[اختر التاريخ]

|  |
| --- |
| [اكتب العنوان الفرعي للمستند] | Ghazal |

|  |  |
| --- | --- |
| **العنوان** | **Electronic Security V.S Hacking** |

**تقديم : صبا عبد المجيد عيسى**

**بإشراف : م. علي جنيدي**

**تاريخ : 2015 – 2016**

# ملخص :

يعدّ هذا البحث باباً للدّخول في عالم الاختراق والهاكر ،حيث يتحدّث عن الاختراق آليته ،أسبابه بالإضافة إلى التّعريف بالهاكر وأنواعه .. وإلى جانب آخر ،فإنّه يتطرّق إلى أمن الشبكات اللاسلكية والخوارزميّات المُتّبعة لذلك ،وفي النّهاية تمّ الشّرح بشكل موجز عن توزيعة كالي لينكس وأهم الأدوات التي تعتمدها ؛بالإضافة إلى ذكر العديد من الخطوات الواجب على المستخدم اتّباعها لحماية ملفاته الشخصّية ..



**المركز الوطني للمتميزين**

***National Center For The Distinguished***

# مخطط البحث :

***الباب الأوّل***

* *الفصل الأول : مفهوم الاختراق ،أسبابه وأنواعه*
* *ما هو الاختراق*
* *أسباب الاختراق ودوافعه*
* *أنواع الاختراق*
* *الفصل الثّاني : Hackers*
* *من هو الـ Hacker*
* *أساليب الهاكر*
* *آليات الهاكر*

***الباب الثاني***

* *الفصل الأول : التّعرف على بعض المفاهيم*
* *ما هي الـ port*
* *الـ ip*
* *الفصل الثاني : التّعرف على بعض الملفات الخبيثة*
* *الفصل الثّالث : آليّة الاختراق*

***الباب الثالث***

* *الفصل الأول : الخصوصيّة المكافئة للشّبكة السلكيّة WEP .*
* *الفصل الثاني : الوصول المحمي للشبكة اللاسلكيّة WPA .*
* *الفصل الثّالث : خوارزميّات التّشفير المُتّبعة للحماية .*
* *خوارزميّة RC4*
* *خوارزميّة AES*
* *الفصل الرّابع : Wps .*

***الباب الرّابع***

* *الفصل الأوّل : Kali Linux*
* *تاريخ Kali Linux*
* *مميزات توزيعة Kali Linux لاختبار الاختراق*
* *الفصل الثاني : Kali Linux & Hacking*
* *الفصل الثالث : الحماية من الاختراق*

# مقدمة

*عصرنا الحالي عصر التطور التكنولوجي والمعلوماتيّ ،فقد بات استخدام وسائل التكنولوجيا جزءا لا يتجزّأ من حياتنا اليوميّة ،فمن منّا اليوم بمعزلٍ عن استخدام أحدث أجهزة الاتّصال ؟؟!! ومَن منّا الآن لا يزال بعيداً عن شبكات التّواصل الاجتماعي ؟؟!!*

*أجل لقد ربطت شبكة الإنترنت العالم مع بعضه وجعلته صغيراً لدرجةٍ لا يتجاوزُ فيها حدود قريةٍ صغيرة ،أو حتّى أقلّ ،ولكن وبالرّغم من كلّ التّطور الذي توصلنا إليه في يومنا هذا لايزال حلم التّجدد المستمر والتّطور نصب أعين الكثير من المبرمجين والمطورين ،وقد بات الإنترنت الحاضنة الأمثل لأفكارهم وتجاربهم ،من هنا ومن رحم هذه التّجارب ولد مصطلح الاختراق ،فما هو الاختراق ؟ من هم المخترقون ؟؟ وهل بقي الاختراق ضمن إطار التطوير والمنفعة العامّة ،أم أنّه خرج عنه وبات يهدد الأمن ؟؟!! وإن كان كذلك فما هي الاجراءات اللازمة لحماية ملفاتنا الشخصيّة من أيدي المخربين ؟؟ وبما أن معظم عمليات نقل البيانات باتت تتمّ بشكل لاسلكي ،فما هي المعايير الّتي اعتمدت لحفظ الأمن اللاسلكي ؟؟!!*

*كلّ هذه الاستفسارات كانت الدّافع لهذا البحث الّذي سيجيب عنها جميعاً ،بالإضافة إلى أننا سنتطرّق على نظام كالي لينكس الذّي يعدّ ذو دور مهم ورائد في مجال الاختراق والحماية من الاختراق ...*

# الباب الأول

## الفصل ألأول : مفهوم الاختراق ،أسبابه وأنواعه

### ما هو الاختراق :

*يسمى الاختراق باللغة الانجليزية Hacking وباللغة العربية الاختراق أو التجسس ،والاختراق بشكل عام هو القدرة على الوصول إلى هدف معيّن بطرق غير مشروعة عن طريق ثغرات في نظام الحماية الخاص ،وعندما نتكلّم عن الاختراق بشكل عام فنقصد بذلك قدرة المخترق على الدخول إلى جهاز شخص ما بغضّ النّظر عن الاضرار التي قد يحدثها ،فحينما يستطيع الدّخول إلى جهاز آخر فهو مخترق Hacker ،أمّا عندما يقوم بحذف ملف أو تشغيل آخر أو جلب ثالث فهو مخرّب Cracker ..[[1]](#footnote-1)*

### أسباب الاختراق ودوافعه :

*لم تنتشر هذه الظاهرة لمجرد اللعب وإن كان العبث وقضاء وقت الفراغ من أبرز العوامل التي ساهمت في تطورها وبروزها إلى عالم الوجود ،ويمكن تلخيص دوافع الاختراق بالدوافع الثلاث الآتية :*

1. *الدّافع السّياسي والعسكري*

*ممالا شك فيه أن التطور العلمي والتقني أدّيا إلى الاعتماد بشكل شبة كامل على أنظمة الكمبيوتر في أغلب الاحتياجات التّقنية والمعلوماتية ؛فمنذ الحرب الباردة والصراع المعلوماتي و التّجسسي ،ومع بروز مناطق جديده للصراع في العالم وتغير الطبيعة المعلوماتية للأنظمة والدول ، أصبح الاعتماد كليّاً على الحاسب الآلي وعن طريقه أصبح الاختراق من أجل الحصول على معلومات سياسيّة وعسكريّة واقتصاديّة مسألةً أكثر أهميّة.*

1. *الدّافع التّجاري*

*من المعروف أنّ الشّركات التّجارية الكُبرى تعيش هي أيضاً فيما بينها حرباً مستمرة ،وقد بيّنت الدّراسات الحديثة أنّ عدداً من كبرى الشّركات التّجارية يُجرى عليها أكثرَ من خمسينَ محاولة اختراقٍ لشبكاتها كلّ يوم.*

1. *الدّافع الفردي*

*بدأت أولى محاولات الاختراق الفرديّة بين طلاب الجامعات في الولايات المتحدة كنوع من التّباهي بالنجاح في اختراق أجهزة شخصيّة لأصدقائهم ومعارفهم وما لبثت أن تحولت تلك الظّاهرة إلى تحدّي فيما بينهم في اختراق أنظمة الشّركات ثمّ مواقع الإنترنت ،ولا يُقتصر الدّافع على الأفراد فقط بل توجد مجموعات ونقابات أشبه ما تكون بالأندية وليست بذات أهداف تجارية .*

*كما أن هنالك بعض الأفراد في شركات كبرى في الولايات المتّحدة ممن كانوا يعملون مبرمجين ومحللي نظم تم تسريحهم من أعمالهم للفائض الزائد بالعمالة فصبّوا جُمّ غضبهم على أنظمة شركاتهم السّابقة فاقتحموا تلك الشّركات وخرّبوا كلّ ما وقع تحت أيديهم من معلومات حسّاسة بقصد الانتقام .[[2]](#footnote-2)*

### أنواع الاختراق :

*يمكن تقسيم الاختراق من حيث الطّريقة إلى ثلاثة أقسام :*

1. *اختراق المزودات أو الأجهزة الرّئيسيّة للشركات أو المؤسّسات أو الجهات الحكوميّة*

*وذلك باختراق الجدران النّاريّة الّتي توضع عادةً لحمايتها وغالباً ما يتمّ ذلك باستخدام المحاكاة Spoofing وهو مصطلح يطلق على انتحال الشخصيّة للدّخول إلى النّظام حيث أن حزم الـ IP تختوي على عناوين للمرسل والمرسل إليه وهذه العناوين ينظر إليها على أنها عناوين مقبولة وسارية المفعول من قبل البرامج وأجهزة الشّبكة ،ومن خلال طريقة التّعرف بمسارات المصدر Source Routing فإن حزم الـ IP تمّ إعطاءها شكلا تبدو معه وكأنّها قادمة من كمبيوتر معيّن بينما في حقيقة الأمر ليست قادمة منه ،وعلى ذلك فإنّ النظام إذا وثق بهويّة عنوان مصدر الحزمة ؛فإنّه يكون بذلك قد حوكي (خُدع) وهذه الطّريقة هي ذاتها الّتي نجح فيها مخترقوا الـ Hotmail في الولوج إلى معلومات النّظام ذات مرّة ..*

1. *اختراق الأجهزة الشّخصيّة و العبث بما تحويه من معلومات*

*وهي وللأسف طريقة شائعة ؛وذلك لسذاجة أصحاب الأجهزة الشّخصيّة من جانب ولسهولة تعلّم برامج الاختراقات وتعدّدها من جانب آخر .*

1. *التّعرض للبيانات أثناء انتقالها والتّعرف على شفرتها إذا كانت مشفّرة*

*وهذه الطّريقة تستخدم في كشف بطاقات الائتمان وكشف الأرقام السرية للبطاقات البنكيّة ATM ،وفي هذا السّياق نحذّر من أمرين لا يتمّ الاهتمام بهما بشكا جدّي ،وهما عدم كشف أرقام بطاقات الائتمان لمواقع التّجارة الإلكترونية إلا بعد التّأكد بالتزام تلك المواقع بمبدأ الأمان ؛أمّا الثاني فبقدر أهميّته العالية إلا أنه لا يؤخذ على مأخذ الجديّة ،فالبعض عندما يستخدم بطاقة السّحب الآلي من أماكن البنوك النّقديّة ATM لا ينتظر خروج السند الصّغير المُرفق بعمليّة السّحب أو أنّه يلقي به في أقرب سلّة مهملات دون أن يكلّف نفسه عناء تمزيقه جيّداً ،ولو نظرنا إلى ذلك المستند سنجد أرقاماً تتكوّن من عدّة خانات طويلة هي بالنّسبة لنا ليست بذات أهميّة ،ولكننا لو أدركنا أن تلك الأرقام ليست إلا عبارة عن انعكاس الشريط الممغنط الظّاهر في الجهة الخلفيّة لبطاقة الـ ATM ،وهذا الشّريط هو حلقة الوصل بيننا وبين رصيد البنك الّذي من خلاله تتمّ عمليّة السّحب ،لأدركنا أهميّة التّخلص من المستند الصّغير بطريقة مضمونة ونقصد بالضّمان هنا عدم تركها فالهاكر المحترف يمكنه استخراج رقم الحساب البنكي والتّعرف على الأرقام السريّة لبطاقة الـ ATM .[[3]](#footnote-3)*

