وزارة التعليم العالي والبحث العلمي

جامعة تكريت /كلية التربية للعلوم الانسانية

قسم التاريخ/المرحلة الاولى/ مسائي

المادة حاسبات

الاختراق الإلكتروني

إعداد

م.م محمد جليل ابراهيم

1447هـ

2026-2025م

هو قيام شخص غير مخول أو أكثر بمحاولة الدخول الكترونياً إلى الحاسوب أو الشبكة عن طريق شبكة الإنترنت وذلك بغرض الإطلاع، والسرقة، والتخريب، والتعطيل باستخدام برامج متخصصة.

- أنواع الاختراق الإلكتروني:

يمكن تقسيم الاختراق من حيث الطريقة المستخدمة إلى ثلاثة أقسام:

1. المزودات أو الأجهزة الرئيسية للشركات والمؤسسات أو الجهات الحكومية وذلك باختراق الجدار الناري FirewaII والتي توضع لحمايتها يتم ذلك باستخدام المحاكاة لغرض الخداع Spoofing وهو مصطلح يطلق على عملية انتحال شخصية للدخول إلى النظام، إذ ان حزم البيانات تحتوي على عناوين للمرسل والمرسل إليه وهذه العناوين ينظر إليها على أنها عناوين مقبولة وسارية المفعول من قبل البرامج وأجهزة الشبكة.
2. الأجهزة الشخصية والعبث بما فيها من معلومات وتعد من الطرق الشائعة لقلة خبرة أغلب مستخدمي هذه الأجهزة من جانب ولسهولة تعلم برامجيات الاختراق وتعددها من جانب أخر.
3. البيانات من خلال التعرض والتعرف على البيانات أثناء انتقالها ومحاولة فتح التشفير اذا كانت البيانات مشفرة وتستخدم هذه الطريقة في كشف أرقام بطاقات الائتمان وكشف الأرقام السرية لبطاقات البنوك.

- مصادر الاختراق الإلكتروني:

1. مصادر متعددة ويكون مصدرها جهات خارجية تحاول الدخول إلى الجهاز بصورة غير مشروعة بغرض قد يختلف حسب الجهاز المستهدف.

ومن الأمثلة عن المصادر المتعمدة للاختراق الإلكتروني:

- المحترفون والهواة، لغرض التجسس دون الإضرار بالحاسوب.
- اختراق شبكات الاتصال والأجهزة الخاصة بالإتصال للتنصت أو للإتصال المجاني.
- اختراق لنشر برنامج معين أو لكسر برنامج أو لفك شفرتها المصدرية (Crackers).
- أعداء خارجيون وجهات منافسة.
- مجرمون محترفون في مجال الحاسوب والإنترنت.

2. مصادر غير متعمدة وهي تنشأ بسبب ثغرات موجودة في برامجيات الحاسوب والتي قد تؤدي إلى تعريض الجهاز إلى نفس المشاكل التي تنتج عن الأخطار المتعمدة.

- المخاطر الأمنية الاكثر انتشارا:

a. الفيروسات (Viruses) : هي برامج مصممة للانتقال إلى أجهزة الحاسوب بطرق عدة وبدون أذن المستخدم، وتؤدي إلى تخريب أو تعطيل عمل الحاسوب أو أتلاف الملفات والبيانات.

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

c. ملفات دعائية (Adware) : هي برامج مصممة للدعاية والإعلان وتغيير الإعدادات العامة في أجهزة الحاسوب مثل تغيير الصفحة الرئيسية للمتصفح وإظهار بعض النوافذ الدعائية أثناء اتصالك بالإنترنت وتصفحك للمواقع الإلكترونية.

d. قلة الخبرة في التعامل مع بعض البرامج: مع ازدياد استخدام الإنترنت من عامة الناس غير المتخصصين، واستخدامهم وتعاملهم مع برامجيات متطورة الخاصة بخدمة تطبيقات الإنترنت وبشكل مستمر وبدون خبرة كافية لكيفية التعامل مع تلك البرامجيات، قد يفتح ثغرة في جهاز الحاسوب تمكن الأخرين من اختراق الجهاز.

e. أخطاء عامة: مثل سوء اختيار كلمة السر أو كتابتها على ورقة مما يمكن الأخرين من قراءتها أو ترك الحاسوب مفتوح مما يسمح للأخرين (خاصة غير المخولين أو الغرباء) بالدخول لملفات الحاسوب أو تغير بعض الإعدادات.

