ورقة بعنوان:

طرق وأساليب الاختراقات والتهديدات الأمنية للشبكات اللاسلكية والحلول الحديثة والسياسات الامنية لأمن المعلومات والحماية

اعداد:

د. ياسر الملك احمد سليمان أحمد
المملكة العربية السعودية – جامعة بيشة
كليه العلوم والآداب–قسم علوم الحاسوب ونظم المعلومات –النماص
البريد الإلكتروني: Dr.yaserking@hotmail.com
تلفون :966531328793+

المستخلص

الشبكة تقنية تستخدم لربط أجهزة الكمبيوتر وتسمح للمستخدمين بالاتصال بالإنترنت في أي منطقة التغطية، تمثل الشبكات اللاسلكية المحلية تقنية واسعة الانتشار، نظراً لما تقدمه من دعم لجميع الميزات التي تقدمها الشبكات السلكية التقليدية،

تهدف هذه الورقة الى توضيح ما هية الشبكات اللاسلكية والتعرف على مفهوم أمن وحماية الشبكات اللاسلكية والآليات المستخدمة في تلك الحماية.

النتائج التي توصل اليها الباحث في ان هناك ثغرات أمنية في هذه الشبكات ومن الاسهل للقراصنة الاختراق وسرقة البيانات، معرفة الثغرات الأمنية تساهم إلى حد كبير في حل مشاكل الاختراق في الشبكة اللاسلكية ضد محاولات التسلل والاختراق.

أهمية الورقة في التعرف علي سبل تحقيق الأمن في الشبكات اللاسلكية، وكتابة دراسة أمنية واقعية للشبكات اللاسلكية، ودراسة طرق كتابة السياسات الأمنية الخاصة بالشبكات اللاسلكية.

Abstract

Network technology used to connect computers that allows users to connect to the Internet in any coverage area, representing local wireless network technology and widespread, because of its support for all the features provided by traditional wired networks, This paper aims to clarify what deity wireless networks and get to know the concept of security and protection of wireless networks and the mechanisms used to such protection.

The findings of the researcher in that there are security gaps in these networks, it is easier for hackers to infiltrate and steal data, knowledge of the security gaps contribute greatly to solving the problems of penetration in the wireless network against intrusion attempts and penetration.

The importance of the paper to identify ways to achieve security in wireless networks, writing and realistic study of security for wireless networks, and to study ways of writing own security policies to wireless networks

كلمات مفتاحية:

البروتوكول:

اللغة بين الأجهزة المتصلة بالشبكة، بهدف تبادل المعلومات .

الاختراق:

الوصول لهدف معين بطريقة غير مشروعة.

الثغرات الأمنية:

عبارة نقاط الضعف في النظم والبرمجيات.

جدار الحماية :

لحماية الشبكة من المتطفلين الغير مصرح لهم.

1- المقدمة

تمثل الشبكات اللاسلكية المحلية تقنية واسعة الانتشار، نظراً لما تقدمه من دعم لجميع الميزات التي تقدمها الشبكات السلكية التقليدية، وأصبح اليوم للشبكات اللاسلكية قواعدها ومعاييرها التقنية التي ساهمت في استقرار هذه التقنية وبالتالي الاعتماد عليها في الإنتاج في مختلف بيئات الأعمال، وخصوصاً مع سهولة استخدامها وأسعار نقاط الوصول (Access Point)المنخفضة، بالإضافة لدعم الشبكات اللاسلكية في معالجات الأجهزة المحمولة واتساع انتشار هذه التقنية، حيث لا يكاد يخلو منزل أو منشأة من نقاط الوصول للشبكات اللاسلكية وبقدر الانتشار لهذه التقنية بقدر ما تزيد أهمية العناية بتطبيق الإجراءات الأمنية لحماية الشبكات اللاسلكية، فهناك ثغرات أمنية في هذه الشبكات قد تسبب مشاكل للمستخدمين والثغرات الأمنية يقصد بها مشكلة أو ضعف في نظام الشبكة اللاسلكية قد تسهل على المتسللين اختراقها وسرقة بيانات مهمة والتسبب بخسائر مادية للأفراد والشركات إن معرفة الثغرات الأمنية يساهم وبشكل كبير في تصميم شبكة لاسلكية محصنة من محاولات التسلل والاختراق لذلك كان لابد من مجموعة من التساؤلات وهي كالاتي:

