کرک کردنWEP

امنیت شبکه **آرش طاهر کلاته 882980**

WEPیکی از اولین الگوریتم‌های تدوین شده توسط IEEE برای تامین امنیت شبکه‌های بیسیم است که به عنوان بخشی از استاندارد ۸۰۲,۱۱ معرفی شد. WEP خود از روش RC4 برای رمز گذاری استفاده میکند.

الگوریتم WEP به تدریج و با آشکار شدن اشکالات امنیتی شدید، منسوخ شده و هم‌اکنون بیشتر از WPA استفاده میشود . هرچند هنوز هم تعداد زیادی از کاربران خانگی از WEP استفاده میکنند.

در حال حاضر دو روش کلی برای کرک کردن WEP وجود دارد : روش FMS و روش Chopping attack که ما به اولی می‌پردازیم.

در این روش از نقطه ضعف موجود در RC4 استفاده می‌کند : داشتن کلید ضعیف در بردار اولیه

Weak key : قسمت کوچکی از کلیدها که در آن نقاط رفتار رمزکنند نامطلوب است و با داشتن تعداد کافی از آن می‌توان به تدریج به سمت متن اولیه حرکت کرد؛

Initialization vector : یک ورودی تصادفی که در مراحل اولیه رمز گذاری بر روی داده عمل میشود تا حدس زدن رابطه بین رمز و عبارت اصلی برای مهاجم سخت بشود.

از بین ۱۶ میلیون بردار اولیه برای WEP, محققان چیزی در حدود ۹۰۰۰ تا کلید ضعیف پیدا کرده‌اند که می‌توان از آنها برای شکستن رمز استفاده کرد. معمولا برای کرک کردن WEP چیزی مابین ۱۵۰۰ تا ۵۰۰۰ بردار لازم است که برای به دست آوردن آنها به تقریبا ۵ میلیون بسته رمز شده احتیاج داریم . سپس این بردارها داده میشوند به Key Scheduling Algorithm و Pseudo Random Generator تا بایت به بایت کلید اصلی به دست آید

تمام این کارها به سادگی، با داشتن کمی امکانات بر هر کسی ممکن است. چیزهایی که لازم داریم باری این کار شامل یک دستگاه گیرنده وایرلس و برنامه‌های مربوط به این دریافت و شکستن قفل‌های WEP است؛ از قبیل

air...-ng (تمام برنامه‌های مورد نیاز را می‌توان بر روی توزیع لینوکس Backtrack پیدا کرد .)

مشکل اصلی در این روش این است که کپچر کردن تعداد کافی بسته میتواند بسیار وقت‌گیر باشد . در حالت عادی کار گوش دادن به بسته‌ها ممکن است هفته‌ها و بعضا ماه‌ها طول بکشد، اما خوشبختانه می‌توان با تزریق کردن بسته به شبکه به این کار صورت بسخشید . برای این منظور معمولا از بسته‌های ARP استفاده میشود.

مراحل کار در کلّ به صورت زیر است:

ابتدا در کنسول airmon-ng را اجرا می‌کنیم تا واسطه‌های شبکه خود را پیدا کنیم.

مک خود را ترجیحا عوض می‌کنیم و سپس برنامه airmon رو روی یکی از اینترفیس‌های شبکه خود فعال می‌کنیم که دنبال قربانی بگردد . کانالی که هدف روی آن کار می‌کند و (BBSID مک آدرسAccess point ها) آن را استخراج و روی آن گوش میدهیم.

در انتها با استفاده برنامه aircrack داده‌های جمع شده را برای تحلیل و شکستن رمز به کار میگیریم.