- برامجيات خبيثة Malware:

Malware هي اختصار لكلمتين Malicious Software وهي برامج مخصصة للتسلل لنظام الحاسوب أو تدميره بدون علم المستخدم وما إن يتم تثبيت البرامجية الخبيثة فإنه من الصعب إزالتها. وبحسب درجة البرمجية من الممكن أن يتراوح ضررها من إزعاج بسيط (بعض النوافذ الإعلانية غير المرغوب بها خلال عمل المستخدم على الحاسوب متصلاً أم غير متصلاً بالشبكة) إلى أذى غير قابل للإصلاح يتطلب إعادة تهيئة القرص الصلب على سبيل المثال. من الأمثلة على البرامجيات الخبيثة هي الفيروسات وأحصنة طروادة.

- فايروسات الحاسوب:

هي برامج صغيرة خارجية صممت عمداً لتغيير خصائص الملفات التي تصيبها وتقوم بتنفيذ بعض الأوامر إما بالحذف أو التعديل أو التخريب وفقاً للأهداف المصممة لأجلها ولها القدرة على التخفي، ويتم خزنها داخل الحاسوب بإحدى طرق الانتقال لإلحاق الضرر به والسيطرة عليه.

- الأضرار الناتجة عن فايروسات الحاسوب:

1. تقليل مستوى إداء الحاسوب.
2. إيقاف تشغيل الحاسوب وإعادة تشغيل نفسه تلقائياً كل بضع دقائق أو إخفاقه في العمل بعد إعادة التشغيل.
3. تعذر الوصول إلى مشغلات الأقراص الصلبة والمدمجة (وحدات الخزن) وظهور رسالة تعذر الحفظ لوحدات الخزن.
4. حذف الملفات أو تغيير محتوياتها.
5. ظهور مشاكل في التطبيقات المنصبة وتغير نوافذ التطبيقات والقوائم والبيانات.
6. تكرار ظهور رسائل الخطأ في أكثر من تطبيق.
7. إفشاء معلومات وأسرار شخصية هامة.

- صفات فايروسات الحاسوب:

1. القدرة على التناسخ والانتشار Replication.
2. ربط نفسها ببرنامج أخر يسمى الحاضن (المضيف Host).
3. يمكن أن تنتقل من حاسوب مصاب لاخر سليم.

- مكونات الفايروسات:

يتكون برنامج الفايروس بشكل عام من أربعة أجزاء رئيسة تقوم بالأتي:

1. الية التناسخ The Replication Mechanism نسمح للفايروس أن ينسخ نفسه.
2. الية التخفي The Hidden Mechanism تخفي الفايروس عن الاكتشاف.
3. الية التنشيط The Trigger Mechanism تسمح للفايروس بالانتشار.
4. الية التنفيذ The Payload Mechanism تنفيذ الفايروس عند تنشيطه.

- أنواع الفايروسات:

تقسم الفايروسات إلى ثلاثة أنواع :

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

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

3. حصان طروادة (Trojan Horse): فايروس تكون الية عمله مرفقاً (ملحقاً) مع أحد البرامج، أي يكون جزءاً من برنامج دون ان يعلم المستخدم. سمي هذا البرنامج بحصان طروادة لأنه يذكر بالقصة الشهيرة لحصان طروادة، إذ اختبأ الجنود اليونان داخله واستطاعوا اقتحام مدينة طروادة والتغلب على جيشها.

- أهم الخطوات اللازمة للحماية من عمليات الاختراق:

الحفاظ على جهاز الحاسوب ضد هذه الملفات بشكل كامل صعب جداً مادام الجهاز مربوط بشبكة الإنترنت، لكن يمكن حماية الحاسوب بنسبة كبيرة وتقليل خطر الإصابة بالاختراقات الالكترونية والبرامج الضارة باتباع الخطوات الأتية:

1. استخدام نظم تشغيل محمية من الفايروسات كنظم يونكس ولينكس ومشتقاتها. وتم بناء هذه النظم بحيث لا يمكن ان يدخل اليها أي برنامج خارجي الإ بموافقة وعلم المستخدم بشكل واضح وصريح، كما ان ملفات النظام الأساسية تكون محمية من أي تغير او تلاعب حتى عن طريق الخطأ غير المتعمد.