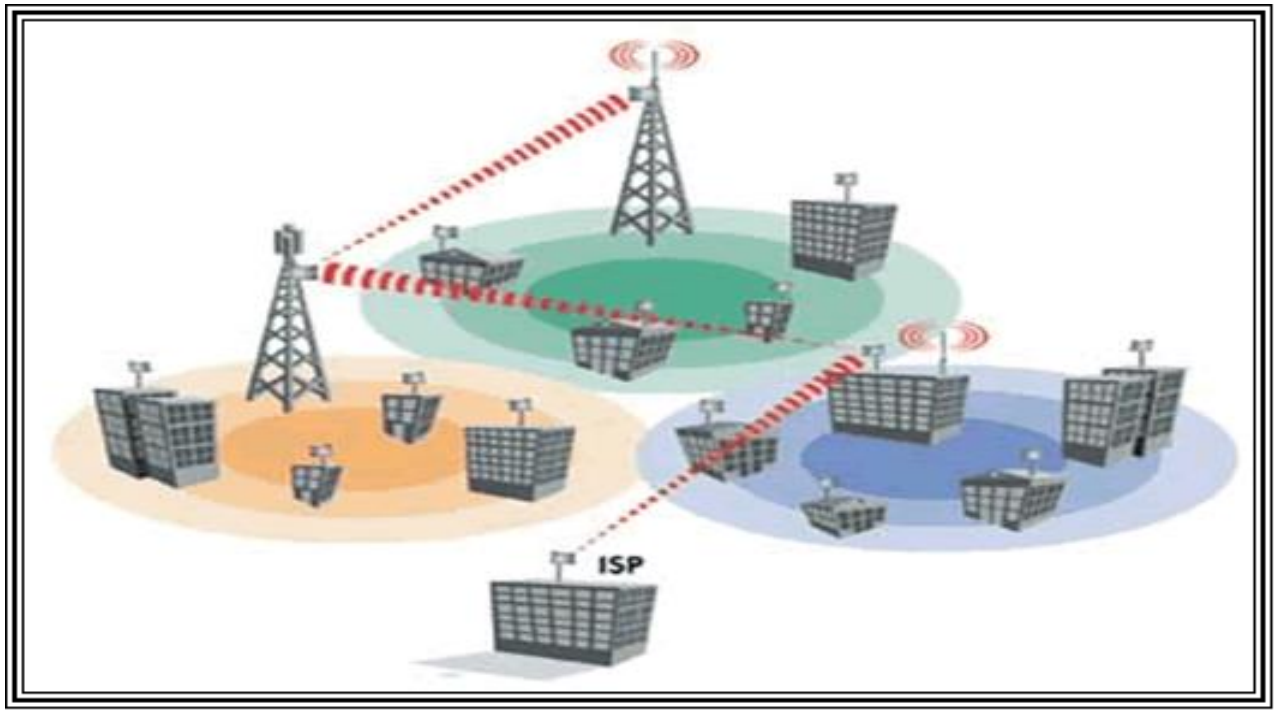
1- التعرف على الشبكات اللاسلكية؟

2- ما هي مكونات الشبكات اللاسلكية؟

3- ماهي المهددات الأمنية في الشبكات اللاسلكية؟

4-ماهي طرق الحماية للشبكات اللاسلكية؟

استخدام الشبكات اللاسلكية في تزايد مستمر وبقدر انتشار هذه التكنولوجيا مما يزيد أهمية الرعاية من خلال تطبيق الإجراءات الأمنية لحماية الشبكات اللاسلكية، وإهمال هذا الجانب من بيانات المستخدم والأنظمة المتصلة بالشبكة اللاسلكية في خطر كبير من المتسللين والدخلاء.

