العنوان:	أختبار وتخطيط أمنية الشبكات اللاسلكية
المؤلف الرئيسي:	خوجلي، أحمد خوجلي الصديق
مؤلفين آخرين:	فتوح، سيف الدين(مشرف)
التاريخ الميلادي:	2016
موقع:	الخرطوم
الصفحات:	1 - 88
رقم MD:	829240
نوع المحتوى:	رسائل جامعية
اللغة:	Arabic
الدرجة العلمية:	رسالة ماجستير
الجامعة:	جامعة النيلين
الكلية:	كلية علوم الحاسوب وتقانة المعلومات
الدولة:	السودان
قواعد المعلومات:	Dissertations
مواضيع:	أمن الشبكات اللاسلكية، أمن المعلومات
رابط:	http://search.mandumah.com/Record/829240

بسم الله الرحمن الرحيم

جامعة النيلين

كلية علوم الحاسوب وتقانة المعلومات

كلية الدراسات العليا

برنامج الماجستير

قسم تقانة المعلومات

بحث تكميلي لنيل درجة الماجستير في تقانة المعلومات

بعنوان:

أختبار وتخطيط أمنية الشبكات اللاسلكية

إعداد الطالب:

أحمد خوجلي الصديق خوجلي

إشراف

أ.د.سيف الدين فتوح

2016م

بسم الله الرحمن الرحيم

)وَقُــلِ اعْمَلُــوا فَسَيَــرَى اللَّــهُ عَمَلَكُــمْ وَرَسُولُهُ وَالْمُؤْمِنُونَ وَسَتُرَدُّونَ إِلَىٰ عَـالِمِ الْغَيْــبِ وَالشَّــهَادَةِ فَيُنَبِّئُكُــم بِمَــا كُنتُــمْ تَعْمَلُونَ(

صدق الله العظيم

سوره التوبه الاية (105-106)

إلهي لايطيب الليل إلا بشكرك ولايطيب النهار إلى بطاعتك .. ولاتطيب اللحظات إلا بذكرك ولا تطيب الآخرة إلا بعفوك .. ولا تطيب الجنة إلا برؤيتك
الله جل جلاله
إلى من بلغ الرسالة وأدى الأمانة .. ونصح الأمة .. إلى نبي الرحمة ونور العالمين ..
سيدنا محمد صلى الله عليه وسلم

إلى من كلله الله بالهيبة والوقار .. إلى من علمني العطاء بدون انتظار

إلى من أحمل أسمه بكل افتخار .. أرجو من الله أن يمد في عمرك لترى ثماراً قد حان قطافها بعد طول انتظار وستبقى كلماتك نجوم أهتدي بها اليوم وفي الغد وإلى الأبد

والدي العزيز....

إلى ملاكي في الحياة .. إلى معنى الحب وإلى معنى الحنان والتفاني .. إلى بسمة الحياة وسر الوجود إلى من كان دعائها سر نجاحي وحنانها بلسم جراحي إلى أغلى الحبايب
أمي الحبيبة.....
إلى من آنسني في دراستي وشاركني همومي تذكاراً وتقدير

أصدقائى....

شكر وعرفان

الى الشموع التى زابت فى كبرياء ..... لتنير كل خطوه فى دربنا.....لتذلل كل عائق امامنا

فكانو رسلا للعلم والأخلاق

هل يستطيع احد ان يشكر الشمس لانها أضاءت الدنيالكنى سأحاول رد جزء من جميليكم

بان اكون كما اردتمونى(أنسانيه قبل ان اكون مهنيه).