## الفصل الثّاني : *Hacker*

### من هو الـ *Hacker*

*هذه الكلمة تعود إلى ستينيّات القرن العشرين حيث وصف مبرمجو تلك الفترة بالـ Hacker نظراً للخبرة الواسعة والتّعامل السّلس مع أسطر الأوامر وحلّ جميع المشاكل البرمجيّة وتمكّنهم من برمجة لوغاريتمات تفهمها الحواسيب ،ومنه فالـ Hacker هو أيّ شخص قادر على التّعامل مع الكمبيوترات والأجهزة الرّقميّة بخبرة ودراية وكذلك يكون قادر على إنشاء وحل مشاكل داخل هذه الأنظمة ،ولكن قد ارتبطت هذه الكلمة فيما بعد بالشّر فأصبح الشّائع لدى العامّة أنّه ذلك الشّخص السّيئ الّي يسرق معلوماتهم الهامّة ويخرّب أجهزتهم ويتسبّب لهم في خسائر ماديّة ومعنويّة رغم أنهم لم يفعلوا له شيء ،لكن الحقيقة ليس بالضّرورة أن يكون كلّ الهاكر سيّئين لهذه الدّرجة فهم ينقسمون إلى ثلاثة أنواع لكلّ منهم توجهه الخاصّ ،ويُعرَفون حسب أهدافهم على النّحو التّالي :*

***الهاكر الأخلاقي (الهاكر الأبيض)***

*وهو الشّخص المصرّح له فحص شبكات وأنظمة شركة معيّنة لقاء مقابل مادي بهدف كشف الخلل داخل هذه الأنظمة وتصحيحه بدون إلحاق أي ضرر بها ،بهدف زيادة مستوى الأمان والحماية ،أي وببساطة هو شخص يستعمل قدرته العلميّة في التّعامل مع الأجهزة الرّقميّة وكشف الثّغرات الأمنيّة في الإطار القانونيّ فقط ،وفي العادة يسمّى مُختَبِر حماية .*

***الهاكر اللاأخلاقي (الهاكر الأسود)***

*هو الشّخص السّيئ الّذي يعمل كذلك على كشف نقاط الضّعف داخل الشّبكات والأنظمة ولكن بقصد التّخريب والتّدمير أو السّرقة سواء بهدف الرّبح المادي أو التّهديد أو الدّفاع على قضيّة معيّنة لكن في الغالب يكون الامر بداعي التّسلية وإبراز إمكانيّاته .*

***الهاكر الرّمادي***

*من الصّعب شرح أو فهم شخصيّة هذا الهاكر فهو أصلاً لا يعلم من هو فأحياناً يكون أسود وأحياناً يكون أبيض حسب الظروف الّتي يمرّ بها وحسب مزاجه الخاص فهز مزيج بين الأبيض والأسود .*

### أساليب الهاكر

***هجمات حجب الخدمة DOS :*** *عمليّة خنق السيرفر وذلك من خلال إغراقه بالبيانات إلى أن يصبح بطيئاً أو حتّى قد يتعطّل وينفصل كليّاً عن الشّبكة .*

***تجاوز سعة المخزّن المؤقّت Buffer Overflow :*** *يتمّ الهجوم عن طريق إغراق ذاكرة الخادم بالطّلبات فيصاب بالشّلل .*

***الثّغرات الأمنيّة Exploits :*** *يقوم الهاكر في هذه الحالة بدراسة معمّقة للسيرفر من جميع الجوانب وجمع المعلومات المتعلقة به مثل نوع نظام التّشغيل ،المنافذ المفتوحة في السيرفر ،البرامج المثبتة عليه ،وغيرها من الأمور المهمّة التي تساعده فيما بعد على تحديد وإيجاد ثغرة داخل النّظام تمكّنه من الولوج إلى إدارة السيرفر بصفة مسؤول والعبث به كما يشاء .*

***أحصنة طروادة Trojan horse :*** *يزرع الهاكر داخل الجهاز المستهدف برنامج متنكر على هيئة ملفات برامج الإدارة حيث يعمل الأخير على فتح باب خلفي يمكن الهاكر من التّسلل في الخفاء إلى السيرفر والتجسس ...[[4]](#footnote-4)*

### آليات الهاكر

***التّنصّت Sniffing :*** *الاستشعار وأخذ البيانات والمعلومات من الشّبكة عن طريق ما يُسمّى ببرامج المسح scan والتي تُسجّل كلّ ما يدور بين الكومبيوترات وفي هذه الحالة يجب أن يكون الجهاز الذي يقوم بالمسح مرتبط بالشّبكة ،فيقوم بقراءة كافّة البيانات الّي تمر بالشّبكة وتحليلها .*

***الهندسة الاجتماعيّة Social Engineering :*** *وهي أسلوب انتحال شخصيّة أخرى حيث يستخدمها الهاكر للحصول على معلومات مطلوبة للاقتحام ؛حيثُ يتمّ إقناع الشّخص المراد أخذ المعلومات منه بأنّ الهاكر صديق أو ما شابه ،أو أحد الأفراد الّذين يحقّ لهم الحصول على المعلومات ،لدفعه إلى كشف المعلومات الّتي لديه والّتي يحتاجها الهاكر ،وفي هذه الحالة يجب على الهاكر عند استخدام أسلوب الهندسة الاجتماعيّة أن يكون شخص قويّ الشّخصيّة ذو أسلوب على الإقناع .*

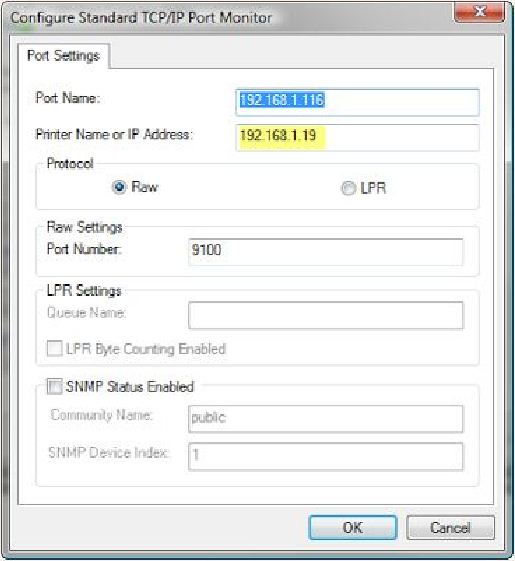
***تقصّي الشّبكات اللّاسلكيّة War driving :*** *عمليّة البحث مكانيّاً على وجود شبكات لا سلكيّة ،حيث يبحث الهاكر عن شبكات الـ Wi-Fi ويحاول استغلال وجود بيانات مشتركة بين المستخدمين لهذه الشّبكات وثغرات في الأجهزة الموصولة بالشّبكة تمكّنه من اختراقها .[[5]](#footnote-5)*

# الباب الثّاني

## الفصل الأوّل : التّعرف على بعض المفاهيم

### ماهي الـ Port

*يمكن وصفها ببوابات للجهاز ،وهناك عدد من المنافذ في كلّ جهاز ولكلّ منها غرض محدد وهذه المنافذ هي الّتي تسمح بنقل البيانات سواء بالاستقبال أو الإرسال وكلّ برنامج له بورت معيّن داخل النّظام .*

**

رسم توضيحي 1 : *Port Setting*

*يبلغ عدد البورتات في النّظام 65535 بورت بحيث تكون أوّل 1023 بورت محجوزة بأسماء بروتوكولات معيّنة مثل http و dnc .... [[6]](#footnote-6)*

### Ip

*لكل جهاز مرتبط بالإنترنت عنوان أو رقم خاص به مثل الهواتف تماماً فإنّ كل هاتف له رقم خاص به و يتّصل بهاتف آخر ،وكما لا يوجد هاتفان يحملان الرّقم ذاته كذلك لا يوجد جهازان مرتبطان بالإنترنت يحملان الرّقم ذاته ،بالتّالي يمكننا اعتبار الـ ip address بمثابة هويّة الحاسوب تقريباً ،وإنّ الـ ip هي اختصار لـ internet protocol .*

*وتكمن فائدته من خلال مساعدته في تبادل الملفّات عبر الإنترنت ،وإمكانيّته في تحديد وكشف المواقع من خلال وضع الـ ip في موقع ما مهمّته الكشف عن المواقع ،وهو يتكون من 4 أرقام وكل جزء منها يشير إلى عنوان معين فأحدها يشير إلى عنوان البلد والثاني يشير إلى عنوان الشركة الموزعة والثالث إلى المؤسسة المستخدمة والرابع هو المستخدم ..ورقم ip متغيّر وغير ثابت فهو يتغيّر مع كل دخول إلى الإنترنت ...[[7]](#footnote-7)*

## الفصل الثّاني : التّعرف على بعض الملفّات الخبيثة

*توجد العديد من الملفّات الخبيثة ولكلّ منها آلية ووظيفة معيّنة ،سنتعرّف الآن على بعض هذه الملفّات ونميّز فيما بينها ،ولكن وقبل التّحدّث عن هذه البرامج سوف نقسّمها إلى مجموعتين ،المجموعة الأولى هي Malware "البرمجيات الخبيثة" والمجموعة الثّانية هي Spyware "برمجيّات التّجسس*

***البرمجيات الخبيثة***

*البرمجيات الخبيثة عبارة عن أيّ فيروسات تمّ تصميمها من أجل تدمير وإتلاف الحاسوب الخاص بك بدلا من سرقة البيانات والمعلومات الحساسة الّتي قد تكون مخزّنة عليه ،وتتضمّن الفيروسات العاديّة و Rootkits, Worms, Trojans والعديد من الأمور الأخرى ..*

***برمجيّات التّجسس***

*برمجيات التّجسس عبارة عن برنامج يتمّ تنصيبه على الحاسوب الخاص بك بدون علمك ،ويقوم هذا البرنامج بتجميع معلوماتك وبياناتك الحسّاسة وإرسالها إلى حاسوب آخر .*

