جامعة الموصل
كلية التربية للعلوم الصرفة
قسم الفيزياء

Computer basics

أساسيات الحاسوب

المرحلة الاولى

مدرس المادة

م.م. سيف ميسر محمد فاضل

الفصل الاول

الحاسوب والبرامج التطبيقية

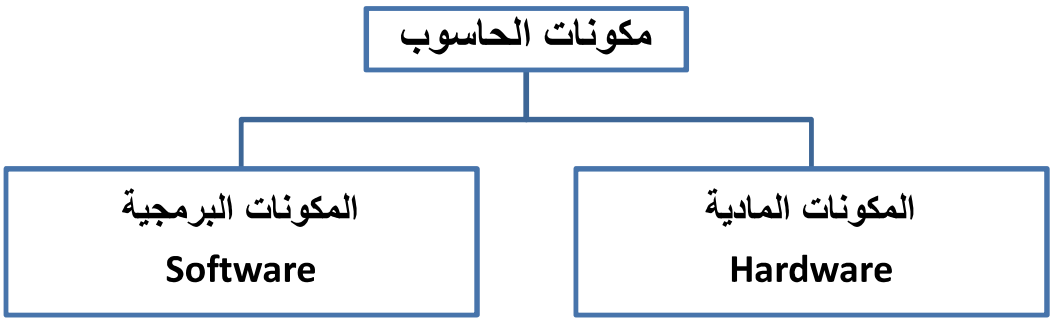
الحاسوب : يعرف الحاسوب بأنه جهاز لمعالجة البيانات أو المعلومات بعمليات حسابية ومنطقية بصفة آلية ودون تدخل بشريأثناء التشغيل وعادةً ما يعمل بالترقيم الثنائي . كما يعرف الحاسوب أنه عبارة عن جهاز إلكتروني يقوم بإستقبال البيانات ومن ثم معالجتها وتخزينها أو إظهارها للمستخدم بصورة أخرى .

خصائص الحاسوب :

- ❖ سرعة إنجاز العمليات.
- ❖ سرعة دخول البيانات و استرجاع المعلومات .
- ❖ القدرة على تخزين المعلومات .
- ❖ دقة النتائج و التي تتوقف أيضا على دقة المعلومات المدخلة للحاسوب .
- ❖ تقليص دور العنصر البشري خاصة في المصانع التي تعمل آليا .
- ❖ سرعة إجراء العمليات الحسابية و المنطقية المتشابكة .
- ❖ إمكانية عمل الحاسوب و بشكل متواصل دون تعب .
- ❖ تعدد البرمجيات والبرامج الجاهزة والتي تسهل استخدام الحاسوب دون الحاجة إلى دراسة علم الحاسوب و هندسة الحاسوب .
- ❖ إمكانية اتخاذ القرارات وذلك بالبحث عن كافة الحلول لمسألة معينة وأن يقدم أفضلها وفقا للشروط الموضوعة والمتطلبات الخاصة بالمسألة المطروحة .
- ❖ قابلية الربط والاتصال من خلال شبكات الحاسوب حيث يمكن ربط أكثر من جهاز مع إمكانية التحاور ونقل البيانات والمعلومات فيما بينها .

مكونات الحاسوب

تنقسم مكونات الحاسوب الى قسمين رئيسيين كما هو موضح في الشكل (1) :



شكل (1)

مكونات الحاسوب

المكونات المادية : تعد هذه المكونات عتاد الحاسوب وما يحتويه من اشياء تم صنعها واهمها :

- وحدة المعالجة المركزية (Processing Unit).
- وحدة الذاكرة (Memory Unit).
- وحدات الإدخال (Input Units).
- وحدات الإخراج (Output Units).
- وحدات التخزين (Storage Unit).

