مذكرة تخرج تقني سامي في أمن وحماية شبكات الحاسوب

إهـــــــــــــداء

أهدي هذا العمل المتواضع إلى اخي الذي لم يبخل علي يوماً بشيء وإلى أمي التي زودتني بالحنان والمحبة

الى امي الغاليه التي ليس لها مثيل بهذا العالم لله يطول عمرك و يبعد عنك كل سوء و شر... اللهم ارحمهما كما ربياني صغيرا

إلى أستاذي العزيز الفاضل ....: لقد رسمت في ذهني صورة عني لا تغيب ما حييت. رعاك الله في نفسك وأهلك أجمعين كما رعيت طلاب ابناء المسلمين

إلى وأبي إلى أهلي وعشيرتي إلى أساتذتي إلى زملائي وزميلاتي إلى كل من علمني حرفا

أهدي هذا البحث المتواضع راجياً من المولى عز وجل أن يجد القبول والنجاح

مقـــدمة

الحمد لله رب العالمين، وصلى الله وسلم على نبينا محمد وعلى آله وصحبه ومن تبعهم بإحسان إلى يوم الدين:

الحمد لله الذي لولاه ما جرى قلم, ولا تكلم لسان, والصلاة والسلام على سيدنا محمد (صلى الله عليه وسلم) كان أفصح الناس لسانا وأوضحهم بيانا ثم أما بعد:

إنه من دواعي سروري أن أتيحت لي هذه الفرصة العظيمة لأكتب في هذا الموضوع الهام ؛ الذي يشغل بالنا جميعا لما له من أثر كبير في حياة الفرد والمجتمع وهو موضوع (أمن وحماية شبكات الحاسوب)

مما لاشك فيه ؛ أن هذا الموضوع هو من الموضوعات الهامة في حياتنا ، ولذا سوف اكتب عنه في السطور القليلة القادمة متمنيا من الله أن ينال إعجابكم ؛ ويحوز على رضاكم ، وأبدأ ممسكا بالقلم مستعينا بالله لأكتب على صفحة فضية كلمات ذهبية تشع بنور المعرفة بأحرف لغتنا العربية لغة القرآن الكريم .

إن استخدام شبكات توصيل الحواسيب الألى أثبتت نجاحا باهرا في مجال أنظمة المعلومات الحديثة وخاصة في الشركات والبنوك والمستشفيات البلديات المتفرعة التي لها أكثر من فر ع.

حيث أدى استخدام الشبكات إلى توفير جهد كبير جدا كان يبذل في تداول المعلومات والبيانات بين أفراد منظومة أي نظام معلومات .

لقد صدق أحد العلماء يسمي ((ماكلوهان)) فقد قال ان العالم سوف يصبح قرية كونية. القد تدخلت لاختراعا ت ولابتكارات مثل :الكهرباء- الكمبيوتر- التليفون- القمر الصناعي- الألياف الضوئية – الكوابل...الخ ان التداخل الذي حدث هذه الأيام بين التطور السريع في الحواسيب الآلية والاتصالات يعد من المعالم الرئيسية والذى سيكون له أثر كبير على نمط الحياة في المستقبل الحاسبات والاتصالات بالسرعة الهائلة في تطويرها من ناحية ود خولها في العديد من مجا لات الحياة التي لم تكن متاحة من قبل.... واصبح لدينا عشرات الألاف من الأجهزة التي تحتوي على كم هائل من المعلومات. وكان نقل هذه المعلومات من حاسب الى اخر يتم من خلال الأشرطة الممغنطة وللفلاش ميموري .....وخير تطورت الاتصالات بين الحواسيب كوسيلة النقل المعلومات المخزنة من حاسب الى أخر ..فمنذ حوالى سنوات قليلة شهد العالم ثورة صغيرة عندما أصبح الكمبيوتر الشخصي جهازا شائع الاستخدام لدى الكثير في المنزل أو في المكتب ...الخ إذ أصبح وسيلة تساعدهم على اعداد الميزانية او معالجة الكلمات وكانوا سعداء بذلك .وفي خلال هذه السنوات قامت ثورة اخرى اهم من سابقتها هذه الثورة في قيام شبكات الحاسوب.

ان جهاز الحاسوب الشخصي شئ عظيم والكن يزداد عظمة عندما تحقق به اتصال من خلال شبكات الكمبيوتر بجهاز كمبيوتر اخر

تمهيد:

الشبكات NETWORKS

الشبكات بشكل عام هي وصل الحواسيب الموضوعة على مساحة محددة من أجل الاستخدام المشترك للمعلومات .الشبكات تقدم إمكانيات مذهلة في مجال تبادل المعطيات ومجال التعامل مع الملفات لعدد من المستثمرين بآن واحد معاً ، بالإضافة إلى بساطة المشاركة في **الملفات** – **FILES- فايلزس** - يمكن لمستثمري الشبكة أن يتشاركوا في **الطابعات PRINTERS** و**سواقات الأقراص الليزرية CD-ROM** و**المودم MODEM** وحتى **جهاز الفاكس FAX** .وعموماً يقصد بالشبكة التفاعل المتداخل بين أجهزة الكمبيوتر أي كيف تعمل الأجهزة فيما بينها ضمن شبكة اتصال لتحسين قدراتك في إنجاز الأمور . وشبكات الاتصال وضعت عموماً للمشاركة في أمور مثل معالجة النصوص وبرامج أوراق العمل وفي الطابعات وفي الربط على أجهزة كمبيوتر وشبكات واسعة وأنظمة البريد هي وظيفة شبكة الاتصال .

1) تعريف الشبكة :

هي عبارة عن مجموعة من أجهزة الحاسوب متصلة ببعضها البعض بغرض التواصل وتبادل المعطيات واستخدام الموارد

2) فوائد استعمال الشبكة :

- مشاركة المعطيات والمعلومات
- مشاركة التطبيقات والأقراص والأجهزة : توفر المشاركة في البرمجيات التي تم تثبيتها على الخادم

3) تصنيف الشبكات :

تصنف الشبكات حسب :

✔وسيلة الربط :

- الشبكات السلكية : هي شبكات تستخدم الأسلاك للإتصال ونقل المعلومات
- الشبكات اللاسلكية : هي شبكات تستخدم الربط اللاسلكي

- شبكات الحاسوب Computer Networks

تتكون شبكة الحاسوب في ابسط صورها من حاسوبين متصلين ببعضهما عن طريق قابلو توصيل Connection Cable ، تنتقل البيانات عن طريقه بين الجهازين بسهولة ويسر .
وفضلاً عن إمكانية تبادل المعلومات بين الأجهزة المتصلة بالشبكة يمكن لهذه الأجهزة المشاركة فيما بينها في الموارد Resources والملحقات Peripheral المتصلة بهذه الأجهزة . ويمكن تصنيف شبكات الحاسوب اعتماداً على المساحة التي تشغلها إلى ثلاثة أنواع

أنواع الشبكات :

✔ هنالك أربعة أنواع رئيسية من الشبكات الحاسوب :

تقسم الشبكات إلى عدة أنواع نسبة إلى المساحة الجغرافية التي تغطيها وهي كالآتي:

A. الشبكات المحلية (Local Area Network LAN) وهي الشبكات التي تضم مجموعة من الحواسيب التي تنتشر في مساحة جغرافية صغيرة مثل بناية أو عدد من البنايات ضمن مؤسسة كبيرة أو حرم جامعي.

B. الشبكات متوسطة المدى(Metropolitan Area Network MAN) وهذه الشبكة تغطي مساحة جغرافية

C. الشبكات واسعة النطاق (Wide Area Network WAN) وهذه الشبكات هي اكبر أنواع الشبكات في العالم ويمكن أن يصل مداها إلى تغطية الكرة الأرضية كلها (كما في الشبكة العنكبوتية الانترنت)

D. الشبكة الشخصية (PAN) : هي الشبكة التي تستعمل في البيت وتربط الأجهزة القريبة من بعضها

✔الشبكة العالمية (Internet):

الشبكة العالمية هي الانترنت حيث يتم الاتصال بها عبر أجهزة الستالايت (Satellite) و كابلات متحد المحور (Coaxial Cable) والانترنت هي (World Wide Web) أو (WWW) أو ما يسمى بالشبكة العنكبوتية وهي تتكون من خدمات معلوماتية واسعة تسمح للمستخدمين لتصفح المعلومات.

• **شبكة الانترنت :** وهو شبكة الشبكات التي تربط الحواسيب عبر العالم، صممت في أمريكا أساسا لأغراض عسكرية بحتة أيام الحرب الباردة فظهرت في ذلك الوقت شبكة Arpanet ونمت هذه الشبكة وأصبحت نظاماً متكاملاً بعد ذلك . وفي عام 1990 تخلت الحكومة الأمريكية عن الشبكة وأعطت حق الإدارة إلى مؤسسة العلوم الوطنية وفي عام 1991 تخلت المؤسسة عن الشبكة لصالح الشركات التجارية وبذلك فتح الباب أمام أضخم عمل وبناء صممه الإنسان إذ توسعت وانتشرت وضمنت في داخلها كل أنواع الشبكات 4 [WAN/LAN/MAN/ PAN].
يُدعى كل حاسوب مرتبط على شبكة الانترنت بالمضيف Host Computer . وهكذا فهنالك الملايين من هذه المضيفات المتنوعة والمرتبطة مع بعضها البعض . يملك كل مضيف عنواناً رقمياً Numeric IP Address وعنواناً اسمياً Domain Address .

✔تصنيفات الشبكات (Network Classifications) :

شبكة الزبون / الخادم (Client / Server):
يعرف هذا النوع من الشبكات بالشبكات ذات المخدم تستخدم أحد حواسيبها لحفظ المعطيات ذات الاستخدام الجماعي، وتلبية طلبات الخدمة الواردة من محطات العمل
أ – محاسن شبكات المخدم والزبون: .
* تؤمن سرعة كبيرة في معالجة المعطيات.
* تملك نظام حماية آمن للمعلومات وتؤمن السرية كذلك.
* سهولة في التحكم إذا ما قورنت بالشبكات المتكافئة.
ب - عيوب شبكات المخدم والزبون:
* تتطلب هذه الشبكات تخصيص حاسوب لاستخدامه كمخدم وبالتالي فإن هذه الشبكات تكون عادة أغلى سعراً.
* تتعلق سرعة أداء الشبكة ووثوقيتها بالمخدم المستخدم.
* هذه الشبكات أقل مرونة بالمقارنة مع الشبكات المتكافئة

•شبكة الند للند (Peer To Peer):

الشبكات المتكافئة هي الشبكات التي لا يكون فيها مركز واحد للتحكم بالعلاقة بين محطات العمل ، وليس فيها جهاز واحد لحفظ المعطيات ، يكون نظام التشغيل في هذه الشبكة موزع على كافة محطات العمل ، لذلك فإن كل محطة عمل تكون قادرة على تنفيذ مهام المخدم في تلبية الطلبات الواردة من محطات أخرى إضافة إلى وظائف المستخدم التي تمثله، أي ترسل طلبات إلى محطات عمل أخرى ، وهذا كله بآن واحد معاً ، كافة الأجهزة المتصلة بكافة محطات العمل من طابعات وأقراص صلبة وسواقات أقراص ليزرية وغيرها ، تكون متاحة بشكل كامل لكل مستثمر في الشبكة في حالة الحصول على إذن مدير الشبكة

أ. محاسن الشبكات المتكافئة:

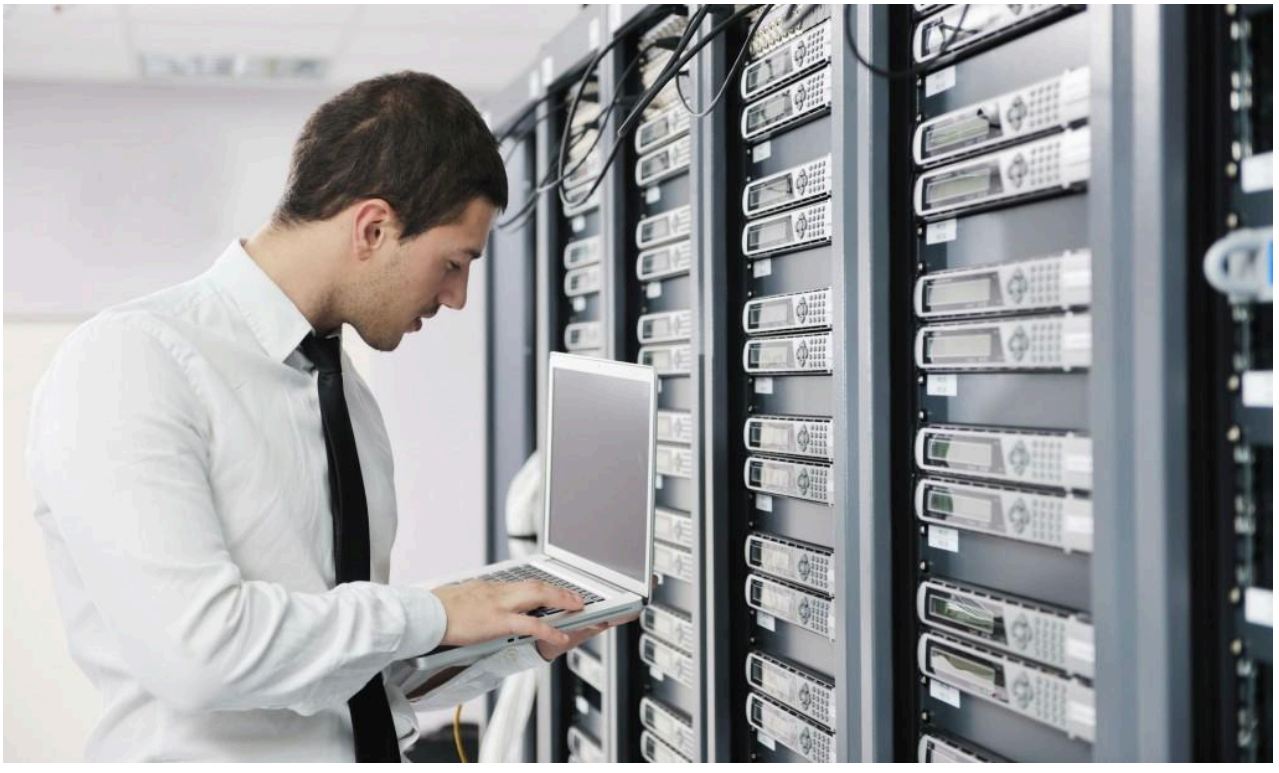
* كلفة هذه الشبكات قليلة ، إذ أنها تستخدم كافة الحواسيب المتصلة بالشبكة كمحطات عمل.
* وثوقيتها عالية ، إذ في حال تعطلت إحدى محطات العمل ، يتعذر الوصول إلى بعض المعطيات التي تحويها الشبكة وليس كلها.

ب. سلبيات الشبكات المتكافئة:

* الإرتباط الوثيق بين فعالية الشبكة وعدد المحطات التي تعمل بآن واحد في نفس اللحظة.
* صعوبة تنظيم التحكم الفعال بين المحطات

شبكات الحاسوب

مجموعة من ا الحواسيب التي تتوزع على مواقع مختلفة و تربط بينها وسائل الاتصالات المختلفة و تقوم بجمع و تبادل البيانات الرقمية و الاشتراك في المصادر المرتبطة بها .
و من هنا يتضح لنا أن شبكات الحاسوب تقوم بار سال البيانات الرقمية من أجهزة الحواسيب إلى وحداتها الطرفية و بين أجهزة الحاسوب بعضها البعض باستخدام وسائل الاتصال المختلفة كالأقمار الصناعية و الكوابل المحورية و الأسلاك الهاتفية.



● الإنترنت

لإنترنت بدأت فكرة الإنترنت في أوّل الستينيات في الولايات المتحدة الأمريكية؛ حيث كان الهدف منها المساعدة في الأعمال العسكريّة. يمكن تعريف الإنترنت بأنّه شبكة اتّصالات عالميّة يتم من خلالها تبادل المعلومات والرسائل.. الانترنت هو عالم أخر هو عالم جميل مليء بالمتعة والتسلية والمرح فبعضنا يستخدمه بحسن ويحسن استخدامه وبعضنا يستخدمه بسوء ويسيء استخدامه.الانترنت هو عبر الأقمار الصناعية تقوم ببحث ما يريده المستخدم وتظهر له النتائج كامله من جهه موثوق بها منذ بزوغ نجم الإنترنت وهي تستحوذ على اهتمام كثير من الناس لأسباب كثيرة ومتعددة.

✔طرق الاتصال بالإنترنت:

شهدَ هذا العصر الذي نعيش فيه ثورةً علميّة لم يشهد التاريخ مثلها، ويتميّز هذا العصر بالتكنولوجيا الهائلة التي انبثقت فيه بحيث إنّ البعض أخذَ ينعتهُ بعصر الجنون والخيال، وقد أعطى الله الإنسان قُدرات هائلة لا يستطيع الإنسان اكتشافها إلاّ إذا دعتهُ الحاجة لذلك، وتتنوّع هذهِ القُدرات بين القدرات الجسديّة والفكريّة، والتي بدورها تعتبر هيَ من قامت بإنتاج الحضارات واستخرج العلوم الكامنة وأبرزها للنور حيث الاكتشافات والاختراعات. ومن أبرز ما ظهَرَ في هذا العصر التكنولوجيّ المتسارع النموّ هوَ ظهور شبكات الاتصالات الحديثة التي تقوم على خدمة العالم عبر الحدود والقارات والمُحيطات بالربط السلكيّ واللاسلكيّ لخدمة التواصل بين الدول والجماعات الأفراد، فقديماً كانَ جهاز التلغراف الذي ابتكره موريس صاحب الشفرة الخاصّة هوَ الوسيلة الأضخم لتبادل المعلومات عبر العالم، واليوم نرى كيف انتشرت شبكات الاتصال السلكي والهواتف الأرضيّة وشبكات الهواتف المتنقّلة عبر خدمات الاتصالات اللاسلكيّة، وأبرز ما ظهَرَ من وسائل الاتصالات الحديثة هو ظُهور شبكة الإنترنت، التي تُقدّم خدمة المعلومات وتبادل البيانات والحصول على المعلومة بأقلّ وقت ممكن وبأعلى دقّة عبر المواقع الإلكترونيّة التي تُعدّ بالملايين والتي تقع ضمن شبكة الإنترنت التي نحن بصدد الحديث عنها. شبكة الإنترنت تقوم هذه الشبكة باحتضان مواقع إلكترونيّة توفّر بدورها وسائل الحصول على المعلومات والبيانات وكذلك القدرة على ربط الحواسيب والأجهزة الذكيّة من خلالها، وشبكة الإنترنت لها استخدامات علميّة وعمليّة وعسكريّة ولوجستية، وتخضع بعض مواقعها لرقابة الدول الكُبرى وخصوصاً في مواقع التواصل الاجتماعيّ التي توفّرها شبكة الإنترنت. طُرق الاتصال بالانترنت يكون الوصول إلى هذهِ الشبكة من خلال عدّة طُرُق ووسائل فهُناك الأجهزة المُستخدمة في الوصول لهذهِ الشبكة وهُناك وسائل الاتصال والربط التي من خلالها يتمّ الدخول إلى الشبكة، وأيّاً كانَ الأمر فشبكة الانترنت هي عبارة عن شبكة واسعة النطاق لها عناوين شبكيّة (IP Addresses) يكون من خلالها توفير

واحتضان المواقع الإلكترونيّة وكذلك الوصول إليها من خلال أجهزة الكمبيوتر أو أجهزة الهواتف الذكيّة المحمولة. وتكون قنوات الربط والاتصال بشبكة الإنترنت من خلال إمّا الخطوط الأرضيّة الثابتة التي توفّرها شركات الاتصالات الأرضيّة، ويكون الربط هذا ربطاً سلكيّاً وما يُسمّى بـ (ADSL)، وهو خطّ مُستأجر لاستخدامات شبكة الإنترنت من خلال شبكة الهواتف الأرضيّة. والطريقة الأخرى الأكثر انتشاراً هي الاتصال بالإنترنت من خلال الهواتف المتنقّلة أو من خلال التطبيقات اللاسلكيّة والتي بالعادة يتمّ توفيرها من خلال مزوّدي خدمات الإنترنت ومزوّدي شبكات الهاتف الخلويّ، حيث بإمكانك الاتصال بالإنترنت من خلال هاتفك أو من خلال جهاز الكمبيوتر وبوجود تغطية لاسلكيّة للموقع الذي تقطن فيه وبتكنولوجيات بثّ الاتصال كتكنولوجيا الجيل الثالث والرابع.

✔طريق اتصال بإنترنت

- يمكن الاتصال بالانترنت بطريقتين :

الأولى: التقنية السلكية
عن طريق الاتصال الهاتفي
عن طريق الاتصال المباشر

الثانية: عن طريق التقنية اللاسلكية
إما بإستعمال طريق تقنية الويفي
أوبإستعمال طريق تقنية الويماكس

✔وسائل الاتصال بالإنترنت:

هناك العديد من المتطلبات منها:

1 جهاز حاسوب و ملحقاته
2 خط هاتفي و مودم
3 مجهز أو مزود الخدمة
4 اسم الدخول
5 كلمة المرور

✔أشهر متصفحات بالإنترنت:

بعد أعوام من سيطرة متصفح اكسبلورر internet explorer على شبكة الإنترنت ,,
ظهرت الكثير من المتصفحات الاخرى .. ومعها ظهر التنافس القوي بينهم
البعض منها سرعان ما اجتذب العديد من المستخدمين إليه لكفاءته وسرعته وسهولة استخدامه و خلوه من الثغرات الأمنية ..ومميزات أخرى تكتشفها باستخدامك للمتصفح وبين أيديكم أفضل وأشهر المتصفحات ولكم الاختيار

✔وأشهر المتصفحات:

متصفح الفايرفوكس . Mozilla Firefox_ . متصفح جوجل كروم --Google Chrome
Browzar---متصفح أفانت Avant-- متصفح تورش torch

✔استخدامات الانترنت:

● المواقع الالكترونية:

الموقع الإلكتروني هو تلك المساحة الالكترونية المحجوزة ضمن خادم ما وتحت اسم نطاق معيّن في الشبكة العنكبوتية – الإنترنت .
ويمكن تقسيم المواقع الإلكترونية حسب أهدافها وغايتها كما يلي :
موقع شخصي يحتوي على معلومات تتعلق بالسيرة الذاتية.
موقع دعائي لبيع منتج معين.
موقع إخباري، حيث يقدم أحدث المستجدات مثل مواقع الصحف.
موقع معلوماتي، لتبادل المعلومات حول موضوع محدد أو هواية ...
موقع موجه (إقناعي أو دعوي)، أي يستخدم للدعاية السياسية التي تهدف إلى توجيهك لوجهة نظر معينة.
موقع تعليمي، لتدريس وحدة أو حلقة دراسية .
موقع خدماتي تسجيلي، للتسجيل في دورات، للحصول على معلومات أو منتجات . موقع للتسلية

● مواقع التواصل الاجتماعي

من أشهرها:
تويتر Twitter ، جوجل Google+ ، الفيسبوك face book

● محركات البحث:

محرك البحث هو برنامج يمكن المُستخدِمين من البحثَ عن كلمات محددة أو مواقع أو صور أو غيرها ضمن مصادر الإنترنت المختلفة، وينقسم محرك البحث إلى ثلاثة أجزاء رئيسة هي:
برنامج العنكبوت
برنامج المُفهرِس
برنامج محرك البحث.
ومن الأمثلة على محركات البحث:
غوغل google
ياهوyahoo
Ping

فيروسات الحاسوب:

تمهيد:

شبح الفيروسات مخيف جدا لكل من يعرف مقدار الضرر الذي قد يسببه . حيث لا يدرك الكثير من المستخدمين مقدار الخطر الذي تشكله الفيروسات إلا بعد أن يقوم احد الفيروسات بالتسبب في خسارة كبيرة وخصوصا في الشركات والمصارف والوقاية منها خير من قنطار علاج. و بالتأكيد إن هذا أمر لا نقاش فيه عندما يتعلق الأمر بالفيروسات. حيث أن ضياع احد الملفات التي تحتوي حسابات الشركة قد يكلفك الكثير من المال لإعادة إنشائه بينما قد تكلفك الوقاية من الفيروسات والاحتفاظ بنسخة احتياطية من المعلومات المهمة مبلغ من المال لا يكاد يذكر

✔الفيروس:

الفيروس يمكن تشبيهه بمرض معدي يصيب الإنسان ويحتاج للمضاد الحيوي للقضاء عليه وهذا المضاد الحيوي. هو عبارة عن برنامج أو جزء في الشفرة التي تدخل إلى الحاسب الآلي لهدف التخريب وتتميز بقدرتها على نسخ نفسها إلى نسخ كثيرة وقدرتها على الانتقال من مكان إلى مكان ومن حاسب إلى حاسب والاختفاء وتغطية محتوياتها. مكافحة الفيروسات المنتشرة ومن أشهرها افيرا و الكاسبر سكاي والنورتن .....الخ

وهذه فيروسات الكمبيوتر هي الأكثر شيوعاً من بين مشاكل أمن المعلومات التي يتعرض لها الأشخاص والشركات. وفيروس الكمبيوتر هو برنامج غير مرغوب فيه ويدخل إلى الجهاز دون

إذن ويقوم بإدخال نسخ من نفسه في برامج الكمبيوتر، والفيروس هو أحد البرامج الخبيثة أو المتطفلة. والبرامج المتطفلة الأخرى تسمى الديدان أو أحصنة طروادة أو برامج الدعاية أو برامج التجسس.
يمكن للبرامج الخبيثة أن تكون فقط للإزعاج من خلال التأثير على استخدامات الكمبيوتر وتبطيئه وتتسبب في حدوث انقطاعات وأعطال في أوقات منتظمة وتؤثر على البرامج والوثائق المختلفة التي قد يرغب المستخدم في الدخول إليها. أما البرامج الخبيثة الأكثر خطورة فيمكن أن تصبح مشكلة أمنية من خلال الحصول على معلوماتك الشخصية من رسائلك الإلكترونية والبيانات الأخرى المخزنة في جهازك.
أما بالنسبة لبرامج الدعاية وبرامج التجسس فهي مزعجة في الغالب وتؤدي إلى ظهور نوافذ دعائية منبثقة على الشاشة. كما أن برامج التجسس تجمع معلوماتك الشخصية وتقدمها إلى جهات أخرى تطلب الحصول عليها لأغراض تجارية.
يمكنك حماية كمبيوترك وحماية نفسك باستخدام برامج مناسبة لمكافحة البرامج الخبيثة غير المرغوب فيها والتي قد تكون نتائجها مدمرة للملفات والمستندات المهمة ،وبعضها. يتلف الكروت mother board.والأخطر انهيار نظام التشغيل بالكامل وعدم عمل الجهاز بالكامل. والتي تقوم بالحد من انتشار الفيروس في العادة معظم الفيروسات تأتي على شكل ملف تنفيذي exe منتقلة من جهاز إلى جهاز آخر ، فهذا الفيروس اللعين يربط نفسه ببرنامج تطبيقي في الأغلب وأحيانا كثيرة بالصور وملفات الفيديو المشبوهة وعند تحميلها على الجهاز، فهي لن تعمل إلا إذا قمت أنت بتشغيلها فأنت بذلك تعطيها الأمر لبداية عملها من حيث لا تعلم ويتفاوت ضرر كل فيروس عن الآخر حسب قوته وحجمه والغرض الذي أنشئ من اجله فبعضها يدمر الهاردوير وبعضها يدمر بعض المهام الرئيسية البسيطة في الجهاز

a) **خصائص الفيروس :**

1 القدرة على التخفي عن طريق الارتباط مع برامج أخرى ويبدأ العمل بمجرد تشغيل هذا البرنامج.