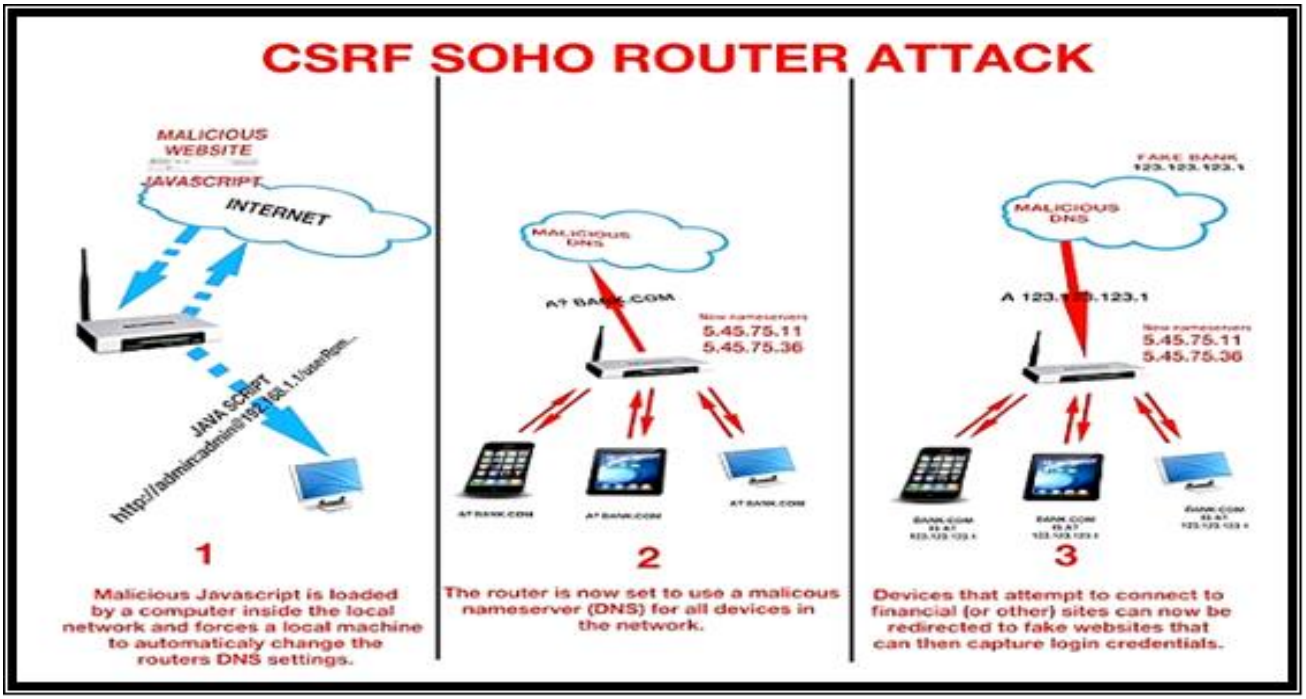


الشكل (1) يوضح الاتصال بالشبكة اللاسلكية [على ابوالحسن، الشبكات اللاسلكية، 2012]

2- **مشاكل ومخاطر الشبكات اللاسلكية :**

أصبحت عمليات القرصنة على الشبكات اللاسلكية في الفترة الأخيرة كثيرة جداً ومتنوعة واكتشاف عمليات القرصنة الخطيرة التي تستهدف أجهزة التوجيه اللاسلكية (أجهزة التوجيه) أصبح بالأمر الصعب، لجأت القراصنة على استخدام مجموعة متنوعة من التقنيات التي ساعدتهم على الوصول إلى هذه الأجهزة وإجراء تغييرات على نظام DNS الذي يستخدم لترجمة عناوين النطاقات وتوجيهها إلى عنوان IP المستخدم جهاز الكمبيوتر لتحديد الويب الخاصة بالجهاز وأشارت الخوادم.