أما الشكر الذي من النوع الخاص فنحن نتوجه بالشكر أيضا إلى كل من لم يقف إلى جانبنا ، ومن وقف في طرقنا وعرقل مسيرة بحثنا، وزرع الشوك في طريق بحثنا فلولا وجودهم لما أحسسنا بمتعة البحث ، ولا حلاوة المنافسة الإيجابية، ولولاهم لما وصلنا إلى ما وصلنا إليه فلهم منا كل الشكر

نشكركم جميعكم على جهودكم معنا

مستخلص البحث:

يعتبر أختبار الأختراق من المفاهيم الامنيه التى اصبح مـن المهـم تطبيقها فى اي مؤسسة حيث يلعب المختبر او فريق الاختبار دور المخترق اومجموعه المخترقين، ويعمل إختبار الإختراق على رفع المستوى الامنى والعلمى لدى افراد المؤسسة.

يتم من خلال هذا البحث تطبيق مفهوم أختبار الاختراق للشـبكات اللاسـلكيه عـن طريـق حزمـة AirCrack-ng المختصـة بكسـر وتصديع المفتاح المخصص للشبكة اللاسلكية.

وتـوفير واجهـات رسـومية للحزمـة ممـا يسـهل علـى مسـتخدم التطبيق استخدامه بسـهولة ويسـر وقيـاس ومقارنـة النتائـج فـى انظمة تشغيل مختلفة.

وتنفيذ اختبار حجب الخدمـة عـن المسـتخدمين المتواجـدين فـى الشــبكة بصــوره ســريعه ممــا يســهل التحكــم فــى الشــبكة والمستخدمين المتواجدين فيها.

Abstract:

The penetration test of security concepts that has become important to be applied in any organization where he plays the laboratory or testing the role of team breached hackers.

Penetration Testing works to raise the level of security and the members of the Scientific Foundation.

Through this research the application of the concept of penetration testing for wireless networks pack by AirCrack-ng, professional fractured and key allocated to the wireless network.

And the use of tools to exploit the gaps and clear the target area and identify the target and break the key Devoted to this goal.

And provide graphical interfaces for the package making it easy for the user application to use easily and conveniently and measuring and comparing the results in different operating systems.

And use the package ETTERCAP-NG in the implementation of a number of internal tests, professional channels linking web server and a number of the victim and clear target network to know where the Zodiac.
And implementation of test denial of service for users in the network and the rapid making it easier Network control and online users.

الفـــــــهرس

فهرس الأشكال والجداول:

الفصل الأول
مشكلة وأهمية وأهداف البحث

1-1: الشبكات اللاسلكية

هى مجموعة من الأجهزة المرتبطة مع بعضها البعض لتبادل المعلومات و الاستفادة من الموارد الموجـودة فـي الشـبكة مـن خلال وسط تراسلي لاسلكي –علـى الهـواء-و ذلـك يعطـي حريـة تنقل الإجهزة المرتبطة بها مادامت داخل نطاق الشبكة. [1]

انتشـرت الشـبكات اللاسـلكية فـي هـذا العصـر انتشـاراً مـذهلاً وأصبحت تستخدم بشكل واسع في الاتصال ونقل وتبادل البيانات

بين أجهزة الحواسيب في المنازل و في الشـركات و القطاعـات الكبيرة.

تمثل الشبكات اللاسلكية التقنية الأحدث في عالم الشبكات اليوم، فالتخلص مـن الكـابلات وإزعاجهـا يُعـد أمـراً مـذهلاً، وتُعـد الشبكات اللاسلكية من أهم التطورات في الحواسيب الشخصية،

تستعمل الشبكات اللاسلكية بروتوكولات وبرمجية الشبكة نفسها التي تستعملها الشبكه السلكية. وتستخدم الشبكة اللاسلكية عدة أنماط، ويتكون النمـط البسـيط مـن شـبكة لاسـلكية تتكـون مـن حاسبين أو أكثر يتراسلون مع بعضهم البعض مـن دون كـابلات أو أي أجهزة وسيطة وهو نمط Ad-hoc ويشبه هـذا النمـط أحيانـاً نمط peer-to-peer حيـث تكـون علـى اتصـال مباشـر مـع كـل جهاز آخـر ضـمن بينـة لا مركزيـة متاحـة للجميـع كمـا فـي تقنيـة Bluetooth، وهي سـهلة التكـوين مقارنـة بـالنمط الآخـر الأكـثر تعقيداً. أما النمط الآخر فهـو يعمـل علـى مركزيـة نقطـة وصـول WPA واحدة أو أكثر ويـدعى Infrastructure. ويكـون التواصـل بين الأجهزة مرتبطاً عن طريق ذلك الوسيط. ويتطلب هذا النمط المزيد من التخطيط للشبكة ويعد أكثر تعقيداً من حيـث التكـوين خلافاً للنمط السابق ولكن تـوفر المزيـد مـن التحكـم فـي عمـل الشبكة.[1]