2 يتواجد في أماكن إستراتيجية كالذاكرة ويصيب أي ملف يوجد بالذاكرة

3 سرعة التكاثر والانتشار والانتقال بالعدوى

4 الفيروس يربط نفسه ببرنامج آخر يسمى الحاضن host

B) **أعراض الإصابة :**

1- تكرار رسائل الخطأ في أكثر من برنامج

2- ظهور رسالة تعذر الحفظ لعدم وجود مساحة كافية على الذاكرة أو القرص

3- تكرار اختفاء بعض الملفات التنفيذية

4- بطأ شديد في بدأ التشغيل (إقلاع الجهاز)

5- بطأ تنفيذ بعض التطبيقات وفي بعض الأحيان رفض بعض التطبيقات التنفيذ

6- تحويل الملفات إلى اختصارات لا تفتح ولا تنفذ

أولا : مما يتكون الفيروس

1- برنامج فرعي ليصيب البرامج التنفيذية ..

2- برنامج فرعي لبدء عمل الفيروس ..

3- برنامج فرعي لبدء التخريب ..

ثانياً: أنواعها :

1- يبدأ عمل الفيروس التخريبي إذا تحقق شرط معين كتاريخ - أو فتح برنامج أو انتقال من نظام إلى نظام.

2- يبدأ عمل الفيروس التخريبي بمجر التشغيل الحاسب وتعمل على نسخ نفسها لإعادة تشغيلها.

3- يبدأ عمل الفيروس التخريبي بمجرد الانتقال ولمرة واحدة .

الفيروس هنا مفهومة هنا هو عبارة عن أمر أو عدة أوامر يعطي معكوس أو انتشار على ماهو مفهوم به الفيروس الخاص بالفيروسات الحية نفس الشيء يفعله الفيروس بالنسبة للكمبيوتر أما أن يكون خبيث أو تجسس أو سارق أو مدمر الخبيثة هو الاسم الأكثر عمومية لأية برامج ضارة مصممة على سبيل المثال التسلل، تجسس على جهاز كمبيوتر أو تعريضه للتلف أو غيره من الأجهزة القابلة للبرمجة أو نظم معقدة، مثل نظام حاسوب المنزل أو المكتب والشبكات والهاتف المحمول والمساعد الشخصي الرقمي، الجهاز الآلي أو الروبوت.

: مصادر التهديد الأمني لمستخدمي شبكة الإ نترنت:

1- الفيروسات 7 Virus - مصادر متعلقة بالبريد الإلكتروني Email

2- ديدان الإنترنت Worms

3- التروجانات Trojans

4- الاختراق Hacking

5- التجسس على البريد الإلكتروني Spy

6- راصدي لوحة المفاتيح Keyloggers

ما هي مراحل العدوى

1- مرحلة الكمون : حيث يختبأ الفيروس في الجهاز لفترة ..

2- مرحلة الانتشار : و يبدأ الفيروس في نسخ نفسه و الانتشار في البرامج وإصابتها ووضع علامته فيها ..

3- مرحلة جذب الزناد: و هي مرحلة الانفجار في تاريخ معين أو يوم معين .. مثل فيروس تشرنوبيل ..

4- مرحلة الإضرار : و يتم فيها تخريب الجهاز ..

إذا الفيروس ينتقل هنا بواسطة فلاش أو انترنت من جهاز إلى جهاز آخر ويعمل بمجرد تشغيلها وأفضل بيئة لانتقال الفيروس هي البريد الالكتروني والمواقع الإباحية أو المشبوهة. هي البرامج التي تكون قادرة على تكرار هيكلها أو التأثير من خلال دمج نفسها أو إشارات إلى نفسها ،إلى الملفات أو الهياكل القائم عليها الحاسوب واختراقها. وعادة ما يكون لها أيضا حمولة خبيثة تهدف إلى تهديد أو تعديل إجراءات أو بيانات الجهاز المضيف أو النظام من دون موافقة. على سبيل المثال عن طريق حذف ،إفساد أو بإخفاء معلومات عن صاحبها.

كيفية عمل الفيروسات

✔ تعمل الفيروسات . بتاريخ أو وقت محدد

بعد تنفيذ أمر معين في البرنامج المصاب

بدأ النشاط بعد التكاثر و الوصول إلى رقم معين من النسخ.

و بعد ذلك يقوم الفيروس بعدة أنشطة تخريبية منها

عرض رسالة تحذيرية عن امتلاء الذاكرة

حذف أو تعديل بعض الملفات

تقوم بمسح كل المعلومات من القرص الصلب

تكرار ونسخ نفسه حتى يشل جهازك تماما

أنواع الفيروسات[1]:

==========

1: فيروسات قطاع التشغيل Boot Sector Virus

وهو الذي ينشط في منطقة نظام التشغيل وهو من اخطر أنواع الفيروسات حيث انه يمنعك من تشغيل الجهاز

2: فيروسات الماكرو Macro Virus

وهي من أكثر الفيروسات انتشارا حيث أنها تضرب برامج الأوفيس و كما أنها تكتب بالوورد او Notpad

3- فيروسات الملفات: File Virus

وهي تنتشر في الملفات وعند فتح أي ملف يزيد انتشارها ..

4- الفيروسات المخفية : Steath Virus

وهي التي تحاول آن تختبئ من البرامج المضادة للفيروسات و لكن سهل الإمساك بها

5- الفيروسات المتحولة أو فيروس متعدد الأشكال Polymorphic virus وهي الأصعب على برامج المقاومة حيث انه صعب الإمساك بها وتتغير من جهاز إلي آخر في أوامرها .. ولكن مكتوبة بمستوى غير تقني فيسهل إزالتها

6- فيروسات متعددة الملفات Multipartite Virus

تصيب ملفات قطاع التشغيل و سريعة الانتشار ..

7- فيروسات الدودة Worm

وهو عبارة عن برنامج ينسخ نفسه على الأجهزة و يأتي من خلال الشبكة و ينسخ نفسه بالجهاز عدة مرات حتى يبطئ الجهاز وهو مصمم لإبطاء الشبكات لا الأجهزة و بعض الناس تقول أن هذا النوع لا يعتبر فيروس حيث انه مصمم للإبطاء لا لإزالة الملفات و تخريبها ..

8- الباتشات Trojans:

وهو أيضا عبارة عن برنامج صغير قد يكون مدمج مع ملف آخر للتخفي عندما ينزله شخص و يفتحه يصيب ال Registry و يفتح عندك منافذ مما يجعل جهازك قابل للاختراق بسهولة و هو يعتبر من أذكى البرامج فمثلا عند عمل سكان scan هناك بعض التورجن يفكك نفسه على هيئة ملفات غير محددة فيمر عليها scan دون التعرف عليه ومن ثم يجمع نفسه مرة ثانية

أشهر الفيروسات التي انتشرت عن طريق الرسائل الإلكترونية:

✔1- Love You

✔2- Meet Melissa

✔3- Buble Boy

إحذر بماذا تربط جهازك:

فلاش اليو إس بي USB Flash Disk هي الطريقة الأكثر شيوعا التي ينتقل عبرها الفيروسات، بحيث أن أغلب الفيروسات خاصة فيروسات التجسس لها خاصية الانتقال، حيث أنها تنسخ نفسها تلقائيا في فلاشة الـ USB دون أن يدري المستخدم بذلك، فمثلا بمجرد ربط الفلاشة الخاصة بك بجهاز يحتوي على فيروس، هذا الفيروس سينسخ نفسه في الفلاشة لينتقل إلى جهاز آخر عند ربط هذه الفلاشة به. ينصح جدا بوقف التشغيل التلقائي أو ما يسمى بالـ Autorun من اليو إس بي.

1/انواع الفيروسات تأليف: الدكتور عبد الماجد الخليدي

أشهر الفيروسات

أشهر الفيروسات على الإطلاق هو شيرنوبل و مالسيا وفيروس الحبLove ..

متى يصيبنا هذا الفيروس ::

- عدم تحميل تحديثات الويندوز لتقفل ثغرات الويندوز و الإكسبلورر
- عدم تحديث برامج الانتي فيروس من وقت طويل
- الانتي فايروس الذي لديك ضعيف ولا يستطيع كشف مثل هذه الفايروسات
- الفايروس ذو إصدار جديد ولم يتم كشفه من قبل برامج الانتي فيروس
- عدم وجود بجهازك انتي فيروس

:: طريقة انتشاره ::

طريقه انتشاره ,, يقوم بإرسال نفسه إلى عناوين البريد الالكتروني

التي يحصل عليها بالبحث في صفحات الانترنت

التي تنتهي باللواحق التالية :

ASP, CFM, CSV, DOC, EML, HTML, PHP, TXT, WAB

ويصيب جميع أنظمة ويندوز ويستحدث ملفات بالأسماء التالية :

,csrss.exe, inetinfo.exe, lsass.exe

services.exe, WowTumpeh.com, eksplorasi.pif

أو عن طريق الفلاش ميموري او سي دي مصاب.

لأن معظم الفيروسات تغلق جميع امتدادات system.exe

:: ماهي إضرارها:

1- يتم إعادة التشغيل بمجرد تحميل ملف تنفيذي : برنامج مثلا

2- - تباطؤ أداء الكمبيوتر ، أو حدوث أخطاء غير معتادة عند تنفيذ البرنامج

3- يقوم بتعطيل الرجستري ,, أي لن تستطيع الدخول إلي الرجستري

4- يقوم بوضع صفحات ويب في مستنداتك وظهور رسائل أو تأثيرات غريبة على الشاشة

5- يقوم بنشر ونسخ نفسه بشكل سريع في مجلداتك تصل نسخه إلي الألف النسخ

6- بطء شديد في الجهاز

7- يقوم بإخفاء خيار - خيارات المجلد - من قائمة الأدوات

8- يقوم بنسخ نفسه على هيئة صورة مجلد ,, ولكن هو في الحقيقة ليس مجلدا وإنما هو تطبيق ولكن بصورة مجلد ,, وعند الدخول إلي المجلد هذا فانك تقوم بمساعدته على نسخ نفسه أكثر ..

9- زيادة في زمن قراءة القرص إذا كان محمياً وكذلك ظهور رسالة FATALI/O ERROR

10- ظهور مساحات صغيرة على القرص كمناطق سيئة لا تصلح للتخزين

استهلاك مساحة تخزين عالية

11- استغلال جزء كبير من ذاكرة الكمبيوتر

12- التعدي على حقوق الملكية الفكرية بالتعديل دون موافقة من مالكي البرامج أو الملفات

13- تجبر على تشغيل برمجيات مضاد الفيروسات مما يشكل عبئا على المستخدم

14- حذف، تعديل، أو تخريب الملفات والمجلدات

15 - مسح الذاكرة الصلبة

خطوات عمل الفيروس :

تختلف طريقة العدوى من فيروس لآخر و من نوع لآخر و هذا شرح مختصر لكيفية عمل الفيروسات : -

1- تحدث العدوى لبرنامج تنفيذي و لن تشعر بأي تغيير فيه

2- عندما يبدأ البرنامج المصاب بالعمل يبدأ نشاط الفيروس كما يلي : -

(أ)- ينفذ البرنامج الفعلي الخاص بالبحث , فيبحث الفيروس عن البرامج ذات الامتداد .exe أو .com أو .. و إن وجد أي منها يحضر جزء صغير من بداية البرنامج إلى الذاكرة و من ثم يبحث عن علامته فان وجدها ترك البرنامج و بحث عن غيره و إذا لم يجدها يضعها في أول البرنامج .

(ب)- بعد ذلك تكون حدثت العدوى فتحدث عملية التخريب التي تسبب الأخطاء عند عمل البرنامج المصاب .

3- بعد ذلك يعود التحكم للبرنامج مرة أخرى (بعد أن كان الفيروس يتحكم فيه) ليبدو أنه يعمل بصورة طبيعية .

4- بعد ذلك تكون عملية العدوى انتهت يتم التخلص من الفيروس الموجود في الملف التنفيذي الأول حيث أن الفيروس قد انتشر في البرامج الأخرى

لا يقوم الفيروس بإدخال نفسه في ملف صورة حيث أن ملفات الصور لا تحتوي على أوامر للمعالج كم أنها لا تحمل الصيغة التي يفرضها ويندوز من أنواع الملفات التي يمكن أن تحتوي فيروسات : exe, com, doc, dll, drv, fnt, vxd, scr,ocx, vbx, vbs, bat الفيروس لا يبدأ بالانتشار إذا لم يتم تشغيله. تذكر أن بعض الملفات يتم تشغيلها تلقائيا من قبل ويندوز كما هو الحال في التشغيل التلقائي أو إلى الملفات المستخدمة مع الأقراص المدمجة[1]

---

1 - الوقاية من الفيروسات تأليف: عادل الزبيدي

:: كيف نعرف بأن جهازنا مصاب بهذا الفيروس ::

هناك أربع طرق لمعرفه ما إذا كان بجهازك فيروس أو لا

✔ **الطريقة الأولى ::** قم بتحميل أي ملف ينتهى بـ exe على سبيل المثال أي برنامج مثلا :إذا قام الجهاز بإعادة التشغيل فتأكد أن جهازك مصاب بهذا الفيروس

✔:: الطريقة الثانية ::

أذهب إلي أي مجلد على سبيل المثال اذهب إلي جهاز الكمبيوتر ومن أعلى اختار - أدوات - ومن ثم انظر على القائمة المنسدلة هل يوجد بها خيارات المجلد أذا لم يكن موجود فأنت مصاب بهذا الفيروس

✔:: الطريقة الثالثة ::

أذهب إلي ابدأ ومن ثم تشغيل وأكتب regedit . أذا ظهر لديك رسالة خطأ فإذا أنت مصاب بالفيروس

✔:: الطريقة الرابعة ::

أذهب إلي ابدأ ومن ثم تشغيل وأكتب cmd إذا أعاد الجهاز التشغيل أذا أنت مصاب بالفيروس

● :: الأداة الأولى ::::::

أسم الأداة / انتي برونتوك -en:: الأداة الثانية :: أسم الأداة / F1-Brontok-Sx :: الأداة الثالثة :: أسم الأداة / remover

بعدما حذفنا الفيروس بواسطة هذه الأدوات ,, نقوم بإعادة التشغيل ,, ونذهب ونطبق الخطوات الأربع التي تم ذكرها بالأعلى ,, لتتأكد أن جهازك أصبح خاليا من هذا الفيروس

الرابط.

/http://www.zshare.net/download/58965344da9dcc3d

الأدوات صغيره الحجم وبإجمالي 500 k

و تقسم الفيروسات إلى قسمين:

فيروسات تقليدية Classic Virus و هي برامج هدفها تخريب النظام و إحداث أعطال و أخطاء فيه بشكل رئيسي
و هناك نوع جديد من الفيروسات يستخدم أسلوب الإحقان بالملفات حيث يضيف جزء من كوده البرمجي إلى الملف فيصيبه و يصبح جزء منه و بشكل عام تضع الفيروسات قيودا و تعديلات في الريجستري فمثلاً تمنع المستخدم من استخدام إدارة المهام و إظهار الملفات المخفية و ملفات النظام بطئ بسبب استهلاكها لموارد النظام و غيرها الكثير

✔تقسم الفيروسات إلى :

1) File Viruses و تتبع واحدا على الأقل من هذه الأساليب لإصابة النظام :
(أ) فيروسات منحقنة تصيب الملفات التنفيذية و في هذه الحالة عندما يكتشفه مضاد فيروسات يعطيك خيار التصحيح(Disinfect , Cure , Repair ,…etc) حيث يختلف حسب نوع مضاد الفيروسات الذي تستخدمه و من أشهر هذه الفيروسات فيروس سالتي الشهير Sality و فيروس Mabezat و للأسف أكثر الفيروسات من هذا النوع.

(ب) فيروسات تكرر الملفات الموجودة على الجهاز Duplicate Files حيث تمتلئ ذاكرة الجهاز بسبب تكرار الملفات (تخيل لديك ملفات و بيانات شركة و تملئ 75% من ذاكرة الجهاز فإذا بدء الفيروس بنسخ كل ملف مرة واحدة تكون النتيجة الجهاز لا يملك ذاكرة كافية) و لهذا تسمى هذه الفيروسات بفيروسات الشركات مثل فيروس Temp.exe.

(ت) و هذه الفيروسات تعمل نسخ عن نفسها في مسارات مشهورة بالجهاز

,%SystemRoot%, %Temp% , %userprofile%

%etc %systemdrive

(ث) فيروسات تستعمل ميزات ملفات النظام :
1) Boot sector viruses و هي فيروسات تصيب الملفات المسؤولة عن إقلاع الجهاز و النظام . فتضيف نفسها إلى ملفات الإقلاع و قد تغير مسار تلك الملفات . و لا تصيب إلا الأقراص المرنة .
هذه الفيروسات انتشرت في التسعينيات من القرن الماضي و لكن مع تقدم معالجات 32 بت و تناقص استخدام الأقراص المرنة تضاءل عددها مع أنه من الناحية التقنية يمكن إنشاء هكذا فيروسات تعتمد على ال Cd و على الفلاشات .
2) Macro viruses و هذه الفيروسات تصيب ملفات محررات النصوص مثلMS Word -MS Exel- Power Point
و هذا النوع من الفيروسات غير منتشر و نادر .
حيث بمجرد فتح مثل هذه الفيروسات تصاب الملفات الأخرى بهذا الجهاز .
مثال عليها أحد الفيروسات ما أن تفتحه بالجهاز حتى تمحى كل ملفات الأوفس التي تعمل بالجهاز حتى و لو كانت مخزنة .
3) Script Viruses و هي فيروسات تستخدم الأكواد للغات رمزية (جافا سكريبت , فيجوال بيسك سكريبت , ,Php, ملفات باتش ,...الخ)
و هي تصيب النظام و تؤدي إلى تحويل الأكواد إلى عمليات تخل بالنظام .

لأن معظم الفيروسات تغلق جميع امتدادات system.exe

مضادات الفيروسات:

هي البرامج التي تقوم بحماية الحاسوب من هجمات الفيروسات وبقية البرامج الخبيثة التي تشكل تهديدا على المعلومات والملفات ، وتستطيع أن تمنعها من الدخول ، كما تعمل على اكتشافها وإزالتها أو تعطيلها، تعتمد برامج مضادات الفيروسات على قاعدة بيانات تدعى تعريف الفيروس لتكتشف البرامج الخبيثة .ونذكرمنها :

Kaspersky ;Avast ;Avira ;AVG ;Symantec

هي برامج ذات أوامر معينة أحيانا تكون مضادة لجهات معينة مثل الحاسوب الشخصي، وأحيانا أخرى تكون عامة للداخل والخارج من الإنترنت مثل أجهزة الخوادم والاستضافات، وعادة ما توظف مجموعة متنوعة من الاستراتيجيات. تشتمل على الفحص المستند على الكشف عن نماذج معروفة من البرمجيات الخبيثة في كود قابل للتنفيذ. "exe" ومع ذلك، فمن الممكن للمستخدم أن يكون مصابا ببرمجيات خبيثة جديدة، كما يمكنها أيضا التعرف على الفيروسات الجديدة، أو مختلف أشكال الفيروسات الموجودة بالبحث عن أكواد البرمجيات الخبيثة المعروفة (أو تكون هناك اختلافات طفيفة في هذا الكود) وفي الملفات، بعض برامج الحماية من الفيروسات أو مضادات الفيروسات ويمكنها التنبؤ بما سوف يقع إذا فتح الملف بمحاكاته وتحليله

مكافحة التجسس:

هناك نوعان من التهديدات الرئيسية بالنسبة لبرامج التجسس : التجسس بجمع البيانات من الحاسوب إلى جانب طرف ثالث. دوري تلقائيا يشغل ويعرض، أو يحمل إعلانات. بعض أنواع دوري هي أيضا برامج التجسس والتي يمكن تصنيفها على النحو البرمجيات الخصوصية الغازية. دوري غالبا ما تكون متكاملة مع برامج أخرى.