المكونات البرمجية Software :

1- **نظام التشغيل** : هو مجموعة من البرامج والتعليمات وظيفتها الاساسية ادارة مكونات الحاسوب المادية وتنظيم العمل عليه ، مثل نظام التشغيل windows ونظام التشغيل Linux ، ومن وظائف نظام التشغيل :

- تأمين عمليات الادخال والاخراج.
- ادارة العمليات المخزونة في الحاسوب كتنظيم ملفات المستخدمين .
- حماية المستخدمين بعضهم من بعض وحماية مكونات الحاسوب من الاعطال فضلاً عن حماية برامج المستخدمين وملفاتهم .
- تأمين الاتصال مع حواسيب اخرى وإمكانية تبادل البرامج والبيانات معها .

2- **البرامج التطبيقية** : هي البرامج التي تلبي احتياجات محددة للمستخدمين ويمكن تصنيفها حسب الجهة التي تقوم بتطويرها الى نوعين :

- برمجيات التطبيقات الخاصة (User Programs) : فكل مبرمج يمكنه كتابة البرامج الخاصة بمجاله ، مثلاً برنامج لحل المسائل ، وآخر لإعداد اختبار الكتروني او برامج تحليل احصائي وغيرها .
- برمجيات التطبيقات الجاهزة (Packages): وتقوم بتطويرها شركات انتاج البرمجيات والشركات الصانعة للحواسيب ، وهي مصممة لتلبية متطلبات شريحة كبيرة من المستخدمين، ومن الامثلة عليها مجموعة برامج Microsoft Office 2007 التي صممتها وطورتها شركة Microsoft .

مجموعة برامج Microsoft Office 2007

تعد هذه المجموعة من اهم وأفضل البرامج التطبيقية الجاهزة التي انشأتها شركة Microsoft في العام 2007 . اذ تتيح للمستخدم ان يعالج كافة الامور الطباعية والحسابية وحتى ارسال الرسائل الالكترونية . ولمجموعة Office 2007 واجهة موحدة لجميع البرامج وهي سهلة الاستخدام وذلك عن طريق تبويبات (قوائم) موجهة تحتوي على مجموعات منطقية لأوامر ووظائف البرنامج ، وداخل كل مجموعة هناك مجموعة من الادوات. فضلاً عن العديد من مربعات الحوار ضمن مجموعات منسدلة تعرض الخيارات المتوفرة مع تلميحات واضحة ومعاينة نموذجية مما يوفر للمستخدم مساعدة كبيرة في انتقاء ما يناسبه من خيارات لذا فان واجهة التطبيق Office 2007 تقدم للمستخدم الادوات الاكثر فائدة لانجاز أي مهمة .

2- **البرامج التطبيقية** : هي البرامج التي تلبي احتياجات محددة للمستخدمين ويمكن تصنيفها حسب الجهة التي تقوم بتطويرها الى نوعين :

- برمجيات التطبيقات الخاصة (User Programs) : فكل مبرمج يمكنه كتابة البرامج الخاصة بمجاله ، مثلاً برنامج لحل المسائل ، وآخر لإعداد اختبار الكتروني او برامج تحليل احصائي وغيرها .
- برمجيات التطبيقات الجاهزة (Packages): وتقوم بتطويرها شركات انتاج البرمجيات والشركات الصانعة للحواسيب ، وهي مصممة لتلبية متطلبات شريحة كبيرة من المستخدمين، ومن الامثلة عليها مجموعة برامج Microsoft Office 2007 التي صممتها وطورتها شركة Microsoft .

مجموعة برامج Microsoft Office 2007

تعد هذه المجموعة من اهم وأفضل البرامج التطبيقية الجاهزة التي انشأتها شركة Microsoft في العام 2007 . اذ تتيح للمستخدم ان يعالج كافة الامور الطباعية والحسابية وحتى ارسال الرسائل الالكترونية . ولمجموعة Office 2007 واجهة موحدة لجميع البرامج وهي سهلة الاستخدام وذلك عن طريق تبويبات (قوائم) موجهة تحتوي على مجموعات منطقية لأوامر ووظائف البرنامج ، وداخل كل مجموعة هناك مجموعة من الادوات. فضلاً عن العديد من مربعات الحوار ضمن مجموعات منسدلة تعرض الخيارات المتوفرة مع تلميحات واضحة ومعاينة نموذجية مما يوفر للمستخدم مساعدة كبيرة في انتقاء ما يناسبه من خيارات لذا فان واجهة التطبيق Office 2007 تقدم للمستخدم الادوات الاكثر فائدة لانجاز أي مهمة .