*سنتكلّم الآن عن الفيروسات وأشكالها المتعددة ...*

***Virus***

*الفيروس عبارة عن برنامج بسيط يقوم بعمليّة نسخ ذاتيّة ويستطيع التنقّل من حاسوب إلى آخر من أجل القيام بذلك ،يحتاج الفيروس إلى السّيطرة على نلفّ exe وإتلافه ،وعند تشغيل ذلك الملف يقوم الفيروس بالانتشار والانتقال إلى ملفات exe أخرى ،وبمعنى آخر يتمكّن الفيروس من الانتشار والسّيطرة على الحاسوب ،ولكن لكي يتمّ ذلك يحتاج الفيروس لمساعدة المستخدم عن طريق فتح الملفات التّنفيذيّة "ذات الامتداد exe" ،ومن أكثر أنواع الفيروسات انتشارا Macro Virus ،وهذه الفيروسات تستحوذ على ملفات Microsoft المعروفة مثل Word, Power Point, Excel ,Outlook .*

***Worm***

*برمجيات worms أو كما يطلق عليها (الدّودة) تتشابه بشكل كبير مع الفيروس ،باستثناء أنّها تستطيع نسخ نفسها بنفسها ،فهي لا تحتاج إلى ملف تنفيذي للقيام بهذه العمليّة ،فهي غالباً ما تستخدم الشّبكة للقيام بذلك ،مما يجعلها أخطر من الفيروسات ،كما أنّ بإمكانها إتلاف الشّبكة ككل .*

*تنتشر برمجيّات Worms بسبب الثّغرات في نظام التّشغيل ،لذلك يفضّل تحميل وتنصيب التّحديثات المختلفة لنظام التّشغيل في أسرع وقت ممكن .*

***Rootkit***

*هذا النّوع من البرمجيات الخبيثة من أصعب الأنواع التي يمكن إيجاديها والتّعرف عليها ،فهي دائما ما تحاول إخفاء نفسها عن المستخدم ،نظام التّشغيل وبرامج مقاومة الفيروسات ،وهذا النّوع من البرمجيّات يستطيع تنصيب نفسه على الحواسيب من خلال العديد من الطرق منها الثّغرات في نظام التّشغيل .*

*بعد تنصيب الـ Rootkit على اجهاز يقوم بإخفاء نفسه عن المستخدم والسّيطرة على نظام التّشغيل وبرامج الـ Software المقاومة لها وإجبارها على التّعرف عليها في المُستَقبِل ،أو قد تقوم بإلغائها تماماً ،كما أنه من الممكن أن تقوم بتنصيب نفسها بداخل نواة نظام التّشغيل ،وغالباً ما يكون الحلّ الوحيد في هذه الحالة هو إزالة نظام التّشغيل وتنصبه مرّة أخرى .*

***Trojan***

***رسم توضيحي 2 : Trojan Sympol***

*الـ Trojans أو كما يعرفه البعض باسم (حصان طروادة) ،ومن الواضح أنّه سميّ بهذا الاسم وفقاً للتاريخ اليوناني القديم ،هو عبارة عن برمجيّات خبيثة لا تقوم بإعادة نسخ نفسها ،ولكن بدلاً من ذلك يقوم هذا النّوع من البرمجيّات بتنصيب نفسه على الحاسوب الخاص بالمستخدم ،وكانّه برنامج Software عادي ،فهذه البرامج تخدع المستخدم وتقدّم نفسها بشكل عادي لتقنعه بعمليّة التّنصيب . فور تنصيب الـTrojans على الحاسوب ،لا يحاول الاستحواذ على ملف تنفيذي مثل الفيروس ،ولكن بدلاً من ذلك تمكّن هذه البرامج مستخدمها من التّحكم في الحاسوب بشكل لاسلكي .[[8]](#footnote-8)*

## الفصل الثّالث : آليّة الاختراق

*قبل التّحدث عن آليّة الاختراق يجب أن نأخذ فكرة عامّة عن ماذا يحدث عندما يريد حاسوب أن يتبادل شيء ما مع حاسوب آخر. عندما تحدث عمليّة التبادل بين حاسوبين نحتاج إلى حزمة من البيانات (Packet) ،ويجب أن تحتوي هذه الحزمة على عنوان (Address) و منفذ (Port) :*

*ا****لعنوان The address***

1. ***Mac :*** *وهو عنوان ثابت ،وكلّ حاسوب يملك mac خاص به ويكون قد تمّ وضعه من قبل الشّركة ولا يمكن تعديله .*
2. ***Ip :*** *أيضاً لكلّ حاسوب عنوان ip خاص به ،ولكن هذا العنوان غير ثابت فهو قابل للتغيّر وكما أشرنا سابقاً يوجد نوعان للـ ip address وهما عناوين خاصّة وعناوين عامّة ،وعند نقل البيانات نحتاج إلى Source ip ( الخاص بالحاسوب المرسل ) ،وإلى destination ip ( الخص بالمستقبل ) ؛وذلك من أجل الـ respond (أي لكي يتمكّن من عكس حزمة البيانات "Packet" ) .*

***المَنْفذ The port***

*عندما تخرج الـ packet ،لا تستطيع الخروج بمفردها بل تحتاج إلى طريق معيّن ومحدّد وبما أن البورتات هي بمثابة بوابات الجهاز ؛فلذلك عند عملية تبادل البيانات بين حاسوبين يجب تحديد منفذ الخروج "Source port" ومنفذ الدّخول "destination port" ،وكما قلنا سابقاً فإنّ أوّل 1023 منفذ تكون محجوزة ببروتوكولات محدّدة ؛فبذلك يستطيع المرسل أن يخرج من أي منفذ فوق هذا الرّقم ،أيّ يكون الـ Source port أكبر تماماً من 1023 وأصغر أو يساوي 65535 (وهو العدد الكلّي للمنافذ في الجهاز) ،بينما يكون الـ destination port أصغر أو يساوي 1023 .*

والآن سنتحدّث عن عمليّة الاختراق ..

*فلنفرض أنّه لدينا حاسوبان هما xو y ويريد الحاسوب x اختراق الحاسوب y فعندها يكون x عبارة عن المُخترِق ""hacker ويكون y عبارة عن الضّحيّة victim" " ،ولكي تتمّ عمليّة الاختراق توجد برامج خاصّة للاختراق تمتلك إعدادات خاصّة ،ومن خصائص هذه البرامج أنّها تصنع ملفّات صغيرة مثل الـ Trojan ويكون حجمها صغير (30kb, 100kb ,500kb ) ،وعند عمليّة الاختراق يرسل x الملفّ إلى y عن طريق البريد الإلكتروني أو من خلال دمجه بصورة أو فيديو مع الإشارة إلى أن x يكون قد قام بعمليّة فتح البرنامج (البرنامج الخاص بالتّهكير ) وعند وصول الملف إلى الجهاز y يقوم الـ Trojan باتّصال عكسي "Reverse Connection" ويظهر ذلك على جهاز الهاكر ،وعندها يتمكّن من تصفّح جميع محتويات الجهاز ويقوم بما يريد (أي أنّه يملك التّحكم الكامل)*

ولكن هل من الممكن أن تتم العمليّة المعاكسة ؟ أي هل يمكن للـ Trojan أن يتّصل بالبرنامج ؟؟

*عندما كان الاتّصال بالإنترنت عن طريق خطّ الهاتف كان real ip وبالتّالي كان الاتّصال بالنّت يتمّ بشكل مباشر ،وكان عندما يرسل الـ Trojan كان يُكتَب في إعداداته (عندما يُضغط عليك أرسل الـ ip إلى البريد الإلكتروني) ،وبالفعل عندما يضغط الضّحيّة عليه يُرسل الـ ip إلى البريد الإلكتروني وعندها يقوم الهاكر في كتابته على البرنامج وبعد ذلك يتّصل الهاكر بالضّحيّة لأنّ كلاهما يملك real ip وبالتّالي سيكون مسار الحزمة "packet" صحيح ...*

*أما الآن فالاتّصال بالإنترنت لم يعد عن طريق خط الهاتف بل عن طريق ADSL وهو يحتاج إلى راوتر ؛أي أنّ التّعامل مع شبكة الإنترنت أصبح يتمّ بشكل غير مباشر فيجب أن يخرج الـ Trojan من الـ ip الخاص بالراوتر وهو متغيّر وهذا غير مناسب ..*

*ولكن يوجد حلان لهذه المشكلة :*

* *الحل الأوّل : أن تذهب إلى الـ Server وتطلب تثبيت الـ ip الخاص بالرّاوتر ،ولكنّ هذه عمليّة مكلفة .*
* *الحل الثّاني : نكتب مكان الـ ip في إعدادت الـ Trojan اسم (السم يبقى ثابت) ونربط الـ ip الخاص بالرّاوتر به ونقوم بعملية إعادة توجيه "forward" وندخل إلى الرّاوتر عن طريق اسمه ،ثم ندخل إلى خياراته ،وبعد ذلك نمرّر الـ packet إلى الـ private ip في الشّبكة الدّاخليّة "internal network" ولكن إذا كان الرّاوتر محمي بكلمة سرّ فهنالك حلّ إضافي وهو أن نقوم بشبكة وهميّة VPN ،حيث تقوم بالاتصال بأحد المواقع الّتي تعطيك real ip - وليس private ip - فور الاتّصال بها ،بالتّالي يصبح جهازك متّصل بالنّت مباشرة وعندها تكتب الاسم بشكل عادي في إعدادات الـ Trojan وعندها ستُوجَّه الـ packet إلى راوتر الشّركة ثمّ إلى الـip الخاص بك ...*

# الباب الثّالث

*منذ أن ظهر الحاسوب ظهرت فكرة الرّبط بين حاسوب وآخر ممّا أدى إلى ظهور الشّبكة ،والشّبكة هي عبارة عن مجموعة من الحواسيب المتّصلة مع بعضها البعض سواء أكان هذا الاتّصال عن طريق الكابلات أو عن طريق الأمواج اللاسلكيّة ،ومن هنا أصبح لدينا نوعان من الشّبكات : الشّبكات السّلكيّة و الشّبكات اللّاسلكيّة .*

*انتشرت الشّبكات اللّاسلكيّة في هذا العصر انتشارا مذهلاً وأصبحت تُستخدم بشكل واسع في الاتّصال ونقل وتبادل البيانات بين أجهزة الحواسيب في المنازل وفي الشّركات وفي القطّاعات الكبيرة .*

*الشّبكات اللاسلكيّة تختلف عن نظريتها السّلكيّة ؛حيث أنّ البيانات تنتقل في الهواء عوضاً عن الأسلاك وبالتّالي فإنّ التّجسّس على البيانات المنقولة بواسطة الشّبكة اللاسلكيّة لا يتطلّب من المخترق الاتصال فيزيائيّاً بأسلاك الشّبكة ،بل يمكن نظريّاً لأيّ شخص - يقع ضمن مجال تغطية الشبكة اللاسلكيّة – استراق النّظر إلى البيانات المنقولة مالم تكن محميّة بشكل ملائم ،وهذا شيء غير جيّد عند نقل وتبادل البيانات المهمّة والحسّاسة والسّريّة والأمنيّة ،فهو بذلك لا يحفظ الخصوصيّة وهو أيضاً لا يحفظ سلامة البيانات ؛حيث أنّها تكون عرضة للتّعديل من أيّ أحد .*