أفضل طرق الحماية:

بالنسبة للدودة والتروجان يعتبر الافيرا بكامل تحديثاتها أقوى أداة في القضاء عليهما وبالنسبة للفيروس افاست و الكاسبر سكاي والنود بكامل تحديثاتها أقوى.. فهي تختلف من شخص لآخر ومن وجهه نظرالغالبية هذه ثلاث برامج ممتازة في هذا المجال بالإضافة لبرامج أزالة الباتشات وملفات التجسس

الوقاية من الإصابة بالفيروسات :

في الماضي، كان انتشار الفيروسات من كمبيوتر شخصي إلى آخر، يتم من خلال القرص المرن Floppy Disk أو غيره من وسائل الحفظ والاختزان، ولكن، مع انتشار الإنترنت، فان مخاطر انتقال الفيروسات أصبح أضعافا مضاعفة، فمن السهولة بمكان انتشار الفيروسات إلى آلاف الأجهزة بكبسة زر ومع أن احتمال انتقال الفيروسات عبر وسائط الاختزان المنقولة لا يزال قائما، إلا أن الشائع اليوم هو انتشار الفيروسات من خلال البريد الإلكتروني•

1. فالغالب اليوم، أن يشق الفيروس أو التروجان طريقه إلى كمبيوترك الشخصي من خلال مرفقات البريد الإلكتروني، وبمجرد أن تقوم بفتح الملف المرفق، فان الفيروس يخرج من قمقمه ليصيب جهازك، وربما لينسخ نفسه، ناقلا العدوى إلى جميع العناوين الإلكترونية الموجودة في كتاب العناوين Address Book[1]

2. المواجهة مع الفيروسات:

كل كمبيوتر معرض للإصابة بالفيروس هذه الأيام، وليس هناك كمبيوتر آمن مائة في المائة• فالفيروسات الجديدة منتشرة الآن على شبكة الإنترنت، بانتظار إيجاد ثغرات تنفد منها، لتدمر الأجهزة والبيانات التي فيها• أما الطريقة المثلى في الوقاية فهي تحميل برنامج مقاوم للفيروسات والقيام بتحديثه من حين إلى آخر، لتكون لديه المناعة الكافية بمواجهة الفيروسات الجديدة• كل ذلك لن يغنيك عن اتخاذ الحيطة والحذر[2]

1/الفيروسات ومخاطرها تأليف: المبرمج: محمد الداوود

2/ نفس المرجع

• كيف تتجنب الفيروسات:

المسح ضد الفيروسات Virus Scanning : تستطيع أن تقوم بعملية مسح فورية مجانية لكمبيوترك الشخصي ضد الفيروسات من الموقع التالي www.centralcommand.com/ اضغط على الوصلة Free Online Virus Scan لتنتقل إلى صفحة جديدة، حيث تقوم بإدخال البيانات الشخصية وبعدها تبدأ عملية الفحص الفوري لجهازك•

راقب امتدادات ملحقات Extensions الملفات المرفقة: تستطيع أن ترصد فيروسا داخل ملف مرفق، إذا دققت في اسم الملف• فإذا كان منتهيا بالامتداد •VBS فانه سيكون مثار شك وريبة، لأن هذا الاسم لن يكون لملف نصي بالهيئة وورد، وانما ملف فيجوال بيسك سكريبت الذي قد يحتوي على فيروس•

وقايـــة كتـــاب العنـاويـــن Address Book في أوت لو اكسبريس 6 تســتطيع أن توقــف الفيروســات، عن نســخ نفســها وإرســال هــذه النســخ إلى عناويــن البريد الالكترونيــة الموجـودة في كتاب العناوين، وذلك على النحو التالي، اختر Tools Options ثم اختر التبويبة Security وضــع علامــة الصــح في المربــع الصغــير بجانــب العبــارة Warn me when other applications try to send mail as me

تحذير لي عند محاولة التطبيقات --other لإرسال البريد مثلي

1- فحص جميع الأقراص الغريبة أو التي استخدمت في أجهزة أخرى قبل استعمالها

2- تهيئة جميع الأقراص اللينة المراد استخدامها على جهازك .

3- عدم تنفيذ أي برنامج مأخوذ من الشبكات العامة مثل إنترنت قبل فحصه .

4- عدم إقلاع الكمبيوتر من أي قرص لين قبل التأكد من خلوه من الفيروسات .

5- عدم ترك الأقراص اللينة في السواقة عند ما يكون الجهاز متوقفا عن العمل .

6- التأكد من خلو سواقة الأقراص اللينة قبل إعادة إقلاع الجهاز .

7- عدم تشغيل برامج الألعاب على الجهاز ذاته الذي يتضمن البيانات والبرامج الهامة

8- حماية الأقراص اللينة ضد الكتابة لمنع الفيروسات من الانتقال إليها .

9- استخدام برامج أصلية أو مرخصة .

10- استخدام كلمة سر لمنع الآخرين من العبث بالكمبيوتر في غيابك .

11- الاحتفاظ بنسخ احتياطية متعددة من جميع ملفاتك قبل تجريب البرامج الجديدة .

12- تجهيز الكمبيوتر ببرنامج مضاد للفيروسات واستخدامه بشكل دوري.

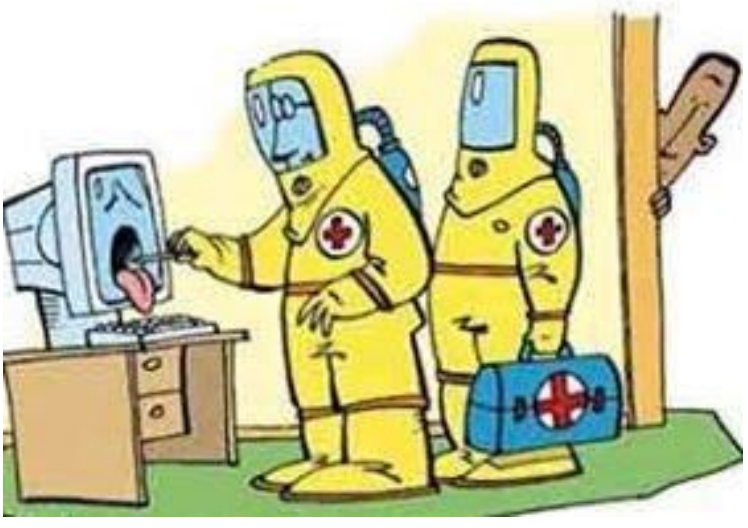
13- تحديث البرامج المضادة للفيروسات بشكل دائم لضمان كشف الفيروسات الجديدة.

14- الاحتفاظ بنسخة DOS نظيفة من الفيروسات ومحمية ضد الكتابة لاستخدامها عند الإصابة.

15- الانتباه للأقراص اللينة الواردة من المعاهد والكليات (الأماكن التقليدية للفيروسات).

16- إغلاق الجهاز نهائياً وإعادة تشغيله عند ظهور عبارة non bootable diskette .

خدمة فورية للقضاء على الفيروسات الخطيرة: إذا شككت بأن كمبيوترك أصيب بفيروس خطير مثل الفيروس نيمدا على سبيل المثال، فاذهب إلى الموقع التالي
www.centralcommand.com/jan1.html تجد قائمة بأخطر 12 فيروسا ودودة كمبيوترية، ومن الموقع تحصل على رزمات برمجية للقضاء عليها•



● الدودة و التروجان

✔الدودة:

ديدان الانترنت: قادرة على التكاثر والانتشار بسرعة كبيرة لتصيب الأجهزة

الدودة هي جزء فرعي من الفيروس وتختلف عنه بأنها أوسع انتشارا لأنها تنتقل من جهاز إلى آلاف الأجهزة بدون تدخل الإنسان ، في حاله الإصابة بالدودة فإنها تلقائيا تقوم بنسخ نفسها لآلاف المرات وبأشكال مختلفة وبالتالي تقوم بإرسال نفسها لبقية الأجهزة تلقائيا وأفضل طريقه لكشفها سريعا ظهور نافذة طلب الاتصال اتوماتيكيا بدون طلبك فهي تقوم بهذه العملية لنشر نفسها تلقائيا بواسطة طرق الاتصال المختلفة أنت فانتبه ففي هذه الحالة لديك دودة. وأضرار الدودة تكمن في زيادة في استخدام مصادر الجهاز فيحصل في الجهاز تعليق بسبب قله الرام المتوفر وأيضا تسبب الدودة في توقف عمل الخوادم فعلى سبيل المثال :- لو كان عندك دودة فستقوم الدودة بنسخ نفسها ثم إرسال لكل شخص من هم لديك في القائمة البريدية نسخة وإذا فتح احدهم هذه الرسالة ستنتقل إلى كل من لديه هو في قائمته البريدية وهذا يولد انتشاراً واسع جداً

✔أضرارها:

- تقوم بمسح أو تدمير المعلومات من البرامج التطبيقية كبرامج المحاسبة وقواعد المعلومات

- التكاثر حتى تملأ الذاكرة و تعطل الجهاز الضحية

- إعادة تشغيل الجهاز(البلاستر) / أشهر الديدان: البلاستر الذي احدث خسائر كبيرة عبر المنفذ 135

الحماية من هذا التهديد:

- استخدام برمجيات الحائط الناري

- تنزيل المضادات الخاصة بالدودة

✔التروجان:

التروجان مزعج جدا وليس ضارا كالفيروسات والدودة ولا يتكاثر مثل الدودة ولا يلحق نفسه ببرنامج مثل الفيروس ولا ينتشر أيضا سواء عن تدخل بشري أو لا، فهو ينتقل عبر زيارة احد المواقع المشبوهة وأحيانا يطلب منك تحميل برنامج معين.

وهنا الزائر قد ينخدع في ذلك فيعتقد انه برنامج وهو في الحقيقة تروجان .

أضرار التروجان تكمن في مسح بعض الأيقونات على سطح المكتب. مسح بعض ملفات النظام. مسح بعض بياناتك المهمة. تغير الصفحة الرئيسية للإنترنت إكسبلورر. عدم قدرتك على تصفح الانترنت.وأيضا التروجانات تقوم بوضع باكدور في جهازك من ما يسمح بنقل بياناتك الخاصة إلى الطرف الآخر بدون علمك، وهذا اخطر مافي الموضوع. تتجسس وتقوم بجمع المعلومات والبيانات و التعرف على كلمات العبور و تدمير الملفات ومن ثم ارسالها لمصدرها (المرسل) وهو عادة ما يكون فرد أو موقع أو منظمة لجمع المعلومات..

الحماية من هذا التهديد:

- تعطيل خاصية قبول و تشغيل البرامج في المتصفح مثل الجافا و الأكتف إكس و الجافا أبليتس
- استخدام برامج الحماية من الفيروسات
- استخدام جدران النار
- تجنب تنزيل البرامج المجانية مجهولة المصدر إلا بعد فحصها

● حصان طروادة

حصان طروادة (بالإنجليزية: Trojan Horse)، هي شفرة صغيرة يتم تحميلها مع برنامج رئيسي من البرامج ذات الشعبية العالية، ويقوم ببعض المهام الخفية، غالباً ما تتركز على إضعاف قوى الدفاع لدى الضحية أو اختراق جهازه وسرقة بياناته.

حصان طروادة (اسم) برنامج كمبيوتر يبدو أنه مفيد ولكنه في الحقيقة يسبب الأضرار. تنتشر أحصنة طروادة عندما ينخدع الأشخاص بفتحهم برنامجاً يعتقدون بأنه من مصدر شرعي. لحماية المستخدمين بشكل أفضل،.كما يمكن تضمين أحصنة طروادة في البرامج التي تقوم بتحميلها مجاناً. لا تقم أبداً بتحميل برنامج من مصدر لا تثق به. قم دائماً بتحميل التحديثات والتصحيحات التي توفرهاMicrosoft

هو نوع من البرمجيات الخبيثة التي لا تتناسخ من تلقاء نفسها والذي يظهر لكي يؤدي وظيفة مرغوب فيها ولكن بدلا من ذلك ينسخ حمولته الخبيثة. وفي كثير من الأحيان يعتمد على الأبواب الخلفية أو الثغرات الأمنية التي تتيح الوصول الغير المصرح به إلى الكمبيوتر أو الجهاز الهدف. وهذه الأبواب الخلفية تميل إلى أن تكون غير مرئية للمستخدمين العاديين.أحصنة طروادة لا تحاول حقن نفسها في ملفات أخرى مثل فيروسات الكمبيوتر. أحصنة طروادة قد تسرق المعلومات، أو تضر بأنظمة الكمبيوتر المضيف وقد تستخدم التنزيلات بواسطة المحركات أو عن طريق تثبيت الألعاب عبر الإنترنت أو التطبيقات القائمة على الإنترنت من أجل الوصول إلى أجهزة الكمبيوتر الهدف.والمصطلح مشتق من قصة حصان طروادة في الأساطير اليونانية لأن أحصنة طروادة تستخدم شكلا من أشكال "الهندسة الاجتماعية"، وتقوم بتقديم نفسها على أنها غير مؤذية، ومفيدة، من أجل إقناع الضحايا لتثبيتها على أجهزة الكمبيوتر الخاصة بهم.

.

.

سبب التسمية:

لتشابه عمله مع أسطورة حصان طروادة الخشبي الذي اختبأ به عدد من الجنود اليونانيون وكانوا سببا في فتح مدينة طروادة

ينبغي أن نفهم أن الحاسوب تقريبا يشبه المدينة في القصة فله حائط (جدار ناريfirewall/pare-feu) وله حاكم أو مستخدم هو أنت وله منافذ و أبواب (port) والحصان هنا يشير الى البرامج والاشياء التي تقوم بتحميلها من الانترنت وتدخلها إلى حاسوبك و الجيش الذي يختبئ في الحصان هو الفيروس.

مهمة فيروس حصان طروادة:

تجدر الإشارة إلى أن أحصنة طروادةtrojan horse كثيرة ومتنوعة وليست شكلا واحدا رغم اشتراكها في نفس الاسم. فبرامج الحمايةantivirus تستخدم هذا الاسم فقط لوصف كل فيروس له خاصية التجسس التي سنشرحها بعد قليل.

أحصنة طروادة Trojan تقسم إلى :

1) Backdoors و هي الأخطر لأنها تأخذ صلاحيات مدير نظام و تعمل بسرية تامة و من دون علم المستخدم . و تستخدم شبكة محلية أو الإنترنت للتحكم بجهاز الضحية و تتبع سلوك أدوات مدير النظام Remote Administrator Tool = RATو الفرق الوحيد بين التروجانات و برامج الإدارة هي أن التروجانات تنزل و تعمل بدون علم المستخدم بينما أدوات الإدارة تكون واضحة و تعطيك رسالة أنها تراقب النظام و هذا النوع يستخدم للتحكم بروتوكول TCP\IP و هو نفس البروتوكول المستخدم بالمسنجر و إدارة مقاهي الإنترنت و بعض البرامج و هذا النوع يتكون من جزأين الأول بجهاز الضحية يعمل بشكل خفي بحيث يتلقى الأوامر من المخترق و الثاني عند المخترق الذي بعث التروجان

- أشهرأنواعه:1

ومن أشهر فيروسات

(شرنوبل – منيك – منسي – الحب – دعوة حضور حفل زفاف)

{Chernobyl – bronco – x copy – Melisa – explore zip}

<u>خطورتها تكمن في :</u>
إرسال و إستقبال الملفات من و إلى جهاز الضحية
الدخول للملفات الخاصة و إمكانية حذفها و تعديلها
توجيه المستخدم إلى موقع إنترنت بدون إرادته و تغيير الصفحة الرئيسية أيضاً .
سرقة المعلومات الخاصة و كلمات السر
تشغيل البرامج و الأجهزة المرتبطة بالجهاز (طابعة أو كمرة ....الخ)
إعادة تشغيل الجهاز و إطفاءه
General Trojansأحصنة طروادة عامة و هذا النوع يخرب الجهاز و يسرق البيانات من جهاز الضحية و أغلب مبرمجين البرامج الخبيثة يضيفون خصائص كثيرة لهذا النوع
PSW Trojans و هو سارق كلمات السر حيث يقوم بفحص المواقع التي تحفظ بها كلمات السر و يأخذها ثم يرسلها للشخص الذي كونه . و بالعادة يسرق
معلومات عن النظام و الرقم التسلسلي لنظام التشغيل (بالدول الغربية نظام التشغيل غالي فسرقة الرقم التسلسلي مهم جداً)
بيانات الدخول للإنترنت (رقم البطاقة و كلمة المرور للإنترنت)
كلمات السر للألعاب على الشبكات (بعض الألعاب على الشبكة تكون بمقابل مادي)
كلمات السر للإيميل و المواقع

Trojan Clickers و هذا النوع يقوم بتوجيه الضحية لموقع معين بدون إرادته و الهدف منه هو إما زيادة العدد للزائرين لموقع معين أو إستنفاذ حجم التبادل الشهري لموقع أو الهجوم على موقع أو مخدم معين بواسطة DOS Attack أو أخذ الضحية لموقع معين حيث يكون هذا الموقع مصاباً فيتم تنزيل فيروس أو برنامج أخر بجهاز الضحية .
قد تقوم هذه البرامج أيضا من منع المستخدم من الدخول إلى مواقع معينة كمواقع شركات الحماية و التحديث فلا يستطيع المستخدم تحديث مضاد فيروساته .
Trojan Downloaders و هي برامج تتميز بصغر حجمها و وظيفتها تنزيل برامج أخرى (تروجانات أو فيروسات) إلى جهاز الضحية .
فمثلا دمج أحدهم برنامج مكرك مع تروجان كامل (100 كيلوبايت) سيلفت الانتباه فيلجأ إلى دمجه مع برنامج صغير لا يتعدى 5 كيلوبايت وظيفته عند الإتصال بالإنترنت تحميل الملف الكبير من الإنترنت و فتحه بجهاز الضحية
Trojan Droppers و هي برامج هدفها إخفاء البرامج الخبيثة عن أعين المستخدم أو عن مضاد الفيروسات
كل ملف بالجهاز له توقيع رقمي يختلف عن غيره و مضاد الفيروسات يحوي بداخله تواقيع الفيروسات و البرامج الخبيثة (التحديث هو عملية إضافة تواقيع البرامج الحديثة المكتشفة إلى أرشيف البرنامج) فيقوم هذا النوع من البرامج بتشفير الكود البرمجي للبرنامج الخبيث و تغير توقيعه الرقمي فيصبح ملفا غير مكتشف بالنسبة لمضاد الفيروسات و يمر من قبضته .

و تحوي هذه البرامج على خيارات لإيهام الضحية أن البرنامج الذي تم إخفاؤه ملف سليم عن طريق تشغيل تطبيق أخر أو إظهار رسالة خطأ توهم المستخدم أن الملف سليم
مثال : دمج فيروس مع صورة فعند الضغط على البرنامج المشفر يظهر للضحية صورة أو دمج فيروس مع برنامج مسروق فيضغط الضحية على ملف التنصيب و ينصب البرنامج بشكل طبيعي و لا يدري أنه ينصب و بشكل خفي في جهازه فيروساً
Trojan Proxies و هي برامج تستخدم لتحويل جهاز الضحية لبروكسي يمكن الذي أرسل التروجان إلى استخدامه للدخول للإنترنت بشكل متخفي .
و هذا النوع منتشر بكثرة بين الذين يستخدمون الرسائل المزعجة لكي يتمكنوا من الدخول لأعداد كبيرة من الأجهزة و بشكل متخفي لإرسال رسائل من أجهزة غيرهم .
Trojan Spies و هذا النوع يستخدم للتجسس على نشاطات الضحية (ليس فقط كلمات السر كما في PSW Trojans بل على نشاطات أخرى) مثل تصوير سطح المكتب أو صور من الكمرة أو أية نشاطات يقوم بها المستخدم
Trojan Notifiers و هي فقط لإعلام المخترق الذي أرسل التروجان بنجاح إصابة الجهاز بالبرنامج الخبيث حيث ترسل للمخترق معلومات عن الجهاز و IP و المنافذ المفتوحة .
كثير من Backdoors و PSW Trojans ترسل مثل هذه التنبيهات أيضاً .
Rootkits و هي برامج تقوم بإخفاء نشاطات التروجانات عن البرامج و لكن بطريقة لا تثير الريبة أبداً حيث تبقى مثلا إدارة المهام فعالة و لكن لا تظهر فيها أية نشاطات للتروجانات و لا تظهر بلوحة العمليات و تقوم بإخفاء نفسها بمفاتيح بالريجستري و قد تقوم أيضا بسرقة المعلومات الخاصة كسارق كلمات السر و تتميز هذه البرامج أنها تضيف نفسها كملفات نظام و تأخذ حقوق المدير .
ArcBombs و هي ملفات مؤرشفة صممت لتخريب الملفات المضغوطة حيث تتضاعف أحجامها تلقائيا ألوف المرات فتتخرب و يمتلئ الجهاز بملفات فارغة تسمى قنابل الهواء
خطورتها تكمن في إصابة خوادم الإنترنت و مخدمات البريد الإلكتروني .
هناك ثلاث أنواع لها الأول :
النوع الأول يملئ الملفات المضغوطة بمعلومات و بيانات مكررة
النوع الثاني يخرب الملفات المضغوطة
النوع الثالث يضغط الملفات بشكل صغير جدا فمثلا حجم 5 جيجا يصبح 200 كيلو بايت

* تتكون فيروسات من أربع اجراءت رئيسة :

1 – أليه تناسخ. 4 - أليه تنفيذ.

2 – إليه تخفي. 3– أليه تنشيط.

2- خصائص الفيروسات:

انتشار – 1
القدر علي تخفي – 2
القدر علي تدول – 3

-كيف يدخل حصان طروادة الى حاسوبك:

هذا الفيروس يمكن أن يدخل الى الحاسوب أثناء تصفحك لمواقع مصابة به أو تستهدف زوارها مثل مواقع الهكرز والاختراق الاجنبية خاصة إذا كنت لا تملك برنامج حماية أو كان غير مشغل أو أن معلوماته قديمة أي لم تقم ب (up date/mise a jour) كما يمكن أن يدخل جهازك حينما تقم بتحميل ملف أو برنامج أو لعبة مصابة بالفيروس

بعد دخول الفيروس الى الحاسوب يقوم بالاختباء أولا عن برامج الحماية بحيث يتجه الى ملف داخل ويندوز يسمى32 system كما يقوم بنسخ نفسه في كل الملفات الموجودة على حاسوب وهو ما سيضطرك إلى حذف كل الملفات المصابة أذا أردت التخلص من الفيروس.

و الأخطر من ذلك أنه يفتح نافذة أو بوابة في جدار الحماية في حاسوب بحيث يمكن المتجسس (صانع الفيروس) من الدخول إلى حاسوب من غير إذنك وطبعا معرفة كل ما يجري به بل والتحكم فيه كليا. ثم يرسل تقارير يومية إلى المتجسس ،وبذلك يخفض من سرعة الحاسوب والانترنت.مثل هذه الفيروسات يمكن أن تقضي تماماً على أقراص التخزين إضافةً إلى الكشف عن تفاصيل هامة للمستخدم كالأسماء وكلمات المرور لحساباته أو كلمات مرور البطاقات الائتمانية لأي شخص مجهول على الانترنت وبإمكانه أيضاً التأثير على نظام التشغيل ويعتبر ويندوز الأكثر تأثراً به نظراً لاستخدامه من قبل أعداد ضخمة من المستخدمين وضعف مقاومته لهذه الفيروسات

التخلص من الفيروس حصان طروادة:

لإزالة حصان طروادة، فإنه يجب أولاً العثور على الفيروس, ثم تثبيث برامج حماية حديثة النسخة وقوية مثل (avast/kaspersky/avira). ثم عمل سكان للجهاز ومن ثم حذف الفيروس فإذا لم تنفع هذه الطريقة فسيكون لزاما علينا عمل تهيئة كاملة للجهاز.

يعتبر فيروس Trojan horse أو ما يسمى حصان طروادة من أخطر الفيروسات وأكثرها انتشاراً على الحواسيب والأجهزة الذكية والذي يجب التخلص منه بأسرع وقت ممكن وإن لم يحصل ذلك يبدأ الفيروس بتعطيل الاتصال بالشبكة والأخطر من ذلك يسهل هذا الفيروس تعرض الحاسب أو جهازنا الذكي :التلفون" للقرصنة من قبل المخترقين أو الهاكرز وبالتالي يصبح بإمكانهم القيام تنفيذ الهجمات الالكترونية انطلاقاً من هذه الحواسيب . قبل أن نتعلم كيفية مواجهة هذا الفيروس الخطير أصدقائي يجب علينا أن نعرف ما هو حصان طروادة ؟
هو عبارة عن برنامج يعمل على كسر جدار الأمان وعلى الأغلب يكون متواجد في بعض الملفات التي يتم الحصول عليها من الانترنت كالملفات الموسيقية والصورية والروابط عندما يصل إلى أحد أقراص التخزين يبدأ بإطلاق العنان لإجرامه . مثل هذه الفيروسات يمكن أن تقضي تماماً على أقراص التخزين إضافةً إلى الكشف عن تفاصيل هامة للمستخدم كالأسماء وكلمات المرور لحساباته أو كلمات مرور البطاقات الائتمانية لأي شخص مجهول على الانترنت وبإمكانه أيضاً التأثير على

نظام التشغيل ويعتبر ويندوز الأكثر تأثراً به نظراً لاستخدامه من قبل أعداد ضخمة من المستخدمين وضعف مقاومته لهذه الفيروسات . هناك العديد من الطرق التي من الممكن إتباعها لنجنب أنفسنا أن نكون ضحية لمثل هذا النوع من الفيروسات ويعتبر أهمها الحذر من تحميل أو استخراج ملفات مهما كان نوعها من أي مصدر غير موثوق ولكن بالنسبة للمستخدمين الذين استطاع حصان طروادة الوصول إلى حواسيبهم او أجهزتهم الذكية يجب على الفور اتخاذ خطوات فورية لإزالته من محركات الأقراص قبل أن يبدأ بإحداث مشاكل يكون فيما بعد من الصعب حلها وبالتالي نحن بحاجة إلى إجراء عملية إصلاح للنظام ومن ثم إعادة تهيئته Reformat الأمر الذي قد يستغرق ساعات طويلة تختلف باختلاف النظام المستخدم . وفي بعض الحالات قد تكون الإزالة تمت بطريقة غير صحيحة مما يؤدي إلى عودة الفيروس مرة أخرى وعندها سنكون بحاجة لاستخدام خطوات أقوى لحل المشكلة كما يجدر التنبيه على أن أغلب برامج مكافحة الفيروسات تقوم بمكافحة التروجان والتعرف عليها ولكنها ليست بقوة وقدرة البرامج السابقة المتخصصة فيها. لذلك تحتاج إلى برنامج مكافحة التروجان بالإضافة إلى برنامج مكافحة الفيروسات.