متطلبات تشغيل Office 2007

- **المعالج** : يجب ان يكون المعالج بسرعة 500 ميكا هرتز او اكثر وللاستخدام الامثل تحتاج الى معالج Pentium 4.
- **الذاكرة** : 256 ميكا بايت من الذاكرة المساعدة Ram او اكثر .
- **القرص الصلب** : تتعلق مساحة القرص المطلوبة بالخيارات التي يقوم المستخدم بتعيينها اثناء عملية تثبيت برنامج Office 2007 وكذلك تتعلق ايضاً بالاصدارات المستخدمة ، وفيما يلي قائمة بمساحة القرص المطلوبة لكل اصدار :
  - Microsoft Office Standard Basic 1.5 كيكا بايت .
  - Microsoft Office Standard 1.5 كيكا بايت .
  - Microsoft Office Standard Home and Student 1.5 كيكا بايت .
  - Microsoft Office Professional 2 كيكا بايت .
  - Microsoft Office Small Business 2 كيكا بايت .
  - Microsoft Office Professional Plus 2 كيكا بايت .
  - Microsoft Office Enterprise 2 كيكا بايت .
- **نظام التشغيل** : Microsoft Windows XP بجميع اصداراته فضلاً عن Microsoft Windows 7 بإصداراته المختلفة ايضاً وما يتطور عنه .
- **شاشة بدقة** (768 × 1024) او اعلى .

برامج مجموعة Office 2007

تتكون مجموعة Office بصيغتها الافتراضية من تسع برامج لكل برنامج هناك وظائف متعددة يقوم بها عن طريق المستخدم وهي :

وسوف ندرس من خلال محاضراتنا القادمة البرامج التالية :

1- Microsoft Office Word 2007.

2- Microsoft Office Excel 2007.

3- Microsoft Office PowerPoint 2007.

مميزات مجموعة برامج Office 2007

تعتبر Microsoft Office Professional 2007 مجموعة كاملة من البرامج الإنتاجية وقواعد البيانات التي تساعد المستخدم في توفير الوقت وتنظيم الأعمال. اذ يمكن للمستخدم تطوير مواد احترافية للطباعة والبريد الإلكتروني والويب بسهولة. وكذلك يمكنه إنشاء مستندات الأعمال الديناميكية وجداول البيانات والعروض التقديمية سريعاً بالإضافة إلى إنشاء قواعد البيانات دون ضرورة وجود خبرة سابقة. ومن اهم **ميزات** مجموعة Office 2007 مايلي :

1- مساعدة المستخدم في العثور على ميزات البرنامج التي يحتاج إليها واستخدامها بشكل أسهل وأسرع . حيث يتم عرض القوائم وأشرطة الأدوات المستندة إلى المهام وفقاً للميزة التي تستخدمها.

2- يتضمن Microsoft Office Word 2007 قوالب وأدوات جديدة تعمل على تسهيل إعادة استخدام المحتويات وتطبيق التنسيق ذات المظهر المحترف ومعاينة التغييرات سريعاً . كما يتيح إنشاء عروض تقديمية ديناميكية بسرعة وسهولة أكبر من ذي قبل، بما يحتويه من مكتبة شاملة من السمات وتخطيطات الشرائح القابلة للتخصيص وأدوات الرسم الجديدة التي

تساعد في إنشاء تخطيطات فعالة ورسومات SmartArt والجداول ومعاينة تغييرات التنسيق سريعاً .

3- يوفر أدوات جديدة تمكن المستخدم من تصفية المعلومات وفرزها ورسمها ووضع تصور لها بحيث تستطيع تحليل معلومات الأعمال بسهولة أكبر من ذي قبل.

4- إدارة معلومات الأعمال باستخدام الأدوات الجديدة لإنشاء قواعد البيانات وتنظيم المعلومات ووضع تصور لها بسهولة. حيث يتيح للمستخدم إنشاء قواعد البيانات الجديدة بسهولة بدون أن يتطلب ذلك أي خبرة مسبقة.