بالإضافة إلى طريقة أخرى تتيح لهم التحكم في كلمات المرور لاسلكية WPA شبكة WPA2 / عن بعد، وحتى الآن، وهذه الهجمات، التي تشمل أكثر من 300 ألف جهاز في مجموعة واسعة من البلدان، فمن الواضح أن هناك نقاط ضعف في التوجيه والمودم وغيرها من الأجهزة التي تعتمد على أجهزة نظام التشغيل الداخلية الخاصة به، فمن الضروري لملء هذه الفجوات الملايين من المستخدمين يتعرضون للخطر.



الشكل (2) يوضح القرصنة التي تستهدف أجهزة التوجيه اللاسلكية (الموجهات) [فادي عمروش، السياسات الأمنية في الشبكات اللاسلكية،2012]

هناك العديد من الأسباب التي قد تخفض من أداء الشبكة اللاسلكية أو توقف عملها بالكامل.

قد يتسبب وجود نقاطٍ مخفيةٍ في تدنٍ كبيرٍ في الأداء، كما قد تتسبب الفيروسات، برمجيات الند للند Peer-to-Peer إضافة إلى الرسائل المرسلة عشوائياً SPAM، وغيرها في تخفيض سعة نقل البيانات المتوفرة للوصول المخول إلى الخدمات الأساسية.

3- التهديدات الأمنية للشبكات اللاسلكية:

1- خطر التجسس، قد يصل المستخدمون غير المخولين إلى البيانات المنقولة عبر شبكتك اللاسلكية استخدم التشفير على مستوى الوصلة ضمن التوصيلات اللاسلكية

2- خطر اختطاف البيانات المنقولة، قد يتمكن المستخدمون غير المخولين من تطبيق هجمات الشخص الوسيط راقب نسبة الإشارة إلى الضجيجSNR ، معرّف مجموعة الخدمات SSID إضافة إلى العنوان الفيزيائي لنقطة الولوج AP MAC المستخدمة في التوصيلات.

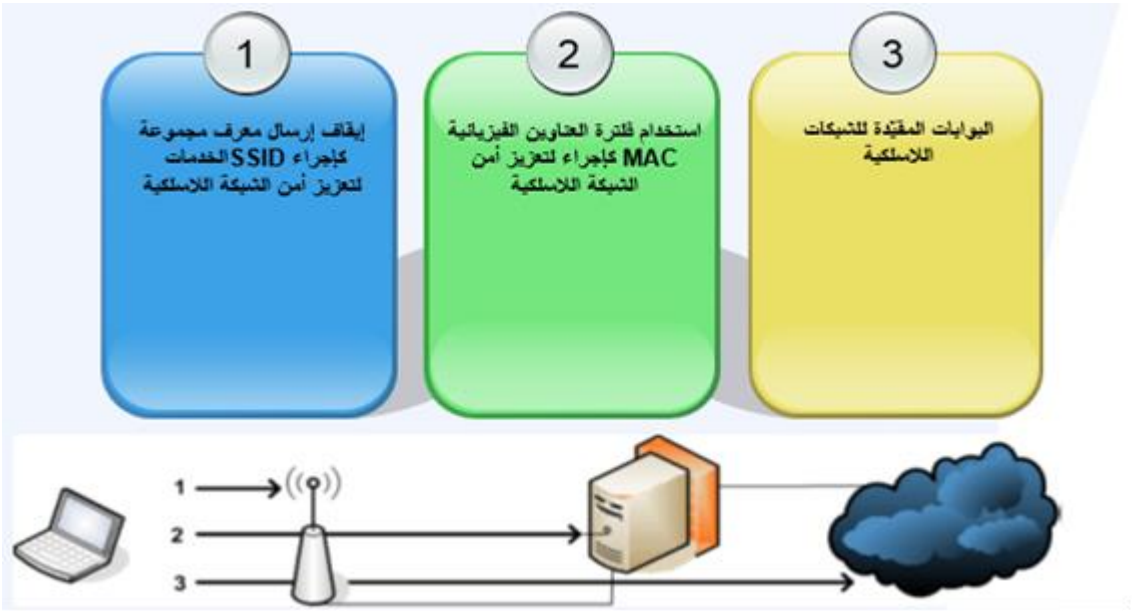
3- خطر الوصول غير المخول إلى شبكتك وإلى الإنترنت قم بإعداد بوابة مقيدة.Captive Portal