✔-احتياطات يجب اتخاذها:

صحيح أنه لا توجد وسيلة حاسمة تستطيع الكشف عن جميع الفيروسات ولكن استخدام وسائل متعددة يشبه تماماً وضع عوائق متعددة أمام المهاجم .

-يستطيع مستخدمي الحاسب الشخصي اتخاذ بعض الإجراءات التي تحمي إلى حد كبير بياناته الهامة ومنها :

1-احتفظ بنسخ احتياطية من البرامج والبيانات مأخوذة على فترات متقاربة .

2-احتفظ بهذه النسخ وبأصول البرامج في مكان آمن بعيداً عن الحاسب الشخصي .

3-احتفظ بسرية كلمة المرور وقم بتغييرها من وقت لآخر .

4-أغلق الجهاز قبل أن تترك مكانك أمامه .5 لا تستخدم النسخ المقلدة أو المنسوخة من البرامج

6-قم بتركيب نسخه حديثه من أحد برامج مكافحة الفيروسات . 7-احتفظ لديك بالرقم المتسلسل للجهاز وللقرص الصلب .

8-لا تقم بتحميل أي بيانات شخصية دون التنسيق مع مسؤول أمن المعلومات .

9-عند حدوث مشكلة أو الشك بوجود فيروس اتصل فوراً بمسؤول مساندة المستفيدين وأخطره بما حدث وبما قمت به من إجراءات .

10-ضع شريط الحماية أو أغلق فتحة التأمين للأقراص المرئية بعد الانتهاء من استخدامها لمنع الكتابة عليها بشكل غير مقصود .

11-افحص البرامج الجديدة قبل استخدامها للتأكد من خلوها من الفيروسات .

12-تأكد عند شراء البرمجيات الجديدة من أن الصندوق لم يفتح من قبل .

13-عند إعادة استخدام أقراص مرنه قديمة قم بتهيئتها (Format) بدلاً من مجرد مسحها (Delete) .

● التدخلات الخارجية

✔الاختراق الأمني:

الاختراق بشكل عام هو القدرة على الوصول لهدف معين بطريقة غير مشروعة عن طريق ثغرات في نظام الحماية الخاص بالهدف... وحينما نتكلم عن الاختراق بشكل عام فنقصد بذلك قدرة المخترق على الدخول إلى جهاز شخص ما بغض النظر عن الأضرار التي قد يحدثها، فحينما يستطيع الدخول إلى جهاز آخر فهو مخترق (Hacker) أما عندما يقوم بحذف ملف أو تشغيل آخر أو جلب ثالث فهو مخرب (Cracker)

الهاكر: الهاكر هو الشخص الذي يقوم بإنشاء وتعديل البرمجيات والعتاد الحاسوبي. وقد أصبح هذا المصطلح ذا مغزى سلبي حيث صار يطلق على الشخص الذي يقوم باستغلال النظام من خلال الحصول على دخول غير مصرح به للأنظمة والقيام بعمليات غير مرغوب فيها وغير مشروعة. غير أن هذا المصطلح (هاكر) يمكن أن يطلق على الشخص الذي يستخدم مهاراته لتطوير برمجيات الكمبيوتر وإدارة أنظمة الكمبيوتر وما يتعلق بأمن الكمبيوتر

✔اللصوصية (Phishing) :

يستخدم مصطلح (Phishing) للتعبير عن سرقة الهوية، وهو عمل إجرامي، حيث يقوم شخص أو شركة بالتحايل والغش من خلال إرسال رسالة بريد إلكتروني مدعياً أنه من شركة نظامية ويطلب الحصول من مستلم الرسالة على المعلومات الشخصية مثل تفاصيل الحسابات البنكية وكلمات المرور وتفاصيل البطاقة الائتمانية. وتستخدم المعلومات للدخول إلى الحسابات البنكية عبر الإنترنت والدخول إلى مواقع الشركات التي تطلب البيانات الشخصية للدخول الى الموقع. هناك برامج لمكافحة اللصوصية Phishing والكشف عن هوية المرسل الحقيقي، وأفضل وسيلة لحماية الشخص من نشر معلوماته الشخصية لمن يطلبها هو أن يكون مؤسسة فعلية يطلبون من عملائهم إرسال معلوماتهم الشخصية عبر البريد الإلكتروني.

✔الاختراق[1]

الاختراق، شيء لم تسلم منه حتى الشركات الكبرى فما بالك بالمستخدمين العاديين. لقد أصبح شبكة الانترنت مكانا يعج بالفيروسات والبرامج الضارة والمتطفلين، حيث أصبح من الضروري على المستخدم حماية جهازه من أجل الحفاظ على خصوصيته وحماية حساباته البنكية الإلكترونية وكلمات السر الخاصة.

لقد تعددت وتطورت طرق ووسائل الاختراق بشكل كبير جدا خلال السنوات الأخيرة، حيث يمكن للمخترق أو الهاكر أن يخترق جهاز الضحية دون إرسال أي ملف أو موقع ملغوم، فكل ما يحتاجه المخترق لكي يخترقك هو عنوان الاي بي الخاص بجهازك، أو أن يكون في نفس شبكة الواي فاي wi fi التي أنت به

✔برامج التجسس

تثبت خلسة على الأجهزة للتجسس على المستخدمين أو للسيطرة جزئيا
الحاسوب الشخصي، فهي تهدف إلى التعرف على محتويات الحاسوب.
برامج التجسس يمكنها جمع مختلف المعلومات الشخصية، مثل تصفح
الانترنت ورصد المواقع التي تمت زيارتها. ويمكن لهذه البرامج أيضا أ
تسيطر على الحاسوب، وتتحكم فيه وتقوم بعدة مهام، مثل: إضافة برامج
.سرقة بيانات وأرقام حسابات، كلمة المرور أو ارقام بطاقات الائتمان

هو قيام شخص أو أكثر بمحاولة الوصول الى جهازك عن طريق شبكة الإنترنت وذلك باستخدام برامج متخصصة

✔طرق الاختراق

- باستخدام برامج الاختراق وذلك بإرسال باتش يقوم بفتح منفذ
- الإسكان
- الثغرات الجديدة
- ثغرات المتصفح

:الحماية من هذا التهديد

استخدام الجدران النارية -
تعطيل خاصية المشاركة في الملفات والطباعة
قفل المنافذ -

أسباب الاختراق ودوافعه[2]

لم تنتشر هذه الظاهرة لمجرد العبث وإن كان العبث وقضاء وقت الفراغ من أبرز العوامل التي ساهمت في تطورها وبروزها إلي عالم الوجود. وقد أجمع بعض المؤلفين

أن الدوافع الرئيسية للاختراق تتلخص في ثلاث نقاط أوجزت على النحو التالي :

1/الدافع السياسي والعسكري: مما لاشك فيه أن التطور العلمي والتقني أديا إلى

2/- الدافع التجاري: من المعروف أن الشركات التجارية الكبرى تعيش هي أيضا فيما بينها حربا مستعرة (الكوكا كولا والبيبسي كولا على سبيل المثال) وقد بينت الدراسات الحديثة أن عددا من كبريات الشركات التجارية يجرى عليها أكثرمن خمسين محاولة إختراق لشبكاتها كل يوم .

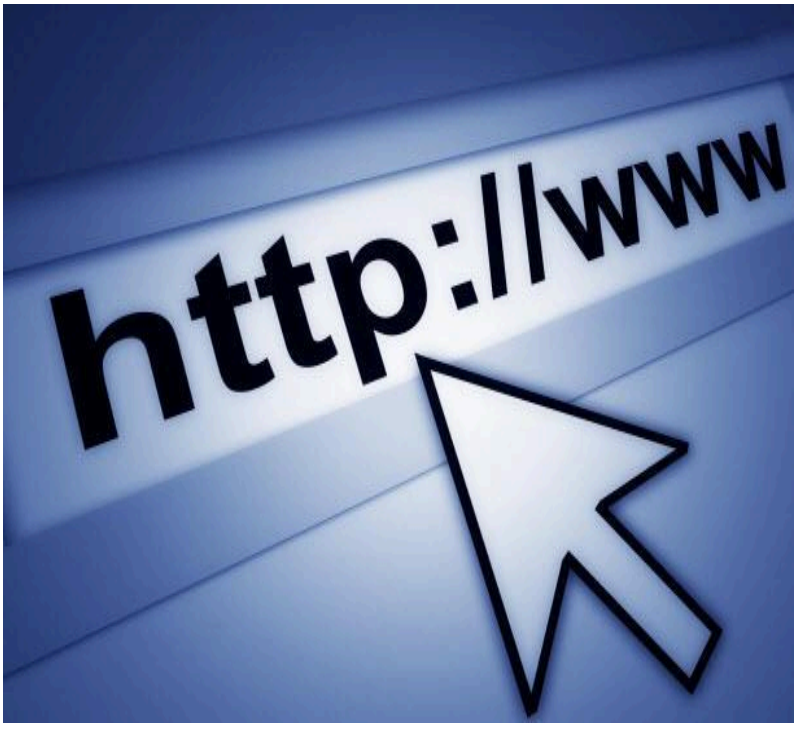
3/الدافع الفردي: بداءت أولى محاولات الاختراق الفردية بين طلاب الجامعات بالولايات المتحدة كنوع من التباهي بالنجاح في اختراق أجهزة شخصية لأصدقائهم ومعارفهم وما لبثت أن تحولت تلك الظاهرة إلي تحدي فيما بينهم في اختراق الأنظمة بالشركات ثم بمواقع الإنترنت. ولا يقتصر الدافع على الأفراد فقط بل توجد مجموعات ونقابات أشبه ما تكون بالأندية وليست بذات أهداف تجارية .بعض الأفراد بشركات كبرى بالولايات المتحدة ممن كانوا يعملون مبرمجين ومحللي نظم تم تسريحهم من أعمالهم للفائض الزائد بالعمالة فصبوا جم غضبهم على أنظمة شركاتهم السابقة مقتحمينها ومخربين لكل ما تقع أيديهم علية من معلومات حساسة بقصد الانتقام . وفي المقابل هناك هاكرز محترفين تم القبض عليهم بالولايات المتحدة وبعد التفاوض معهم تم تعيينهم بوكالة المخابرات الأمريكية السي أي اى وبمكتب التحقيقات الفيدرالي الأف بي أي وتركزت معظم مهماتهم في مطاردة الهاكرز وتحديد مواقعهم لإرشاد الشرطة إليهم .

✔ **سبل الحماية منهاً**: ومن أشهر وأفضل برامج الحماية من الهاكرز:

عليك بالحذر والحرص الدائمين لحماية نظامك كي لا يكون عرضة للهجمات بسبب نقاط الضعف فيه، ويمكنك تركيب برامج فعالة لجعل استخدام الإنترنت أكثر أماناً لك.

تجنب المواقع الغريبة والمواقع المشبوهة.

ابتعد عن المواقع الإباحية لأنها مليئة بالفيروسات وملفات التجسس، كما عليك الابتعاد عن المواقع الغريبة والمواقع التي تحمل عناوين ويب طويلة وغير مفهومة.



ما يقوله جوجل صحيح .....فإذا قمت بعمل بحث على موقع ووجدت جوجل يحذرك من هذا الموقع لا تدخل على هذا الموقع لأنه قد يضر بجهازك.....فقد يحتوى على برمجيات خبيثة وسوف تنزل على جهازك من دون أن تشعر وسوف تكون بذلك ضحية لأى هاكر

1/ لحماية الجهاز الكمبيوتر من الهجماة داخلي و الخارجي تأليف: محمود غيث بوحروره

2/ نفس المرجع

احذر من رسائل البريد الإلكتروني الغير المعروفة:

انتبه واحذر إذا كنت تتلقى رسائل البريد الإلكتروني من الناس بشكل عشوائي. إذا كان لديك أي شكوك في الرسالة فلا تقم أبدا بفتح أي ملف مرفق بها، كما عليك الحذر من الرسائل المزورة التي تطلب منك معلومات خاصة كرقم البطاقة البنكية وغيرها، طرق الإحتيال الإلكترونية متنوعة جدا، هنالك رسائل تصلك على أنها من أحد البنوك التي لديك حساب بها وتطلب منك إعادة إدخال المعلومات أو تدعي أنك حسابك سيغلق في حال لم تدخل معلوماتك من جديد... والخدعة تكون في الرابط الذي بالرسالة، حيث أنك إذا دخلت على الرابط فستدخل إلى موقع مزور شبيه جدا بالأصلي يقوم بتسجيل وسرقة كافة المعلومات التي ستدخلها، لهذا يجب الإنتباه جدا إلى نطاق الموقع.

- **مصادر متعلقة بالبريد الالكتروني:**

أولا : الملفات المرفقة التي تحتاج لفتح ..الحذر الشديد عند فتح الملفات الملحقة بالرسائل الإلكترونية و لذلك ننصحك بعدم فتح الملفات المرفقة اذا كانت من احد الأنواع التي سنذكرها في السطور التالية خاصة اذا لم تكن من شخص معروف لديك و هذه الملفات الملحقة الخطيرة تنتهي بأحد هذه الاختصارات :

(EXE.)

Executable Files الملفات القابلة للتنفيذ

و هذا يعني وجود ملف تنفيذي و هي خطيرة جدا لأنها تنفذ الأمر المطلوب منها دون أذن منك

(COM.)

Command Files القيادة الملفات وهذا يعني وجود ملف به أوامر للتنفيذ مرتبطة بأي جزء من الملف و تبدأ بالعمل بعد مرور وقت معين أو حين الضغط على جزء معين

(BAT.)

Batch Files

و هذا يعني وجود أمر معين موجه لأحد ملفات نظام التشغيل في جهازك

(APP.)

Application

وهذا يعني وجود ملف به برنامج تطبيقي و هي خطيرة لأنها ممكن أن تكون أحد برامج التجسس

ثانيا : الملفات المرفقة ذاتية التشغيل:

و هي قادرة على أن تقوم بالعمل حال فتحك لبرنامج البريد الإلكتروني

و دون الحاجة لفتح المرفقات و تقوم بإعادة تحميل نظام التشغيل لديك ومن ثم العمل في الخفاء

وتقوم بإضافة نفسها في كل رسالة ترسلها دون علمك لتصيب بها بقية الأصدقاء

W--SS--.kak

و من أهم الأمثلة على ذلك

SON OF BUBBLEBOY

و الطريقة الوحيدة لحماية نفسك من مثل هذه النوع هو الغاء وحجب خاصية من متصفحك وهي

Allow --SS--ing

✔الحماية من هذا التهديد:

-استخدام برنامج مضاد للفيروسات

وضع كلمات العبور في جهازك لتقييد استخدام أي شخص أخر لجهازك

ايضا قم دائما بتنظيف بريدك من الرسائل القديمة والغير مهمة .

❖ الخطوات الرئيسية لتأمين الشبكات من الاختراق والثغرات الأمنية

نقرأ يومياً عن أنشطة الهاكرز وعن الاختراقات والثغرات وحملات التجسس الإلكترونية في جميع أنحاء العالم سواء كانت الحكومية أو الخاصة لدرجة تجعلك تشعر أن هذا العالم سينفجر في أي لحظة! ومثل هذه الأمور تجعل المسئولين في قسم تكنولوجيا المعلومات في أي مكان يضعوا في حساباتهم إضافة عمليات إستباقية كفحص الشبكات بشكل دوري ومستمر للتأكد من عدم وجود أي مخاطر أو تهديدات تواجههم وتتكون عملية الفحص الرئيسية من خمس نقاط أساسية وتكون كالتالي :-

✔التعامل مع كلمات المرور الافتراضية

فعلاً شيء غريب عدم تعامل المديرين مع كلمات المرور الإفتراضية ففي الكثير من الأحيان نرى إختراقات لشركات كبرى سببها غير تغير كلمة المرور الإفتراضية على جهاز ما وهذا يجعل المخترقين يصلوا بسهولة إلى بعض مناطق غير مصرح بها.

✔فحص الخدمات التى تعمل على أنظمة التشغيل

مشكلة موجودة مع أنظمة تشغيل شركة مايكروسوفت بالتحديد وهى وجود بعض الـ service التى تعمل بشكل إفتراضي على الرغم من عدم إحتياج المستخدم لها والتى من الممكن أن تسبب الكثير من المشاكل الأمنية لأحقاً.

✔التحكم في الـ Remote access

لن أتحدث في هذه النقطة عن بروتوكولات Telnet, SSH, RDP فقط بل حتى البرامج التى تعمل بنفس الطريقة وتستخدم بروتوكولات أخرى مثل GoToMyPC, LogMeIn, PCAnywhere, TeamViewer, WebEx, Splashtop Remote, Screenconnect, RealVNC, Mikogo, Ericom Blaze, AetherPal Bomgar وغيرها من البرامج التي توفر إمكانية

الوصول عن بعد, لكن مثل هذه البرامج لأبد من إغلاقها وحظر البروتكولات التي تستخدمها وذلك في محاولة لتقليل من المخاطر التي تتعرض لها الشبكة.

البورتات:

فحص البورتات هي أحد العمليات التي نقوم بها لتحديد الأنظمة التي تعمل في الشبكة في محاولة لاكتشاف إذا ما كان هناك الفايرول مفعل أم لا وهل حاسوب مستهدف من قبل أحدهم؟ وبالطبع هناك الكثير من الأدوات والبرامج المتخصصة في هذا النوع من الفحص مثل ,NMap Foundstone Vision, Portscan 2000, incloak, Superscan, Angry IP Scanner, Unicornscan وهناك أيضاً مواقع مثل ,zebulon, confickerworkinggroup .t1shopper, ShieldsUp

✔: إغلاق المنافذ:

يأتي نظام الويندوز وبه خدمات اتصالات عديدة والكثير منها غير مستخدم..

وعادة يكون من الأفضل إيقاف بعضها إن لم يكن جميعها .. علم جميعا أن وراء كل منفذ مفتوح يوجد برنامج معين يقوم بالاتصال عن طريقه تماما مثل تردد موجات الراديو كل محطة تستخدم تردد معين ولكي نغلق المنفذ لابد من إيقاف البرنامج أو الخدمة التي تستخدمه.والقصد بذلك المستخدم العادي الذي لا يرتبط نظامه بأنظمة أخرى كما في الشركات وغيره. نعلم جميعا أن وراء كل منفذ مفتوح يوجد برنامج معين يقوم بالاتصال عن طريقه تماما مثل تردد موجات الراديو كل محطة تستخدم تردد معين ولكي نغلق المنفذ لابد من إيقاف البرنامج أو الخدمة التي تستخدمه

✔تقييم مدى تأثير نقاط الضعف

هناك الكثير من الأدوات التى تستخدم في فحص نقاط الضعف المتواجدة في قواعد البيانات (مثلاً) وحتى مع الأنظمة والبرامج المختلفة وذلك للتحقق من أي شيء يمكن أن تشكل خطراً على الشبكة لكن لأبد أن يكون المسئول عن الشبكة على دراية تامة بأخر التحديثات والتطورات التقنية لأن من

الممكن أن تكون قواعد البيانات أو الأنظمة الموجودة في شركته مؤمنه وتكون الثغرات من بعض البرامج مثل الجافا أو المتصفحات أو حتى من الفلاش وهكذا.

هناك نقطة فارقة ليس لها علاقة بعمليات التأمين ولكن بالمسئولين وهى الوعى الأمنى فعندما يكون المسئول على دراية بالطرق التي من الممكن أن يهاجم من الهاكرز وبالتحديد الطرق البدائية والمشهورة فذلك سيساعده كثيراً على تأمين الشبكة المسئول عنها وتفادى الوقوع أى مشاكل لاحقاً, الجدير بالذكر أن كل نقطة من هذه النقاط مؤلف عليها كتب ونشر عنها تقارير عديدة لذلك لا يجب الإستهانة بها.

● ارقام المنافذ:

1- إذهب إلى قائمة أبدا start ثم تشغيل أختر run

2- ثم فى Run اكتب Cmd

3- ثم اكتب هذا الأمر netstat –a ولاحظ المسافة بين حرف (T) وعلامة (-)

4- ثم اضغط (Enter)

5- سيتم عرض جميع المنافذ المفتوحة في جهازك والتي تكون بعد الرمز (:) مباشرة أما ما قبل الرمز فهو اسم الكمبيوتر الخاص بك الذي تم تعريفه عند تجهيز شبكة الاتصال

6- والآن قارن أرقام المنافذ التي تظهر لك مع أرقام المنافذ التالية وهي المنافذ التي يفتحها في العادة ملف (الباتش) التي ببرامج التجسس أو التخريب ...

فأن وجدت رقم من ضمن أرقام المنافذ فان جهازك قد اخترق من قبل هاكر وعليك في هذا الحالة التخلص أولا من ملف التجسس ثم بعد ذلك عليك بإغلاق المنافذ المفتوحة ....

وان لم تجد رقم من هذه الأرقام في تقرير الدوس فان جهازك في أمان ولم يتم اختراقه

10034 -1045 – 4590 – 6711- 7300 – 7301 - 7306 - 7303 - 7308 -30029 – 30100 - 30101 - 30102 – 31337 – 30338 – 31339 – 31666 – 54320- 54321 - 6711- 6776 - 1234 – 1999 – 0 - 43002 - 5401 - 0954 - 1176 - 0037- 1037 - 6037 - 3037 - 8037 - 92003 - 00103 - 10103 - 20103 - 73313 – 83313 – 93313

الطريقة الأولى:-

هذه الطريقة تستطيع اغلاق جميع البورتات (الثغرات الأمنية) الموجودة بكل الأجهزة:

1- اذهب إلى قائمة أبدا start ثم تشغيل run

2- ثم اكتب الأمر التالي command.com

3- ستظهر لك نافذة اكتب فيها هذه الكلمة ping host ثم أضغط Enter

4- ثم أكتب ping port ثم أضغط Enter

5- ثم انتظر و أكتب ping port1027 ثم أضغط Enter

6- و انتظر ثم اكتب ping port80 ثم أضغط Enter

7- ثم اكتب ping أو proxy ping أو ping ***** ثم أضغط Enter

8- ثم اكتب ping port و أضغط Enter

* انتظر لفترة تقريباً من 15الى20دقيقة وإذا لم تختفي النافذة قم بإغلاقها واعد تشغيل الجهاز.