الشبكات اللاسلكية تختلف عن نظيرتهـا السـلكية حيـث البيانـات تنتقل فيها في الهواء عوضاً عن الأسلاك وبالتالي فـإن التجسـس على البيانات المنقولة بواسطة الشبكة اللاسلكية لا يتطلـب مـن المتلصص الاتصال فيزيائيًا بأسلاك الشبكة، بـل يمكـن نظريًـا لأي شخص يقع ضمن مجال تغطية الشبكة اللاسلكية اسـتراق النظـر إلى البيانات المنقولة ما لم تكن محمية بشكل ملائم وهذا شـيء غير جيد عند نقل وتبـادل البيانـات المهمـة والحساسـة والسـرية والأمنيـة فهـو بـذلك لا يحفـظ الخصوصـية وهـو أيضـاً لا يحفـظ البيانات سليمة حيـث أنهـا تكـون عرضـة للتعـديل مـن أي أحـد.

1-2: مشكله البحث

تكمن مشكلة في الضعف الموجود في هذا النوع من الشبكات,وذلـك لان كـثيرين ينـدفعون لـتركيب شـبكات لاسـلكية نسبة لمميزاتها سواء في مناطق عملهم او في منازلهم دون ان يكـون لهـم درايـة بكيفيـة عمـل الشـبكات والطريقـة الصـحيحة لتهيأتها وهذا يقود حتما الي انشاء شبكات غيـر امنـة ,كمـا تشـير بعض التقديرات (الولايات المتحدة الامريكيـة) الـي ان 15%مـن الشبكات اللاسلكية تعرضت لهجمات ومابين 40% الي 50%من الشبكات اللاسلكية مستوي الحماية فيهـا ضـعيف او انـه لايوجـد فيها اي نوع من الحماية علي الاطلاق.

نقاط ضعف الشبكات اللاسلكية:

1. سهولة تركيـب الشـبكة وتشـغيلها,فـان كـثيرا ممـن يقـوم بتشغل هذه الشبكات هم من الاشـخاص الـذين ليـس لهـم درايـة كافيـة بـامن المعلومـات وبالتـالي لا يعرفـون كيـف يهيئـون الاعـدادات بشـكل صـحيح فيـتركون ثغـرات امنيـة كبيرة في الشبكة.

2. سهولة تعرضها للهجمات التي تؤدي الـي تعطيـل الخدمـة الذي يجعـل اعضـاء الشـبكة اللاسـلكية غيـر قـادرين علـي تبادل المعلومات بينهم وهذا يعتـبر اخطـر انـواع الهجمـات التي تتعرض لها الشبكة وذلك للاعتبارات الاتية:

أ. إن الشبكات اللاسلكية تعتمد علي نطـاق تـرددي ضـمن الكهرومغنطيسي لنقل البيانات, ويمكن بسهولة التشـويش علي النطاق الترددي لتوفر الاجهزة اللازمة ورخص ثمنها.

ب. هناك ثغرات في تصميم البروتوكول الذي يـدير عمليـة انضمام الاعضاء الي الشبكة اي بروتكولات :

- برتوكول الخصوصية المكافئة (WEP: Wired Equivalent Privacy)
وهو بروتوكول يستخدم لمنح الشبكة كلمة سر تتيح حماية الشبكة من الإختراق من قبل المستخدمين.
- بروتوكول (Wi-Fi Protected Access (WPA))

وهو بروتوكول جاء بديل لبرتوكول WEP بعد الضعف الــذي حصل له وهو بروتوكول أكثر أمنية من الإختراق.