*لذلك أنشأ المعهد الدّولي لمهندسي الكهرباء والإلكترون (( Institute of Electrical and Electronic Engineers IEEE معايير أمنيّة لحفظ الاتّصال اللاسلكي ليضمن بذلك سلامة البيانات وخصوصيّتها أثناء انتقالها عبر الشّبكة . ومن أكثر المعايير شيوعاً مجموعة معاييرIEEE 802 LAN/WAN والّتي تتضمّن معيار شبكات الإنترنت (IEEE 802.3) ومعيار الشّبكات اللاسلكيّة (IEEE 802.11) ،كما أنّه وضع معايير وبروتوكولات لتشفير الاتّصال اللاسلكي ؛بحيث تبدو البيانات المرسلة كالطّلاسم بناءً على قواعد تشفير معيّنة لا يستطيع فكّها إلّا الجهة المُستقبلة .*

*إنّ تشفير الاتّصال لا يمنع المتلصصين من الاطّلاع على البيانات المرسلة على الشّبكة ،ولكن وعلى الأقلّ يقوم بحفظ محتوياتها وقيمتها فكلّ ما سيحصلون عليه هو مجموعة من الرّموز والإشارات الّتي لن يعرفوا معناها لعدم معرفتهم بقواعد التّشفير .*

*وتتضمّن أهم بروتوكولات التّشفير في الشّبكات اللاسلكيّة كلّا من بروتوكول الخصوصية المكافئة للشبكة السلكيّة WEP (Wired Equivalent Privacy ) ،وبروتوكول الوصول المحمي للشّبكة اللاسلكيّة WPA (Wi-Fi Protected Access) .[[9]](#footnote-9)*

## الفصل الأوّل : الخصوصية المكافئة للشبكة السلكيّة WEP

*هو أحد البروتوكولات الشّائعة الاستخدام لتشفير البيانات المنقولة عبر الشّبكات اللاسلكيّة لمنع المتلصّصين من الحصول عليها أو تعديلها ،وهو اختصار (Wired Equivalent Privacy) وتعني خصوصيّة التّوصيل المتكافئ ،وقد شكّل جزء من المعيار الأساسي للشبكات اللاسلكيّة IEEE 802.11 في عام 1999 م ،ويعتبر هذا التّشفير هو الأصل لمستخدمي هذا المعيار .*

*ولأنّ تأمين الشّبكات اللاسلكيّة أصعب من تأمين الشّبكات السلكيّة بحسب طبيعتها واعتمادها على البثّ الّذي يتيح للآخرين التقاطه ،جاءت فكرة هذا البروتوكول لإعطائها الأمان والخصوصيّة المماثلة الّتي توفّرها الشّبكات السّلكيّة .*

*يستخدم WEP خوارزميّة تشفير تُدعى RC4 - والّتي سنتحدّث عنها بشكل مفصّل لاحقاً – ولكن وبشكل عام تقوم RC4 بتقسيم البيانات المرسلة إلى مجموعة أجزاء حجم كلّ منها واحد بايت ثمّ تأخذها الواحد تلو الآخر ،يدخل إليها واحد بايت وتعالجه باستخدام مفتاح معيّن لتنتج واحد بايت آخر مختلف عن البايت المدخل وهكذا لجميع الأجزاء الأخرى ،ويسمّى هذا النّوع من التّشفير بالتّشفير التّدفقي (Stream Cipher) ،وتتميز RC4 بأنّها متناظرة ؛أي أنّها تفكّ تشفير البيانات بطريقة معاكسة لطريقة تشفيرها .*

*يستخدم WEP مفتاح سرّي مشترك يتمّ تداوله لجميع أعضاء الشّبكة ،أي أنّه على المرسل والمستقبل معرفة المفتاح لتشفير البيانات ولفك التّشفير ؛فالمرسل يشفّر البيانات ويرسلها وعندما تصل إلى المستقبل بفكّ تشفيرها باستخدام المفتاح نفسه المتّفق عليه وبذلك يمنع المتلصصين من قراءة البيانات والتّعديل عليها ،ويجب أن يعرف المفتاح على نقطة الوصول للشبكة (Access Point) وجميع أعضاء الشّبكة .*

*وينقسم مفتاح السّريّة المشترك لأعضاء الشّبكة اللاسلكيّة إلى جزئين :*

* ***الأوّل :*** *يسمّى القيمة الابتدائيّة (Initial Vector) وهو عبارة عن 24 Bit وهو لا يشفّر .*
* ***الثّاني :*** *عبارة عن 40 Bit أو 104 Bit وهو الّذي تستخدمه الخوارزميّة RC4 لتشفير البيانات ،ويقوم بعض منتجي الأجهزة بالتّرويج لها بالقول بأنّ طول المفتاح السّري الّذي تستخدمه 128 Bit ،وفي حقيقة الأمر هو مكوّن من 104 Bit مضافاً إليها القيمة الابتدائية 24 Bit .*

*هناك نوعان من WEP بناء على طول المفتاح المستخدم :*

* *WEP64 وتعني (40 Bit + 24 Bit "Initial vector" ) .*
* *WEP128 وتعني (104 Bit + 24 Bit "Initial vector" ) .[[10]](#footnote-10)*

*ويوجد أسلوبان لاستخدام المفاتيح في WEP :*

* *تستخدم كل الأجهزة ومحطّة الوصول على الشّبكة مفتاح واحد يسمّى المفتاح الافتراضي ،وعند إنشاء الشّبكة يُحمّل هذا المفتاح على جميع الأجهزة وتبرمج نقطة الوصول AP لاستخدامه . وتظهر المشكلة عندما يقرر بعض الأعضاء تغيير المفتاح ،فإذا تمّ تغيير المفتاح أوّلا في نقطة الوصول فسوف ينقطع اتّصال جميع الأعضاء بالشّبكة ،أمّا إذا تمّ إرسال رسالة إلى الأعضاء أن يغيّروا المفتاح إلى مفتاح آخر فلا شيء يثبت وصول الرّسالة إليهم جميعاً لأنّهم قد لا يكونون جميعاً على اتّصال بالشّبكة في ذلك الوقت .*
* *يستخدم كلذ جهاز مفتاحاً خاصّاً به لا يعرفه غيره إلّا نقطة الوصول ،وتسمّى هذه المفاتيح بمفاتيح المقابلة Key mapping key . وتظهر المشكلة عند إرسال نقطة الوصول رسالة عامّة للجميع Broadcast ،وتمّ حلّها باستخدام مفتاح افتراضي مشترك ليكون بذلك كلّ جهاز يحمل مفتاحين . ولكنّ العمليّة أصبحت أصعب بالنّسبة لنقطة الوصول فيجب أن يكون لديها قائمة بمئات المفاتيح ،وكلّما وصل إليها رسالة مشفّرة تبحث في القائمة عن المفتاح الخاص بهذا العضو لفك تشفيرها ،وهذه القائمة تحتج إلى حجم كبير في الذّاكرة وتوجد نسخة منها على كلّ نقطة مرور بالشّبكة ،وبالتّالي أصبحت إدارة المفاتيح أصعب وخاصّة في الأنظمة الكبيرة .*

*لم يدم WEP طويلاً ،فقد كان هدفاً للمتلصصين الّذين تمكّنوا من اختراقه بسهولة بعد عدّة محاولات ،وقد قامت عليه عدّة دراسات بغرض كشف عيوبه ،ومكامن الضّعف الّتي سهّلت اختراقه ،وكان منها :*

1. *يستخدم WEP مفتاح سري مشترك لجميع أعضاء الشبكة اللاسلكية وبالتالي يصعب تغييره بشكل دوري وخصوصاً بالقطاعات الكبيرة وهذا يجعل عمر المفتاح المشترك يطول مما يسهل عملية كشفه واختراق الشبكة.*
2. *المفتاح السري هو مشترك لجميع الأعضاء ويتم توزيعه يدوياً بينهم وهذا يجعل فرصة تسربه أكبر فهو عرضة أكثر لهجوم الهندسة الاجتماعية (Social Engineering Attack) وبالتالي اختراق الشبكة بكل سهولة.*
3. *ضعف في إدارة المفاتيح أي أنه عند تغيير المفتاح لابد من إخبار جميع الأعضاء وهذا يتطلب مزيداً من التكاليف والوقت خصوصاً أن عملية التغيير لابد أن تكون بشكل دوري لرفع مستوى الأمان لكن WEP لا يوجد لديها وقت ثابت لتغيير المفتاح وهذا يضعفها.*
4. *عند إرسال البيانات فإنّها ترسل على شكل أجزاء Packets فإنّ WEP لا يتحقّق من كلّ جزء وبهذا لا يستطيع ضمان سلامة الرّسالة المرسلة من التّعديل عليها .*
5. *WEP لا تحدد هوية الأعضاء نظراً لأنها تستخدم مفتاحاً مشتركاً واحداً لجميع الأعضاء وهذا يسهل عملية انتحال شخصية العضو وإرسال الرسائل وتعديل البيانات والاطلاع عليها دون أن يشعر بقية الأعضاء بذلك.*
6. *ا لمفتاح الذي تستخدمه قصير إضافة إلى أن القيمة الابتدائية فيه تكون غير مشفرة عند إرسال البيانات وهذا يساعد على معرفة عنوان المرسل والمستقبل ويسهل على المهاجمين استنتاج بقية المفتاح .*
7. *خوارزمية RC4 ضعيفة ويُبين ذلك دراسة نظرية لخوارزمية جدولة المفتاح الخاص بخوارزمية RC4 أجريت نهاية 2001م على يد الباحثين Adi Shamir وIstik Mantin وScott Fluhrer دعيت فيما بعد (FMS) و التي تبين أن الضعف يسمح للمهاجم في ظروف معينة استنتاج بعض من بايتات المفتاح السري لتوليد مفتاح ما عن طريق تحليل البايت الأول من المفتاح. وقد قام باحثون آخرون بتطبيق هجوم FMS على إحدى الشبكات التي تستخدم WEP لتشفير بياناتها وتمكنوا من استنتاج الرقم السري الذي يبلغ طوله 128-bit و يُعد هذا الهجوم اختراقاً كلياً لا يتطلب أي معدات خاصة ويمنح المهاجمين حرية الدخول إلى الشبكة وفك تشفير جميع البيانات المرسلة وإرسال الرسائل للآخرين بصفة شرعية و كل ذلك بعد القيام بعملية التوثيق (authentication) باستخدام المفتاح المشترك ،وقد قضى هذا الهجوم على بروتوكول WEP بشكل نهائي.*

*لذلك فإن WEP لا يتناسب مع القطاعات الكبيرة ،بل يمكن استخدامه في الشّبكات اللاسلكيّة المنزليّة أو في المؤسسات الصغيرة ،وهناك بعض الحلول لمعالجة هذه النقاط والتقليل منها :*

