



بررسی امنیت و تست نفوذ در پروتکل WEP

احمدشهاب ارکان، مهدی آقا صرام، علی محمدلطیف

۱- کارشناس ارشد شبکه های کامپیوتری، دانشگاه ارومیه

۲- استادیار گروه مهندسی کامپیوتر، دانشگاه یزد

۳- استادیار گروه مهندسی کامپیوتر، دانشگاه یزد

As.arkan@sepanta.com

نام ارائه دهنده: احمدشهاب ارکان

خلاصه

امروزه شبکه های محلی بی سیم که از آن ها با عنوان شبکه های وای فای نیز یاد می شود؛ در همه جا یافت می شوند. این روزها کم تر سیستمی راغب به استفاده از تکنولوژی شبکه های مبتنی بر سیم است. گستردگی روزافزون این دسته از شبکه ها الزام تامین امنیت در ارتباطات بی سیم را افزایش داده است. هم سان با رشد تکنولوژی بی سیم در ارتباطات و انتقال اطلاعات، حمله ها و نفوذهای غیرمجاز نیز رشد کرده اند. در این مقاله ابتدا به معرفی پروتکل های امنیت شبکه های وایرلس پرداخته و سپس تست نفوذ و حمله برای پروتکل امنیتی WEP بررسی خواهد شد.

کلمات کلیدی: شبکه های بی سیم، تست نفوذ، امنیت شبکه

۱. مقدمه

انتقال داده در شبکه های بی سیم از طریق هوا صورت می گیرد، بنابراین محافظت از محرمانگی داده ها امری ضروری محسوب می شود و بهترین راه حل استفاده از رمزنگاری است. کمیته WLAN (IEEE 802.11) پروتکل های زیر را برای این منظور تعریف کرده است:

- Wired Equivalent Privacy (WEP)
- Wi-Fi Protected Access (WPA)
- Wi-Fi Protected Access v2 (WPA v2)

کمیته WLAN، در ابتدا پروتکل رمزنگاری Wired Equivalent Privacy (WEP) و به دنبال آن WPA را با هدف ایجاد مکانیزم های رمزنگاری بی عیب و نقص برای شبکه های بی سیم طراحی کرد [1]. ولی با گذشت زمان و گسترش بهره برداری از آن ها دردنیای واقعی، مشخص شد که این مکانیزم ها، معایب نفوذپذیری دارند. مکانیزم های رمزنگاری شبکه های بی سیم، همواره در معرض خطر حملات رمزنگاری (Cryptographic Attack) بوده اند. این امر با WEP در اوایل سال ۲۰۰۰ آغاز و در نهایت منجر به شکسته شدن کامل آن شد [2-4]. در سال های اخیر، تهدیدها رفته رفته، WPA را نیز نشانه گرفته اند، اگرچه در حال حاضر، حمله ی موفقی برای شکستن WPA، در شرایط عمومی گزارش نشده است ولی حملات موفقی تحت شرایط خاص، عملی می باشند. در ادامه به معرفی پروتکل های رمزنگاری پرداخته و حمله به WEP شرح داده خواهد شد.

۱-۱ رمزنگاری WEP در شبکه های بی سیم

Wired Equivalent Privacy (WEP) پروتکل امنیتی برای رمزنگاری داده های ارسالی در شبکه های بی سیم می باشد که پیکربندی آن ساده بوده و در حالت بدون security، اطلاعات می توانند به راحتی شنود شوند. اگرچه پروتکل WEP اولین تلاش برای ایمن سازی شبکه های بی سیم بوده