البرماجيات الخبيثة (Malware)

سيف الحسيني

مفهوم أمن المعلومات

هي مجموعة من السياسات والإجراءات الفنية المتخذة من أجل منع الأشخاص الغير مخولين من الدخول إلى الشبكات وتغيير معلوماتها سواء بهدف سرقتها أو تدمير نظم المعلومات.

العوامل التي تساعد على اختراق أنظمة المعلومات

- **مشاكل الأجهزة والمعدات المادية:** مثل الأخطاء الناتجة عن الإعدادات الغير صحيحة الخاصة بالأجهزة والأعطال المتكررة .
- **مشاكل برمجية:** خطأ في البرمجيات ، خطأ في تنزيل البرامج وتغييرات غير مسموح بها.
- **الكوارث:** مثل الحرائق ، الفيضانات ، مشاكل انقطاع التيار الكهربائي.
- **استخدام الشبكات والكمبيوترات خارج سيطرة المنظمة:** مثل استخدام الشبكة من قبل شركات أخرى عالمية

البرامج الخبيثة التي تهدد أنظمة المعلومات

يقصد بالبرمجيات الخبيثة هي أي برنامج يعطي بعض السيطرة أو السيطرة الكاملة على الحاسوب الخاص بك لمن قام بتصميمه لهذا الغرض.

و الأضرار التي تقوم بها هذه البرامج قد تكون خفيفة كتغير اسم المؤلف لمستند ما أو كبيرة مثل الوصول الكامل للحاسوب دون المقدرة على تعقبها.

ويمكن يتصنيف أنواع البرمجيات الخبيثة على النحو التالي:

1. الفيروسات (Viruses)
2. الديدان (Worms)
3. برامج التجسس (Spywares)
4. أحصنة طروادة Trojan Horses

الفيروسات Viruses

- فيروسات الكمبيوتر هي برامج تقوم بمهاجمة وإتلاف برامج معينة ، وتنتقل الى برامج أخرى عند تشغيل البرامج المصابة ، كما تقوم بالتلاعب بمعلومات الكمبيوتر المخزنة
- ينتقل الفيروس إلى جهازك عندما تقوم بنقل ملف ملوث بالفيروس إلى جهازك أو عند زيارة احد المواقع المشبوهة أو إثناء تبادل الفلاشات مع الأصدقاء و ينشط الفيروس عند محاولة فتحه ويمكن أن يصلك ايضا عن طريق البريد الإلكتروني على هيئة مرفقات.

الديدان Worms

- ديدان الحاسوب هي الفيروسات التي تقوم بإنشاء نسخ من تلقاء نفسها
- يمكن أن تسبب الضرر بشكل واسع.
- على عكس الفيروسات، التي تتطلب نشر ملفات المضيف المصابة. الديدان تعتبر برنامج مستقل ولا يحتاج إلى برنامج مضيف أو مساعدة أشخاص للنشر.

برامج التجسس Spywares

- هي مماثلة لبرامج الإعلانات، ولكن لديها نوايا ضارة. في حالة التجسس، المستخدم يجهل هذا الغزو.
- يمكن لبرامج التجسس جمع ونقل المعلومات الشخصية.
- بسبب ما تقوم به هذه البرامج من نقل للمعلومات دون علم المستخدم، تصنف هذه البرامج على أنها برمجيات مقتحمة للخصوصية

The Trojan Horses أحصنة طروادة

- وهو من البرمجيات الخبيثة التي تبدو أنها برمجيات سليمة. تقوم بخداع المستخدمين من أجل تحميلها وتطبيقها على أنظمتهم.
- فيتم بذلك تنشيطها، وتبدأ بمهاجمة النظام، فتؤدي إلى بعض الأمور المزعجة للمستخدم أو بعض الأضرار

أضرار الإصابة بالفيروسات و البرامج الخبيثة

1. تعطيل الحاسوب
2. ظهور شاشة الموت الزرقاء
3. سرقة النقود إلكترونيا
4. بعض الأمور المزعجة للمستخدم مثل تغير سطح المكتب و حذف الملفات
5. تسرق البيانات
6. إتلاف البرمجيات و التسبب في الحرمان من استخدام بعض الخدمات
7. تبطئ الحاسب
8. تبطئ الاتصال بالانترنت

التهديدات لأمن المعلومات

الجريمة المعلوماتية: هي تعبير شامل يشير إلى جريمة تتعلق باستعمال إحدى وسائل تقنية المعلومات لغرض خداع الآخرين وتضليلهم، أو من أجل تحقيق هدف معين لجهة معينة.

