محاضرة رقم 12	
الكلية	التربية للعلوم الانسانية
القسم	علوم القران والتربية الإسلامية
المادة باللغة العربية	الحاسوب
المادة باللغة الانجليزية	Computer
المرحلة	الأولى
السنة الدراسية	2024 – 2023
الفصل الدراسي	الثاني
المحاضر	م.م. مصطفى مصلح
العنوان باللغة العربية	الاختراق الالكتروني
العنوان باللغة الانجليزية	Electronic Intrusion
المصادر والمراجع	1. اساسيات الحاسوب وتطبيقاته المكتبية . الجزء الاول / ا.م.د. زياد محمد عبود ، ا.د. غسان حميد ، ا.م.د. امير حسين
	2. مقدمة في علم الحاسوب (Computer science)، سامي عامري 2015م.

المحاضرة الثانية عشر

الاختراق الالكتروني (ELECTRONIC INTRUSION)

❖ **الاختراق الالكتروني :** هو قيام شخص غير مخول او اكثر بمحاولة الدخول (الوصول) الكترونيا الى الحاسوب او الشبكة عن طريق شبكة الانترنت وذلك بغرض الاطلاع ، السرقة ، التخريب ، والتعطيل باستخدام برامج متخصصة.

- أنواع الاختراق الالكتروني : الاختراق الإلكتروني يشمل عدة أنواع من الهجمات والتهديدات الأمنية. بعض الأمثلة الشائعة للاختراق الإلكتروني تشمل سرقة الهوية، وسرقة البيانات، واستخدام برامج خبيثة مثل الفيروسات وبرامج التجسس وبرامج الفدية، واستغلال ثغرات في الشبكات الحاسوبية، وهجمات الاحتيال الإلكتروني، وهجمات الحجب الموزعة.

- **يمكن تصنيف الاختراقات الإلكترونية إلى ثلاث فئات بناءً على الطرق المستخدمة :**

1- الاختراقات المباشرة : تشمل هذه الفئة الهجمات التي يتم فيها اختراق الأنظمة الحاسوبية مباشرةً عن طريق استغلال ثغرات موجودة في البرامج أو الأجهزة. قد يتم استخدام التصيد الاجتماعي للحصول على معلومات تسمح بالوصول غير المصرح به.

2- الاختراقات غير المباشرة : تشمل هذه الفئة الهجمات التي يتم فيها استغلال الثغرات في الشبكات أو البروتوكولات للوصول إلى الأنظمة الحاسوبية. قد تشمل الهجمات عمليات الاستنساخ غير المصرح بها أو الاختراقات الناجمة عن البرمجيات الخبيثة التي تنتشر عبر الشبكة.

3- الهجمات الاجتماعية : ترتكز هذه الفئة على استغلال الثقة والتلاعب بالبشر للوصول إلى المعلومات الحساسة أو الأنظمة. يتم استخدام تقنيات التصيد الاجتماعي والهندسة الاجتماعية لإقناع الأفراد بتقديم معلومات شخصية أو كلمات مرور أو تنفيذ إجراءات غير آمنة.

- **مصادر الاختراق الالكتروني** :

1- مصادر متعمدة : يكون مصدرها جهات خارجية تحاول الدخول الى الجهاز بصورة غير مشروعة بغرض قد يختلف حسب الجهاز المستهدف.

- من الأمثلة على المصادر المتعمدة للاختراق الالكتروني :

1- المحترفون والهواة ، لغرض التجسس دون الاضرار بالحاسوب
2- اختراق شبكات الاتصال والأجهزة الخاصة بالاتصال للتصنت او الاتصال المجاني
3- اختراق لنشر برنامج معين او لكسر برنامج او لفك شفرتها المصدرية
4- أعداء خارجيون وجهات منافسة
5- مجرمون محترفون في مجال الحاسوب والانترنت

2- مصادر غير متعمدة : وهي تنشا بسبب ثغرات موجودة في برامجيات الحاسوب والتي قد تؤدي الى تعرض الجهاز الى نفس المشاكل التي تنتج عن الاخطار المتعمدة.