* *تقييد حقوق الوصول لتسمح بدخول عناوين MAC معينة .*
* *استخدام أقصى طول للمفتاح 128بت لزيادة صعوبة اختراق الشبكة .*
* *استخدام البروتوكول WPA2,WPA بدلاً من هذا البرتوكول .*
* *التحقق من اتّخاذ المستخدمين احتياطات الأمان اللّازمة .*[[11]](#footnote-11)

## الفصل الثّاني : الوصول المحمي للشّبكة اللاسلكيّة WPA

*وهو أحد بروتوكولات تشفير البيانات المتنقلة عبر الشبكة اللاسلكية ،صُمم بعد كشف الثّغرات الأمنية لبروتوكول WEP ، وهو اختصار (Wi-Fi Protected Access) ،وتعني الوصول المحمي هو عبارة عن برنامج (Firmware) صممته مجموعة WI-FI alliance عام 2003 م ،ثم اعتمد فيما بعد كجزء من المعيار الأساسي للشبكات اللاسلكية IEEE 802.11 في عام 2004م تحت مسمى WPA2.*

*تعد WPA مرحلة انتقالية وسيطة بين WEP و IEEE 802.11i يزيد من مستوى حماية البيانات ويتحكم في دخول المستخدمين إلى الشبكة اللاسلكية فلا يسمح إلا للأعضاء المصرّح لهم وهذا ما يجذب القطاعات والشركات الكبيرة لاستخدامه.*

*وتستخدم WPA بروتوكول تكامل مفاتيح التشفير المؤقتة TKIP وهو اختصار (Temporal Key Integrity Protocol) ويعتمد على خوارزمية RC4 التي يستخدمها بروتوكول WEP بينما تستخدم WPA2 خوارزمية تشفير عالميّة معياريّة جديدة تدعى AES .[[12]](#footnote-12)*

*كما أن WPA تدعم تكامل البيانات وسلامتها من العبث أثناء تنقُّلها على الشبكة باستخدام تقنيّة فحص سلامة الرسائل لميشيل MMIC وهو اختصار (Michael Message Integrity Check) ،ويعيب عليها البعض أنها إذا أحسّت بوجود مهاجم فإنها تعطل الشبكة عن العمل لمدة 30 ثانية وهذا يجعل العمل يتم ببطء.*

*WPA حلت مشكلة WEP فيما يتعلق بالتحقق من الهوية ؛فهي تضمن التوثيق ثنائي الاتجاه فكل من المُستقبل والمرسل يتحقق من هوية الأخر وذلك بتنفيذها لمعيار IEEE 802.1x واستخدام بروتوكول EAP وهو اختصار (Extensible Authentication Protocol)،ففي القطاعات الكبرى لابدّ من توفر خادم للتحقق من هوية المستخدم (Authentication Server) أما في المؤسسات الصغيرة والمنازل فلا داعي لوجود الخادم ويكفي استخدام المفتاح السري PSK وهو اختصار (Pre-Shared Key) وإدخال الرّقم السري اللازم لدخول المستخدم إلى الشبكة.*

*لكل عضو في الشبكة التي تستخدم WPA مفتاح سري خاص به يحدد هويته وصلاحيّاته على الشبكة وجميع هذه المفاتيح السريّة لكل الأعضاء تُحمل على نقطة الوصول وعندما يريد العضو الاتصال بالشبكة اللاسلكية يقوم بإدخال الرقم السري ثم تتحقق نقطة الوصول من هويته ثم تعطيه مفتاح سري خاص به وتتكرر هذه العملية في كل مرة يتصل العضو بالشبكة.*

*ويتكون المفتاح في WPA من 128 Bit و يماثل في ذلك بروتوكول WEP ولكنه يختلف في أن القيمة الابتدائية له 48 Bit بدلاً من 24 Bit ،وتكمن قوة WPA وصلابته في أنّ المفاتيح تتغيّر تلقائياً حيث لا يمكث المفتاح طويلاً مع المستخدم مما يصعب على المهاجم اختراق هذا النظام.*

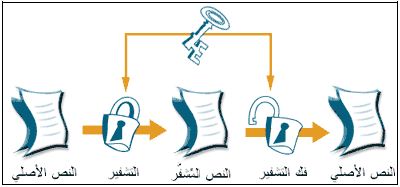
*ولكنّ WPA تمتلك أيضاً نقاط ضعف ،والّتي تتمثل بما يلي :*

* *قد تتوقف الخدمة وُيمنع المستخدم من دخول الشبكة إذا أدخل الرقم السري أكثر من مرة بصورة خاطئة وتسمى Dos وهي اختصار (Denial of service) .*
* *قد يحصل المهاجم على المفتاح السري أثناء الإرسال ويستخدم الهجوم المعجمي (Dictionary attack) للحصول على الرقم السري وبالتالي يدخل إلى الشبكة .*
* *WPA تستخدم خوارزمية تعتمد على RC4 وبالتالي فإن نقاط الضعف لا تزال موجودة حيث لم ينتهي الخطر بل زاد تعقيد العملية ،ولكنّ هذه المشكلة حُلت باستخدام WPA2 التي تستخدم خوارزمية تشفير ASE.*[[13]](#footnote-13)

## الفصل الثّالث : خوارزميّات التّشفير المُتّبعة للحماية

*إنّ خوارزميّات التّشفير من أهمّ الخوارزميّات الّتي اتُبعت في مجال الحماية ،وللتشفير عدّة أنواع أو أقسام ويُعدّ التشفير المتناظر أو ما يُعرف بالمفتاح السّري أحدُها ،و يعتمد فيه كلّ من المرسل والمستقبل المفتاح السّري ذاته ،حيث يقوم الأوّل باستخدام المفتاح لتشفير الرّسالة بينما يستخدمه الثّاني لفك تشفير الرّسالة وقراءتها .*

*أي أنّه في هذا النّوع من التشفير يكون ال مفتاح المستخدم للتشفير هو نفس المفتاح المستخدم لفك التّشفير ،وفي بعض الاحيان يكونان مختلفان ولكن يمكن اشتقاق أحدهما بسهولة من الآخر .*



رسم توضيحي 3 : التشفير المتناظر

*ومن أقسام التّشفير المتناظر التّشفير التّدفقي Stream Cipher وفي هذا النّوع يتمّ تشفير كل Bit من الرّسالة على حدة .[[14]](#footnote-14)*

*و تُعدّ خوارزميّة RC4 إحدى خوارزميّات التّشفير التّدفقي .*

### خوارزمية RC4

*كما أشرنا سابقاً فإن هذه الخوارزمية تندرج تحت خوارزميات التّشفير التّدفقي (Stream Cipher) الّتي تُعدّ بدورها قسم من أقسام التّشفير المتناظر .*

*صُممت من قبل Ron Rivest لشركة RSA لحماية البيانات سنة 1987م ،و سميّت RC4 اختصاراً لـ Rivest Cipher 4 ،كانت هذه الخوارزميّة سريّة حتّى سنة 1994م حيث تمّ نشر شفرتها المصدريّة على الانترنت بطريقة غير شرعيّة من قبل جهة مجهولة ،الشّفرة الّتي نشرت مطابقة تقريباً للخوارزميّة RC4 وتؤدّي نفس تطبيقاتها .*

*هذه الخوارزميّة من أكثر خوارزميّات التّشفير التّدفقي استخداماً ،وهي تستخدم في البروتوكولات المعروفة مثل بروتوكول طبقة المداخل الآمنة SSL (Secure Sockets Layer) وذلك لحماية حركة سير الانترنت Internet traffic .*

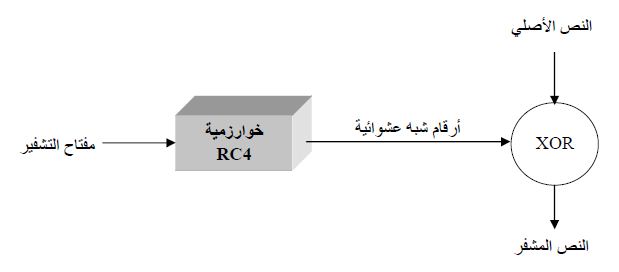
*لم تعد هذه الخوارزميّة تؤمّن الحماية التّامة لذلك لم يعد ينصح باستخدامها في الانظمة الحديثة ،ولكنّها مازالت تستخدم بكثرة في التّطبيقات المختلفة والعوامل الرّئيسية الّتي أدّت إلى انتشار استخدامها هي سهولتها حيث يمكن حفظ الخوارزميّة بأكملها في دقائق ،كذلك سرعتها في التّشفير وفك التّشفير .[[15]](#footnote-15)*

***فكرة عمل خوارزمية RC4***

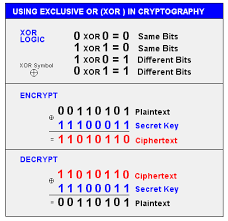
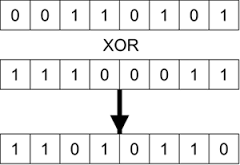
*الخوارزميّة RC4 بحدّ ذاتها ولكنّها تولّد قيم شبه عشوائيّة Pseudo-random values تسمّى المفتاح المتدفّق Keystream يستخدم في التّشفير وذلك بعمل XOR له مع النّص الأصلي ،ويستخدم لفكّ التّشفير بعمل XOR له مع النّص المشفّر ،هذا المفتاح المتدفّق يتولّد بواسطة مفتاح آخر يحدده المستخدم .*

*عمليّة XOR هي عمليّة منطقيّة يتمّ فيها مقارنة رقمين ثنائيين ،إذا كانا متشابهين تكون نتيجة العمليّة صفر ،أمّا إذا كانا مختلفين فتكون النّتيجة واحد .*

*عندما تزود الخوارزميّة بالمفتاح الّذي يحدّده المستخدم يتمّ تكوين جدول يسمّى جدول يسمّى جدول الحالة State Table يحتوي على جميع الحالات المحتملة ،وبعد ذلك يتمّ توليد القيم شبه العشوائيّة الّتي تستخدم في التّشفير وفك التّشفير .[[16]](#footnote-16)*



رسم توضيحي 4 : طريقة عمل الخوارزميّة *RC4*



رسم توضيحي 6 : آلية عمل البّوابة المنطقيّة *XOR* - (1).

رسم توضيحي 6 : آليّة عمل البّوابة المنطقيّة XOR - (2) .