ويمكن تصنيف الجرائم المعلوماتية على النحو التالي:

1. **جرائم هدفها نشر المعلومات:** مثل الحصول على أرقام البطاقات الائتمانية
2. **جرائم هدفها نشر معلومات غير صحيحة:** مثل نشر المعتقدات الخاطئة أو التشكيك في القرآن والسنة.
3. **استخدام تقنية المعلومات كوسيلة لأداء الجريمة:** مثل تزوير بطاقات الائتمان والتحويل بين الحسابات المصرفية.
4. **جرائم لها علاقة بانتشار تقنية المعلومات:** مثل قرصنة البرامج الأصلية والتي تكون أسعارها $5000 لتباع بأقل من $10

طرق حماية المعلومات

- برامج مكافحة الفيروسات مثل:

(**Macafee , Kaspersky, Norton**)

- توفير نسخ احتياطية (backup) .
- جدار الحماية.
- استخدام كلمة المرور(Password).

أخلاقيات المعلومات

هي مجموعة من المبادئ والأخلاق تجعل من وسائل تقنية المعلومات والاتصالات بكافة أنواعها وسائل فعالة راقية للاتصال وتبادل المعلومات.

أخلاقيات التعامل مع وسائل تقنية المعلومات

1. أخلاقيات التعامل بين الفرد المستخدم للمعلومات ونفسه:

ينبغي على أي مستخدم لأي وسيلة من وسائل تقنية المعلومات أن يراعي:

- تقوى الله ومراقبته
- تجنب الدخول إلى المواقع المشبوهة الضارة والالتزام بالمواقع التي تتناسب مع العمر وتحقق الأهداف وتحقق الحاجات.

أخلاقيات التعامل مع وسائل تقنية المعلومات

2. أخلاقيات التعامل بين المستخدم للمعلومات وغيره من المستخدمين،

وذلك من خلال ما يلي:

- احترام الملكية الفكرية حيث يجب مراعاة حقوق الملكية الفكرية لأي بيانات أو معلومات . وذلك بوضع مصدر المقالات المقتبسة أو غيرها من الإعمال.
- الحفاظ على خصوصية وإسرار الآخرين وعدم نشرها
- الابتعاد عن التزوير والخداع.
- تجنب الإضرار بالآخرين عن طريق إرسال البرامج الضارة لأجهزتهم وأنظمتهم المعلوماتية .
- الحذر من نشر أو توفير محتوى غير لائق ومخل بالآداب.

أخلاقيات التعامل مع وسائل تقنية المعلومات

3. أخلاقيات التعامل بين المستخدم وبين أجهزة التكنولوجيا ذاتها:

وذلك من خلال ما يلي:

- عدم إساءة استعمال أجهزة الكمبيوتر خصوصاً العام منها كأجهزة الجامعات والمكتبات العامة.
- الحرص على سلامة أجزاء الجهاز وبرامجه ومحتوياته سواء من تكسير أو تحميل برامج تثقل أو تسبب تلف الأجهزة.
- الحفاظ على اسم المستخدم وكلمة السر وعدم إعطائها للآخرين من غير المصرح لهم استخدام الأجهزة.
- تجنب إتلاف أو تغيير أو محو أية بيانات أو معلومات بدون وجه حق.
- عدم التقاط أو تسجيل أو جمع البيانات أو المعلومات و إعادة استخدامها بشكل غير قانوني.