- لإخفاء جهازك من الشبكة بدون برنامج :

1- اذهب إلى قائمة أبدا start ثم تشغيل run

2- فى Run اكتب Cmdسوف تظهر شاشة سوداء

3- اكتب هذا الأمر net Config Server /hidden:yes

4- ثم انتظر نصف ساعة و ستجد ان جهازك قد اختفى من الشبكة مع العلم أن ذلك لا يؤثر

على الـ Share أو إذا كنت تستخدم برنامج مثل الـ Pcany Where أو Net Support

6- و للتراجع عن هذا الأمر اكتب في الشاشة السوداء Net Config Server /hidden:no

7- ثم انتظر نصف ساعة واعمل Restart للجهاز وسوف يظهر الجهاز كما كان

ملحوظا وهذا الأمر تم تجربته على نسخة Xp /sp2

وتم تجربته أيضا على شبكة بنظام Domain و على شبكة بنظام WorKGruop وتم بنجاح

أهمية هذه الحركة:

عندما تقوم بإخفاء جهازك عن الشبكة المحلية أو حتى العالمية سيكون من سابع المستحيلات أن يتم اختراق جهازك إلا من أفضل مخترقين العالم ربما فهذه الحركة مهمة لكل واحد يشبك على الإنترنت أو حتى على شبكة محلية أو أي شبكة

الطريقة الثانية :

- لإغلاق ثغرات الوندوز إكس بي ~ ويندوز Xp ~ فقط :-

1- أذهب إلى قائمة أبدا start ثم تشغيل run

2- في Run اكتب Cmd

3- ثم أكتب netstat -ano لترى المنافذ المفتوحة

في حوالي 17 منفذ مفتوح وفي حالة استماع listen

4- قم بنسخ الأوامر التالية وألصقها في الدوس

```
sc config messenger start= disabled
sc config w32time start= disabled
sc config netbt start= disabled
sc config policyagent start= disabled
sc config policyagent start= disabled
sc config ssdpsrv start= disabled
exit
```

إيقاف خاصية مشاركة الملفات :

1- أذهب إلى قائمة أبدا start ثم settings ثم control panal

2- ثم أدخل network connections

الجانب التطبيقي

3- أضغط click right ثم properties

4- أحذف علامة صح من أمام أختيار

file and printer sharing for Microsoft networks

5- ثم أضغط ok

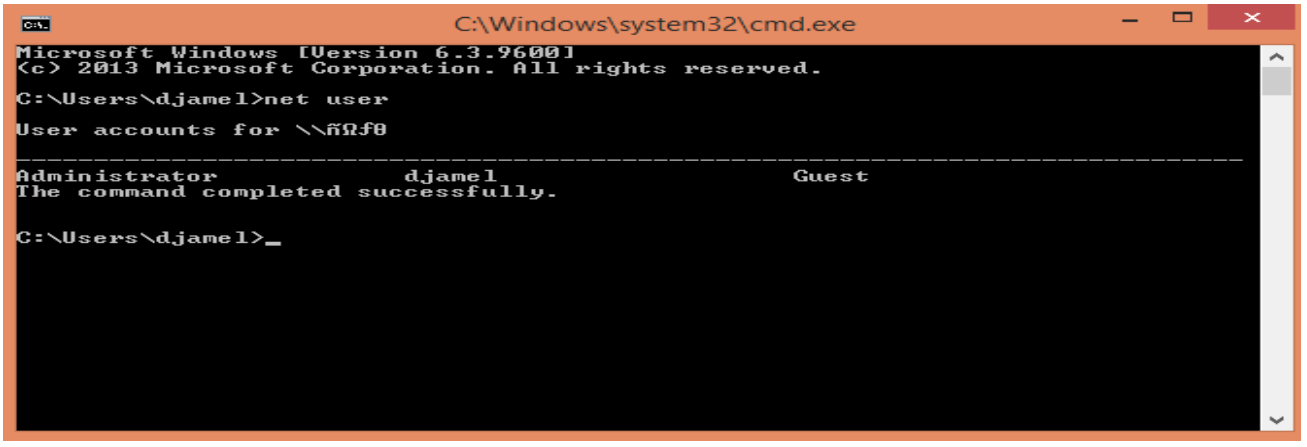
- لإغلاق جميع البورتات والمنافذ المفتوحة بجهازك لحمايتك من الاختراق من قبل الهاكرز :-

1- أذهب إلى قائمة أبدا start ثم تشغيل run

2- في Run اكتب ftp –rc

- و بهذا تكون قد أغلقت جميع البورتات المفتوحة بجهازك

اقوى جاسوس من الاستخبارات الأمريكية في جهازك احذفه : يعني لايوجد



:- للتخلص منه قم بالأتى -

1- إذهب إلى قائمة أبدا start ثم تشغيل run

2- فى Run اكتب Cmd

3- ثم أكتب net user

:- إذا كانت النتيجة كالتالي موجود فى نظام تشغيلك server أذنSupport_388945a0

:- ثم قم بكتابة الأمر التالى مع مراعاة الفواصل

net user SUPPORT_388945a0 /delete

ثم أكتب الأمر Exit

و للتأكد من الحذف قم بأعادة الخطوات الأولى ستجد أنه تم حذف

الجانب التطبيقي

كيف تعرف ان جهازك مخترق مهم جدا :-

الطريقة الأولى

نفتح قائمة أبدأ 

ثم نختار Run 

ثم نكتب الامر التالى system.ini ثم نضغط ok

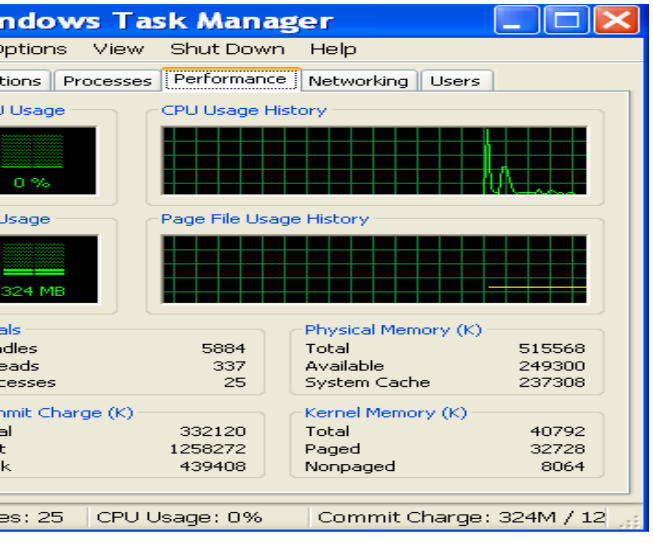
بعد ذلك سوف تظهر لنا مفكرة note pad بها بعض الأوامر كما بالصورة

INCLUDEPICTURE "http://s002.radikal.ru/i198/1005/73/3f71202e74d0.jpg" * MERGEFORMATINET

INCLUDEPICTURE "http://i065.radikal.ru/1005/09/b229ff60f9dc.jpg" * MERGEFORMATINET

اذا ظهر لك رقم 850 كما هو محدد بالصورة فان جهازك سليم 100 % وغير معرض للاختراق
اما اذا ظهر لك الرمز woa فهذا يعنى ان جهازك مخترق وبه ملفات تجسس وسهل جدا أن يتم اختراقه في أي وقت ويفضل أن تقوم بمحو الملفات الخاصة بأسرع وقت حتى لا يتم نقلها أو نقوم بعمل باسورد

الطريقة الثالثة



(Alt + ctrl + Delete) .. عند الضغط على الأزرار
سوف تفتح معك نافذة إدارة المهام: اذا وجدت الرسم البياني المشابة لمخطط القلب بالاعلى ..
مرتفع ويمشي بخط مستقيم .. أعرف ان جهازك مهكر , ولتقم بعمل الفورمات فورااااا .

ما هي أهم الاحتياطات التي يجب اتخاذها للحماية من الهاكرز ؟

أ- استخدم أحدث برامج الحماية من الهاكرز والفيروسات وقم بعمل مسح دوري وشامل على جهازك في فترات متقاربة خصوصاً إذا كنت ممكن يستخدمون الإنترنت بشكل يومي

ب- لا تدخل إلى المواقع المشبوهة مثل المواقع التي تعلم التجسس والمواقع التي تحارب الحكومات أو المواقع الاباحية وكذلك صفحات الخبيث indexالتي تحوي أفلاماً وصوراً خليعة لأن الهاكرز يستخدمون أمثال هذه المواقع في إدخال ملفات التجسس إلى الضحايا حيث يتم تنصيب ملف التجسس (الباتش) تلقائياً في الجهاز بمجرد دخول الشخص إلى الموقع !!

ج- عدم فتح أي رسالة إلكترونية من مصدر مجهول لأن الهاكرز يستخدمون رسائل البريد الإلكتروني لإرسال ملفات التجسس إلى الضحايا .

ح- عدم استقبال أية ملفات أثناء (الشات) من أشخاص غير موثوق بهم وخاصة إذا كانت هذه الملفات تحمل امتداد وتكون أمثال هذه الملفات (ahmed.pif.jpg) أو أن تكون ملفات من ذوي الامتدادين مثل (love.exe) مثل (exe) عبارة عن برامج تزرع ملفات التجسس في جهازك فيستطيع الهاكرز بواسطتها من الدخول على جهازك وتسبب الأذى

والمشاكل لك ..

خ- عدم الاحتفاظ بأية معلومات شخصية في داخل جهازك كالرسائل الخاصة أو الصور الفوتوغرافية أو الملفات المهمة وغيرها من معلومات بنكية مثل أرقام الحسابات أو البطاقات الائتمانية ..

ذ- قم بوضع أرقام سرية على ملفاتك المهمة حيث لا يستطيع فتحها سوى من يعرف الرقم السري فقط وهو أنت .

د- حاول قدر الإمكان أن يكون لك عدد معين من الأصدقاء عبر الإنترنت وتوخي فيهم الصدق والأمانة والأخلاق .

ر- حاول دائماً تغيير كلمة السر بصورة دورية فهي قابلة للاختراق .

ت- تأكد من رفع سلك التوصيل بالإنترنت بعد الانتهاء من استخدام الإنترنت .

ث - لا تقم بإستلام أي ملف وتحميله على القرص الصلب في جهازك الشخصي إن لم تكن متأكدا من مصدره .

chat

تجنب التعامل مع برامج المحادثة الأتيه وايضا يفضل حذفها من الجهاز واذكر منها :-

ICQ ---------- yahoo ---------- ------ skyp

العاب الكمبيوتر

يجب الحرص أيضا من التعامل من العاب الكمبيوتر خاصة التي تحتاج إلى تشات من الموقع أو التي تكون تحت عناوين مشبوهة مثل وألعاب اليانصيب للحظ السعيد وغيرها من الألعاب
- --- الحذر عند إقفال النوافذ المنبثقة: النوافذ المنبثقة هي النوافذ التي تقفز على شاشة الكمبيوتر لديك عند ذهابك إلى مواقع إلكترونية محددة. وبعض المواقع الإلكترونية تحاول خداعك لتنزيل برامج تجسس أو برامج دعاية في جهازك من خلال الضغط على موافق (OK) أو اقبل (Accept) الموجودة في النافذة المنبثقة. وعليك إتباع وسيلة آمنة لإقفال هذه النوافذ آلا وهي الإقفال من مربع العنوان (X) الموجود في أعلى النافذة.

فكر ملياً قبل تنزيل ملفات من الإنترنت:

يمكن كذلك أن تُصاب بفيروسات وبرامج دعاية وبرامج تجسس من خلال تنزيل برامج وملفات أخرى من الإنترنت. فإذا كان البرنامج مجانياً ومزود من قبل مطور برمجيات مجهول، فهو من المرجح أن يحتوي على برمجيات إضافية وغير مرغوب فيها أكثر مما لو كانت قد تمت بتنزيل أو شراء برنامج من مطور برمجيات مشهور ومرموق.

ولحسن الحظ، فإن نظام الترشيح المعمول به في المملكة العربية السعودية، يحمي مستخدمي الإنترنت من الدخول مصادفة إلى معظم المواقع الإلكترونية الخطيرة، ولكن من الحكمة والتعقل توخي الحذر عند تنزيل ملفات من الإنترنت أو إقفال النوافذ المنبثقة غير المرغوب فيها.

برامج مراقبة بيانات الشبكة Packet Sniffers:

طريقة فعالة لمراقبة الحركة المرورية عبر الشبكة باستخدام أحد برامج مراقبة بيانات الشبكة، حيث يتم من خلاله تجميع البيانات الداخلة والخارجة، وهي طريقة ممكن أن تكون مفيدة في الكشف عن محاولات التسلل عبر الشبكة، وكذلك يمكن استخدامها لتحليل مشاكل الشبكة وتصفية وحجب المحتوى المشكوك فيه من الدخول إلى الشبكة. جهاز الكمبيوتر لديك إذا كنت تعتقد أن لديك فيروساً، لأنه يمكن للفيروس الانتشار إلى تلك الأقراص.

● كيف تحمي جهازك من الاختراق بدون برامج :-

عندما تكتشف أن جهازك مخترق الأفضل أن تقوم بعمل فورمات للجهاز لأن أحياناً ملفات الباتش تجدد نفسها حتى لو حذفتها أما إذا لم تستطع أو لا تريد عمل الفورمات

فعليك أتباع الأتى:-

قم بحذف ملف الباتش الذى يساعد على الأختراق بواسطة ملف تسجيل النظام Registry

و ذلك بأتباع الطريقة الأتية :-

1- من قائمة Start نختار 2 Run- ثم نكتب في خانة التشغيل Run الأمر 3 regedit- ثم نفتح المجلدات التالية حسب الترتيب في قائمة Register Editor :

HKEY_LOCAL_MACHINE

Software- Microsoft- Windows- Current Version- Run- Run once

-والآن من نافذة تسجيل النظام Registry Editor انظر إلي يمين النافذة بالشاشة المقسومة ستشاهد تحت قائمة Names أسماء الملفات التي تعمل مع قائمة بدء التشغيل ويقابلها في قائمة Data عناوين الملفات .

-لاحظ الملفات جيدا فإن وجدت ملف لايقابلة عنوان بالـ Data أو قد ظهر أمامه سهم صغير ---> فهو ملف تجسس إذ ليس له عنوان معين بالويندوز

و إذا لم تجده تحقق من الملفات إذا وجدت أسم غريب أبحث عنه فى جوجل سوف يعطيك معلومات عن الملف إن كان ضار أم لا .

- فإذا وجدت ملف إختراق تخلص منه بالضغط على الزر الأيمن للفارة ثم Delete

** لو وجدت أحدى العناوين الأتية الموجودة فى Date أحذفها :-

NET POWER

C:\WINDOWS\NET POWER.EXE /nomsg

Explorer32

C:\WINDOWS\Expl32.exe

ole C:\WINDOWS\SYSTEM.ljsgz.exe

حماية شبكات الحاسبات اللاسلكية WiFi في الدوائر والمؤسسات الحكومية

الجانب التطبي

على قاعة المؤتمرات الفيديوية في مركز البحث والتأهيل المعلوماتي، اقيمت ورشة

العمل الخاصة بحماية شبكات الحاسبات اللاسلكية WiFi في الدوائر والمؤسسات وقد بين المحاضر المدرس المساعد مغرب عبد الرضا مكي من قسم الشبكات في المركز ان الشبكة اللاسلكية تعتبر من أكثر وسائط ربط الشبكات والاتصالات في الوقت الراهن ولا تكاد تخلو شبكة من استخدام هذه الوسائط سواء في الاستخدام المنزلي أو في للعمل, وقد وضح المحاضر أن أساس

عمل البيئة اللاسلكي هو وجود خوارزميات تشفير كلمات المرور المعتمدة حالياً والتي تكون عرضة للكسر من قبل المخترق وهي (WEP, WAP و WAP2) اخطر هذه الخوارزميات وأكثرها عرضة للكسر هي خوارزمية WEP وهي مختصر لـ Wired Equivalent Privacy التي المكتشفة سنة 1999 وهي معتمدة إلى الآن. كما وضح المحاضر أنواع مفاتيح التشفير للخوارزميات المختلفة منها المفتاح المشارك بين الطرفين (Shared Key) المستخدم في خوارزميات التشفير التناظري (Symmetric encryption) وطريقة المفتاح الخاص والعام (Private and Shared Key) المستخدم في تبادل المعلومات في الخوارزميات غير المتناظرة (Asymmetric encryption). تستخدم عدة تطبيقات لغرض كسر خوارزميات التشفير معتمدة على أكثر من طريقة بعضها متقدم لا يمكن استخدامه إلا من قبل المختصين في مجال الاختراق المتقدم والأخرى سهلة وبدائية يمكن لأي شخص لديه معلومات بسيطة عن الشبكات اللاسلكية استخدام تطبيقات معدة لاختراق هذه الشبكات، ويجب الحذر من هكذا برامج لسهولة استخدامها وكثرة العابثين بها لاختراق الشبكات اللاسلكية. أكد المحاضر ان ليس من الضرورة ان يكون هدف المخترق الحصول على خدمة الانترنت في الشبكة، بل قد تحتوي شبكة مؤسسة ما على معلومات حساسة مخزنة في سيرفرات خاصة يمكن للمخترق الاطلاع عليها وانتهاك خصوصية هذه المؤسسة ومعلوماتها. للحماية من هكذا اختراقات يجب المراقبة الدائمة على مستخدمي الشبكة ومعرف امكان اتصالهم وعمل كلمات مرور اكثر امناً باختيار رموز (مثل !@#$%&) وحروف كبيرة وصغيرة (BbAa) في تشفير كلمات المرور واختيار خوارزميات لتشفير كلمات المرور مثل WAP2 مع العلم ان هذه الخوارزمية يمكن اختراقها لكن بصعوبة نسبية, والحرص على تغيير كلمات المرور بشكل دوري لكي لا تنتشر كلمة المرور بين مستخدمين غير مصرح لدخولهم للشبكة او استخدام طريقة البروكسي (Proxy) في التصريح للمستخدمين او ربط المستخدمين المصرح لهم عن طريق MAC address. وقد حضر الورشة مجموعة من المهتمين بهذا الخصوص من الكليات ومراكز الحاسبة فيها.[1]

لتحمي أمن الاتصال الشبكي اللاسلكي:

قم بتغيير اسم مسؤول الشبكة؛

قم بتفعيل خدمة التشفير WAP أو WEP؛

أطفئ بث معرّف الخدمة وقم بتغيير الاسم الافتراضي لموجه الشبكة اللاسلكي الخاص بك؛
اتبع النصائح المذكورة حول كيفية الحماية من البرامج الخبيثة وهجمات المخترقين.

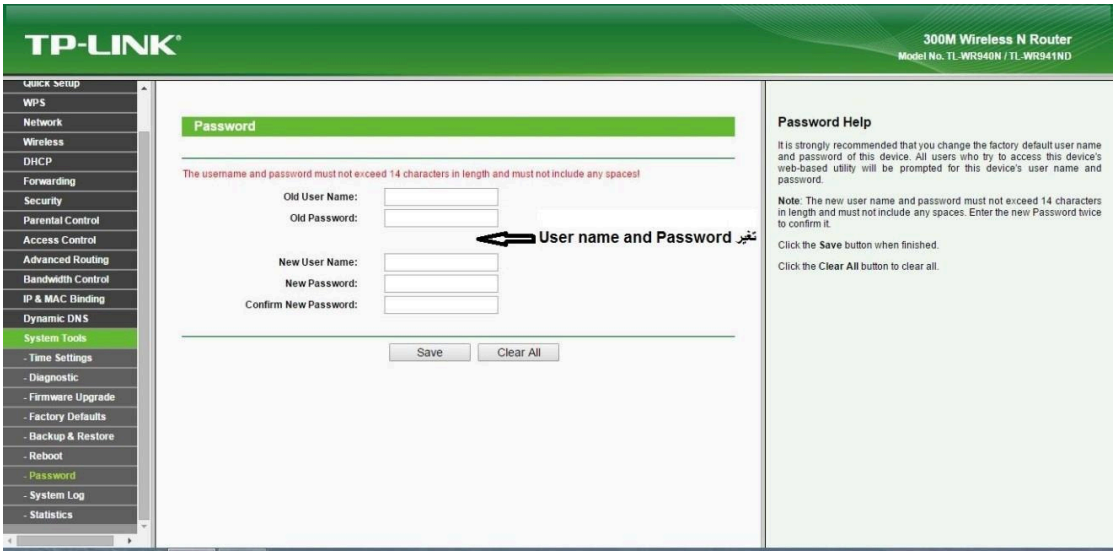
هناك بعض الخطوات التي بإمكانك اتخاذها لحماية الاتصال الشبكي اللاسلكي وموجه الشبكة بهدف تقليل المخاطر:

قم بتغيير كلمة سر لمسؤول الشبكة الخاص بموّجه الشبكة اللاسلكية. من السهل على المخترق أن يكتشف كلمة السر الافتراضية الخاصة بالمصنّع وأن يحصل على إمكانية الولوج إلى الاتصال الشبكي اللاسلكي الخاص بك. تجنب استخدام كلمة السر التي يمكن اكتشافها بسهولة: اتبع الإرشادات الموجودة في القسم التالي/ اختيار كلمة السر .

قم بتعطيل بث معرّف الخدمة (Service Set Identifier) لتمنع جهاز الاتصال الشبكي اللاسلكي من التعريف بوجوده.

قم بتفعيل خدمة التشفير في إعدادات الاتصال الخاصة بك: تشفير WPA هو الأفضل (في حال لم يدعمه جهازك استخدم تشفير WEP).

قم بتغيير اسم الدخول الخاص بمعرف الخدمة في حاسبك الآلي. من السهل على المخترق أن يكتشف الاسم الافتراضي الخاص بالمصنع وأن يستخدم هذه البيانات ليحدد مكان الاتصال الشبكي اللاسلكي الخاص بك. تجنب استخدام كلمة السر التي يسهل اكتشافها بسهولة: اتبع الإرشادات الموجودة في القسم التالي: اختيار كلمة السر '



1/الشبكة اللاسلكية تأليف مغربي عبد الرضا م

الجانب التطبيق

أمن شبكات المعلومات :

Information Networks Security

لقد أوضحنا فيما سبق الأهمية الكبيرة لشبكات المعلومات وما تقدمه من خدمات كبيرة على كافة المستويات، ومن تلك الأهمية تنبع أهمية أن يكون هناك مستوى معين من الأمان في هذه الشبكات حماية للمستخدمين والمعلومات التي تحتويها، فقد انتشرت في السنوات الأخيرة العديد من المشاكل

والجرائم التي تتعلق بأمن المعلومات واختراق العديد من شبكات المعلومات على مستوى العالم، بل وصل الأمر إلى اختراق أعلى الشبكات سرية في العالم مثل شبكة المخابرات الأمريكية CIAوغيرها من الشبكات، ولنا أن نتصور ما يمكن أن يمثله ذلك من تهديد للدول في عصر أصبحت فيها الحرب هي حرب المعلومات وليس حرب الأسلحة كما كان سابقاً....

ويمكننا تعريف "أمن شبكات المعلومات" على أنه مجموعة من الإجراءات التي يمكن خلالها توفير الحماية القصوى للمعلومات والبيانات في الشبكات من كافة المخاطر التي تتهددها، وذلك من خلال توفير الأدوات والوسائل اللازم توفيرها لحماية المعلومات من المخاطر الداخلية أو الخارجية...

حماية شبكات المعلومات Network Protection

"الوقاية خير من العلاج" .. فيما سبق تم استعراض أهم المخاطر التي تواجه شبكات المعلومات وتحول دون حماية المعلومات في داخلها، ورأينا أنها تنقسم إلى عدة أقسام منها ما يمكن التحكم فيه ومنها ما يحدث دون تدخل من الإنسان، والسؤال الآن الذي يمكن طرحه هو هل يمكن تفادي هذه المخاطر والأضرار؟ وما هي الوسائل التي يمكن عن طريقها تجنب حدوث مثل هذه المشاكل والاختراقات في شبكات المعلومات التي تخصنا؟ وهذا ما سنناقشه في الفقرات التالية.

جراء فحص للنظام بشكل منتظم:

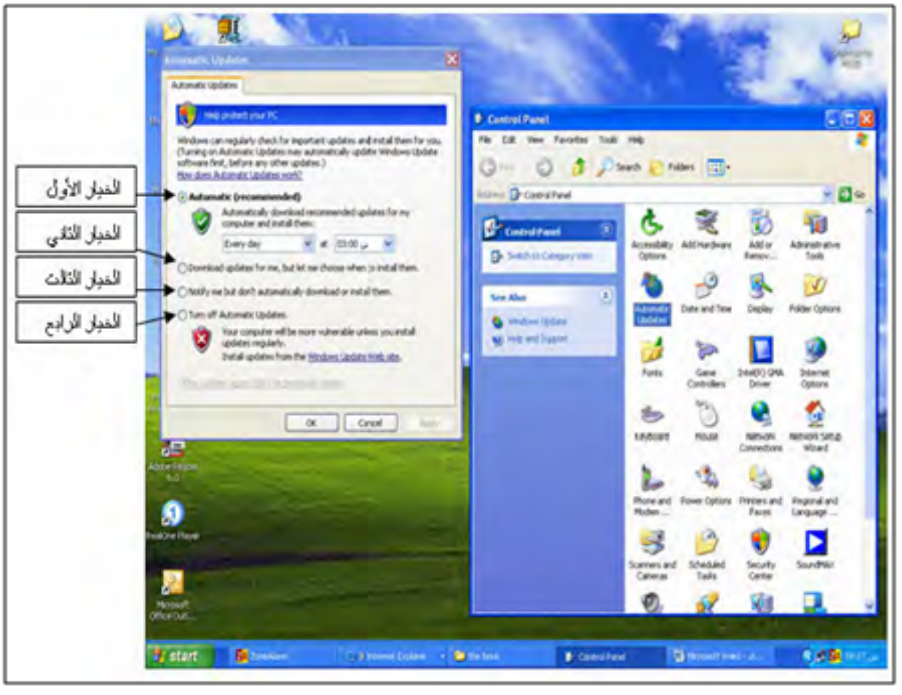
قم بإجراء فحص للنظام مرة واحدة في الأسبوع أو أكثر، كما بإمكانك ضبط برنامجك مكافح الفيروسات ليقوم بهذه العملية تلقايا ويكررها وفق جدول زمني تحدده أنت.

