أمن الشبكات اللاسلكية

إن للشبكة اللاسلكية أخطاراً تهدد أمنها كغيرها من الشبكات، سواء كانت هـذه المخاطر مشتركة بين الشبكات السلكية واللاسلكية أو كانت مخـاطر مخصـصة أو موجودة فقط في الشبكات اللاسلكية وما تحتويه من معايير وغيرها.

وهنا سنحاول قدر الإمكان التركيز على تأمين البيئة الشبكية اللاسلكية من أغلب المخاطر التي قد تهددها. فلا يوجد أمن 100% ولكن علينا قدر الإمكان أن نقتـرب من هذه النسبة بتنفيذ بعض الأمور التي ستساعد على جعل الشبكة آمنة قدر الإمكان.

من المعروف أن من أخطر ما يهدد الشبكات هذه الأيام هـي هجمـات حجـب الخدمة التي قد تتعرض لها وفي كثير من الأحيان يصعب تفاديها إن تمت بـصورة دقيقة ومركزة. إن منفذي هجمات حجب الخدمة الموزعة **DDoS** أو **Distributed Service Denial of** يحتاجون إلى عدد كبير من الأجهزة لكي ينفـذوا هجمـاتهم فتراهم يبرمجون برمجيات تعمل على أتمتة الهجوم والاستيلاء على أجهزة الحاسـب ومن ثم الانتقال إلى الأجهزة المجاورة وغيرها بصورة تلقائية سريعة وإذا كان جهاز الحاسب غير محمي بصورة كافية فانه سيقع ضمن قائمة الأجهزة التي تنتظر الأوامر من المهاجمين لتنفذ الهجوم. في العادة فان الأجهزة المصابة لا يتم حذف الملفات منها لكن يتم استعمالها جميعاً في وقت واحد في الهجوم على شبكة معينة أو موقع معـين وتلك الأجهزة تسمى بال**zombies**.

من أكثر الجهات التي ينصب اهتمام المهاجمين على الاستيلاء على أجهزتها هي الشركات الكبيرة والجامعات والكليات التي تحمل عدد كبير مـن أجهـزة الحاسـب المتصلة بالإنترنت بشكل متواصل وإن لم يتخذ المسؤولين عن هذه الشبكات الحـذر من أمور عديدة فان نسبة تعرض أجهزة شبكتهم للاشتراك في هجوم أمر وارد.

و بما أن اغلب الشركات والجامعات بدأت بالتوجه إلى استعمال الشبكات اللاسلكية فان نسبة الخطر في ضلوع أجهزتها بطبيعة الحال ترتفع لأسباب عديدة أولها أن الأجهزة لن تكون في العادة موجودة في مكان ثابت بل تتحرك وربما تخرج من مبنى الشركة نفسها! لذا وجب الحذر من اتخاذ كافة الوسائل الممكنة من جعل الشبكة اللاسلكية آمنة قدر المستطاع.

إن الأجهزة المحمولة التي تملك كرت شبكة لاسلكي موصل بمقوي للإرسال, بإمكانها أن تشارك في نقل الملفات والتعامل كما لو كانت في مبنى الجامعة أو الشركة أو الكلية وفي الحقيقة من الممكن أن تبعد كيلومترات عنها! وإذا كانت نقاط الاتصال الموجودة في المؤسسة أو الجامعة لم يتم ***تضبيط*** إعداداتها بطريقة سليمة ولم يتم تعديل الإعدادات الافتراضية المعروفة لدى كل باحث, فان أي شخص على بعد أميال (باستخدام مقوي للإرسال) يستطيع الدخول بكل سهولة على الشبكة.