بواسطة
سيف الحسيني

المقدمة

مصطلح السايبر أتاك أو ما يرادفه في الإنكليزية Cyber Attack، أصبح لغة معروفة ولهجة محفوظة لخبراء التكنولوجيا في وقتنا المعاصر، ليس من باب الاهتمام والفضول، بل المخاطر الكبيرة التي يحملها هذا الهجوم جعلته حاجة ضرورية وليس فكرة من عوالم الرفاهية.

مفهوم السايبر أتاك

يقصد بهذا المفهوم ما يمكن ترجمته إلى "هجوم رقمي أو إلكتروني" وهو عملية هجوم على نظام حاسوبي أو شبكة أو فعلياً أي جهاز يتمتع باتصال بالإنترنت. يقوم المخترقون باستخدام عدة أدوات تساندهم في إجراء هذه الهجمات، عادة ما تكون برامج خبيثة أو تجسسية وعدة طرق أخرى مشابهة.

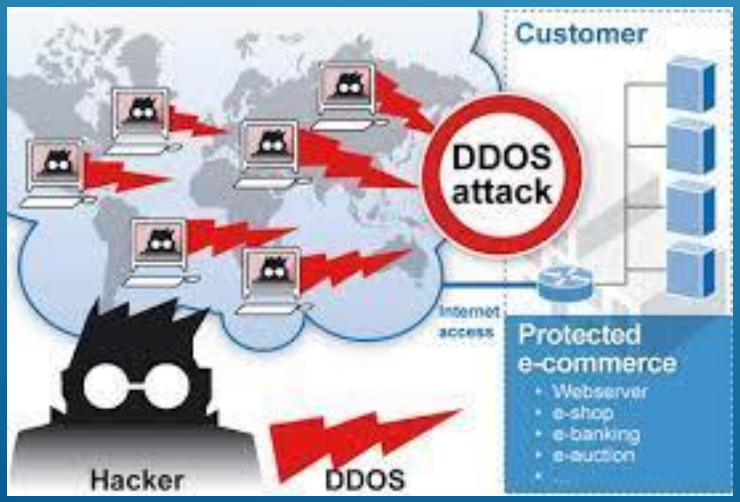
أنواع السايبر أتاك

يمكن تقسيم أشهر الأنواع المختلفة لهذا الهجوم إلى عشر أنواع رئيسية، سنقدم لكم فكرة مختصرة عن كل واحدة منها، وهي كما يلي:

- هجمات حجب الخدمة DoSو DDoS
- الهجوم الوسيط MITM
- هجمات الخداع الإلكتروني
- هجمات التصيد Drive-by
- هجمات كلمة المرور.
- هجمات حقن تعليمات الاستعلام البنيوية SQL
- هجوم حقن الشيفرة المصدريّة عبر موقع وسيط XSS
- هجوم التنصت
- هجوم البرمجيات الخبيثة أو المسيئة