الجانب التطبيقي

لتحديث التلقائي Automatic Update:

يعد التحديث الدائم والتلقائي للبرامج وأنظمة التشغيل من أهم نقاط حماية أمن شبكات المعلومات، ذلك أن عملية بناء هذه النظم هي غاية في التعقيد ولا تخلو من بعض الأخطاء التي تحدث في فترات البناء وتعمل الشركات عادة على إيجاد التحسينات المستمرة لسد نقاط الضعف في هذه البرامج والأنظمة، وهذه التحسينات تتاح دائماً فيما يعرف بالتحديثات، ومن تاتي أهمية أن يقوم

الشخص بعمليات التحديث الدائم للبرامج والأنظمة التي يتبناها في جهازه الشخصي على المستوى الفردي وعلى مستوى البرامج والأجهزة المستخدمة في شبكات المعلومات، ونظراً لصعوبة مطالبة الشركات لمستخدمي هذه البرامج بتحديث البرامج بأنفسهم فإن معظم الشركات المصنعة لهذه البرامج قامت بإضافة خاصية التحديث الآلي والتلقائي لهذه البرامج، ولكي تعمل هذه الخاصية يقوم البرنامج المثبت في الشبكة بالاتصال تلقائياً وعلى فترات معينة بالشركة المنتجة له والقيام بالبحث عن آية تحديثات جديدة وتنزيلها تلقائياً.



حافظ على تحديث برامج وجهازك:

نظراً لأن الفيروسات تتغير باستمرار، فمن الأهمية بمكان قيامك بالتحديث المستمر لنظام التشغيل الموجود في جهازك وبرنامج جدار الحماية الناري وبرنامج مكافحة الفيروسات المركب في جهازك، بحيث يتم إدخال آخر تحديثات صدرت عن هذه البرامج. وسيقوم برنامج مكافحة الفيروسات بسؤالك تلقائياً بتحديث البرنامج وعليك التأكد من قيامك بالتحديث. علماً بأن الكثير من برامج مسح الفيروسات يمكن الحصول عليها مرة كل سنة، وننصحك بترقية البرنامج بعد ذلك حفاظاً على تضمين جهازك آخر التحديثات

التخزين الاحتياطي Backup

النسخ الاحتياطي Backupهو عمل نسخ احتياطية من محتويات الحواسوب أو شبكات المعلومات وحفظ هذه النسخ الاحتياطية في مكان آمن بعيد، بحيث يمكن الرجوع إليها في حالة حدوث أعطال أو حوادث وكوارث للشبكة وتدميرها لأي سبب كان، وعادةً ما يتم أخذ هذه النسخ بشكل دوري

وفق النظام المتبع على الشبكة أسبوعياً أو شهرياً أو حتى يومياً، كما أنه في أغلب الأحوال يتم أخذ هذه النسخ بطريقة آلية من النظام نفسه في وقت محدد.

وتعد هذه الطريقة من أهم وأسهل الطرق التي يمكن من خلالها الحفاظ على سلامة المعلومات الخاصة بشبكات المعلومات وخاصة في حالة التدمير الكامل للشبكة أو اختراقها بهدف محو وتدمير البيانات والمعلومات المتاحة عليها، وتكون في هذه الحالة النسخ الإحتياطية هي الملاذ الآمن لمحتويات الشبكات، وأخذ النسخ الاحتياطية من محتويات شبكات المعلومات تعد من أبجديات الأمن والسلامة للمعلومات والشبكات أي أنها من بديهيات العمل في مجال حفظ شبكات المعلومات. ويقدم المختصون بشبكات المعلومات والنظم عدة نصائح يجب على الفرداتباعها عند القيام بعمل نسخ احتياطية من محتوى شبكات المعلومات وهي:-

1- حفظ النسخ الاحتياطية Backupفي مكان بعيد وآمن وسري، ويفضل أن يكون المكان بعيد عن مقر الشبكة الأم أو المؤسسة المالكة للشبكة تفادياً لضياع هذه النسخ في حالة قيام الكوارث الطبيعية في نفس المكان، فيكون قد ضاعت المعلومات الأصلية والنسخ الاحتياطية أيضاً معها.

2- اختيار وسائط تخزين ذات جودة عالية تقاوم عوامل الزمن ولا تتقادم تكنولوجياً بسرعة.

- القيام بعمليات النسخ الاحتياطي بشكل دوري وفقاً للسياسة المتبعة والإجراءات الخاصة بالمؤسسة المالكة لشبكة المعلومات، وفي كل الأحوال ينبغي ألا تزيد المدة عن شهر.

عمل نسخ احتياطية من ملفاتك

لتفادي فقد ملفات العمل لديك في حالة تعرض كمبيوترك للإصابة بالفيروسات، عليك التأكد من عمل نسخ احتياطية لملفاتك المهمة. وإذا كنت تقوم بشكل منتظم بعمل نسخ احتياطية للمعلومات الموجودة في جهازك على أقراص صلبة خارجية أو أقراص ضوئية قابلة للكتابة أو أقراص مرنة، فلا تضع أقراص النسخ الاحتياطية المساندة في

أختار أحد نقاط الاستعادة

يوصي "استعادة النظام" تلقائياً باستخدام أحدث نقطة استعادة أنشئت قبل حدوث تغيير كبير كتثبيت أحد البرامج مثلاً. يمكن الاختيار أيضاً من قائمة نقاط الاستعادة. حاول استخدام نقاط الاستعادة التي تم إنشاؤها على الفور قبل وقت بدء مشاهدة المشاكل. يتوافق وصف نقاط الاستعادة التي تم إنشاؤها تلقائياً مع اسم الحدث،

الجانب التطبيقي

المقصود بـ "حماية النظام"

"حماية النظام" هي ميزة تقوم بشكل منتظم بإنشاء معلومات وحفظها حول ملفات نظام الكمبيوتر والإعدادات الأخرى. تقوم ميزة "حماية النظام" أيضاً بحفظ الإصدارات السابقة من الملفات التي

قمت بتعديلها. وهي تقوم بحفظ هذه الملفات في نقاط الاستعادة, التي تم إنشاؤها مباشرة قبل أحداث النظام الهامة، مثل تثبيت برامج تشغيل البرامج أو الجهاز. يتم إنشاؤها أيضاً تلقائياً مرة كل سبعة أيام في حالة عدم إنشاء نقاط استعادة أخرى في الأيام السبعة السابقة، ولكن يمكنك إنشاء نقاط الاستعادة يدوياً في أي وقت.

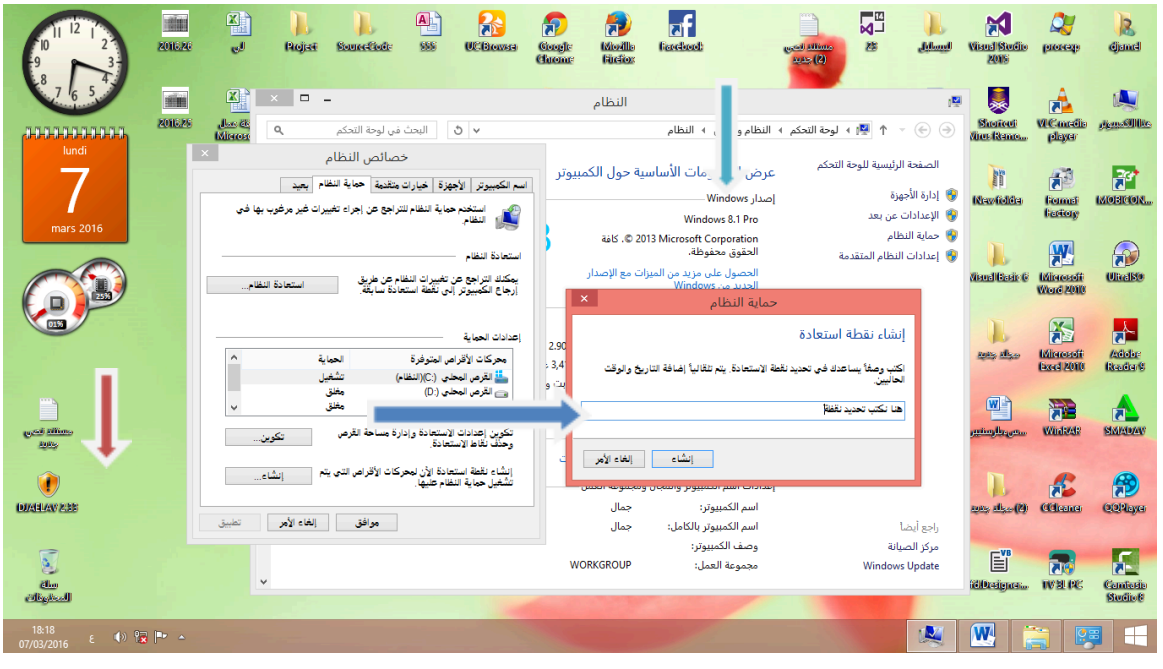
يتم تشغيل "حماية النظام" تلقائياً على محرك الأقراص الذي تم تثبيت Windows عليه. من الممكن تشغيل "حماية النظام" على محركات الأقراص التي تم تهيئتها باستخدام نظام ملفات NTFS.

توجد طريقتان للاستفادة من "حماية النظام":

إذا كان الكمبيوتر يعمل ببطء أو إذا لم يكن يعمل بشكل صحيح، يمكنك استخدام "استعادة النظام" للعودة إلى ملفات نظام الكمبيوتر والإعدادات إلى نقطة زمنية سابقة باستخدام نقطة الاستعادة. لمزيد من المعلومات حول "استعادة النظام"، راجع استعادة النظام: الأسئلة المتداولة.

إذا قمت بحذف ملف أو مجلد أو تعديلهما بطريق الخطأ، فيمكنك استعادتهما إلى الإصدار السابق الذي تم حفظه كجزء من نقطة الاستعادة. لمزيد من المعلومات حول الإصدار

عمل نسخ احتياطية



لاو ل شي نذهب الى خصائص ثم حماية النظام ثم ختير القرص ثم إنشاء ثم كتب اسم نقطة

الجانب التطبيقي

الحصول على جدار حماية ناري (Firewall) :

تعريف الجدار الناري::

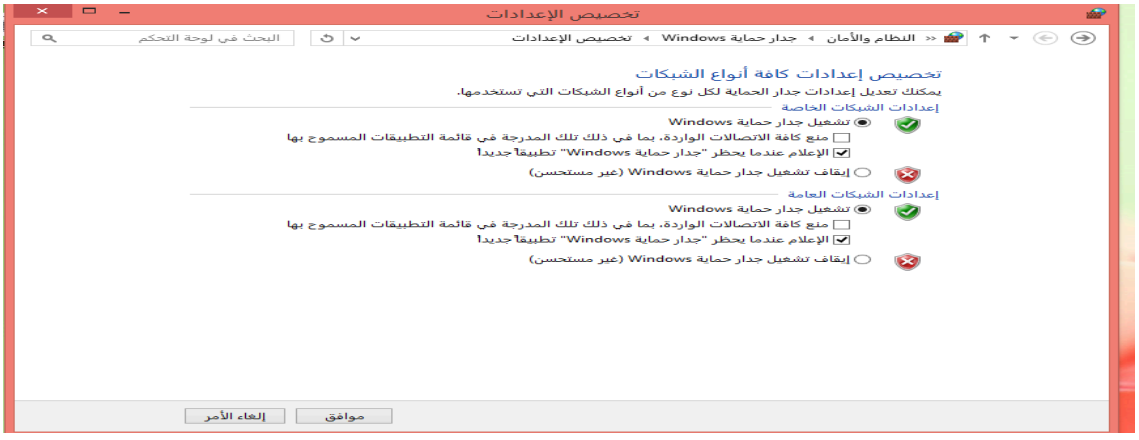
هو عبارة عن جهاز (Hardware) أو نظام (Software) يقوم بالتحكم في مسيرة و مرور البيانات (Packets) في الشبكة أو بين الشبكات و التحكم يكون إما بالمنع أو بالسماح , غالبا يستخدم عند وجود الإنترنت و التعامل مع بروتوكولات TCP/IP و لكن ليس شرطا

جدار الحماية هو الحاجز الذي يحمي جهاز الكمبيوتر الخاص بك أو شبكة كمبيوترات من أي اختراقأو برامج خبيثة مثل الفيروسات والبرامج الدودية وملفات التجسس والمتسللين والمعتدين الذين يحاولون الوصول إلى جهازك عبر الإنترنت التي تحاول الوصول إلى جهاز الكمبيوتر الخاص بك عبر شبكة الإنترنت ويعتبر تركيب جدار حماية ناري أكثر الطرق فاعلية، وأهم خطوة أولية يمكنك اتخاذها لحماية جهاز الكمبيوتر لديك هو القيام بتركيب جدار حماية ناري قبل الدخول إلى الإنترنت للمرة الأولى والإبقاء عليه عاملاً في كافة الأوقات.

وجدار الحماية نظام مؤلف من برنامج (software) يثبت على جهاز الكمبيوتر ويعمل كحاجز في وجه القراصنة يمنعهم من الدخول إلى جهازك والسماح فقط للبرامج و وظيفة الإعدادات ومتى ينبغي استخدامها. يمكن لجدار الحماية أن يساعد في منع المتطفلين أو البرامج الضارة (مثل الفيروسات المتنقلة) من الحصول على حق الوصول إلى الكمبيوتر من خلال إحدى الشبكات أو إنترنت. يمكن لجدار الحماية أيضًا أن يساعد في إيقاف الكمبيوتر عن إرسال برامج ضارة إلى أجهزة الكمبيوتر الأخرى.

1. افتح 'جدار حماية Windows عن طريق النقر فوق الزر ابدأ ثم النقر فوق لوحة التحكم. في مربع البحث، اكتب جدار حماية ثم انقر فوق جدار حماية Windows.

2. في الجزء الأيمن، انقر فوق تشغيل جدار حماية Windows أو إيقاف تشغيله. إذا تم مطالبتك بإدخال كلمة مرور مسئول أو تأكيدها، اكتب كلمة المرور أو قم بتأكيدها.الاتصالات



✔ماذا يستطيع أن يفعل الجدار الناري :[1]

- 1إن الجدار الناري يعتبر النقطة الفاصلة التي تبقي الغير مصرح لهم بدخول الشبكة من الدخول لها و التعامل معها بشكل مباشر و التي تقلل من استغلال ثغرات هذه الشبكة و خدماتها كـ IP spoofing , ARP spoofing , Routing attacks , DNS attacks

-يحدد الجدار الناري اتجاه البيانات الصادرة والواردة من و إلى الشبكة2.

3- يحدد الجدار الناري الأنظمة الموثوقة أو (Trusted Systems) و هو الجهاز أو الشبكة أو النظام الموثوق بهم و التي يُسمح لها بالتعامل مع الشبكة الداخلية المحمية

4-يقوم الجدار الناري بمراقبة البيانات العابرة من و إلى الشبكة و أيضا تسجيل و تتبع الأحداث و التنبيه عن أي أخطار أو أحداث غريبة تحصل

5-يقدم الجدار الناري موثوقية التعامل مع بعض بروتوكولات الإنترنت و يقوم بأشياء أخرى تخدم مستخدمين الشبكة المتصلين بالإنترنت كتوفير العتواين (NAT) و حارسا لمنافذ الأشبكة (PAT) , و أيضا يستطيع أن يعمل كذاكرة للمواقع التي تم زيارتها لتسريع الوصول إليها فيما بعد لكامل الشبكة (Cash)

✔ما الذي لا يستطيع أن يفعله الجدار الناري :[2]

1- لا يستطيع الجدار الناري الحماية ضد الهجمات التي تعبر الفايروول نفسه و التي تعتمد على ثغرات في بروتوكولات لا تستطيع الشبكة الاستغناء عنها .

-2لا يستطيع الفايروول الحماية من المخاطر التي داخل الشبكة نفسها أي من الأفراد الذين هم بطيعة الحال داخل الشبكة و قد حصلوا على تلك الثقة التي جعلتهم في داخل الشبكة المحمية

-2لا يستطيع ا الجدار الناري الحماية من الفيروسات و الديدان و الاتصال العكسي في الشبكة و التي تنتشر بسرعة و تسبب خطورة على كامل الشبكة الداخلة حيث تنتقل عبر الرسائل و مشاركة الملفات الخبيثة .

خصائص الجدار الناري Firewall Characteristics))

سنقسم شرح خصائص الجدار الناري إلى قسمين لتوضيح فكرته في العمل :

أهداف تصميم الجدار الناري.

كل البيانات الداخلة و الخارجة من و إلى (كارت الشبكة - على مستوى الجهاز الواحد أو على مستوى الشبكة -) يجب أن تمر بالفايروول أولا قبل الانتقال للطرف الأخر

-1 يكون التحكم في البيانات عن طريق استثنائها أو استئصالها من و إلى الشبكة و متطلبات الشبكة و التي يراها مدير الشبكة هي التي تحدد تلك القواعد .

- أن يكون الفايروول نفسه محصن ضد الاختراق مما يضمن لمستخدميه الثقة لاستعماله لحماية شبكاتهم و أنظمتهم

-2 التقنيات التي يستخدمها الجدار الناري في التحكم

يستخدم الجدار الناري أربع أنواع للتحكم بالوصول إلى الشبكة و التي تسمى Access Control و التي تستخدم غالبا التحكم في الخدمات التي تسمح بالوصول للشبكة للتحكم بالوصول من و إلى الشبكة و لكن هذه ليست الطريقة الوحيدة و سنذكر الطرق الأخرى و هي: Service Control

يحدد الجدار الناري أنواع خدمات الإنترنت و التي تستطيع عن طريقها الوصول من و إلى الشبكة (Inbound , Outbound traffic) . و قد يقوم الفايروول باستثناء أو استئصال البيانات العابرة سواء الخارجة أو الداخلة بالاعتماد على IP address و أيضا بالـ TCP/UDP ports و ذلك بإجبار أجهزة الشبكة بإتباعهم Proxy البروكسي هو عنوان الفايروول سيرفر و الذي توجد فيه قواعد مرور و حجب الخدمات و المواقع و غيرها) حيث بدونه لن تستطيع الحصول على إنترنت .

Detection Control

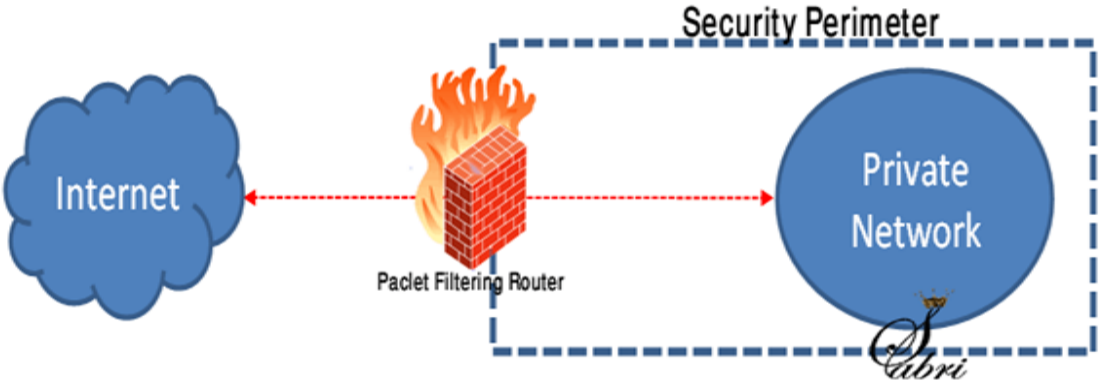
يحدد الجدار الناري هنا اتجاه الخدمات العابرة من و إلى الشبكة و التي يتحكم بها عن طريق السماح بالطلبات و تلبيتها و بهذا يحدد اتجاه البيانات المستثناه والمستأصلة

يحدد الجدار الناري هنا المستخدمين الذي يسمح لهم بالوصول لمكان معين بوضع اسم مستخدم و كلمة مرور و يحدد لهم استخدامات معينة و غالبا تطبق على المستخدمين داخل الشبكة مثل أن يسمح (أو يجبر) باستخدام VPN أو IPsec و غيرها

أنواع الجدران النارية (Types of Firewalls)

هناك ثلاث أنواع للجدران النارية سنوضحها بالرسم و الشرح :

1- Packet-Filters Router



هي عبارة عن مجموعة قو
الصادرة (going PKTs
التجاهل .

Router سمي بذلك لأن
الاتجاهين الصادر و الوار

Packet-Filter قد يفهم أغلبنا الفلترة تعني الاستئصال على الإطلاق لكن الصحيح في الفلترة هي إما الاستئصال أو الاستثناء , فالاستئصال يعني السماح لك و منع البعض , إما الاستثناء فيعني منع الكل و السماح للبعض و طبعا لكلتا الحالتين يجب أن تطبق عليها القواعد Roles الموضوعة من مدير الشبكة

تشغيل أو تثبيت الجدار الناري.

إذا كنت تعمل على نظام التشغيل وندوز Windows فتأكد من تشغيل الجدار الناري، فهو يمنع المتسللين من الوصول إلى جهاز الكمبيوتر الخاص بك عن طريق الحد ومراقبة منافذ الجهاز المفتوحة.

عند شراء جهاز توجيه لاسلكي (Router)، تأكد من أنه يحتوي على جدار ناري، فوجود برنامج وجهاز جدار ناري هو أفضل من مجرد وجود واحد منهم

الجدار الناري تأليف: ساره الشهوبي/1

2/3 نفس المرجع

وظيفة جدار الحماية

وظيفة جدار الحماية الأساسية هي تنظيم بعض تدفق حزمة الشبكة بين شبكات الحاسوب المكونة من مناطق ثقة المتعددة. ومن الأمثلة على هذا النوع الإنترنت - التي تعتبر منطقة غير موثوق بها- وأيضا شبكة داخلية ذات ثقة أعلى ، ومنطقة ذات مستوى ثقة متوسطة، متمركزة بين الإنترنت والشبكة الداخلية الموثوق بها، تدعى عادة بالمنطقة منزوعة..

وظيفة جدار الحماية من داخل الشبكة هو مشابه إلى أبواب الحريق في تركيب المباني. في الحالة الأولى يستعمل في منع اختراق الشبكة الخاصة، وفي الحالة الثانية يعطل دخول الحريق من منطقة (خارجية) إلى بهو أو غرفة داخلية.

من دون الإعداد الملائم فإنه غالباً ما يصبح الجدار الناري عديم الفائدة. فممارسات الأمان المعيارية تحكم بما يسمى بمجموعة قوانين "المنع أولاً" جدار الحماية، الذي من خلاله يسمح بمرور وصلات الشبكة المسموح بها بشكل تخصيصي فحسب. ولسوء الحظ، فإن إعداد مثل هذا يستلزم فهم مفصل لتطبيقات الشبكة ونقاط النهاية اللازمة للعمل اليومي للمنظمات. العديد من أماكن العمل ينقصهم مثل هذا الفهم وبالتالي يطبقون مجموعة قوانين "السماح أولاً"، الذي من خلاله يسمح بكل البيانات بالمرور إلى الشبكة ان لم تكن محددة بالمنع مسبقاً.

نالك العديد من فئات الجدران النارية بناءً على مكان عمل الاتصال، ومكان تشفير الاتصال والحالة التي يتم تتبعها.

1 طبقات الشبكة ومفلترات العبوات(Network Layer and Packet Filters)

الجدار الناري ذو طبقات الشبكة الذي يسمى أيضا مفلترات العبوة، تعمل على رصة أنظمة TCP\IP منخفضة المستوى، ولا تسمح للعبوات بالمرور عبر الجدار الناري دون أن تطابق مجموعة القوانين المحددة. يمكن للمسؤول عن الجدار الناري أن يحدد الأوامر، وإن لم يتم هذا تطبق الأوامر الطبيعية. المصطلح فلتر العبوة نشأ في نطاق أنظمة تشغيل "BSD".

