصویر زیر مشخص کردیم که چگونه mac سیستم را بدست آوردیم.

برای اینکه شخصی را مجاز کنیم که به شبکه وایرلس ما وصل شود میتوانیم این اتصال را محدود به مک کنیم به همین منظور مک دستگاه مورد نظر را در لیست مجاز مک های مودم قرارمی دهیم سپس بوسیله پسورد به شبکه ما متصل شود یعنی در این روش هکر به هر صورتی بتواند پسورد شبکه ما را بدست آورد قادر نخواهد بود به شبکه ما متصل شود زیرا که مک سیستمش بعنوان مک مجاز به مودم ما معرفی نشده و بهمین دلیل نمیتواند حتی با داشتن پسورد به شبکه وصل شود البته این روش را نمیتوان بعنوان یک روش مطمئن استفاده نمود زیرا که هکر اگر کمی زرنگ باشد میتواند مک مودم را بدست آورد و با برنامه MAC CHANGER مک خود را به مک مودم تغییر دهد و به شبکه وصل شود ولی با تمام این توصیفات کار را برای هکر کمی سخت تر میکند

- استفاده از AES رمزنگاری شده بجای TKIP

پروتکل WPA2 از الگوریتم رمزنگاری AES استفاده می‌کند، در حالی که پروتکل WPAاز پروتکلTKIP استفاده می‌کند ولی الگوریتم رمزنگاری آن همان الگوریتم RC4استفاده شده در پروتکل WEP است.

تفاوت دیگر پروتکل‌های WPA و WPA2 در روش محاسبه کد صحت پیام (MIC) می‌باشد. پروتکلWPA برای تولید کد صحت پیام از الگوریتم Michael استفاده می‌کند ولی پروتکل WPA2 از شیوه‌ی زنجیره‌سازی بلوک‌های رمز (CBC) برای تولید کد صحت پیام استفاده می‌کند. با وجود پیچیده بودن الگوریتمMichael ، روش CBC به کار گرفته شده در پروتکل WPA2 برای محاسبه‌ی کد صحت پیام دارای پیچیدگی بیشتر بوده و در نتیجه امنیت بیشتری را تأمین می‌کند.

- استفاده از Shieldeville

شیلدویل ابزاری با عملکردهای خارق العاده دارد است که شرایط نفوذ را برای یک هکر تا مرز بی نهایت دشوار می کند اگر بخواهم این ابزار را بهتر توصیف کنم ، یک هکر برای نفوذ به شبکه ای که شیلدویل روی آن فعال می باشد باید یک زمان چند ماهه حتی یک ساله را برای بدست آوردن یک پسورد بگذراند.

اما Sheildville چه محدودیت هایی اعمال میکند که تا این مقدار دسترسی هکر محدود می شود؟

عملکردهای شیلدویل را تک تک مورد بررسی قرار میدیم:

۱ – ایجاد اکسس پوینت های جعلی با امنیت wpa2 :

هکر برای نفوذ به شبکه وایرلس شما با صدها مودم جعلی روبه رو می باشد یعنی بعبارتی مودم شما بین صدها مودم مخفی شده و امنیت همگی آنها wpa2 می باشد که هکر برای بدست آوردن پسوردهای جعلی هر مودم نیاز دارد ساعتها وقت صرف کند و زمانی که پسورد را بدست می آورد آن پسورد جعلی می باشد و نفوذگر مجبور می شود ماه ها زمان خودش را برای زدن تک تک تمامی آن صد اکسس پوینت جعلی هدر دهد تا بتواند پسورد واقعی را بدست آورد که این کار امری غیر منطقی است

۲ – ایجاد کلاینت های جعلی :

ایجاد کلاینت های (کاربرهای) جعلی مختلف روی هر اکسس پوینت در نقاط مختلف ، باعث گیج کردن هکر می شود و بدست آوردن پسورد را به مراتب سخت تر میکند چرا که یک محیط جعلی ایجاد میکند که قابلیت نگه داشتن حملات handshake را درون خود دارد

۳ – Disconnect شدن مک های جعلی :

اگر شبکه به مک فیلترینگ فعال باشد ، هکر میتواند با جایگزینی مک مودم بجای مک خود به شبکه وصل شود .

اما این برنامه قابلیت تشخیص جعلی بودن مک را دارد و براحتی میتواند هکر را از بین دیگر کاربران تشخیص دهد و مک مرتبط را دیسکانکت کند بدون آنکه شبکه قطع شود

- SNIFF شبکه وایرلس بوسیله KISMET

یک ضرب المثل قدیمی وجود دارد که" بهترین دفاع حمله است" خب حال چگونه باید یک نفوذگر را مورد نفوذ قرار دهیم اصلا آیا همچنین چیزی امکان دارد؟

این یک روش کاملا تجربی هست و به هیچ کس پیشنهاد نمیکنم چون در این روش باید اجازه دهید شبکه وایرلس شما براحتی هک شود و اجازه دهید هکر از شبکه شما استفاده کند این روش برای افراد حرفه ای تر پیشنهاد میشود چرا که باید با ابزارهایی خاص کار کنند

همانگونه که در ابتدا نمایش دادم شبکه وایرلس من دارای رمزنگاری WEP بوده و براحتی پسوردش قابلیت هک شدن دارد و یقینا ذهن همگی معطوف همین قضیه می شود که چرا کسی که مقالات مختلف امنیتی می نوسید امنیت ضعیفی بروی شبکه ی وایرلسش حاکم است.

این امنیت ضعیف کاملا عمدی است ; در ابتدا بوسیله یک روتر میتوانید ترافیک خود را محدود کنید که از ترافیک شما استفاده نکنند سپس بوسیله ابزاری بنام KISMET که یک برنامه قدرتمند در زمینه SNIFF شبکه های وایرلس می باشد ، شبکه وایرلس خود را شنود کنید و کاملا شبکه خود را مانیتورینگ کنید و تمامی اطلاعات حساس از قبیل پسوردهای کسانی که به شبکه شما وصل هستند رو سرقت کنید و اطلاعات هکر را هک کنید

این روش بارها و بارها توسط من تست شده و اطلاعات حساسی را از هکر توانستم بدست بیارم ولی کار کردن با ابزارهای KISMET و خواندن اطلاعات و پکت ها ، کاری دشوار است اگر در این زمینه اطلاعات و تجربه ای ندارید تحت هیچ شرایطی این روش را تست نکنید

""""" تمامی روش های فوق در جهت هر چه محدود کردن نفوذ به شبکه وایرلس می باشد و رعایت آنها یقینا پیامد امن شدن شبکه شما را برایتان به ارمغان می آورد"""""

نویسنده مقاله : شهاب شمسی