***شرح خوارزميّة RC4***

*لبدء عملية التّشفير وفق RC4 نحتاج إلى مفتاح وغالباً ما يكون معرّف بين 40 Bit و 256 Bit ويُمثّل بخمس رموز ولكن وفق تمثيل الـ ASCII الّذي ينقلها إلى القيمة المقابلة لها في النّظام الثّنائي (ومثال على ذلك ،تمثيل الـ ASCII لـ "pwd12" يقابله 0111000001110111011001000011000100110010 في النّظام الثّنائي .*

*الخوارزميّة تنقسم إلى مرحلتين أساسيّتين :*

1. *مرحلة جدولة المفتاح KSA (The Key-Scheduling Phase)*

*for i from 0 to 255*

*S[i] := i*

*endfor*

*j := 0*

*for i from 0 to 255*

*j := (j + S[i] + key[i mod keylength]) mod 256*

*swap (S[i] , S[j])*

*endfor*

*KSA تنشئ مصفوفة S (أحاديّة البعد) التي تحوي 256 مُدخل من الرّقم 0 إلى الـ 255 وفق الجدول التّالي :*

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *255* | *254* | *253* | *…* | *i+1* | *i* | *…* | *2* | *1* | *0* |

*كل عنصر ذو المرتبة i من ال 256 عنصر من المصفوفة S يُبدل مع العنصر ذو المرتبة j وفق العمليّة التّالية :*

*j = [(j + S[i] + key[i mod keylength])mod 256]*

*بحيث يُمثّل j القيمة القديمة لـ j (التي تكون في البداية صفر ) ،و S[i] عبارة عن قيمة العنصر الحالي في الصفوفة S ،بينما key[i mod keylength] يكون إمّا صفر أو واحد .*

*مثال : إذا كنّا في العنصر ذو المرتبة 52 من المصفوفة S وكان الـ keylength عبارة عن 40-bit ؛بالتّالي 52 mod 40 = 12 ،فيكون العنصر 13 (لأنّ عناصر المصفوفة تبدأ من الصفر ) في النّسخة الثّنائيّة من "pws12" يكون 0 . ليكن العنصر ذو المرتبة 0 للمفتاح p ،وقيمته في الـ Ascii هي 112 ،بالتّالي يُحسب j وفق مايلي :*

*j = [(0 + 0 + 112)mod 256] = 112*

*وبعد ذلك يتم التّبديل بين العنصر ذو المرتبة i والعنصر ذو المرتبة j ،لنصل على المصفوفة التّالية وفق عمليّة التّكرار الأولى :*

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *255* | *…* | *114* | *113* | *0* | *111* | *…* | *2* | *1* | *112* |

*وبعد عمليّات التّكرار لـ KSA ،نحصل على مصفوفة شبه عشوائيّة .*

1. *مرحلة توليد القيم العشوائيّة PRGA (The Pseudo-Random Generation Algorithm)*

*i := 0*

*j :=0*

*while Generatingoutput :*

*i := (j + 1) mod 256*

*j := (j + S[i]) mod 256*

*swap (S[i] , S[j])*

*output S [ (S[i] + S[j]) mod 256 ]*

*endwhile*

*تبدأ مرحلة RPGA مع المصفوفة S الّتي خضعت لعمليّة تبديل في مرحلة KSA .في مرحلة PRGA يُبدّل العنصر ذو المرتبة i من المصفوفة S مع العنصر ذو المرتبة j ،والعنصر التّالي في النّص المشفّر هو عنصر من S ذو المرتبة (S[i] + S[j] mod 256) . وفي كلّ عملية تكرار يُعاد حساب الـ i كـ (i + 1)mod 256 ،ويُعاد حساب ال j وفق (j + S[i]mod 256) .ورقم التّكرار يُمثل طول المفتاح ،وكلّ قيمة لـ S تُبدّل على الأقل مرّة واحدة .*

*وتبعاً للمثال السّابق سنختبر عمليّة التكرار الأولى في مرحل PRGA :*

*من أجل i , j = 0 ،تصبح i تساوي 1 بينما تصبح j تساوي (0+S[1])mod256 . حيث S[1] = 124 (وفق نتيجة المصفوفة S في المرحلة KSA ) ،فتصبح j تساوي 124 .وبعد ذلك يتمّ تبديل العنصرين 1 و 124 .وبعد أن تتم عمليات التّكرار يكون المخرج وفق التمثيل الستّ عشري ومثال على ذلك "6CA86FE3CBC33C162595C3E"*

*وفي هذه الحالة وبالنّسبة لراوتر الشّبكة اللاسلكيّة سيتمّ طلب المفتاح من أجل توليد الرّمز . إذا كان المفتاح خاطئ فلن يكون النّص المشفّر المُخرج مناسب ،وبالتّالي لن يُسمح للمستخدم بالاتّصال بالرّاوتر .[[17]](#footnote-17)*

### خوارزميّة AES

*صُممت خوارزميّة الـ AES كخوارزمية تشفير لحماية البيانات الإلكترونيّة من الاختراق أو السّرقة أثناء انتقالها وهي اختصار لـ Advanced Encryption Standard )) ،وهي خوارزميّة مُطوّرة عن خوارزمية الـ RC4 وتختلف عنها من حيث حجم المفتاح ؛بحيث يكون على الأقل بحجم 128-bit أو قد يكون أيضاً 192-bit أو 256-bit .[[18]](#footnote-18)*

*تُستخدم هذه الخوارزميّة بالإضافة إلى خوارزميّة TKIP في بروتوكول حماية الشّبكات اللاسلكية الـ WPA/WPA2 ،وتُعدّ هاتان الخوارزميّتان من الخوارزميّات المُعقّدة الّتي تتغير بشكل مستمر مما يجعل اختراقها من قبل الهكر أمراً صعباً .[[19]](#footnote-19)*

***ملاحظة : يحوي المرجع*** [***(PDF) Announcing the Advanced Encryption Standard "AES"***](file:///D:\Research\AES.pdf)  ***على شرح مُفصّل عن هذه الخوارزميّة بالإضافة إلى الكود البرمجي لها مُرفقاً مع شرح كّ خطوة .***

## الفصل الرّابع : Wps

*هي اختصار لـ ( Wi-Fi Protected Setup )هو عبارة عن وسيلة تمّ تطويرها وتقديمها من قبل اتّحاد Wi-Fi لمساعدة المستخدمين على إعداد اتّصالاتهم اللاسلكية بأجهزتهم ؛فبدون wps سيجد المستخدم نفسه مضطرّاً لاتّخاذ عدّة خيارات قبل أن يتمكّن من الاتّصال بالـ router الخاص به ،مثل خوارزميّة التّشفير وطول كلمة السّر وصيغتها ... الأمر الّذي يعني أنّه يجب أن يكون لدى المستخدم خلفيّة لا بأس بها حول هذه النّواحي . أمّا بالنّسبة لـ wps فكلّ ما على المستخدم القيام به هو الضغط على زر Wi-Fi Protected Setup في حال توفّره وإدخال PIN (بطول 8 أحرف ) خاص بالجهاز ومن ثمّ البدء بالاتّصال مباشرةً .*

*وبقيت هذه الوسيلة مميزة وفعّالة إلى أن قام Stefan Viehböck بالتّبليغ عن خطأ في تصميم wps يؤدّي إلى تخفيض الزّمن لهجوم brute-force بغية كشف الـ PIN ،حيث يتمكن المهاجم من معرفة ما إذا كان النّصف الأول من الأرقام الثّمانية صحيحاً .وبفضل غياب سياسة المنع المؤقّت بعد عدد معيّن من المحاولات الخاطئة في عدد لا بأس به من أجهزة الراوتر التابعة لإحدى كبار الشّركات المصنعه ،فإنّ الهجوم يصبح وارداً بشكل أكبر .*

*عندما تفشل عمليّة المصادقة على الـ PIN ( لأن القيمة خاطئة ) فإنّ الراوتر يقوم بإرسال رد EAP-NACK إلى جهاز الزّبون ،والطّريقة الّتي ترسل بها رسائل EAP-NACK تمكّن المهاجم من معرفة فيما إذا كان النّصف الأوّل من الرّقم الّذي يقوم بتجربته صحيحا ،بالإضافة إلى هذا فإنّ القيمة الأخيرة من الرّقم معروفة لكونها checksum للـ PIN ويمكن حسابها بمجرّد معرفتك للأرقام السّبعة الأولى ،وهذا يعني أنّ عدد المحاولات اللازمة لاكتشاف الـ PIN واحد ينخفض من 108 إلى مجموع 104 (النّصف الأوّل من الرّقم) + 103 (النّصف الثّاني بدون قيمة الـ checksum ) ما يشكّل بالمجمل 11,000 محاولة فقط .*

*من الشّركات الّتي تمّ التأكد من إصابة أجهزتها بهذا الخلل :*

*D-Lin; , Linksys ,Netgear , TP-Lin; ,ZyXEL , Belkin , Buffalo , Technicolor .*

*وكإجراء وقائي على المستخدم القيام بتعطيل خيار WPS (Wi-Fi Protected Setup) الّذي قد يكون باسم "external registrar" أو "Router PIN" وذلك تبعاً للشركة المُصنّعة .[[20]](#footnote-20)*

# الباب الرّابع

## الفصل الأوّل : Kali Linux

### تاريخ kali Linux

*كالي لينكس هو توزيعة لينكس - متخصّصة في مجال الأمن والحماية المعلوماتيّة واختبار الاختراق - الصّادرة عن Offensive Security . هذه النّسخة الحاليّة تمتلك ما يزيد عن 300 أداة أمان وأداة لاختبار الاختراق وهذه الأدوات مصنّفة ضمن مجموعات ،وغالباً ما تُستخدم هذه النّسخة من قبل مُختبرين الاختراق أو الخبراء الأمنيين وهم ناس هدفهم تطوير البرامج واختراق الجهاز أو الموقع لكي يقوموا بتصحيح وتعديل ثغراته . و على عكس التّوزيعات السّابقة الصّادرة عن Offensive Security يستخدم كالي لينكس التّوزيع Debian 7.0 كأساس له . وجاء كالي لينكس كاستمرار لنسل الإصدارات السّابقة ولكن وفي النّهاية فإنّ جميع هذه الإصدارات بما فيها نظام كالي لينكس تُدعم من قبل الفريق ذاته.*

*ووفقاً لـ Offensive Security فإن تعديل الاسم يدلّ على إكمال الشّركات لإعادة بناء إصداراتها السّابقة .والإصدارات السّابقة تكون مُطوّرة من خلال الـ) White Hat والـ SLAX WHAX) ومن قبل فاحصي الحسابات ،ومن هنا نجد أنّ كالي لينكس هو آخر تجسيد لحالة التّدقيق الأمني وأدوات تقييم الاختراق ... [[21]](#footnote-21)*