1-3: أهميه البحث

1. تمثل الشبكات اللاسلكية التقنية الأحدث في عالم الشبكات اليـوم نظـراً لتخلصـها مـن الكيبلات المزعجـة وغيرهـا مـن المعوقات الأخرى.
2. توفر الشبكات اللاسـلكية بصـورة كبيرةحـتى فـي الهواتـف النقالة.
3. بناء بنيـة تحتيـة ملائمـة لتـوفير خـدمات الإتصـالات بصـورة آمنة.
4. تـوفير مقارنـة مـن ناحيـة علميـة بإسـتخدام طـرق إختبـار نشطة.
5. الوقوف علـى الجـوانب الإيجابيـة للشـبكات اللاسـلكية مـن ناحية المعمارية السهلة والغير مقيدة.

1-4: الاهداف

1. إكتشــاف الضــعف الموجــود فــي برتوكــولات الشــبكات اللاسلكية مثل بروتوكولي (WEP-WPA).
2. استخدام حزمة AIR-eng فى عملية الاختبار.
3. توفير واجهات رسومية لحزم الاختبار.
4. قياس ومقارنة طرق الاختبار فى بيئات مختلفة(windows - Linux).
5. تقيم اداء الشبكة من حيث:

- Tx Rate وهو معدل سرعة النقل للكرت المستخدم فـي الجهاز حسب البعد عن الشبكة اللاسلكية.
- Link Quality توضيح جودة الإتصال في نقل الملفات.
- Signal Strength وهـي قـوة الإرسـال حيـث كلمـا بعـد الجهاز من الشبكة قلت قوة الإرسال.
- Data Rate تحديد مقـدرة كـرت الشـبكة علـى الوصـول لنقاط الإتصال الموجودة في المحيط.

6. سهولة إختراق الشبكات اللاسـلكية وتنفيـذ هجمـات حجـب الخدمـة وغيرهـا ومـن الهجمـات الأخـرى علـى المسـتخدمين الموجودين في الشبكة.

1-5: هيكلية البحث:

يتكون هذا البحث من أربعة فصول:

الفصل الأول:

1-1: مقدمة عن الشبكات اللاسلكية.

1-2: مشكلة البحث.

1-3: أهمية البحث.

1-4: أهداف البحث.

1-5: هيكلية البحث.

الفصل الثاني:

2-1: مقدمة عن أمن الشبكات اللاسلكية.

2-2: إختبار الإختراق.

2-3: الباك تراك.

الفصل الثالث:

3-1: مقدمة.

3-2: برتوكول الخصوصية المكافئة (WEP).

3-3: بروتوكول الوصول المحمي (WPA).

3-4: حزمة Aircrack-ng.

3-5: حزمة Ettercap-ng.

الفصل الرابع:

4-1: تصميم الشاشات.

4-2: تنفيذ الشاشات.

الفصل الخامس:

5-1: النتائج والتوصيات.

5-2: الخاتمة.

5-3: المراجع والمصادر.

الفصل الثاني
أمن المعلومات ونظام الباك تراك

2-1: مقدمة

إن خصائص أمن المعلومات بالشبكات اللاسلكية هي(السرية Confidentiality، التحقق من الهوية Authentication، الكمال Integrity، مكافحة الإنكار Non-Repudiation والتوفر Availability) ولذلك يخلص الفصل إلى استعراض بعض التهديدات الأمنية الهامة التي ينبغي معالجتها عند تصميم الشبكات اللاسلكية.

2-2: أمن المعلومات

لكي نتمكن من استيعاب مفهوم أمن المعلومات لا بد من استعراض السياق التاريخي لتطور هذا المفهوم.