❖ **المخاطر الأمنية الأكثر انتشاراً :**

1- الفيروسات (Viruses) : هي برامج مصممة للانتقال الى أجهزة الحاسوب بطرق عدة وبدون اذن المستخدم ، وتؤدي الى تخريب او تعطيل عمل الحاسوب او اتلاف الملفات والبيانات.

2- ملفات التجسس (Spywares) : هي برامج مصممة لجمع المعلومات الشخصية مثل المواقع الالكترونية التي يزورها المستخدم وسجل بياناته وكلمة المرور للحسابات الالكترونية وكذلك تستطيع الحصول على أمور مهمة للمستخدم مثل رقم بطاقة الائتمان دون علمه.

3- ملفات دعائية (Adware) : هي برامج مصممة للدعاية والاعلان وتغير الاعدادات العامة في أجهزة الحاسوب مثل تغير الصفحة الرئيسية للمتصفح وإظهار بعض النوافذ الدعائية اثناء اتصالك بالأنترنت وتصفحك للمواقع الالكترونية.

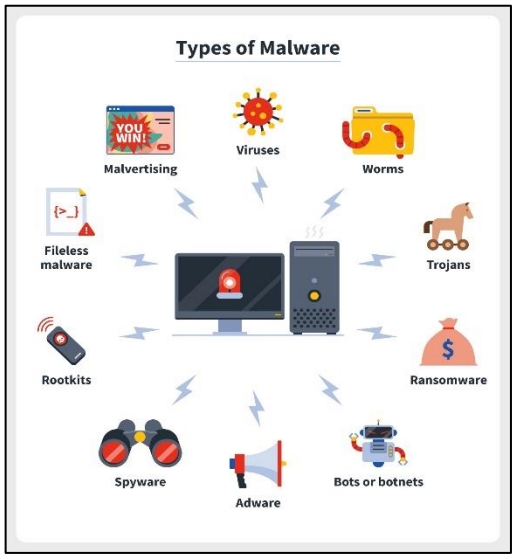
4- قلة الخبرة في التعامل مع بعض البرامج : قلة الخبرة الكافية لكيفية التعامل مع تلك البرامج قد يفتح ثغرة في جهاز الحاسوب تمكن الاخرين من اختراق الجهاز.

5- أخطاء عامة : مثل سوء اختيار كلمة السر، واختيار كلمة سر ضعيفة مثل (123456789 ، 20232023، ...) او ترك الحاسوب مفتوح مما يسمح للأخرين خاصة الأشخاص الغير مخولين او الغرباء من الدخول لملفات الحاسوب او تغير بعض الاعدادات او سرقة البيانات الشخصية.

❖ **برمجيات خبيثة (Malware) :** هي برامج مخصصة للتسلل لنظام الحاسوب او تدميره بدون علم المستخدم. بمجرد تثبيت البرمجية الخبيثة على الحاسوب، يصعب إزالتها بسهولة، درجة خطورة هذه البرامج تتراوح حسب نوع البرنامج الذي يصيب الحاسوب بعضها :

1- إعلانات مزعجة غير مرغوب بها تعمل بشكل تلقائي خلال عمل المستخدم على الحاسوب سواء كان المستخدم متصل او غير متصل بالأنترنت.

2- بعض البرامج تكون خطيرة مباشرة تسبب تعطيل نظام التشغيل عن العمل وهذا يتطلب إعادة تهيئة القرص الصلب.



❖ **فايروسات الحاسوب:** هي برامج صغيرة خارجية صممت عمدا لتغير خصائص الملفات التي تصيبها وتقوم بتنفيذ بعض الأوامر اما بالحذف او التعديل او التخريب وفقا للأهداف المصممة لآجلها ولها القدرة على التخفي.

