الأمن في WiFi

عبدالمحسن الدعفس
423103099

الأمن في WiFi

1)تحديات أمن الشبكة اللاسلكية:

نظرا لمرونة الشبكات اللاسلكية وسهولة تركيبها و كثرة الخدمات التي توفرها فقد انتشرت على نطاق واسع جدا في جميع أنحاء العالم. حيث ورد في تقرير احصائي من In-Stat MDR بأنه يوجد في العالم الآن أكثر من 75 مليون شبكة لاسلكية. أيضا، كانت 95% من الحاسبات المحمولة التي غص بها السوق العالمي مجهزة للعمل على الشبكات اللاسلكية. وكان للطابعات والماسحات الضوئية والموجهات نصيب كبير، فقد جهزت بكروت داخلية للتواصل عبر الشبكة اللاسلكية.

كما ازداد استخدام وتوظيف الشبكات اللاسلكية، إزداد أيضا الخطر الذي يهددها. حيث تواجه الشبكات اللاسلكية نفس المخاطر التي تعاني منها الشبكات السلكية وأكثر. لأن الوسط الناقل في الشبكات اللاسلكية هو الهواء الذي يصعب إخفاؤه وصعوبة منع الآخرين من الوصول إليه. وهذا ما أعطى فرصة قوية لظهور جيل جديد من الهاكرز تتركز مهاراتهم في اختراق هذه الشبكات اللاسلكية دون غيرها.

تعتقد بعض المنشآت أنه لا داعي لإشغال أنفسهم بحماية الشبكة اللاسلكية أو التقليل من أهمية حمايتها حماية مشددة إذا كانت لا تحمل معلومات حساسة، وهذا قد يكلف الكثير فالعديد من المنشآت تقوم بربط الشبكة اللاسلكية بالشبكة السلكية في مكان ما داخل المنشأة. وقد يمكن هذا التوصيل من الدخول إلى موارد المنشأة من خلال الشبكة اللاسلكية.

2) مخاطر وثغرات الشبكة اللاسلكية:

2.1) طبيعة الوسط الناقل في الشبكات اللاسلكية:

بالرغم من المنافع التي قدمتها لنا الشبكات اللاسلكية من توفير في التكاليف وسهولة وسرعة في الوصول إلى جميع الموارد مقارنة بالشبكات السلكية إلا أنها ورثت أكثر المخاطر والثغرات من الشبكة السلكية. بالإضافة لكونها تقنية جديدة فقد استحدثت مشاكل وتهديدات جديدة معها.

لا يمكن اختراق الشبكة السلكية إلا عن طريق اختراق جدار النار أو تخطي الأمن البشري و المادي للوصول إلى الشبكة فيزيائيا. من جهة أخرى، الوسط الناقل في الشبكة اللاسلكية هو الهواء الذ لا يمكن التحكم به. فالموجات تخترق الجدران وتخرج من النوافذ والزجاج في جميع الإتجاهات لتمتد -حسب قوة الإرسال- إلى آلاف الأقدام. والخطورة في ذلك تكمن في تمكن المخترقين من التنصت على الشبكة باستخدام أدوات خاصة تلتقط الموجات وهي في تطور وازدياد.

2.2) نقاط الوصول الغير مؤمنة:

الإعدادات الإفتراضية لنقاط الوصول (Access Points) تكون غير مؤمنة. مثلا يكون هنالك كلمة مرور افتراضية وخصائص التشفير غير مفعلة، وكما هو الحال أيضا في خاصية التحقق من الهوية Authentication. فإذا تم ربط شبكة لاسلكية بخصائصها الإفتراضية بشبكة أخرى - سلكية أو لاسلكية – فإنها تكون بوابة مشرعة الأبواب للمخترقين وغيرهم وتمكنهم من الدخول على الشبكتين معا.

يستطيع المتطفلون تحويل حاسباتهم المحمولة إلى نقاط وصول (Soft Access Points) بواسطة برامج معدة لذلك مثل HostAP و HostPotter أو تركيب نقطة وصول صغيرة عن طريق المنفذ التسلسلي العالمي USB وباستخدام نقاط الوصول (Soft Access Points) يستطيع هؤلاء المتطفلون جعل مستخدم شرعي يقوم بالإتصال على حاسباتهم المحمولة بدون أن يعلم.