لقد ظل هذا المجال من الأمن حتى أواخر السبعينيات معروفاً بإسم أمن الإتصالات Communication Security (COMSEC)) والذي حددته توصيات أمن أنظمة المعلومات والإتصالات لوكالة الأمن القومي في الولايات المتحدة بما يلي:

"المعايير والإجراءات المتخذة لمنع وصول المعلومات إلى أيدي أشخاص غير مخولين عبر الإتصالات ولضمان أصالة وصحة هذه الإتصالات".

تضمنت النشاطات المحددة لأمن الإتصالات COMSEC أربعة أجزاء هي: أمن التشفير Cryptosecurity، أمن النقل Transmission Security، أمن الإشعاع Emission Security والأمن الفيزيائي Physical Security ومن متطلبات أمن المعلومات:

2-2-1: السرية

التأكيد بأن المعلومات لم تصل لأشخاص، عمليات أو أجهزة غير مخولة بالحصول على هذه المعلومات (الحماية من إفشاء المعلومات غير المرخص).[2]

2-2-2: التحقق من الهوية

إجراء أمني للتأكد من صلاحية الإتصال، الرسالة أو المصدر أو وسيلة للتحقق من صلاحية شخص ما لاستقبال معلومات ذات تصنيف محدد (أو التحقق من مصدر هذه المعلومات).

بدأت في الثمانينات مع النمو المضطرد للحاسبات الشخصية حقبة جديدة من الأمن: أمن الحواسيب Computer Security (COMPUSEC)) والتي حددتها توصيات أمن أنظمة المعلومات والإتصالات لوكالة الأمن القومي في الولايات المتحدة بما يلي:

"المعايير والإجراءات التي تضمن سرية، كمال وتوفر مكونات أنظمة المعلومات بما فيها التجهيزات، البرمجيات، البرمجيات المدمجة firmware والمعلومات التي تتم معالجتها، تخزينها ونقلها".

2-2-3: الكمال

تعكس جـودة أي نظـام للمعلومـات مـدى صـحة ووثوقيـة نظـام التشغيل، التكامل المنطقي للتجهيـزات والبرمجيـات الـتي تـوفر آليات الحماية ومدى تناغم بنى المعلومات مع البيانات المخزنة.

2-2-4: التوفر

الوصول الموثوق إلى البيانات وخدمات المعلومـات عنـد الحاجـة إليها من قبل الأشخاص المخولين بذلك.

لاحقاً وفي التسعينات من القرن الماضي تم دمج مفهومي الأمن (أمن الإتصالات وأمن الحواسيب) لتشكيل ما أصبح يعـرف باسـم (أمن أنظمة المعلومات – Information Systems Security INFOSEC). يتضمن مفهوم أمـن أنظمـة المعلومـات الخصـائص الأربعـة المعرفـة مسـبقاً ضـمن مفـاهيم أمـن الإتصـالات وأمـن الحواسيب: السرية، التحقـق مـن الهويـة، الكمـال والتـوفر، كمـا أضيف إليها خاصية جديدة: مكافحة الإنكار.[2]

2-2-5: مكافحة الإنكار (المسؤولية):

التأكيد بأن مرسل البيانات قد حصل على إثبات بوصول البيانـات إلى المرسل إليه وبأن المستقبل قد حصل على إثبات لشخصـية المرسل مما يمنع إحتمال إنكار أي مـن الطرفيـن بـأنه قـد عالـج هذه البيانات.

2-3: أمن الشبكات اللاسلكية

يعتمد تعريف الأمن إلى حد كبير علـى السـياق، لأن كلمـة الأمـن تشير إلى طيف واسع مـن المجـالات ضـمن وخـارج حقـل تقنيـة المعلومـات. قـد نتكلـم مثلاً عـن الأمـن عنـد توصـيف الإجـراءات الوقائية على الطـرق العامـة أو عنـد اسـتعراض نظـام حاسـوبي جديد يتمتع بمناعة عالية ضد فيروسات البرمجيات. لقد تم تطوير أنظمة عدة لمعالجة الجوانب المختلفة لمفهوم الأمن.