2. تثبيت البرامج المضادة أو المكافحة للفايروسات مثل (Norton, Avira, MeAfee, Kaspersky) وبرنامج مكافحة ملفات التجسس مثل AVG Anti-Spyware ذات الإصدارات الحديثة وتحديث النسخة.

3. الاحتفاظ بنسخ للبرامجيات المهمة مثل نظام التشغيل ويندوز وحزمة أوفيس ونسخة من ملفات المستخدم.

4. عدم فتح أي رسالة أو ملف ملحق ببريد إلكتروني وارد من شخص غير معروف للمستخدم أو الملفات ذات امتدادات غير المعروفة.

5. تثبيت كلمة سر Password على الحاسوب والشبكة اللاسلكية الخاصة بالمستخدم مع تغييرها كل فترة، وعدم السماح الإ للمستخدمين الموثوقين بالاتصال واستخدام الحاسوب.

6. عدم الاحتفاظ بأية معلومات شخصية في داخل الحاسوب (كالرسائل الخاصة، الصورالفوتوغرافية، الملفات المهمة، والمعلومات المهمة مثل أرقام الحسابات أو البطاقات الائتمانية)، وخزنها في وسائط تخزين خارجية.

7. عدم تشغيل برامجيات الألعاب على نفس الحاسوب الذي يحتوي البيانات والبرامجيات المهمة، لأنها تعد من اكثر البرامجيات تداولاً بين الاشخاص والتي تصاب بالفايروسات.

8. إيقاف خاصية مشاركة الملفات إلا للضرورة وعمل نسخ احتياطية من الملفات المهمة والضرورية.

9. ثقافة المستخدم وذلك من خلال التعرف على الفايروسات وطرق انتشارها، وكيفية الحماية منها، والأثار المترتبة حال الإصابة بها. ويتم هذا عن طريق التواصل المستمر من خلال زيارة المواقع التي تهتم بالحماية من الفايروسات.

10. فك الارتباط بين الحاسوب والموديم أو الخط الهاتفي عند الانتهاء من العمل، فذلك يمنع البرامج الخبيثة التي تحاول الاتصال من الدخول إلى الحاسوب.

11. تفعيل عمل الجدار الناري Firewall: يقول الجدار الناري بتفحص المعلومات الواردة من الإنترنت والصادرة إليه. ويتعرف على المعلومات الواردة من المواقع الخطرة أو تلك التي تثير الشك فيعمل على إيقافها. إذا قام المستخدم بإعداد جدار الحماية بشكل صحيح، فلن يتمكن المتطفلون (الذين يبحثون عن أجهزة الحاسوب التي لا تتمتع بالحصانة) من الدخول والاطلاع على هذه الأجهزة.

- أضرار الحاسوب على الصحة:

الجلوس لفترات طويلة امام الحاسوب، الجلوس الخاطىء أمام شاشة الحاسوب، والتعرض للأشعة الصادرة من هذه الشاشة الذي يؤثر في العين والإبصار والبشرة والجلد وأفضل وقاية منها هي التأكد من صحة وضعية الجلوس أمام الحاسوب مع الحفاظ على وضع الشاشة بشكل مناسب حتى لا يرفع المستخدم للحاسوب رأسه أو يخفضه كثيراً.

- أثار بدنية ونفسية قصيرة المدى وتشمل توتر وإجهاد عضلات العين والقلق النفسي.

- الأثار البدنية والنفسية بعيدة المدى التي تأخذ فترة اطول لظهورها ومنها ألام العضلات والمفاصل والعمود الفقري وحالة من الأرق والقلق النفسي والانفصال النفسي والاجتماعي عن عالم الواقع والعيش في وسط افتراضي والعلاقات الخيالية لمن يدمنون على الإنترنت وأفضل وقاية لذلك هو التوقف من حين لأخر عن العمل بالحاسوب وبسط الساقين والكاحلين والقيام ببعض التمارين الرياضية الخفيفة لتسريع جريان الدم وتحديد ساعات العمل بالحاسوب في الليل.