- **الاضرار الناتجة عن فايروسات الحاسوب** :

1- تقليل مستوى أداء الحاسوب
2- إيقاف تشغيل الحاسوب وإعادة تشغيل نفسه تلقائيا كل بضع دقائق او إخفاقه في العمل بعد إعادة التشغيل.
3- تعذر الوصول الى مشغلات الأقراص الصلبة
4- حذف الملفات او تغيير محتوياتها
5- ظهور مشاكل في التطبيقات المنصبة وتغير نوافذ التطبيقات
6- تكرار ظهور رسائل الخطأ في أكثر من تطبيق

- **صفات فايروسات الحاسوب :**

1- القدرة على التناسخ والانتشار
2- ربط نفسها مع برنامج اخر يسمى الحاضن (Host)
3- يمكن ان تنتقل من حاسوب مصاب الاخر سليم

- **يتكون برنامج الفايروس بشكل عام من أربعة أجزاء رئيسة هي :**

1- الية التناسخ : تسمح للفايروس ان ينسخ نفسه
2- الية التخفي : تخفي الفايروس عن الاكتشاف
3- الية التنشيط : تسمح للفايروس بالانتشار
4- الية التنفيذ : تنفيذ الفايروس عن تنشيطه

- **تقسم الفايروسات الى ثلاث أنواع :**

1- الفايروس (Virus) : برنامج تنفيذي ذات الامتداد (com, exe, bat, pif,scr) يعمل بشكل منفصل ويهدف الى احداث خلل في الحاسوب وتتراوح خطورته حسب المهمة المصمم لأجلها، فمنها البسيطة ومنها الخطيرة، وينتقل بواسطة نسخ الملفات من حاسوب يحتوي ملفات مصابة الى حاسوب اخر عن طريق الأقراص المدمجة (CD) والذاكرة المتحركة (Flash Memory).

2- الدودة (Worm) : تنتشر فقط عبر الشبكات والانترنت مستفيدة من قائمة عناوين البريد الالكتروني (مثل تطبيق برنامج التحدث الماسنجر) فعند إصابة الحاسوب يبحث البرنامج الخبيث عن عناوين الأشخاص المسجلين في قائمة العناوين ويرسل نفسه الى كل الأشخاص في القائمة مما يؤدي الى انتشاره بسرعة عبر الشبكة.

3- حصان طروادة (Trojan Horse) : فايروس تكون اليه عمله مرفقاً (ملحقا) مع احد البرامج أي يكون جزءاً من برنامج دون ان يعلم المستخدم.

❖ **اهم الخطوات اللازمة للحماية من عملية الاختراق :**

1- استخدام أنظمة تشغيل محمية من الفايروسات كنظام يونكس ولينكس وتوزيعاتها.

2- تثبيت البرامج المضادة للفايروسات (**Antivirus**) مثل (.. , Norton , Avira , Kaspersky) وبرامج مكافحة ملفات التجسس (**Antispyware**) مثل (AVG Anti –Spyware).

3- الاحتفاظ بنسخ للبرمجيات المهمة مثل نظام التشغيل ويندوز ونسخة من ملفات المستخدم.

4- عدم فتح أي رسالة او ملف محلق ببريد الكتروني وارد من شخص غير معروف.

5- تثبيت كلمة سر قوية للحاسبة والشبكة اللاسلكية.

6- عدم الاحتفاظ بأية معلومات شخصية في داخل الحاسوب كـ (الملفات المهمة ، المعلومات المهمة مثل ارقام الحسابات او البطاقات الائتمانية)، وخزنها في وسائط تخزين خارجية.

7- عدم تشغيل برمجيات الألعاب على نفس الحاسوب الذي يحتوي معلومات شخصية.

8- ثقافة المستخدم، وذلك من خلال التعرف على الفايروسات وطرق انتشارها وكيفية الحماية منها، وعدم الدخول الى روابط ومواقع غير موثوقة.

9- تفعيل عمل الجدار الناري (Firewall) ، يقوم الجدار الناري بتفحص المعلومات الواردة من الانترنت والصادرة الية.

10- فك الارتباط بين الحاسوب والموديم عند الانتهاء من العمل فذلك يمنع البرامج الخبيثة التي تحاول الاتصال من الدخول الى الحاسوب.