بنـاء علـى ذلـك فقـد قمنـا بصـياغة مصـطلح "أمـن الشـبكات اللاسلكية" ضمن تصنيف محـدد للأمـن بغيـة تسـهيل مهمتنـا فـي دراسة الأمن في مجال الشبكات اللاسـلكية. تقـوم هـذه الوحـدة بتعريف أمن الشبكات اللاسلكية ضـمن سـياق أمـن المعلومـات،

أي أننا عندما نتحدث عن أمن الشبكات اللاسلكية فإننا نعني أمن المعلومات في الشبكات اللاسلكية WLAN.

2-4: أمن المعلومات والشبكات اللاسلكية:

تعرّف توصيات أمن أنظمة المعلومات والإتصالات لوكالة الأمن القومي في الولايات المتحدة أمن أنظمة المعلومات كما يلي:

"حماية أنظمة المعلومات ضد أي وصول غير مرخص إلى أو تعديل المعلومات أثناء حفظها، معالجتها أو نقلها، وضد إيقاف عمل الخدمة لصالح المستخدمين المخولين أو تقديم الخدمة لأشخاص غير مخولين، بما في ذلك جميع الإجراءات الضرورية لكشف، توثيق ومواجهة هذه التهديدات".[2]

2-5: إختبار الإختراق:

هي عملية إثبات أن نظام ما غير امن، وذلك بمحاولة اختراقه والوصول لمعلومات لا ينبغي الوصول لها والإطلاع عليها إلا من قبل من يحق له. وتعتبر هذه العملية قانونية إذا ما تم

توقيع عقد بين الطرفين وفيه يتـم تحديـد نـوع الـ Penetration Test ومدته وبدايته ونهايته واختيار التطبيقـات أو الأنظمـة الـتي سوف يجرى عليها الاختبار.[3]

2-5-1: أهمية إختبار الإختراق:

في عصر المعلومـات واتجـاه جميـع المؤسسـات والجهـات الحكوميـة والخاصـة إلـى العـالم الرقمـي والبيئـة المعلوماتيـة واعتماد الكثير علـى الخـوادم التطبيقـات الانـترنت، وقيـام جميـع أعمال تلك المؤسسـات أو المنظمـات فـي عملهـا علـى التقنيـة، أصبح بقاء هذه الخدمة لاستمرارية العمل واجبـه وضـرورية لتلـك المنظمـات والمؤسسـات، ومـن هنـا انطلقـت خـدمه الـ Penetration Test كأحد الخدمات المساهمة لتقييم المخـاطر ومحاولـة لوضـع تقريـر نهـائي يوضـح ثغـرات وعيـوب النظـام أو التطبيق وتصنيف خطورة هذه الثغرات، مما يعطـي لمـدير نظـام المؤسسة أو المنظمة تفاصيل لكيفية سد هـذه الثغـرات وتجنـب حدوث أي اختراق أو سرقة بيانات مهمة بالنسبة لهم لا قدر الله.

2-5-2: إستراتيجيات إختبار الإختراق:

إختبار الاختراق يشمل كل ما يتعلق بالحاسب الآلي وشـبكة الانترنت والشبكة السلكية واللاسلكية بما فيهـا البلوتـوث. وحـتى الموظفين أنفسهم يجرى عليهم الاختبار دون علمهم وهذا يسمى Social Engineering .

تحديد نـوع اختبـار الاخـتراق المبـدئي يكـون بطلـب مـن صـاحب النظام المـراد تقييمـه، فهنـاك اختبـار اخـتراق داخلـي Internal وخـارجي External وبعـدها يتـم تحديـد نـوع الهجـوم إمـا يكـون Black Box أو White Box، مبدئيا يحـدد اختبـار الاخـتراق أولا بكونه داخلي أو خارجي.