الجدار الناري ذو طبقات الشبكة عادة ينقسم إلى قسمين فرعيين اثنين، ذو الحالة وعديم الحالة. تتحفظ الجدران النارية ذات الحالة بنطاق يتعلق بالجلسات المفتوحة حالياً، ويستخدم معلومات الحالة لتسريع معالجة العبوة. أي اتصال شبكي يمكن تحديده بعدة امور، تشتمل على عنوان المصدر والوجهة،

مرافئ " UDP " و"TCP"، والمرحلة الحالية من عمر الاتصال (يشمل ابتداء الجلسة، المصافحة، نفل البيانات، وإنهاء الاتصال). إذا كانت العبوة لا تطابق الاتصال الحالي، فسوف يتم تقدير ماهيتها طبقاً لمجموعة الأوامر للاتصال الجديد، وإذا كانت العبوة تطابق الاتصال الحالي بناءً على مقارنة عن طريق جدول الحالات للحائط الناري، فسوف يسمح لها بالمرور دون معالجة أخرى.

الجدار الناري العديم الحالة يحتوي على قدرات فلترة العبوات، ولكن لا يستطيع اتخاذ قرارات معقدة تعتمد على المرحلة التي وصل لها الاتصال بين المضيفين.

الجدران النارية الحديثة يمكنها أن تفلتر القنوات معتمدة على كثير من الجوانب للعبوة، مثل عنوان المصدر، مرفأ المصدر، عنوان الوجهة أو مرفأها، نوع خدمة الوجهة مثل"WWW" و"FTP"، ويمكن أن يفلتر اعتماداً على أنظمة وقيم"TTL"، صندوق الشبكة للمصدر، اسم النطاق للمصدر، والعديد من الجوانب الأخرى.

فلاتر العبوات لنسخ متعددة من "UNIX" هي "IPF" (لعدة) (FREEBSD " "IPFW /MAC OS X)، "PF" (OPEN BSD AND ALL OTHER BSD)، (IPTABELSIPCHAINS (LINUX.

2 طبقات التطبيقات (Application Layer)

تعمل الجدران النارية لطبقات التطبيقات على مستوى التطبيق لرصة"TCP\IP" مثل جميع أزمة المتصفح، أو جميع أزمة "TELNET" و"FTP"، ويمكن أن يعترض جميع العبوات المنتقلة من وإلى التطبيق. ويمكن أن يحجب العبوات الأخرى دون إعلام المرسل عادة. في المبدأ يمكن لجدران التطبيقات النارية منع أي اتصال خارجي غير مرغوب فيه من الوصول إلى الأجهزة المحمية.

عند تحري العبوات جميعها لإيجاد محتوى غير ملائم، يمكن للجدار الناري أن يمنع الديدان(worms) والأحصنة الطروادية (Trojan horses) من الانتشار عبر الشبكة. ولكن عبر التجربة تبين أن هذا الأمر يصبح معقدا جداً ومن الصعب تحقيقه (مع الأخذ بعين الاعتبار التنوع في التطبيقات وفي المضمون المرتبط بالعبوات) وهذا الجدار الناري الشامل لا يحاول الوصول إلى مثل هذه المقاربة.

الحائط الناريXML يمثل نوعاً أكثر حداثة من جدار طبقات التطبيقات الناري.

3 الخادمين النيابيين (Proxy Servers)

الخادم النيابي (سواء أكان يعمل على معدات مخصصة أو برامج الأجهزة المتعددة الوظائف) قد يعمل مثل كجدار ناري بالاستجابة إلى العبوات الداخلة (طلبات الاتصال على سبيل المثال) بطريقة تشبه التطبيق مع المحافظة على حجب العبوات الأخرى.

يجعل الخادم النيابي العبث بالأنظمة الداخلية من شبكة خارجية أصعب ويجعل إساءة استخدام الشبكة الداخلية لا يعني بالضرورة اختراق أمني متاح من خارج الجدار الناري (طالما بقي تطبيق الخادم النيابي سليماً ومعداً بشكل ملائم). بالمقابل فإن المتسللين قد يختطفون نظاماً متاحاً للعامة ويستخدمونه كخادم نيابي لغاياتهم الشخصية، عند اإن يتنكر الخادم النيابي بكونه ذلك النظام بالنسبة إلى الأجهزة الداخلية. ومع أن استخدام مساحات للمواقع الدخلية يعزز الأمن، إلا أن المشقين قد يستخدمون أساليب مثل "IP Spoofing" لمحاولة تمرير عبوات إلى الشبكة المستهدفة.

الجانب التطبيق

4 ترجمة عنوان الشبكة (Network Address Translation)

عادة ما تحتوي الجدران النارية على وظيفة ترجمة عنوان الشبكة (NAT)، ويكون المضيفين محميين خلف جدار ناري يحتوي على مواقع ذو نطاق خاصة، كما عرّفت في"RFC 1918". تكون الجدران النارية متضمنة على هذه الميزة لتحمي الموقع الفعلي للمضيف المحمي. وبالأصل تم تطوير خاصية "NAT" لتخاطب مشكلة كمية "IPv4" المحدودة والتي يمكن استخدامها وتعيينها للشركات أو الأفراد وبالإضافة إلى تخفيض العدد وبالتالي كلفة إيجاد مواقع عامة كافية لكل جهاز في المنظمة. وأصبح إخفاء مواقع الإجهزة المحمية أمراً متزايد الأهمية للدفاع ضد استطلاع الشبكات.

(a) كيف تجد أفضل البرامج لجدار الحماية الناري أو مكافحة الفيروسات؟

لعل أسهل الطرق لإيجاد برامج جيدة لجدار الحماية الناري أو مكافحة الفيروسات هو الذهاب للمحل الذي اشتريت منه جهازك وطلب مشورتهم في هذا الأمر. أما إذا أردت قائمة أفضل برامج جدار الحماية الناري أو مكافحة الفيروسات من الإنترنت، فابحث في الإنترنت عن أفضل البرامج باستخدام الكلمات التالية (Top Firewalls) أو (Top Antivieus) ثم اكتب السنة الحالية، وهناك الكثير من المواقع الإلكترونية تحتوي على قوائم بأفضل البرامج. وعلى سبيل المثال فإن المواقع الإلكترونية الخاصة بمجلات الكمبيوتر تعتبر مصدراً موثوقاً لهذه المعلومات، واحرص على قراءة آخر القوائم لديهم. عند العثور على برنامجين يناسبانك واحد لجدار الحماية الناري والآخر لمكافحة الفيروسات، اذهب للمواقع الإلكترونية لهذه البرامج حيث أن جميع الشركات المطورة لبرامج الموثوقة تقدم الكثير من المعلومات عن برامجهم ضمن مواقعهم الإلكترونية. ابحث عن نبذة (Snapshot) من هذه البرامج ثم اختر قسم المساعدة للحصول على المعلومات حول تنزيل هذه البرامج وتثبيتها في الجهاز واستخدامها

الحصول على برنامج مكافحة فيروسات :

إضافة لبرنامج الحماية الناري (Firewall)، فإن عليك الحصول على برنامج مكافحة فيروسات قبل الدخول إلى الإنترنت للمرة الأولى. حيث يقوم برنامج مكافحة الفيروسات بفحص جهازك لمعرفة الفيروسات الجديدة التي أصيب بها ومن ثم تنظيف هذه الفيروسات بما يكفل عدم إلحاق المزيد من الأذى بجهازك.

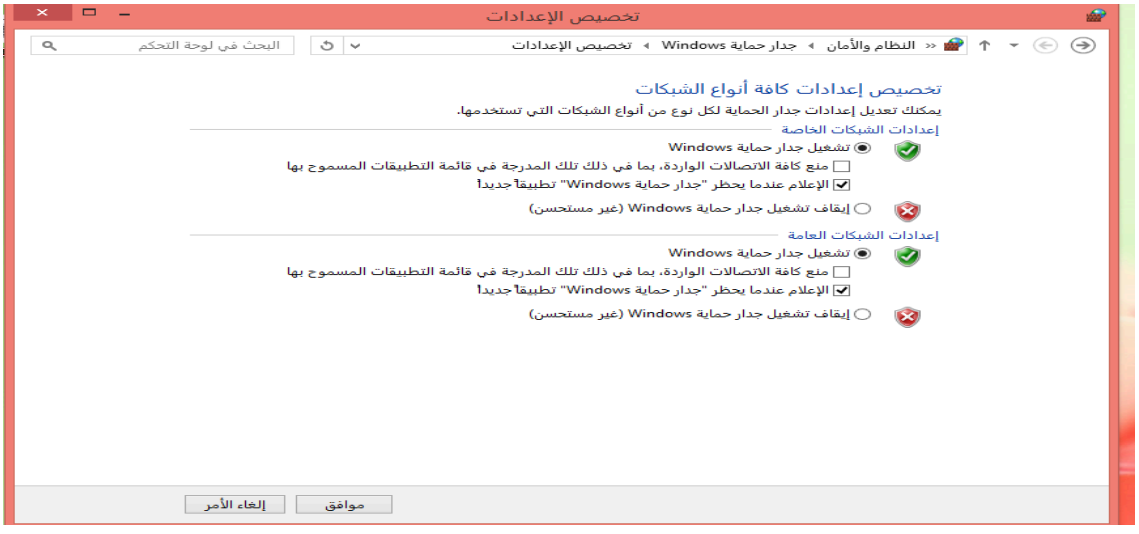
وكما هو الحال في جدار الحماية الناري، فإن عليك الإبقاء على برنامج مكافحة الفيروسات عاملاً في جميع الأوقات بحيث أنه بمجرد تشغيل جهازك يبدأ البرنامج بالعمل للكشف عن الفيروسات مما يضمن التعامل معها بأسرع ما يمكن. كما يقوم برنامج مكافحة الفيروسات بالكشف عن الفيروسات في الأقراص المدخلة في جهازك والبريد الإلكتروني الذي تستلمه والبرامج التي تقوم بتحميلها في جهازك من الإنترنت.

في حالة دخول فيروس إلى جهازك، فإن برنامج مكافحة الفيروسات سينبهك بذلك ومن ثم سيقوم بمحاولة إصلاح الملف المصاب، كما يقوم هذا البرنامج بعزل الفيروسات التي لا يستطيع إصلاحها مع محاولة إنقاذ وإصلاح أية ملفات مصابة يستطيع إصلاحها. هذا علماً بأن بعض برامج مكافحة الفيروسات تطلب منك إرسال الفيروس إلى شركة مكافحة الفيروسات، كي يتسنى لها إدخاله ضمن قاعدة بياناتها إذا كان من الفيروسات الجديدة.

يمكنك شراء برامج مكافحة الفيروسات عبر الإنترنت أو من محلات بيع البرمجيات، كما يستحسن التأكد فيما إذا كان مزود خدمات الإنترنت الذي تتعامل معه يزود مثل هذه البرمجيات. ومما تجدر ملاحظته، أنه في حالة كون جهازك مصاباً بالفيروسات، فمن الخطر شراء برنامج الحماية عبر الإنترنت لأنه يمكن لبرنامج التجسس التلصص على معلومات بطاقتك الائتمانية وسرقتها حتى ولو أدخلتها في صفحة ويب آمنة.

يجب أن يكون برنامج مكافحة الفيروسات مناسباً لجهاز الكمبيوتر لديك والبرامج التي لديك. وهناك العديد من أنواع البرامج المتوفرة التي تناسب مستخدمي أنظمة التشغيل ويندوز ولينكس وماكنتوش

(MacOS). علماً بأن أكثر برامج مكافحة الفيروسات استخداماً هي البرامج المزودة من ماكافي (McAfee)، ونورتن (Norton Antivirus) من سيمانتك (Symantic)، وأنظمة سيسكو (Cisco System) وميكروسوفت (Microsoft).



الجانب التطبيقي

حذف فيروس:

الطريقه الاولى

افيرا و الكاسبر .....الخ

Registry:

الطريقة الثانية: بواسطة ملف تسجيل النظام

-انقر على زر البدء : Start

regedit : الأمر Run -أكتب في خانة التشغيل

-افتح المجلدات التالية حسب الترتيب في قائمة : Register Editor

HKEY_LOCAL_MACHINE

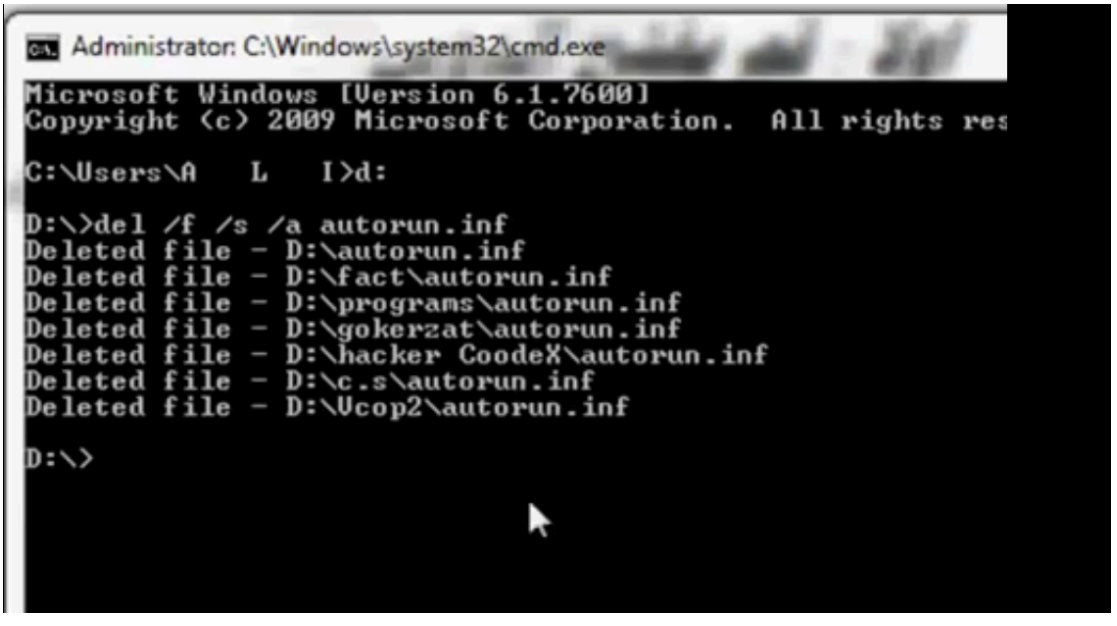
Software - Microsoft- Windows - Current Version - Run - ثم

الطريقة الثالثة:

حذف فيروس اوتورن من القرص المعين او سي

الاول: قم فتح الدوس //الثاني:نقم بتحديد القرص على سبيل مثال القرص :d

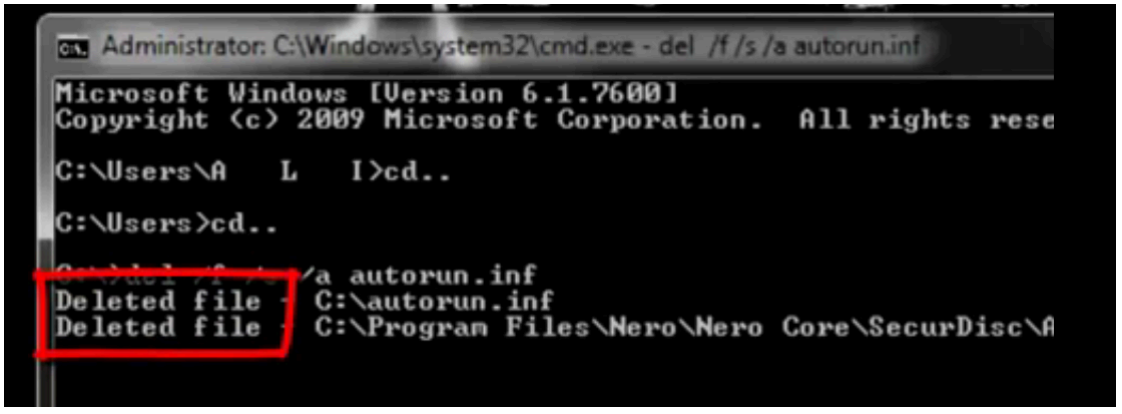
نكتب هذ لامر: del/f/s/a autorun.inf وبعدين نضغط انتر



الجانب التطبيق

القرص :c

نكتب CD..ثم نضغط انتر نتكتب CD...:



: <u>الطريقة الثالث</u> : بواسطة مشغل الدوس Dos

هذه الطريقة كانت تستخدم قبل ظهور الويندوز لإظهار ملفات التجسس مثل الباتش والتروجانز وهي من أسهل الطرق :

Start بقائمة البدء MSDos -افتح الدوس من محث

<u>-أكتب الأمر التالي :</u>

C:/Windows\dir patch.* e

-إن وجدت ملف الباتش فقم بمسحة بالطريقة التالية : C:\Windows\delete patch.*

<u>الطريقة الرابعة</u>

إذهب إلى قائمة أبدا start ثم تشغيل run

فى Run اكتب Cmd ثم أكتب net user

إذا كانت النتيجة كالتالي :- Support_388945a0أذن server موجود فى نظام تشغيلك ثم قم بكتابة الامر التالى مع مراعاة الفواصل :

net user SUPPORT_388945a0 /delete

ثم أكتب الأمر Exit

و للتأكد من الحذف قم بأعادة الخطوات الأولى ستجد أنه تم حذفه

<u>مفهوم مضاد الفيروسات (Antivirus)</u>

هو برنامج حماية قوي يهدف إلى حماية الحاسوب و البيانات حيث أنه يكتشف و يمنع و يزيل البرامج الخبيثة (الفيروسات)

✔**مضاد الفيروسات :** هي البرامج التي تقوم بحماية الحاسوب من هجمات الفيروسات وبقية البرامج الخبيثة التي تشكل تهديدا على المعلومات والملفات ، وتستطيع أن تمنعها من الدخول ، كما تعمل على اكتشافها وإزالتها أو تعطيلها، تعتمد برامج مضادات الفيروسات على قاعدة بيانات تدعى تعريف الفيروس

تثبيت برامج مكافحة الفيروسات:

تثبيت برنامج مكافحة الفيروسات هو أول وأهم خطوة يمكن للمستخدم أن يقوم بها، إذا لم يكن لديك برنامج لمكافحة الفيروسات مثبت فأنت حقا في مشكلة ومعرض بشكل كبير للخطر!

إذا كان السبب لعدم تثبيت برامج مكافحة الفيروسات هو لأنها مكلفة للغاية، يمكن استخدام برامج مكافحة الفيروسات المجانية فهي ليست بقوة البرامج المدفوعة لكنها أفضل من لا شيء. من بين برامج مكافحة الفيروسات :

Avast Anti-Virus(نسخة مجانية متوفرة) Kaspersky (نسخة مدفوعة فقط)

AVG Anti-Virus(نسخة مجانية متوفرة)

[1]Kaspersky Internet Security

كاسبرسكي إنترنت سكيورتي (بالإنجليزية: Kaspersky Internet Security) هي حزمة أمن إنترنت من إنتاج الشركة الروسية كاسبرسكي لاب، صمم للعمل على الأجهزة التي تستخدم مايكروسوفت ويندوز. برنامج كاسبرسكي إنترنت سكيورتي يمكنه اكتشاف وحذف العديد من أنواع البرمجيات الخبيثة، كما أنه يوفر الحماية ضد هجمات القراصنة ويحتوي أيضا على أنتي سبام.

هذا البرنامج يعتبر من أقوى برامج حماية الحواسيب. وهو موقع من قبل شركة مايكروسوفت ليستخدم على نظام وندوز.

أيًا كان الجهاز الذي تستخدمه لإجراء المعاملات المصرفية أو التسوق أو تصفّح الإنترنت أو الاتصال بالشبكات الاجتماعية عبر الإنترنت، فشبكة الإنترنت تنطوي على مخاطر الأمن نفسها، بما في ذلك البرامج الضارة والجرائم على الإنترنت والتصيّد الاحتيالي. لذا من الضروري أن تضمن الحماية لكل أجهزتك المتصلة والبيانات الشخصية التي تخّزنها عليها، من جميع التهديدات التي قد تتعرّض لها عبر الويب

المميزات الرئيسية:[2]

طلِق مجرمو الإنترنت مئات الآلاف من عناصر البرامج الضارة الجديدة كل يوم. لذا، يضيف الأمن السحابي باستمرار مزيدًا من وسائل الحماية من مخاطر الإنترنت والبرامج الضارة. كما أننا نمنع إعلانات الشعارات ونتيح لك تصفية الرسائل المزعجة غير المرغوب فيها. حماية خصوصيتك والحماية ضد سرقة الهوية يتم منع الهجمات الاحتيالية تلقائيًا، بالإضافة إلى أن تقنية حماية كاميرا الويب* (Webcam Protection) تمنع المجرمين من استخدام كاميرا الويب الخاصة بك في التجسس عليك. كما أننا نحول دون تتبع* عاداتك في استعراض صفحات الويب والتقاط معلوماتك الشخصية تتيح لك ميزات الرقابة الأسرية

خصائص البرنامج:[3]

اسبرسكاي إنترنت سكيورتي يحتوي على نفس إمكانيات برنامج كاسبرسكاي أنتي فيرس التي تتلخص في اكتشاف وإزالة الفيروسات وال trojans وديدان الحاسوب (worms) وبرامج التجسس مثل الكي-لوجر (Key-logger). وغيرها

بالإضافة إلى بعض الإمكانيات الأخرى الخاصة بحزمة الإنترنت سكيورتي وهي :

جدار ناري

حماية من هجمات الشبكة Network Attacks

مانع الصور والارتباطات الدعائية

نظام التحكم الأبوي (parental control)

أنتي سبام

حماية صد الفيشنج (Phishing) وهى محاولات السرقة الغير شرعية لكلمات المرور وغيرها من المعلومات الهامة كما تحتوي الحزمة على نظام تحديث آلي لكي يصبح البرنامج قادر علي التعرف على الفيروسات الجديدة دائما وكذلك يستطيع كاسبرسكاي إنترنت سكيورتي أن يقوم بحماية نفسه من الإغلاق أو التعديل الغير شرعي (الذي لا يتم بواسطة المستخدم).

1/ موقع كاسبرسكي 2/3/ نفس الموقع

ويندوز ديفيندر Windows Defender

- افتح Windows Defender بالنقر فوق الزر ابدأ . في مربع البحث، اكتب Defender ثم في قائمة النتائج، انقر فوق Windows Defender.

Windows Defender هو برنامج للحماية من التجسس مضمن في Windows ويعمل بشكل تلقائي عند تشغيله. يمكن أن يساعد استخدام برامج الحماية من التجسس في حماية الكمبيوتر من برامج التجسس وغيرها من البرامج الأخرى غير المرغوب فيها. يمكن تثبيت برامج تجسس على الكمبيوتر دون معرفتك في أي وقت أثناء الاتصال بإنترنت ومن الممكن أن تؤدي هذه البرامج إلى إلحاق الضرر بالكمبيوتر عند تثبيت بعض البرامج باستخدام أحد الأقراص المضغوطة أو قرص DVD أو أي وسائط قابلة للنقل. يمكن أيضاً برمجة برامج التجسس بحيث يتم تشغيلها في أوقات غير متوقعة، وليس فقط عند تثبيتها.

يقدم Windows Defender طريقتين للمساعدة في منع برامج التجسس من إلحاق الضرر بالكمبيوتر:

- الحماية في الوقت الحقيقي. يُنبهك Windows Defender عند محاولة برامج التجسس تثبيت نفسها أو التشغيل على الكمبيوتر. كما يُنبهك أيضاً عند محاولة البرامج تغيير إعدادات Windows المهمة.