إن أغلب الأمور التي من الممكن أن يتم استغلالها هي الإعدادات الافتراضية لنقاط الاتصال **Points Access**, وفي ما يلي بعض الأمور التي ستساعد في تقليل مخاطر الإعدادات الافتراضية:

معّرف الخدمة أو الـ SSID

الـ SSID أو الـ **ID**entifier **S**et **S**ervice تعني معّرف الخدمة. أن كل نقطة اتصال تملك معرّف يكون عبارة عن كلمة أو رقم أو خليط بين حروف وأرقام. يقوم هذا المعرف بالتعريف عن نقطة الاتصال ولنفرض أن نقطة اتصال معينة تملك SSID معين على سبيل المثال هو ***الأكاديمية***. إن أي شخص موجود في مدى التغطية التي تغطيها نقطة الاتصال (المدى يعتمد على أمور عديدة قد تصل إلى كيلو مترات سواء كان في نفس البيت أو المبنى أو كان في الشارع المجاور للبيت) يستطيع أن يدخل إلى الشبكة الخاصة بنقطة الاتصال ذات المعرف (***الأكاديمية***) إذا عرف أن كلمة (***الأكاديمية***) هي الـ SSID الخاص بها. أغلب نقاط الاتصال تحمل

إعدادات افتراضية ويكون المعرف لها معروفاً وفي الغالب يكون كلمة default. إذا لم يتم تغيير هذا المعرف إلى أي شي آخر, فان أي شخص يقع في ضمن مدى نقطة الاتصال يستطيع الدخول للشبكة الخاصة بها بدون عوائق!

من الأمور الموجودة في الإعدادات الافتراضية الخاصة بالـ SSID هو الـ Broadcasting SSID. تقوم نقاط الاتصال بالتعريف عن نفسها بشكل مستمر على مدى التغطية التي تغطيه فتقوم بصورة مستمرة بإرسال إشارات تقوم بالتعريف عن نفسها وبمعرّفها الخاص. بهذه الطريقة يمكن لأي شخص يملك جهاز خاص أو كمبيوتر محمول به كرت شبكة لاسلكية أن يتجه إلى المنطقة التي تغطيها نقطة الاتصال فيحصل بشكل تلقائي على الإشارة مع رقم المعرف فيعرف انه الآن يمكنه الاتصال بشبكة نقطة الاتصال (***الأكاديمية***) من موقعه. يجب تعطيل هذه الخاصية التي تأتي بصورة افتراضية في العادة حتى لا يتمكن ضعاف النفوس من الذين يملكون أجهزة محمولة ذات كروت شبكة لاسلكية من الاقتراب ومعرفة الأماكن (القريبة) من المنزل او المبنى والتي من خلالها يستطيعون الدخول على الشبكة اللاسلكية. يفضل قدر الإمكان تغيير المعّرف بصورة مستمرة بين حين وآخر حتى إن حصل أحد الذين يحاولون اختراق الشبكة على المعرف الخاص بنقطة الاتصال في وقت معين فانه عند تغييره بصورة مستمرة ستصعب مهمته اكثر.

من الممكن أيضا تقليل نسبة الإرسال لنقطة الاتصال بحيث أن يكون مداها قدر الإمكان على المحدود المطلوبة والمسموح بها لا أن تتخطى هذه الحدود وتغطي مساحات خارج نطاق المنزل أو الشركة والتي قد يستغلها البعض في الدخول للشبكة الخاصة.

نستطيع تمثيل مسألة خروج مدى التغطية عن حدود المؤسسة أو المنزل إلى مسافات لا داعي لها كوصول المدى إلى الشارع المجاور بتوزيع أسلاك وكبلات خاصة بالشبكة الداخلية ما على الناس إلا أن يحضروا أجهزتهم ويوصلون كروت

الشبكة بالكبلات والأسلاك ويدخلون على الشبكة الداخلية وهم جالسون في الـشارع المجاور!