### مميزات توزيعة "Kali Linux" لاختبار الاختراق

1. *أكثر من 300 أداة لاختبار الاختراق: حيث أنه بعد مراجعة كل الأدوات الموجودة مسبقاً في توزيعة الباك تراك تم التخلص من عدد كبير من الأدوات التي لا تعمل والأدوات التي يوجد لها أداه مشابهة تقوم بنفس وظيفتها.*
2. *مجانية : مثل سابقتها، حيث أنها مجانية بالكامل وستظل مجانية ،ولن تضطر يوماً للدفع من أجل الحصول عليها.*
3. *مفتوحة المصدر: وذلك كما صرّح المطورون الأساسيون للتوزيعة ،أنها واحدة من شجرة البرمجيات الذي قاموا بتطويرها وهي متاحه للجميع، وبإمكانك التعديل عليها كيفما تشاء.*
4. *متوافقة مع نظام ملفات FHS:حيث أن kali Linux تم تطويرها للتوافق مع التسلسل الهرمي القياسي لنظام الملفات ،كما أنها تسمح للمستخدم بتحديد موقع الملفات الثنائية ،كما أنها تدعم الملفات و المكتبات وغيرها ....*
5. *دعم أجهزة اللاسلكي الموسعة: لقد تم بناء Kali Linux لدعم العديد من الأجهزة اللاسلكية قدر المستطاع ،والعمل معها بشكل سليم دون مشاكل كما أنها متوافقة مع العديد من الـ USB والأجهزة اللاسلكية الأخرى.*
6. *النواة الخاصة بها تم تخصيصها للحقن والتعديل: حيث أن مختبري الاختراق والمطورين كثيراً ما يحتاجون إلى إجراء تقييمات لاسلكية لذلك تم تطويرها على هذا الأساس.*
7. *بيئة تطوير آمنة: فريق كالي لينكس يتكون من مجموعة صغيرة فردية من الأشخاص الموثوقين والذين يتعاملون مع المستودعات باستخدام بروتوكولات متعددة وآمنة.*
8. *تعدد اللغات: من المعروف أن أدوات الاختراق يتم كتابتها بالإنجليزية ،لكنّ كالي لينوكس مكّنت المستخدم من العمل على التوزيعة بلغته الأم ،واختيار الأدوات التي يحتاجها.*
9. *القابلية الكاملة للتّخصيص: حيث صرح فريق التطوير الخاص بالتوزيعة أنّهم يتفهموا أنه من الصعب أن ينال تصميم التوزيعة رضا الجميع ،لذلك فقد عملوا على جعلها قابلة للتعديل قدر الإمكان ،لذلك مكنوا المستخدم من التحكم في كافة الأشياء بداخل التوزيعة وتخصيصها كما يشاء ،على طول الطريق وصولاً إلى النواة على حدّ تعبيرهم.*
10. *دعم نظام ARMEL & ARMHF: ونظراً لأن النظم القائمة على ARM أصبحت أكثر انتشاراً وغير مكلفة، وكما نعلم أنه يجب أن تكون التوزيعة قوية وعلى درجة عالية من الثبات حتى تستطيع إدارة كلا النظامين، لذلك تم العمل على إيجاد توافق بين مستودعي النظامين والمستودع الرئيسي الخاص بالتوزيعة .[[22]](#footnote-22)*

## الفصل الثّاني : Kali Linux & Hacking

*إن كالي لينكس هو توزيعة من توزيعات لينكس وتتميّز توزيعات لينكس بأنّها مفتوحة المصدر وهذا يعني أنّه ليس له حقوق الملكيّة بمعنى أنّه يمكنك تطويره وهذا ما يجعل الهاكرز ومختبري الاختراق يلجؤون إلى استخدام لينكس لأنّه مفتوح المصدر وحرّ ومجاني ويمكن تعديله ،وإنّ كالي لينكس يحتوي على الكثير من الأدوات الّتي تساعد مختبري الاختراق والهاكرز ،وسنعدّد الآن بعض هذه الأدوات وسنذكر فائدة كلّ منها :*

* *Aircrack-ng*

**

*هي عبارة عن مجموعة من الأدوات التي تستخدم في فك تشفير الشّبكات الهوائيّة أو جلب كلمة السّر و قد تمّ وضعها ضمن أفضل عشر أدوات ؛لأنّها قويّة جدّا كما أنّها سريعة .*

* *Burpsuite*

**

*هذه الأداة مفيدة جدّاً لمخترقي المواقع "وعندما نتحدّث عن الاختراق فإنّنا نتحدّث أيضاً عن الحماية فهما وجهان لعملة واحدة" وهي أداة مصمّمة بلغة جافا ويمكن من خلالها عمل بروكسي سيرفر ..*

* *John*

**

*تستخدم هذه الأداة لفكّ تشفير كلمات السّر فهي تتنبّأ بنوع التّشفير ثمّ تقوم بمحاولة فكّه مهما كان نوع التّشفير فعادة قد يقوم المخترق بجلب كلمة السّر ولكنّها تكون مشفّرة ،فهذه الأداة تقوم بفكّ التّشفير له .*

* *Maltego*

**

*هي أداة تستخدم في تحليل وجمع المعلومات والعلاقات بين النّاس والمجموعات والشّبكات والمواقع وهي مبنيّة أيضاً بلغة جافا .*

* *Metasploit*

*وهذه الأداة لها اسم كبير وشائع بين الهار فهي عبارة عن برنامج يحتوي على مجموعة ضخمة من الأكواد الجاهزة لاختراق الأجهزة بعد قيام المخترق بضبط بعض الخصائص .*

* *Nmap*

*هذه الأداة تقوم بفحص الشّبكات كما أنّها تقوم بعدّة اشياء مثل فحص الأجهزة وماهي المنافذ المفتوحة لتقوم بالاختراق من خلالها وتفحص ما إذا كان الجهاز يعمل أم لا ،ويمكن أيضاً اختراق الأجهزة من خلالها .*

* *Sqlmap*

*أداة مهمّة لمن يريد أن يخترق سيرفر قواعد بيانات ؛فهي تجلب لك بعض المعلومات الأساسية عن هذا السيرفر كما تمكّنك أيضاً من اختراق قاعدة البيانات إن وجدت هناك ثغرة .*

* *Webscarab*

*أداة تمكّنك من اختراق المواقع أو بمعنى أدقّ تمكّنك من تعديل البيانات المرسلة فربّما تقوم بملء نموذج وتضع به اسم أو بريد إلكتروني أو لربّما قمت بالشّراء بمبلغ معيّن فإنّك تقدر من خلال هذه الأداة أن تغيّر قيمة المبلغ ؛فهي تعمل كبروكسي بينك وبين الموقع "سيرفر الموقع" .*

* *Wireshark*

*أداة تستطيع من خلالها التّنصت على شبكة وجلب المعلومات المفيدة لك .*

* *Hydra*

*هذه الأداة لها قدرة كبيرة في عالم الاختراق ،وهي أيضاً تستخدم لكسر كلمة السّر ولكن بطريقة أسرع وأقوى ؛فهي تقوم بتجربة كلمات بطريقة موازية (أي مع بعض) وليست متتالية (أي واحدة تلو الأخرى) .[[23]](#footnote-23)*

## الفصل الثّالث : الحماية من الاختراق

* *استخدم أحدث برامج الحمایة من الهاكرز والفيروسات والقيام بمسح دوري وشامل للجهاز في فترات متقاربة خصوصاً إذا كنت من مستخدمي الإنترنت بشكل يومي ..*
* *التأكد من أن Firewall على وضعية on .*
* *استخدام Anti-Virus جيد .*
* *لا تدخل إلى المواقع المشبوھة مثل المواقع التي تعلم التجسس والمواقع التي تحارب الحكومات ؛لأن الهاكرز يستخدمون مثل ھذه المواقع في إدخال ملفات التجسس إلى الضحایا حیث یتم تنصیب ملف التجسس ( الباتش) تلقائیاً في الجھاز بمجرد دخول الشخص إلى الموقع ..*
* *عدم فتح أي رسالة إلكترونية من مصدر مجھول لأن الھاكرز یستخدمون رسائل البريد الإلكتروني لإرسال ملفات التجسس إلى الضحایا .*
* *عدم استقبال أية ملفات أثناء الشات - من أشخاص غیر موثوق بھم - وخاصّة إذا كانت ھذه الملفات تحمل امتداد (exe) أو أن تكون ملفات من ذوي الامتدادین (.gif , .jpg) أو (.bat) أو (dll.) أو (.com) ؛لأنّ أمثال ھذه الملفات تكون عبارة عن برامج تزرع ملفات التجسس في جهازك فیستطیع الهاكرز بواستطها من الدخول إلى جهازك وتسبب الأذى والمشاكل لك ..*
* *حاول دائماً تغییر كلمة السر بصورة دورية ؛فھي قابلة للاختراق ويفضل أن تكون كلمة السر عبارة عن أرقام وحروف ورموز يصعب تخمينها .*
* *لا تدخل بريدك أو أيّ معلومات خاصة بك في المواقع الّتي تطلب منك ذلك (المواقع غير الموثوقة).. فهناك برامج تعمل بشكل مخفي تحفظ جميع النماذج التي تقوم بتعبئتها دون أن تشعر.*[[24]](#footnote-24)

# 

# الخاتمة

*تبيّن لنا من خلال دراسة هذا البحث أن عمليّة الاختراق هي إحدى الوسائل التي يستخدمها المحترفين في سبيل التّطوير والتّحسين ولكن هنالك أشخاص يستخدمون قدراتهم في هذا المجال في سبيل اختراق خصوصيّة غيرهم واقتحامها والحصول على المعلومات الّتي يريدونها ،****وبذلك يمكننا تلخيص نتائج البحث كما يأتي :***

* *الاختراق هو القدرة على الوصول إلى هدف معيّن بطرق غير مشروعة عن طريق ثغرات في نظام الحماية الخاص .*
* *التطوير والتّحسين أسمى أهداف الاختراق .*
* *هنالك العديد من الأشخاص ممن يمتلكون القدرة على الاختراق يستخدمونه لأهداف شخصيّة .*
* *استخدام خوارزميّات التّشفير من أجل أمان الـ Wi-Fi .*
* *يجب أن تكون نظم الحماية والأمان قويّة وفعّالة ،بالإضافة إلى تجديدها بشكل مستمرّ من أجل تلافي الثّغرات ونقاط الضّعف الّتي لن يطول الوقت كي يكتشفها الهكر اللاأخلاقي ويقوم باستغلالها للحصول على المعلومات الّتي يريدها .*
* *Kali Linux أحد أهم الأنظمة الّتي تستخدم في إعداد وبرمجة البرامج الخاصّة للاختراق .*

*وعلينا ألّا ننسى أيضاً اجراءات الحماية ؛وذلك من أجل تجنّب حدوث أي اختراق للبيانات والمعلومات الشخصيّة وهذا على صعيد الفرد العادي ،أمّا بالنّسبة للمطورين والمبرمجين ،فيجب الانتباه إلى بناء برامج وأنظمة قويّة خالية من الثغرات التي تتيح للمخربين استغلالها والدّخول منها ،وكذلك في مجال قواعد البيانات فيجب بناء قاعدة بيانات قويّة لا تحوي أي ثغرات ولا سيّما تلك الّتي تحتوي على بيانات سريّة ...*

