اختبار اختراق الشبكة اللاسلكية

الشبكات اللاسلكية هي شبكات تستعمل أمواج الراديو لنقل البيانات مما سهل عملية توصيل أطراف الشبكة، وهذه السهولة أدت لمحاولة بعض الأشخاص الدخولَ غير المشروع لتلك الشبكة؛ فتوجب القيام ب **"حماية الشبكة اللاسلكية"**.

يقوم أمن الشبكات اللاسلكية على منع أي وصول غير مرخص به إلى الشبكة، ومنع حدوث أي تعديل على البيانات المُتبادَلة أو المخزنة، وكذلك توافر الخدمة على الدوام للمستخدمين المصرح لهم بالوصول للشبكة. وذلك عن طريق تشفير البيانات باستخدام بروتوكولات التشفير، ومنها: WEP، WPA/WPA2.

Wired Equivalent Privacy(WEP): بروتوكول ضعيف تم اختراقه بعد عدة أشهر من إطلاقه؛ ولم يعد صالحاً للاستخدام في عصرنا الحالي.

Wi-Fi Protected Access(WPA/WPA2): بروتوكول تم تطويره في عام ٢٠٠٣، وهو الأساس المُعتمَد عليه حالياً في تأمين الشبكات المنزلية.

طرق اختراق الشبكة اللاسلكية:

١. التقاط Handshake بين الراوتر والمستخدم المشروع واستعماله للتخمين على كلمة سر الشبكة.
٢. التخمين على WPS PIN الخاص بالراوتر.
٣. التوأم الشرير Evil Twin.

4-way handshake: هي العملية التي تتم بين الشبكة والمستخدم للتأكد من حقه في الوصول إلى الشبكة، تقوم بعض الأدوات بالتنصت على الشبكة والتقاط حزم معينة تسمى ب Handshake، بينما يقوم برنامج آخر بفصل المستخدمين من الشبكة (لكي يعيدوا الاتصال و يقوم البرنامج الأول بالتقاط ال Handshake) ، و بعد ذلك يتم استخدام برنامج آخر ليقوم بتجريب عدد كبير من الاحتمالات للبحث عن تطابق مع ال Handshake المُلتقط، فيحصل المهاجم على كلمة المرور.

Wi-fi Protected Setup(WPS): هو بروتوكول يُستعمَل لتسهيل الاتصال بالشبكة، دون الحاجة لإدخال كلمة المرور التي تكون أحيانا طويلة و معقدة و سريعة النسيان؛ و ينقسم إلى قسمان: Push Button Configuration(PBC) ويقوم على ضغط الزر الخاص ب WPS في كل من الراوتر (Access Point) و المستخدم أو المتصل (Client) ؛ يمكن استغلال الوصول الفيزيائي لل Access Point للدخول على الشبكة، النوع الثاني يعتمد على رقم فريد PIN خاص بالراوتر (يكون مطبوعاً على الراوتر عادةً)، ويتكون من ٨ محارف وهذا العدد قليل نسبياً، وكون هذه المحارف مجرد أرقام يجعل الاحتمالات تتقلص بشكل كبير، وفوق هذا؛ يقوم البروتوكول بفحص ٤ خانات ثم ال ٤ خانات الأخرى مما يؤدي إلى جعل الاحتمالات معدودة (٢٠٠٠٠ احتمال بالضبط)،ناهيك عن إيجاد ثغرة خطيرة في البروتوكول تؤدي إلى كشف رقم PIN في ثوانٍ معدودة. ينصح بشدة **بإيقاف تشغيل WPS** إن أمكن ذلك، أو تحديث نظام تشغيل الخاص بالراوتر.

Evil Twin: يقوم المهاجم بالحصول على Handshake الشبكة الأصلية كما هو موضح سابقاً ثم يقوم بعمل شبكة مزورة تشبه الشبكة الأصلية في اسمها وغير محمية بكلمة سر، ويقوم بمنع اتصال المستخدم بالشبكة الأصلية (في Windows xp كانت تختفي الشبكة الأصلية وتظهر المزورة فقط و يتصل بها الويندوز تلقائيا، ولكن تم حل هذه المشكلة في الإصدارات المتقدمة من Widows مثل ٧ و ما بعده)، وبعد اتصال المستخدم بالشبكة الوهمية؛ تتم مطالبته بإدخال كلمة السر لاستخدام الشبكة، فإن قام المستخدم بإدخال كلمة المرور؛ تتم مقارنتها ب ال Handshake الملتقط مسبقاً للتأكد من صحته فإن كان صحيحاً ينجح الهجوم ويتوقف. من أشهر الأدوات للقيام بهذا العمل، أداة Linset.
وهناك طريقة أخرى تقوم على أن ينشأ المهاجم شبكةً خاصةً به ويقوم بعمل هجوم MITM ليتنصت على البينات المتبادلة بين الشبكة والضحايا الذين يتصلون بالشبكة ويكشف كلمات المرور والرسائل وغيرها.

خطوات وقائية لحماية الشبكة اللاسلكية:

١. استعمال تشفير WPA2 والابتعاد عن تشفير WEP.
٢. جعل كلمة المرور صعبة وطويلة مما يجعل من الصعب تخمينها وألا ترتبط بمعلومة خاصة بك.
٣. إيقاف تشغيل خاصية WPS.
٤. تغيير كلمة سر الراوتر الافتراضية وجعلها صعبة وطويلة.
٥. تغيير كلمات السر باستمرار.
٦. استعمال اسم للشبكة Service Set Identifier (SSID) ليس له علاقة بالشخص، كاسمه أو رقم الجوال أو غيره.
٧. إخفاء SSID.
٨. استعمال MAC Filter لتصفية المستخدمين المسموح لهم الاتصال بالشبكة.
٩. استخدام قواعد ACL لتحديد الأجهزة أو الأيبيهات المسموح لها بإدارة الراوتر.
١٠. تجنب الاتصال بأي شبكة مفتوحة لها نفس اسم شبكتك.
١١. عدم الاتصال بالشبكات العامة المفتوحة ما أمكن ذلك، واستعمال VPN عند الحاجة للاتصال بشبكة عامة.