فلترة الـ MAC Address

الـ MAC Address أو الـ Media Access Control Address هـو العنوان الفيزيائي لكروت الشبكة. كل كرت شبكة في العالم يحمل رقم يميـزه عـن غيره, تقوم الشركات المنتجة بوضع أرقام خاصة على أساس نظام الهكـس لتميـز كروت الشبكة عن بعضها ومن المفترض أن لا تكون هذه الأرقام مكررة أبداً. بطبيعة الحال نقطة الاتصال تعتبر من الطبقة الثانية في الـ OSI Model أو الـ Open System Interconnect يعني في طبقة الـ Data Link كالسويتشات فان تعاملها يكون مع الـ MAC Address وليس مـع الـ IP Address. وهنـا يـستطيع المسؤول عن الشبكة اللاسلكية أن يحدد الأجهزة التي يسمح لهـا باسـتخدام نقطـة الاتصال الخاصة به.

كما نعرف فان كل جهاز حتى يتصل بالشبكة اللاسلكية يجب أن يحتوي علـى كرت شبكة لاسلكية وكل كرت شبكة لاسلكية تملك رقم خاص مميز وهو الـ MAC Address ومن المفترض أن المسؤول عن الشبكة يعي ويعلم عدد الأجهزة الموجودة لديه أو لدى شركته والتي يريدها أن تستخدم شبكته اللاسلكية. عندها يستطيع فلتـرة استخدام نقط الاتصال لديه ويحدد الأجهزة بواسطة إضافة أرقام الـMAC الخاصـة بهذه الأجهزة في قائمة الأجهزة المسموح لها باسـتخدام الـشبكة أو اسـتخدام نقـط الاتصال ولا يسمح بغير هذه الأجهزة مهما كانت باستخدام نقاط الاتـصال الخاصـة بشبكته.

تشفير البيانات باستخدام الـــ WEP

أغلب نقط الاتصال تملك إمكانية التعامل مع البيانات المشفرة. باستخدام تقنيـــة الـــWEP أو Wired Equivalent Privacy فان تفعيلها في نقطة الاتصال يمكـــن تشفير استلام وتمرير البيانات المشفرة فقط. لذا يجب على كل مستخدم يريد استخدام الشبكة اللاسلكية أن يفعل خاصية الـــ WEP أي التشفير في جهازه كي يـــتم تبـــادل البيانات بصورة مشفرة تصعب في معظم الأحيان معرفة محتواها إن تم نسخ هـــذه البيانات أثناء مرورها بين الأجهزة.

و كخط دفاع ثاني عند استخدام ميزة التشفير يجب تبادل مفتاح التشفير المسمى بـــ WEP Key فهو عبارة عن أرقام على أساس Hex تحدد درجة التشفير وكلمـــا زاد حجم الرقم زادت صعوبة كسر التشفير وأيضاً زادت المدة التي يتم نقل البيانـــات بعد تشفيرها واستلامها ومن ثم فك تشفيرها. ويعتبر المفتاح خط دفاع ثاني لأنه يجب على الأطراف المستخدمة للشبكة معرفة هذا المفتاح كي يتم تشفير البيانـــات علـــى أساسه ويفضل تغييره بين فترة وأخرى حتى إن وقع في يد أحد المتطفلين فانـــه لـــن يستخدمه لفترة طويلة.

الكلمة السرية الافتراضية Default Password

تأتي نقط الاتصال من الشركات المنتجة لها بكلمة سرية معينة موحدة ومعروفة يجدها المستخدم في الدليل الخاص بال Access Point وفي بعض الأحيـــان تكـــون الكلمة السرية خالية يعني أن عند تسجيل الدخول لنقطة الاتصال لتغييـــر الإعـــدادات يكون اسم المستخدم هو مثلا admin والكلمة السرية غير موجودة! من الواضح انـــه يجب تغييرها إلى كلمة سرية صعبة مكونة من أرقام وحروف .هذه هي الإعـــدادات الافتراضية التي وجدت لتسهل العملية على المستخدمين لكن إن بقيت هكذا فإنها قـــد تؤدي إلى مصائب كبيرة يمكن الحد منها وقـــد يمكـــن تلافيهـــا باتبـــاع التعليمـــات والنصائح.