4- خطر الوصول الغير المخول إلى شبكتك اللاسلكية لا تعتمد على أساليب التحقق من الهوية

باستخدام العنوان الفيزيائي MAC فقط لا ترسل معرّف مجموعة الخدمات SSID الخاص بشبكتك .

5-خطر تحريف البيانات أثناء نقلها لاسلكياً انصح مستخدمي شبكتك باستخدام "التشفير" ضمن الطبقات ذات المستوى الأعلى (HTTPS, Secure SMTP) استخدم التشفير على مستوى الوصلة ضمن وصلاتك اللاسلكية (WPA2).

ونجد ان من المهم جداً في الشبكات اللاسلكية التحقق من الهوية في الشبكات اللاسلكية الشكل (3) يوضح كيف تتم عملية التحقق



الشكل (3) يوضح كيفية التحقق من الهوية في الشبكات اللاسلكية [فادي عمروش، السياسات الأمنية في الشبكات اللاسلكية،2012**]**

4-الاساليب والطرق الحديثة لحماية الشبكات اللاسلكية:

يوضح الباحث عددا من الإجراءات التي يجب تطبيقها لحماية الشبكات اللاسلكية وفيما يلي استعراض:

1. الوصول يجب أن تكون محمية كنقطة المستخدم وكلمة المرور في كلما أراد المستخدم لتغيير إعدادات نقطة الوصول، تجدر الإشارة إلى أن نقطة وصول جديدة (أو التي كانت لاستعادة الافتراضي بواسطة إعدادات) يكون التعرف عليها من قبل الشركة المصنعة محمي بكلمة مرور، يكون ذلك بناء على مبادرة لتغيير كلمة المرور للمستخدم من أجل تجنب المتسللين لدخول الشبكة والتحكم عن طريق تغيير إعدادات نقطة الوصول، وبشكل عام يجب أن يختار المستخدم تتكون كلمة المرور المناسبة لا يقل عن سبعة صناديق لتكون خليطا من الحروف والأرقام.

2. تتركز طرق الحماية الأكثر أهمية في يتم تشفير شبكة لاسلكية، وهناك أكثر من نظام واحد (أو ما يسمى بروتوكول التشفير)، قوة حماية مختلفة.

3. يجب شبكة لاسلكية تغيير معرف (SSID) بحيث لا يعني نوع نقطة الوصول أو مكان وجودها، الافتراضي في نقطة وصول جديدة تشير إلى وصول والشركة المصنعة لها نوع نقطة، مما يسمح للقراصنة فرصة للهجوم على نقطة الوصول والسيطرة، مع الأخذ الاستفادة من الثغرات الخاصة، يجب عليك أيضا تعطيل الإعلان عن الخيار معرف نقطة وصول (بث SSID)

يضيف الباحث أيضا خطوات لحماية الشبكة اللاسلكية:

1. تشفير شبكة لاسلكية.