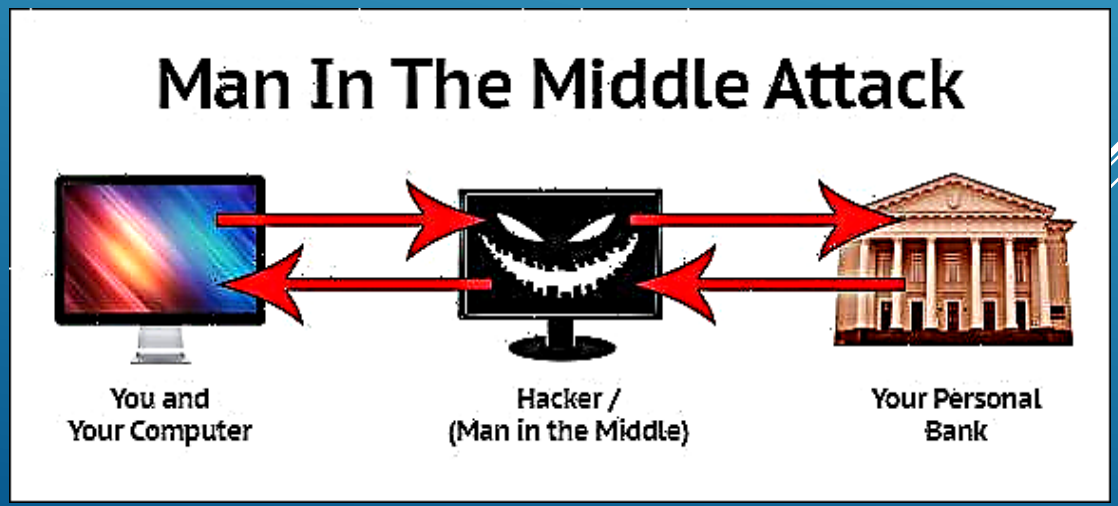
هجمات حجب الخدمةDoS و DDoS

تعتمد فكرة هذا الهجوم على تحميل نظام الضحية فوق قدراته، وبالتالي يجعله غير قادر على الاستجابة لطلبات الخدمة، فهذا النوع من الهجوم يستهدف مصادر النظام، ويتم إطلاق هذه الهجمة من قبل عدة آلات مضيفة.



الهجوم الوسيط MITM

يقوم هذا الهجوم على مبدأ الوسيط أثناء عملية اتصال بين وكيل وخادم. المعتدي يجعل نفسه الوسيط بين الاثنين، وهذه الخطوة تتيح للمعتدي اختراق نظام أحد الطرفين.
يوجد أنواع عديدة من هذا الهجوم، مثل انتحال عنوان IP بحيث يقوم المعتدي بإقناع النظام المستهدف أنه يتواصل مع وكيل موثوق به عبر إرسال عنوان ال IP الموثوق بدلاً من الحقيقي الخاص بالمعتدي، وقبول النظام المضيف لهذا العنوان سيجعله عرضةً للاختراق من قبل المعتدي.

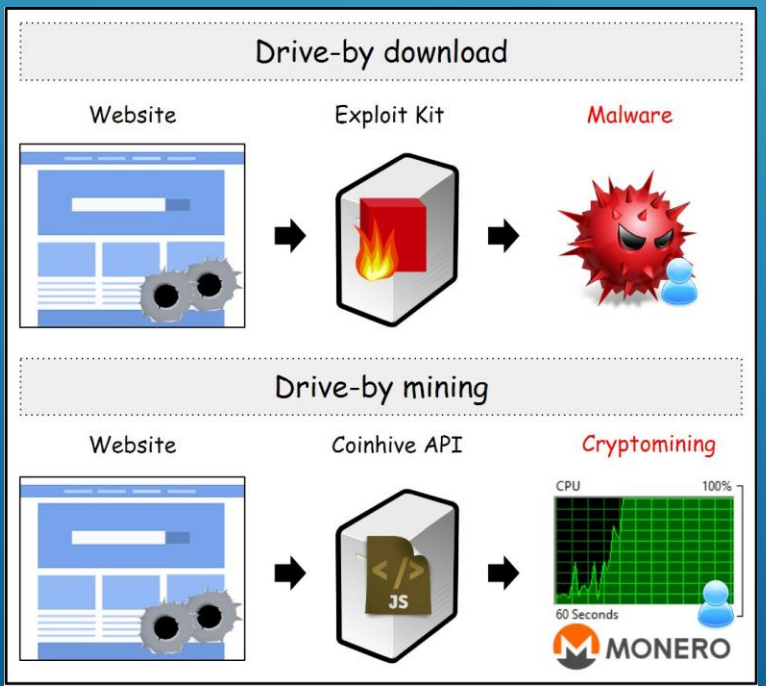


هجمات الخداع الإلكتروني

هجمات السايبر أتاك هذه عبارة عن إرسال لبريد إلكتروني يبدو أنه من مصدر موثوق، وهنالك احتمال أن تحتوي رسالة البريد الإلكتروني على برنامج خبيث يقوم بتنصيب نفسه على حاسوبك أو على رابط لموقع غير قانوني يُرغم حاسوبك على تحميل برنامج خبيث.
تصبح هذه الهجمة أكثر خطورة وتعقيدًا عندما يمضي المعتدي وقته في دراسة الضحية ونشاطاتها لكي يتمكن من خداعها.