# المصطلحات

|  |  |
| --- | --- |
| عربي | انكليزي |
| عنوان | Address |
| خوارزمية تشفير | AES ( Advanced Encryption Standard ) |
| نقطة الوصول | AP ( Access Point ) |
| تجاوز سعة المخزّن المؤقت | Buffer overflow |
| المستقبل | Destination |
| هجمات حجب الخدمة | DOS |
| الثّغرات الأمنيّة | Exploits |
| المُخترق | Hacker |
| عمليّة الاختراق | Hacking |
| المعهد الدولي لمهندسي الكهرباء والإلكترون | IEEE ( Institute of Electrical and Electronic Engineers ) |
| القيمة الابتدائية | Initial Vector |
| عنوان مميز لكل حاسوب | Ip (Internal Protocol ) |
| مرحلة جولة المفاتيح | KSA (The Key-Scheduling Phase( |
| برمجيات خبيثة | Malware |
| حزمة بيانات | Packet |
| مَنفذ | Port |
| مرحلة توليد القيم العشوائيّة | PRGA (The Pseudo-Random Generation Algorithm) |
| خوارزمية تشفير | RC4 |
| اتّصال عكسي | Reserve Connection |
| استجابة | Respond |
| التّنصت | Sniffing |
| الهندسة الاجتماعيّة | Social Engineering |
| عنوان المصدر | Source ip |
| مسار المصدر | Source routing |
| انتحال الشّخصيّة | Spoofing |
| برمجيّات التّجسس | Spyware |
| بروتوكول طبقة المداخل العامة | SSL (Secure Sockets Layer( |
| تشفير تدفّقي | Stream Cipher |
| حصان طروادة | Trojan horse |
| تقصّي الشّبكات اللاسلكيّة | War driving |
| بروتوكول لخصوصيّة المكافئة للشبكات السلكيّة | WEP (Wired Equivalent Privacy ( |
| بروتوكول نقاط الوصول المحميّة لشبكات الـ Wi-Fi | WPA (Wi-Fi Protected Access( |
| إعداد لحماية شبكات الـ Wi-Fi | Wps (Wi-Fi Protected Setup ( |

# المصادر والمراجع

**مواقع الإنترنت :**

**www.alfaiomi.net**

**www.alfarabi-school.org**

**www.ar.docs.kali.org**

**www.elebda3.net**

**http://info.securityinabox.org/**

**www.People.rit.edu**

**www.sans.org**

**www.syr-res.com**

**www.Taqana.net**

**المراجع الأجنبية :**

**The basic of hacking and penetration testing : ethical hacking and penetration testing made easy (Syngress Basics Series)**

**Bindner, J. B. A. Hacking with Kali (Practical Testing Techniques).**

**Chouinard, D. J.-Y. (2002) Design of Secure Computer System CSI4138/CEG4394, Notes on the Advanced Encryption Standard (AES). 1**

**Hamad, A. (2008) Evaluation of the RC4 Algorithm for Data Encryption 49 – 50 – 51**

**Kaylor, D. (2008) RC4 Encryption.**

**Lehmbre, G. Wi-Fi security WEP , WPA and WPA2**

**Siles, R. (2011) Wi-Fi Protected Setup (WPS) PIN Brute Force Vulnerability**

**المراجع العربية :**

**القحيص, م. ع. ا. م. الشبكات اللاسلكية.**

**المؤدب, د. ف. (2006-2007). خوارزميات التشفير**

**شفاعمري, د. م. أمن المعلومات أمن الشبكات اللاسلكية**

**يوسف, ر. (2008) تعريف الاختراق ودوافعه.**

# جدول الرسوم التوضيحية

[رسم توضيحي 1 : *Port Setting* 8](file:///D:\%5e_6.docx#_Toc434651949)

[*رسم توضيحي 2 : Trojan Sympol* 10](#_Toc434651950)

[رسم توضيحي 3 : التشفير المتناظر 16](file:///D:\%5e_6.docx#_Toc434651951)

[رسم توضيحي 4 : طريقة عمل الخوارزميّة *RC4* 17](file:///D:\%5e_6.docx#_Toc434651952)

[رسم توضيحي 6 : آلية عمل البّوابة المنطقيّة *XOR* - (1). 18](file:///D:\%5e_6.docx#_Toc434651953)

[رسم توضيحي 6 : آليّة عمل البّوابة المنطقيّة XOR - (2) . 18](file:///D:\%5e_6.docx#_Toc434651954)

**الفهرس**

[ملخص : 1](#_Toc434652797)

[مخطط البحث : 2](#_Toc434652798)

[مقدمة 3](#_Toc434652799)

[الباب الأول 4](#_Toc434652800)

[الفصل ألأول : مفهوم الاختراق ،أسبابه وأنواعه 4](#_Toc434652801)

[ما هو الاختراق : 4](#_Toc434652802)

[أسباب الاختراق ودوافعه : 4](#_Toc434652803)

[أنواع الاختراق : 5](#_Toc434652804)

[الفصل الثّاني : *Hacker* 5](#_Toc434652805)

[من هو الـ *Hacker* 5](#_Toc434652806)

[أساليب الهاكر 6](#_Toc434652807)

[آليات الهاكر 6](#_Toc434652808)

[الباب الثّاني 8](#_Toc434652809)

[الفصل الأوّل : التّعرف على بعض المفاهيم 8](#_Toc434652810)

[ماهي الـ Port 8](#_Toc434652811)

[Ip 8](#_Toc434652812)

[الفصل الثّاني : التّعرف على بعض الملفّات الخبيثة 9](#_Toc434652813)

[***البرمجيات الخبيثة*** 9](#_Toc434652814)

[***برمجيّات التّجسس*** 9](#_Toc434652815)

[الفصل الثّالث : آليّة الاختراق 10](#_Toc434652816)

[*ا****لعنوان The address*** 10](#_Toc434652817)

[***المَنْفذ The port*** 10](#_Toc434652818)

[الباب الثّالث 12](#_Toc434652819)

[الفصل الأوّل : الخصوصية المكافئة للشبكة السلكيّة WEP 12](#_Toc434652820)

[الفصل الثّاني : الوصول المحمي للشّبكة اللاسلكيّة WPA 15](#_Toc434652821)

[الفصل الثّالث : خوارزميّات التّشفير المُتّبعة للحماية 16](#_Toc434652822)

[خوارزمية RC4 16](#_Toc434652823)

[خوارزميّة AES 20](#_Toc434652824)

[الفصل الرّابع : Wps 20](#_Toc434652825)

[الباب الرّابع 21](#_Toc434652826)

[الفصل الأوّل : Kali Linux 21](#_Toc434652827)

[تاريخ kali Linux 21](#_Toc434652828)

[مميزات توزيعة "Kali Linux" لاختبار الاختراق 21](#_Toc434652829)

[الفصل الثّاني : Kali Linux & Hacking 22](#_Toc434652830)

[الفصل الثّالث : الحماية من الاختراق 23](#_Toc434652831)

[الخاتمة 25](#_Toc434652832)

[المصطلحات 26](#_Toc434652833)

[المصادر والمراجع 27](#_Toc434652834)

[جدول الرسوم التوضيحية 28](#_Toc434652835)

1. [www.elebda3.net-5912.pdf\_Page:3](http://www.elebda3.net-5912.pdf_Page:3) [↑](#footnote-ref-1)
2. يوسف, ر. (2008) تعريف الاختراق ودوافعه.

   [↑](#footnote-ref-2)
3. [WWW.People.rit.edu/aaa4363/epub/page5.html](http://WWW.People.rit.edu/aaa4363/epub/page5.html) [↑](#footnote-ref-3)
4. [WWW.Taqana.net/who-are-hackers](http://WWW.Taqana.net/who-are-hackers) [↑](#footnote-ref-4)
5. [www.alfarabi-school.org/t65-topic](http://www.alfarabi-school.org/t65-topic) [↑](#footnote-ref-5)
6. [www.sans.org/security-resource/idfaq/oddports.php](http://www.sans.org/security-resource/idfaq/oddports.php) [↑](#footnote-ref-6)
7. [www.elebda3.net-8580](http://www.elebda3.net-8580) [↑](#footnote-ref-7)
8. <http://info.securityinabox.org/ar/chapeter_01> [↑](#footnote-ref-8)
9. القحيص, م. ع. ا. م. الشبكات اللاسلكية.

   [↑](#footnote-ref-9)
10. Lehmbre, G. Wi-Fi security WEP , WPA and WPA2

    [↑](#footnote-ref-10)
11. [www.alfaiomi.net/13/](http://www.alfaiomi.net/13/)

    (أمن الشّبكات – معايير تشفير الاتّصال اللاسلكي ) [↑](#footnote-ref-11)
12. شفاعمري, د. م. أمن المعلومات أمن الشبكات اللاسلكية

    [↑](#footnote-ref-12)
13. [www.alfaiomi.net/13/](http://www.alfaiomi.net/13/)

    (أمن الشّبكات – معايير تشفير الاتّصال اللاسلكي ) [↑](#footnote-ref-13)
14. المؤدب, د. ف. (2006-2007). خوارزميات التشفير

    [↑](#footnote-ref-14)
15. Siles, R. (2011) Wi-Fi Protected Setup (WPS) PIN Brute Force Vulnerability

    [↑](#footnote-ref-15)
16. المؤدب, د. ف. (2006-2007). خوارزميات التشفير

    [↑](#footnote-ref-16)
17. Hamad, A. (2008) Evaluation of the RC4 Algorithm for Data Encryption 49 – 50 – 51

    , Kaylor, D. (2008) RC4 Encryption.

    [↑](#footnote-ref-17)
18. Chouinard, D. J.-Y. (2002) Design of Secure Computer System CSI4138/CEG4394, Notes on the Advanced Encryption Standard (AES). 1

    [↑](#footnote-ref-18)
19. [www.syr-res.com/article/3226.html](http://www.syr-res.com/article/3226.html) [↑](#footnote-ref-19)
20. Siles, R. (2011) Wi-Fi Protected Setup (WPS) PIN Brute Force Vulnerability

    [↑](#footnote-ref-20)
21. The basic of hacking and penetration testing : ethical hacking and penetration testing made easy (Syngress Basics Series)

    [↑](#footnote-ref-21)
22. [www.ar.docs.kali.org/general-use/articles](http://www.ar.docs.kali.org/general-use/articles) [↑](#footnote-ref-22)
23. Bindner, J. B. A. Hacking with Kali (Practical Testing Techniques).

    [↑](#footnote-ref-23)
24. [www.elebda3.net-8580/ page:37-38](http://www.elebda3.net-8580/%20page:37-38) [↑](#footnote-ref-24)