هذه الخطوة هي أهم عمل المتخذة لحماية الشبكة اللاسلكية .التشفير المستخدمة يعني اليوم هو (WPA2) و (WPA-PSK) و .(WEP) دون أن يذهب أعمق في التشفير التقنيات (WPA2) هو الاحدث في عالم التشفير صرخة المفضل للغاية لشراء راوتر يدعم هذه التقنية .قبل هذا التشفير يمكن استخدامها لكلمة مرور معقدة تتكون من 64 خانة (أحرف كبيرة وصغيرة وأرقام وعلامات) وأنصح الجميع لاستغلال جميع المجالات المتاحة في سري مجموعة كلمة .ولكن كيف سوف تذكر الرقم السري مكون من 64 خانات؟ ليست هناك حاجة لكتابة PIN في كل مرة تريد الدخول إلى شبكة لاسلكية لأنها سوف تبقى محفوظة في إعدادات الشبكة، ولكن يفضل أن يكتب رقم PIN على ملف TXT وابقائه على بطاقة ذاكرة USB الخارجية .أجهزة التوجيه القديمة المستخدمة نوع تقنية التشفير (WPA) ملاحظة أن التشفير السابق (WPA2)أفضل منه .للتشفير (WEP) أبدا التفكير في استخدامه لأنه يعتبر التشفير ضعيف ويمكن أن تخترق الشبكة في غضون 4 ساعات (ربما بضع دقائق) باستخدام برامج خاصة.

2-استخدام تصفية MAC

على كل بطاقة شبكة هناك هو رمز خاص يسمى بال ماك عنوان يميزها عن غيرها من بطاقة الشبكة .التقطت صورة لبطاقة الشبكة حتى تستطيع أن ترى العناوين .في إعدادات جهاز التوجيه يمكنك ضبط إعدادات معظم، حتى أن هذا لا تسقط على شبكة لاسلكية، ولكن وفقا لقائمة محددة من العناوين.

بعض توضيح الباحث لمجموعة من الاساليب والطرق الحديثة لحماية الشبكات اللاسلكية يجب التطرق الي اهم المميزات التي يجب توافرها في نظام الحماية يسردها الباحث في نقاط

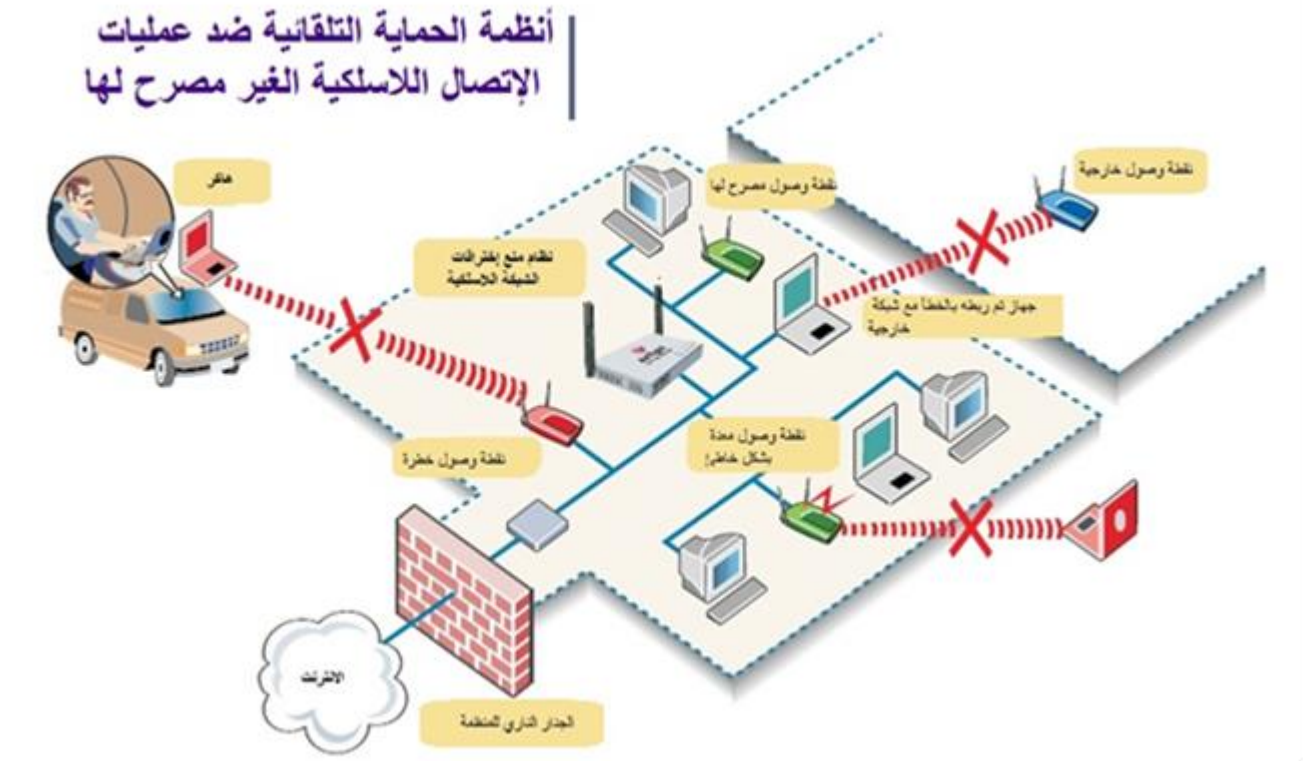
أهم المميزات الواجب توافرها في نظام الحماية:

- على النظام القيام بفحوصات تلقائية لجميع أنواع الثغرات الأمنية التي قد تسبب في الاختراق المفاجئ.
- ينبغي أن يكون هذا النظام قادر على تحديد موقع الثغرات الأمنية بأقل قدر ممكن من التنبيهات الغير صحيحة False-Positive مثال: تنبيه المستخدم بثغرة وهي بالأساس ليست بثغرة أو لا تشكل خطر.
- توفير مستودع (أو قاعدة بيانات) يتم فيها تخزين الثغرات الأمنية وتجارب محاولات الاختراق التي تم حدوثها لكي يستفاد منها في تعزيز أداء النظام لاحقاً.
- إمكانية تمثيل الفحوصات السابقة وعمليات الاختراق على هيئة تقارير دقيقة مصنفة بحسب أنواع الاختراقات ومتسلسلة نسبة إلى خطورتها.
- وتوفر إمكانية لمقارنة التقارير السابقة واقتراح الإجراءات التصحيحية.

أن أنظمة منع الاختراقات اللاسلكية WIPS يجب أن تكون سريعة الاكتشاف ويعتمد عليها، وقادرة على اكتشاف التسلل من معظم أجهزة نقاط الوصول الموجودة حالياً. ويجب الحرص على أن تكون الإعدادات سليمة لنقاط وصول الشبكة اللاسلكية، فهي المفتاح لحماية الشبكة من الاختراق.

ثم تطبيق المفاهيم السابقة ضمن الشبكات اللاسلكية عن طريق استخدام طرق المسح survey للمواقع اللاسلكية، وشرح المفاهيم التقنية لكيفية تحقيق أمن المعلومات في الشبكات اللاسلكية،

الشكل 4 يوضح بعض أنظمة الحماية التلقائية ضد عمليات الاتصال اللاسلكية الغير مصرح لها ويشرح الشكل الآلية المستخدمة عمل نظام منع اختراقات الشبكة اللاسلكية



شكل (4) يوضح لعملية لآلية عمل نظام منع اختراقات الشبكة اللاسلكية [فادي عمروش، السياسات الأمنية في الشبكات اللاسلكية،2012]

النتائج:

انتشار الشبكات اللاسلكية شيئاً فشيئاً ظهور الحاجة لفهم أمن المعلومات ضمن الشبكات اللاسلكية، وصولاً لكتابة سياسة أمنية فعالة للشبكة اللاسلكية.

بالنظر لخصوصية الشبكات اللاسلكية والمخاطر الأمنية التي تواجهها وربما يكون اختراق الشبكة اللاسلكية بوابة لاختراق للشبكة السلكية نظرا لسهولة الوصول إليه.

يشرح الباحث مجموعه من النتائج التي توصل اليها في هذه الورقة:

- خطر التجسس، قد يصل المستخدمون غير المخولين إلى البيانات المنقولة عبر شبكتك اللاسلكية.
- ان الصيانة المنتظمة للأجهزة المستخدمة في الشبكات اللاسلكية يساعد في ضمان المعلومة وسريتها وتنفيذ اختبار دوري لكشف نقاط الضعف من داخل الشبكة واستخدام أدوات قياس اداء الشبكة يمنع من مخاطر الاختراق للشبكة.
- وجود قواعد وأسس أمان واضحة سوف يعطي للجميع سواء كانوا على الشبكة أو الجهة المستفيدة من الشبكة فهم واضح ومعرفة واضحة عن مسؤولياتهم ودور كل واحد منهم في حماية الشبكة.