هجمات التصيدDrive-by

هجمات مثل هذه هي الطريقة التقليدية لنشر وتوزيع برامج خبيثة، وذلك عبر حقن المواقع التي فيها ثغرات أمنية بأمر برمجي خبيث ودمجه مع بروتوكول نقل النص الفائق HTTPفي صفحات الموقع.
قد يقوم هذا البرنامج الخبيث بتنصيب نفسه على حاسب أي شخص يزوره، أو قد يقوم بإعادة توجيهه نحو موقع يتحكم فيه المعتدي.



هجمات كلمة المرور

بما أن كلمة المرور هي العائق الرئيسي بين أي معتدي والمعلومات الخاصة والسرية التي يريد سرقتها، فمن الطبيعي أنه سيحاول سرقة كلمة السر هذه، وقد تتم هجمة السايبر أتاك هذه عبر إطلاع المعتدي على الحياة الخاصة للضحية وأخذ تفاصيل عن مكتب عمله وتاريخ ميلاده وما إلى ذلك، وبعدها سيقوم بتجربة كلمات السر التي يعتقد أنها صحيحة بناء على المعلومات التي جمعها.

هجمات حقن تعليمات الاستعلام البنيوية SQL

أصبحت هذه الهجمة مشكلة معروفة للمواقع التي تعتمد في عملها على قواعد بيانات، وتتم عبر إضافة تعليمات استعلام بنيوية SQL إلى قاعدة بيانات عبر بيانات الإدخال، من الوكيل أو المستخدم وإلى الخادم.

أوامر الاستعلام هذه يتم إدخالها في المدخلات الخاصة بنشاط المستخدم مثل تسجيل الدخول وكلمات السر وتبديلها لكي يتم تشغيل أوامر تعليمات بنيوية معرفة سابقًا.

هجوم حقن الشيفرة المصدرية عبر موقع وسيط XSS

تستخدم هذه الهجمة من السايبر أتاك مصادر إنترنت خارجية لتشغيل نصوص أوامر في متصفح الإنترنت الخاص بالضحية أو البرامج التي يمكن التعديل على نصوصها.
يستطيع المعتدي أن يقوم بحقن أوامر نصوص JavaScript خبيثة في قاعدة بيانات موقع إنترنت، وعندما يقوم الضحية بطلب صفحة من موقع الإنترنت هذا، سيتم تقديمها إليه مع أوامر المعتدي الخبيثة في متصفح الإنترنت كجزء من الجسد الكامل للغة الترميز HTML، مما يؤدي إلى تفعيل نصوص الأوامر الخبيثة، وبعدها سرقة ملف تعريف الارتباط الخاص بالمستخدم.

هجوم التنصت

تحدث هذه الهجمة عبر اقتحام أو اعتراض حركة مرور أو نشاط الويب، وعند القيام بالاعتراض، يستطيع المعتدي أن يجمع ما يجده من معلومات تسبح في شبكة الويب، مثل كلمات السر أو تفاصيل بطاقة مالية رقمية وغيرها من المعلومات الأخرى السرية التي قام صاحبها بإرسالها إلى متلقي خاص عبر الشبكة.
يمكن القيام بالاعتراض عبر التنصت والمراقبة لرسائل الأوامر التي يتم تبادلها في الشبكة أو بإمكان المعتدي أن يزيف هويته على أنه طرف ودي ضمن عملية التبادل والإرسال.

هجوم البرمجيات الخبيثة أو المسيئة

هجمات البرامج الخبيثة هي ببساطة عملية حقن حاسوبك بأي برنامج خبيث لم توافق أو تعلم بعملية تنصيبه في جهازك، ويمكن للبرنامج الخبيث أن يدمج نفسه مع أوامر برمجية أو شبكية موثوقة، وهنالك أنواع عديدة من هذه البرامج، بعضها يُقحم نفسه في الأوامر البرمجية لملفات بصيغة exeويباشر عمله مباشرة فور الضغط عليه، وهنالك أنواع أخرى تعتبر فيروسات صغيرة تلتصق ببرامج مثل Microsoft Wordويتم تفعيلها عند تشغيل البرنامج وثم تستنخ نفسها في أماكن أخرى من النظام.

Thank You