حتى لو تم تفعيل إعدادات الأمان والتشفير والحماية بكلمة سر قوية فيمكن إعادة الإعدادات الإفتراضية بمجرد انهيار النظام أو ارتفاع تردد الكهرباء أو الضغط على زر Reset.

3) أدوات المخترقين:

الأدوات التي تستخدم في اختراق الشبكات اللاسلكية كثيرة ومتاحة مجانا على الإنترنت. وكل أسبوع تظهر لنا أدات جديدة أو تحديت لأخرى قديمة. لذا يجب على مدراء الأمن الاطلاع على هذه الأدوات وتجربتها ليتسنى لهم حماية أنفسهم منها. ومن هذه الأدوات:

- ❖ Cain&Abel: أداة لاسترجاع كلمات المرور بواسطة التنصت على الشبكة وكسر كلمات المرور المشفرة بواسطة:Dictionary أو Brute-Force.
- ❖ Ethereal: محلل للشبكة يقوم باستعراض البيانات المرسلة ويعرض معلومات موجزة ومفصلة عن كل حركة في الشبكة.
- ❖ THC-RUT: أول سلاح يستخدمه المخترقون ضد أي شبكة لاسلكية لاتعرف الكثير عنها. حيث تقوم باستكشاف وتمييز نقاط الوصول الأقل ضغطا باستخدام الـ (Brute-Force).

الهوائيات:

يقوم المخترقون باستخدام هوائيات تجارية للدخول إلى الشبكة اللاسلكية عن بعد أو عن طريق بناء هوائي خاص باستخدام علب رقائق البطاطس Pringles أو استخدام أي اسطوانة معدنية مشابهة. هذه الهوائيات تمكن المخترقين من الوصول إلى الشبكة اللاسلكية 802.11 على بعد عدة آلاف من الأقدام خارج نطاق هذه الشبكة.

5) كسر تشفير الـ WEP:

- o WEPwedgie
- o WEPCrack
- o WEPAttack
- o BSD-Airt
- o AirSnort

كل هذه الأدوات يستخدمها المخترقون لكسر معيار تشفير الشبكات اللاسلكية WEP –Wired Equivalent Privacy-. تقوم هذه الأدوات باستغلال الثغرات في لوغاريتم التشفير للـ WEP . بحيث تقوم بجمع بيانات من الشبكة وتحللها إلى أن تميز الشفرة وتقوم بفكها.

4) المخاطر الأكثر شيوعا في الشبكة اللاسلكية:

نظرا لما تتمتع به الشبكة اللاسلكية من مرونة كبيرة ولا سيما أنها حديثة الولادة في السوق العالمي فهي تعاني من نقص في الخبرة لدى أصحابها خاصة في الجانب الأمني. لذا أود أن ألخص هذه المخاطر في النقاط التالية:

- العلاقات الوهمية:

يستطيع مهاجم الشبكة إجبار أحد المستخدمين الشرعيين بالإتصال بنقطة وصول وهمية وهذا ما يعرف بالعلاقة الوهمية. إذا تمت هذه العملية فإن هذا المهاجم أو المخترق يستطيع الولوج إلى الشبكة عن طريق هذا المستخدم الشرعي. أو تغيير إعدادات الشبكة اللاسلكية بحيث تمكنه لاحقا من الدخول إليها. وغالبا ما تكون نقطة الوصول عبارة عن جهاز محمول مجهز ببعض البرمجيات التي تمثل عمل نقاط الوصول الحقيقية.

ومن الجدير بالذكر أن نقطة الوصول الوهمية تستجيب لطلب المستخدم الشرعي وتقوم بتزويده بعنوان انترنت للدخول للشبكة. بعد ذلك يقوم المخترق –صاحب نقطة الوصول الوهمية- بمسح شامل على جهاز الضحية

للبحث عن ثغرات أهمها ثغرات نظام التشغيل. والغالب أن يكون هذا النظام هو ويندوز المكتظ بالثغرات التي أغفلها مستخدموها. وعند الحصول على أحد الثغرات يقوم المخترق بسرقة المعلومات أو تنصيب فيروسات أو أحصنة طروادة وعمل ما يريد.