يوصي الباحث بعض النصائح لحماية الشبكات :

1-استخدام برنامج جدار الحماية جدار الحماية على جهازك المحمول.

نقاط الاتصال المجاني الساخن من أن تدفع في كثير من الأحيان أقل تأمين وتدفع نقطة لمتابعتها وحماية العملية وتغيير جميع متطلبات السلامة لديها مع التشفير.

2-إيقاف ميزة مشاركة الملفات على الجهاز لمنع وصول أي شخص لامتلاك ملفاتك أو حتى فتح المجال للمشاركة في ذلك، إزالة الخاصية من الملفات في القائمة أدوات خيارات المجلد.

3-إذا كان في ملفات خاصة ومهمة، ثم أغلقت بإحكام مع كلمة مرور. مدى سهولة ضغط الملفات التي تريد حمايتها وفي خيارات ستجد خيار خاص وضع كلمة مرور للملف على الرغم من أن الشخص الذي يقوم ملف من جهاز الكمبيوتر الخاص بك لن تكون قادرة فتحة ودائما استخدام كلمة مرور تتكون من الأرقام والحروف وعلامات الترقيم وأدنى من ثمانية أحرف صعوبة في فك تشفير.

4-هناك أيضا البرامج التي تضع بعد الملفات والمجلدات الكلمات وأيضا البرامج. للحد من استخدامها.

5-إيقاف بطاقة شبكة لاسلكية على جهازك المحمول. أنه لم يتم تشغيل زر الوضع على عبث الأجهزة النقالة. ولكن تم وضعه من أجل إغلاقه بعد الانتهاء من استخدامها. هذا وسوف توفر لك الطاقة الأولى وسيمنع الآخرين من الدخول أو حتى الوصول إلى جهازك.

المراجع

1. على ابوالحسن، الشبكات اللاسلكية (تقنية الحاضر والمستقبل) بغداد ،2012
2. فادي عمروش، السياسات الأمنية في الشبكات اللاسلكية، منشورات الندوة العلمية الخامسة عشرة (أمن الشبكات الحاسوبية).
3. قزانجي، فؤاد يوسف، عصر المعلومات في ظل تطور تكنولوجيا المعلومات، مجلة المنصور، بغداد، 2002.
4. محمد الرشيدى، أساسيات الشبكات، القاهرة، دار الكتب العلمية، 2011.
5. محمد شيخون، المصارف الاسلامية دراسة في تقويم المشروعية الدينية والدور (عمان: دار وائل للطباعة والنشر2002).
6. محمد محمد الهادي، تكنولوجيا المعلومات وتطبيقها، ط 1، دار الشروق، القاهرة، 1989م.

[1] Kelley, D. (2003). The X factor: 802.1 xs may be just what you need to stop intruders from accessing your network. Information Security, 6(8), 60-69.

[2] Kennedy, S. (2004). Best practices for wireless network security. Information Systems Control Journal (3).

[3] McDougall, P. (2004, March 25). Laptop theft puts GMAC customers' data at risk. Information Week Security Pipeline.

[4] Nokia. (2003). Man-in-the-middle attacks in tunneled authentication protocols.

[5] Kevin Beaver, Peter T. Davis, Devin K. Akin. Hacking Wireless Networks for Dummies. Retrieved 2009-02-09.

BIOGRAPHY

Dr. Yasser Elmalik Ahmed Seleman, Sudane

- PhD in Computer Science (Excellent) - Omdurman Islamic University - Sudan.
- M.Sc. In Information Technology - University of Newcastle- USA.
- M.Sc. In Information Technology - TheNational Ribat University .