2-5-2-1: الإختبار من الخارج External Penetration Test:

محاولـة اخـتراق الشـبكة أو النظـام مـن الخـارج، أي لا يكـون المخترق داخل الشبكة المراد اختراقها وهو الأقرب للواقع.

2-5-2-2: الإختبار من الداخل Internal Penetration Test:

يقوم المخترق بإجراء الاختبار من داخل الشـبكة المعنيـة، ويـأتي مكملاً لاختبـار الاخـتراق الخـارجي، لان اخطـر هجمـات الاخـتراق غالبا ما تأتي من الداخل.

2-5-2-3: إختبار Black Box Penetration Test:

وتعني أن المختبر أو المخترق لا يملك أي معلومـات عـن الهـدف أو الأهداف المراد اختراقهـا، عـدا عنـوان الموقـع أو الشـبكة، فلا يعلـم عــن أي شــيء يخــص النظــام أو الشــبكة أو إعــداداته أو موظفيه، وهذا النوع اقـرب للواقـع، فهـو يحـاكي عمليـة اخـتراق فعلية. ولهذا يكون الاختبار أكثر قيمة بالنسبة لصاحب العمل، لأنه يعتمد بشكل أساسي اكتشاف عيـوب النظـام وثغراتـه الواضـحة للإطراف الخارجية.

2-5-2-4: إختبار White Box Penetration Test:

يقوم المختبر في هذا النوع بمعرفـه تفاصـيل عـن النظـام المـرد اخــتراقه، وتفاصــيل الشــبكة وكيفيــة بنائهــا، وإعــدادات النظــام وإصداره، يكون المخترق ملم بمعظم تفاصيل النظام وعليها يبـدأ صياغة سيناريو الاختراق، مع أن هذا النوع غير محبـب مـن اغلـب مدراء الأنظمة، ولكن يكون ذا أهمية اكبر في حالات خاصة. على سبيل المثال خدمة حفظ ملفات تقـدمها جهـة مـا لموظفيهـا، ولا يمكن لأي شخص الدخول إلا باستخدام كلمة مرور ومعـرف، هنـا يكون المخترق كجـزء مـن النظـام بمنحـه حـق الـدخول، وهـدف العمليــة معرفــه مــاذا ســيحدث إذا مــا حصــل احــد المخــترقين معلومات الدخول لأي موظف له الحق بالدخول على الخادم.

2-5-3: أنواع إختبار الإختراق:

بالإضافة إلى الإستراتيجيات التي سـبق ذكرهـا فلابـد مـن تحديـد أنواع الإختبارات التي يقوم بها فريق الإختبار وهي كما يلي:

1. إختبار أمن التطبيقات :

أكثر الشـركات تـوفر خدمـة الـدخول إلـى خـدماتها مـن خلال التطبيقـات عـن طريـق المواقـع الإلكترونيـة وهـذا النـوع مـن الدخول ينشـأ ثغـرات أمنيـة جديـدة؛ لأنـه مـع وجـود الجـدران النارية وأنظمة المراقبة الأخرى يمكن أن يخترق حيث أن سير البيانات يجب أن يكون مسموحاً له من خلال الجـدران الناريـة والهــدف مــن هــذا الإختبــار هــو تقييــم التحكــم بالتطبيقــات وعملياتها.

2. إختبار حجب الخدمة:(denial of service):

إختبار حجب الخدمة هو تقييـم قابليـة النظـام لتحمـل الهجـوم الذي سوف يمنعه من تقديم الخدمـة للآخريـن، فسـوف تمنـع جميع عمليات أومحاولات الدخول على النظام.

3. إختبار الهندسة الإجتماعية:

هــذا الإختبــار مرتبــط بإســتراتيجية إختبــار العمــي أو العمــي المضاعف؛ وهو يشير إلى التقنيات المسـتخدمة فـي التواصـل