- انتحال الشخصية:

من أخطر التهديدات التي تواجهها الشبكات عموما واللاسلكية خصوصا هي انتحال الشخصية. يقوم المخترق بتغيير عنوان الـ MAC ليطابق عنوان موجود في الشبكة لينتحل شخصية هذا المستخدم. هذا التهديد مشابه إلى حد كبير وجود طرف ثالث غير شرعي في الشبكة السلكية Man in the middle ، والأدوات المستخدمة فيها يمكن استخدامها في الشبكة اللاسلكية بسهولة.

مشكلة الشبكة السلكية في الدخول إلى جلسة اتصال بدون معرفة أصحابها تحدث في الشبكة اللاسلكية بطريقة أسهل بكثير مما نتوقع.حيث لا وجود لأسلاك محمية أو مخفية. كل ما هنالك عمل نقطة وصول وهمية وتوجيهها في منتصف جلسة الإتصال.

- تعطيل الخدمات –Denial of Service DoS- :

هناك العديد من الأدوات المتاحة على شبكة الإنترنت مجانا لعمل هجوم DoS مثل Hunter Killer و Wireless LANJack. وهذا النوع من الهجوم يمكن أن يكون ضد مستخدم معين للشبكة لمنعه من الوصول إلى الموارد المتاحة له أو ضد نقطة وصول معينة لمنعها من استقبال اشارات من أي أجهزة أخرى أو ضد جميع الأجهزة المتصل في الشبكة.

5) طرق الحماية:

هناك مسلمات أمنية يجب تطبيقها في جميع جهات ومصادر المنشأة منها الشبكة اللاسلكية، ونظرا لحداثة هذه التقنية وكثرة أنواعها والتطور السريع لها، لذا يجب العناية بها عناية خاصة من جهة ومن جهة أخرى العناية بمن يتصل بها.

المستخدمون للشبكة يجب توعيتهم بأمن المعلومات عموما والتأكيد عليهم بالإبلاغ عما يشكل عليهم أو أي شيء غريب شاهدونه في المنظمة وما حولها. وتفعيل برامج التدريب غير كافية لهم، لذا يجب التأكد بأنهم يطبقون ما تعلموه على الوجه المطلوب.

وبشكل عام يجب على مدير الشبكة التأكد من التالي:

1. سلامة بناء الشبكة وعدم وجود ثغرات يمكن المرور من خلالها.
2. تركيب الجدار الناري في المكان المناسب – خاصة إذا كانت الشبكة اللاسلكية متصلة بشبكة أخرى –
3. تحديث نظم التشغيل لجميع الأجهزة والمزودات.
4. تحديث جميع البرامج المستخدمة لسد الثغرات التي يمكن من خلالها إلحاق الضرر بالشبكة عموما.
5. تحديث بريمجات أجهزة الشبكة – خاصة نقاط الوصول –
6. التعرف على الأدوات المستخدمة في اختراق الشبكات والتأكد من عدم قدرتها على اختراق شبكة المنظمة.
7. حماية الإتصالات بين أجهزة الشبكة (VPN, Authentication, Encryption)
8. مراقبة كل حركة في الشبكة على مدار الساعة في جميع أيام الأسبوع.

المصادر:

1. Wireless LAN Security What Hackers Know That You Don't In-Network: http://wp.bitpipe.com/resource/org_1028180222_467/WLAN_Security-What_Hackers_Know_That_You_Dont_In-Network.pdf?site_cd=secd

2. Network Chemistry White paper Wireless Protection: http://wp.bitpipe.com/resource/org_1143077016_965/NetworkChemistryWhitepaper_WirelessProtection.pdf?site_cd=secd

3. Step-by-Step Guide for Setting Up Secure Wireless Access in a Test Lab: http://www.microsoft.com/downloads/details.aspx?FamilyID=0f7fa9a2-e113-415b-b2a9-b6a3d64c48f5&DisplayLang=en

4. Hidden Wireless Networks with Microsoft Windows http://www.microsoft.com/technet/itsolutions/network/evaluate/hiddennet.mspx

5. Securing Wireless LANs with Certificate Services http://www.microsoft.com/downloads/details.aspx?familyid=cdb639b3-010b-47e7-b234-a27cda291dad&displaylang=en&Hash=FG3J5PF

6. Wireless security: Why such a bad rap? http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci1112909,00.html