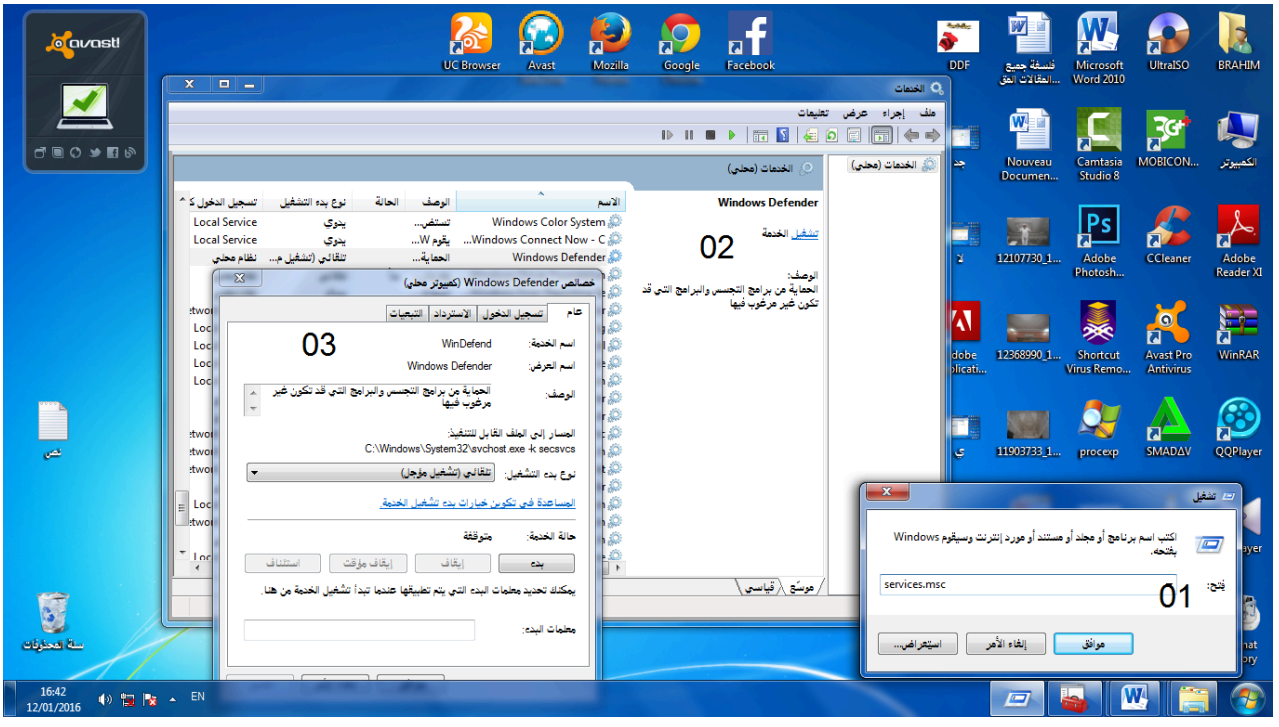
- خيارات الفحص يمكنك استخدام Windows Defender للفحص بحثاً عن برامج التجسس التي قد يتم تثبيتها على الكمبيوتر ولجدولة عمليات الفحص بشكل منتظم وإزالة أي ضرر يتم اكتشافه أثناء الفحص بشكل تلقائي.

عند استخدام Windows Defender، فإنه من المهم جداً توفر تعريفات محدثة. تُعد التعريفات بمثابة ملفات تعمل كموسوعة تنمو باستمرار حول التهديدات المُحتملة للبرامج. يستخدم Windows Defender التعريفات لتنبيهك حول المخاطر المحتملة في حالة تحديد ما إذا كانت البرامج التي يكتشفها برامج تجسس أو غيرها من البرامج غير المرغوب فيها. للمساعدة على المحافظة على التعريفات محدثة، يعمل Windows Defender مع 'Windows Update'

لتثبيت التعريفات الجديدة تلقائياً بمجرد أن يتم إصدارها. يمكن أيضًا تعيين Windows Defender للبحث عن التعريفات المُحدثة عبر الإنترنت

تفعيل Windows Defender: الضغط على المفتاح لاختصار Win + R

كتب الامر services.msc الى تشغيل الخدمات Windows Defender تم نبحث عن



استخدام البرامج المضادة للفيروسات:

هناك شركات عديدة تنتج برامج مضادة للفيروسات من بينها :
Symantec,Command,Mcafee وغيرها... وتعمل تلك البرامج الآتي:

1) فحص ذاكرة الحاسب عند بدء تشغيله بحثًا عن أي فيروسات
2) فحص أقراص التخزين بحثًا عن أي فيروسات، وفي حالة وجودها يتيح إزالتها أو إلغاء الملفات المصابة
3) فحص الملفات المراد تحميلها على جهاز الحاسب سواء كانت تلك الملفات متاحة من خلال الشبكة أو على أقراص مرنة وذلك للتأكد من سلامتها من الفيروسات.
4) فحص الملفات سواء المتاحة للمشاركة أم المنقولة عبر الإنترنت أم المرسلة عبر البريد الإلكتروني للتأكد من خلوها من الفيروسات والتنبيه بوجودها إن وجدت وتوفير الحماية ضدها.
5) الفحص المستمر للنظام للتأكد من خلوه من الفيروسات، والتنبيه عنها في حالة وجودها

البرامج djamel av:

برنامج مكافحة الفيروسات و الملفات الضارة، djamelav تطبيق حماية مجاني و صغير في الحجم يساعدك على مكافحة جميع انواع الفيروسات في الوقت الحقيقي، البرنامج يعمل على رصد و إزالة الفيروسات من جهاز الكمبيوتر كما يعتبر اداة قوية لتنظيف الفلاش ديسك من الفيروسات الخطيرة، يمكنك عمل فحص لجهاز الكمبيوتر و كشف و إزالة جميع الفيروسات و التروجان و البرمجيات الخبيثة المتخفية على جهازك و يعتبر برنامج djamelav من اقوى برامج الحماية المجانية الأكثر فعالية في كشف و رصد الفيروسات الخطيرة، بحيث يمكنه التعرف على الآلاف من الفيروسات و البرامج الضارة. ، يمكنك إستخدام برنامج الحماية سماداف djamelav مع اي برنامج حماية آخر و لن يكون هناك اي تعارض

إصدار البرنامج: 2.23 . حجم البرنامج: 1.32MB ترخيص البرنامج: "مجاني"

آخر تحديث: 08/02/2016 نظام التشغيل: 10 / 7 / 8 متوافق مع جميع انظمة ويندوز

افتح djamel av تظهر أيقونته على سطح المكتب بالشكل التالي:

خصائص البرنامج:

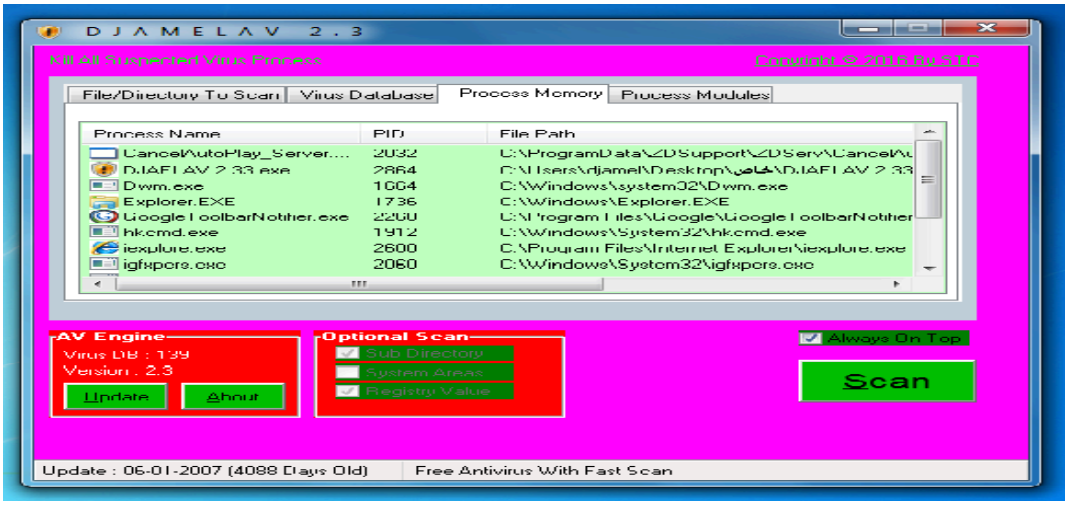
virus database خاص بالتحديثات اليومية للفيروسات

process memory يقضي عن الفيروسات العاملة في الذاكرة كما له process manager أو Task manager خاص به

process model معناه أن لديه سرعة كبيرة في فحص الملفات

file directory to scan إختيار مسار أو ملف للفحص

process virU فيروس عملية DETECTED virus تم اكتشاف فيروس المصابة



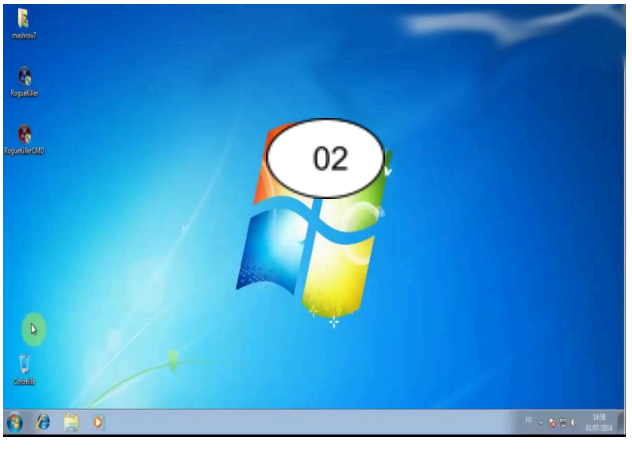
ازالة الفيروسات في الوضع الآمن مع cmd

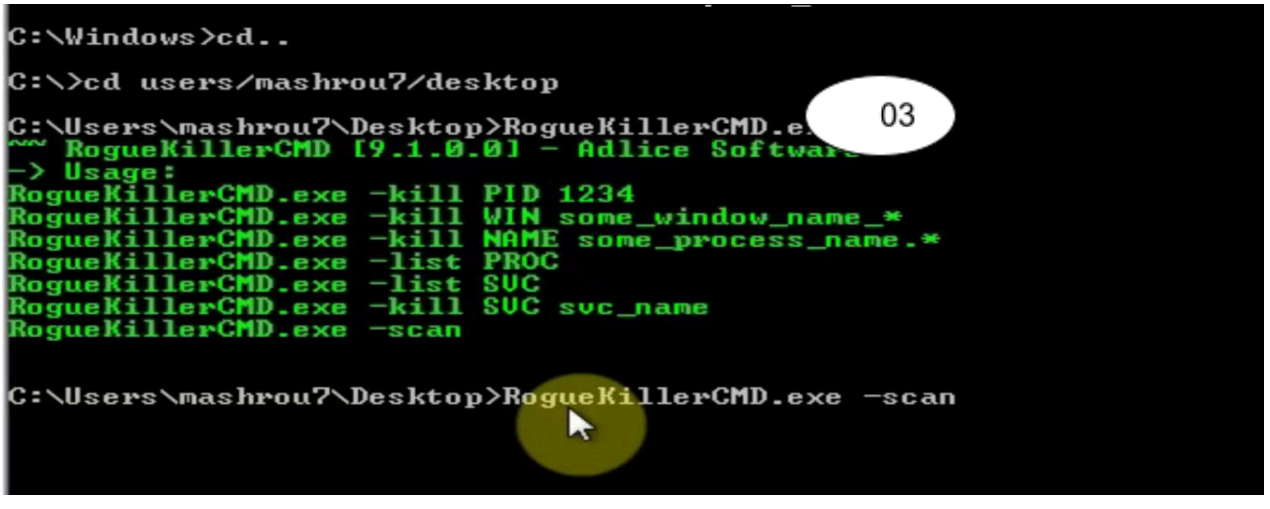
و سيرا على نفس النهج أقدم لك في هذه أداة جديدة تدعى RogueKillerCMD , و هي تابعة لنفس البرنامج RogueKiller الغني عن التعريف , لكن ما يميزها هو

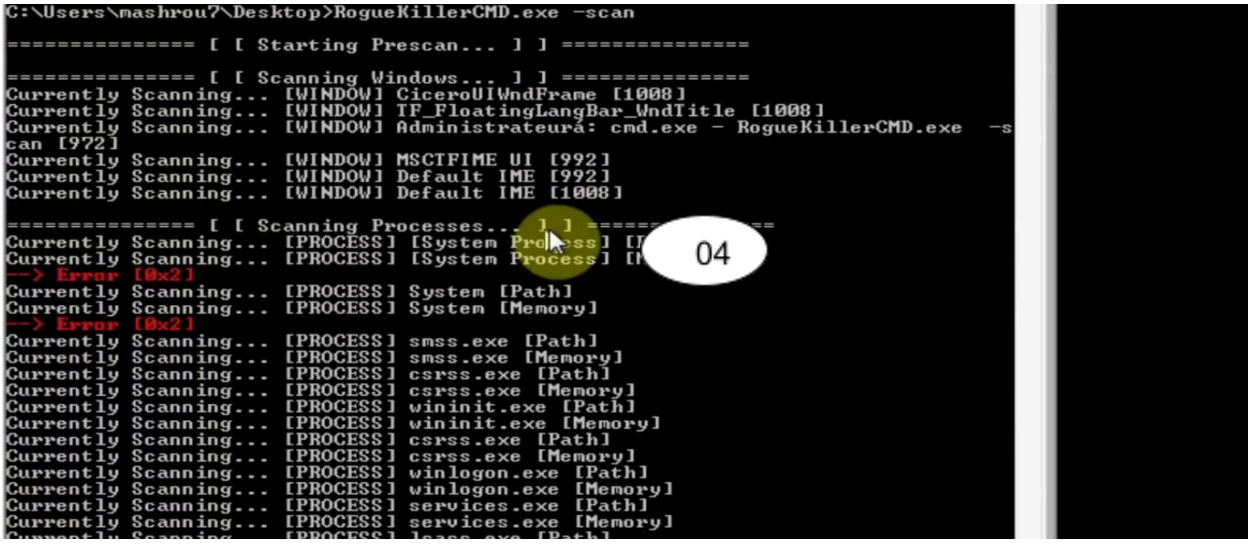
و يمكنك من خلالها حذف الفيروسات و التروجن و بعض البرمجيات الخبيثة الأخرى . و يعتبر إكتشافها هو أصعب شيء بحيث أن حتى برامج الحماية لا تستطيع إكتشافها في هذه لطريقة فعالة ومجربة لحذف الكثير من الفيروسات و البرمجيات الضارة التي لا تستطيع برامج الحماية إكتشافها بحيث سنقوم بعمل scan لجميع ملفات الكمبيوتر عن طريق أداة rogue killer cmd لإظهار الفيروسات ثم مسحها نهائيا من الكمبيوتر لانحتاج لأي برامج معقدة فقط لوحة الأوامر cmd و الموجودة أصلا في الويندوز ثم أداة rogue killer cmd البسيطة

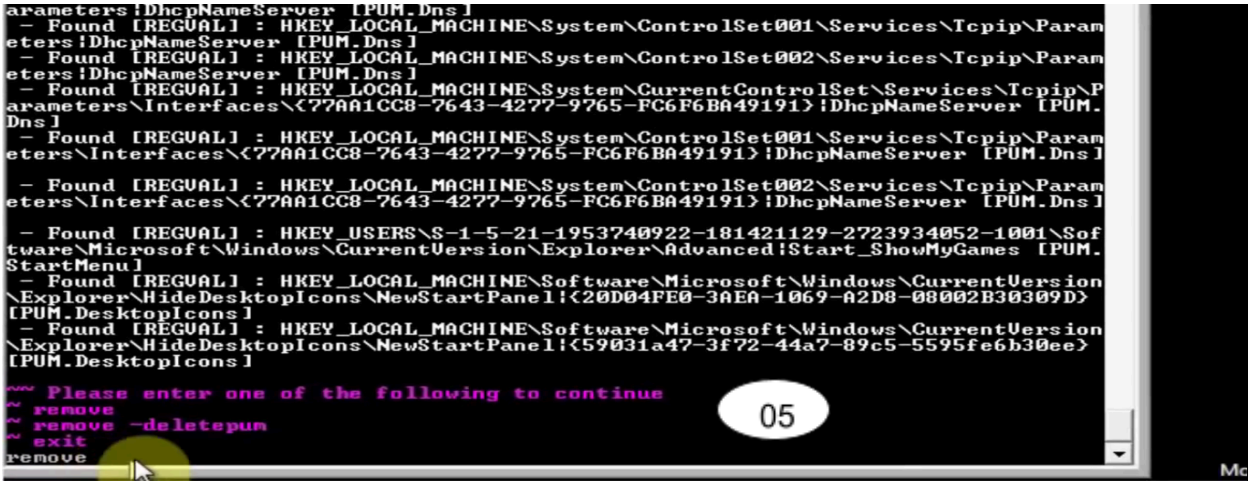
طريقة تفعيل الزر F8 للدخول الى الوضع الامن في الويندوز إضغط هنا .

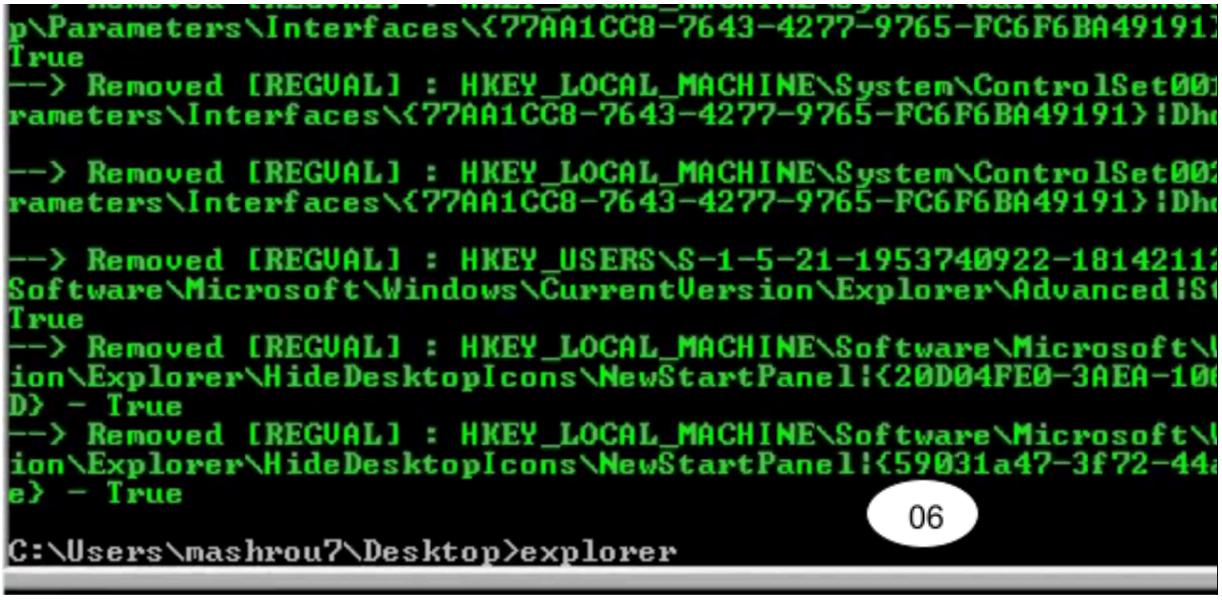
كونها تشتغل عبر ال Safe-Mode-with-Command prompt






C:\Users\mashrou7\Desktop>RogueKillerCMD.exe -scan
========== [[Starting Prescan...]] ==========
========== [[Scanning Windows...]] ==========
Currently Scanning... [WINDOW] CiceroUIWndFrame [1008]
Currently Scanning... [WINDOW] TF_FloatingLangBar_WndTitle [1008]
Currently Scanning... [WINDOW] Administrateur: cmd.exe - RogueKillerCMD.exe -scan [972]
Currently Scanning... [WINDOW] MSCTFIME UI [992]
Currently Scanning... [WINDOW] Default IME [992]
Currently Scanning... [WINDOW] Default IME [1008]
========== [[Scanning Processes...]] ==========
Currently Scanning... [PROCESS] [System Process] [
Currently Scanning... [PROCESS] [System Process] [
--> Error [0x2]
Currently Scanning... [PROCESS] System [Path]
Currently Scanning... [PROCESS] System [Memory]
--> Error [0x2]
Currently Scanning... [PROCESS] smss.exe [Path]
Currently Scanning... [PROCESS] smss.exe [Memory]
Currently Scanning... [PROCESS] csrss.exe [Path]
Currently Scanning... [PROCESS] csrss.exe [Memory]
Currently Scanning... [PROCESS] wininit.exe [Path]
Currently Scanning... [PROCESS] wininit.exe [Memory]
Currently Scanning... [PROCESS] csrss.exe [Path]
Currently Scanning... [PROCESS] csrss.exe [Memory]
Currently Scanning... [PROCESS] winlogon.exe [Path]
Currently Scanning... [PROCESS] winlogon.exe [Memory]
Currently Scanning... [PROCESS] services.exe [Path]
Currently Scanning... [PROCESS] services.exe [Memory]
04


arameters\DhcpNameServer [PUM.Dns]
- Found [REGVAL] : HKEY_LOCAL_MACHINE\System\ControlSet001\Services\Tcpip\Parameters\DhcpNameServer [PUM.Dns]
- Found [REGVAL] : HKEY_LOCAL_MACHINE\System\ControlSet002\Services\Tcpip\Parameters\DhcpNameServer [PUM.Dns]
- Found [REGVAL] : HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{77AA1CC8-7643-4277-9765-FC6F6BA49191}\DhcpNameServer [PUM.Dns]
- Found [REGVAL] : HKEY_LOCAL_MACHINE\System\ControlSet001\Services\Tcpip\Parameters\Interfaces\{77AA1CC8-7643-4277-9765-FC6F6BA49191}\DhcpNameServer [PUM.Dns]
- Found [REGVAL] : HKEY_LOCAL_MACHINE\System\ControlSet002\Services\Tcpip\Parameters\Interfaces\{77AA1CC8-7643-4277-9765-FC6F6BA49191}\DhcpNameServer [PUM.Dns]
- Found [REGVAL] : HKEY_USERS\S-1-5-21-1953740922-181421129-2723934052-1001\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Start_ShowMyGames [PUM.StartMenu]
- Found [REGVAL] : HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\HideDesktopIcons\NewStartPanel\{20D04FE0-3AEA-1069-A2D8-08002B30309D} [PUM.DesktopIcons]
- Found [REGVAL] : HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\HideDesktopIcons\NewStartPanel\{59031a47-3f72-44a7-89c5-5595fe6b30ee} [PUM.DesktopIcons]
~~ Please enter one of the following to continue
~~ remove
~~ remove -deletepum
~~ exit
remove
05


p\Parameters\Interfaces\{77AA1CC8-7643-4277-9765-FC6F6BA49191
True
--> Removed [REGVAL] : HKEY_LOCAL_MACHINE\System\ControlSet00
rameters\Interfaces\{77AA1CC8-7643-4277-9765-FC6F6BA49191}\Dh
--> Removed [REGVAL] : HKEY_LOCAL_MACHINE\System\ControlSet00
rameters\Interfaces\{77AA1CC8-7643-4277-9765-FC6F6BA49191}\Dh
--> Removed [REGVAL] : HKEY_USERS\S-1-5-21-1953740922-1814211
Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\S
True
--> Removed [REGVAL] : HKEY_LOCAL_MACHINE\Software\Microsoft\
ion\Explorer\HideDesktopIcons\NewStartPanel\{20D04FE0-3AEA-10
D} - True
--> Removed [REGVAL] : HKEY_LOCAL_MACHINE\Software\Microsoft\
ion\Explorer\HideDesktopIcons\NewStartPanel\{59031a47-3f72-44
e} - True
06
C:\Users\mashrou7\Desktop>explorer

التشفير (نكريبشن(encryption[1]

تمهيد

تشفير المعلومات (إنكريبشن(Encryption ضمن إطار علم التعمية Cryptography هو عملية تحويل المعلومات من شكلها المقروء أو الواضح إلى شكل لا يمكن معه قراءتها أو معاينتها إلا للمخولين بذلك.

يفيد تشفير المعلومات إذا في اخفاء محتوى الرسائل المتبادلة بين شخصين عن أي شخص يتعرض هذه الرسالة ويحاول قراءتها. كما يفيد التشفير في ابقاء محتوى الملفات المشفرة غير مقروء في حال وقعت هذه الملفات في أيدي شخص أو أشخاص غير مخولين لقراءة محتواها كوقوع القرص الصلب في أيدي الاشخاص الخطأ.

كما لمرسل الرسالة أو لصاحب المعلومات المصلحة في ابقاء المعلومات والرسائل سرية كذلك هناك مصلحة لدى معترضي الرسائل لكسر تشفير الرسائل. كسر التشفير علم قائم بحد ذاته بدأ مع العالم الكندي الذي ابتكر طريقة لكسر تشفير قيصر هي طريقة التحليل الاحصائي Frequency Analysis مكنت مستخدمها من قراءة الرسالة المعترضة المشفرة بتشفير قيصر. هذا بدوره دفع إلى تطور وسائل تشفير أكثر "جودة" ما دفع علم كسر التشفير إلى الأمام وما يزال هذان العلمان يطاردا بعضهما حتى اليوم.

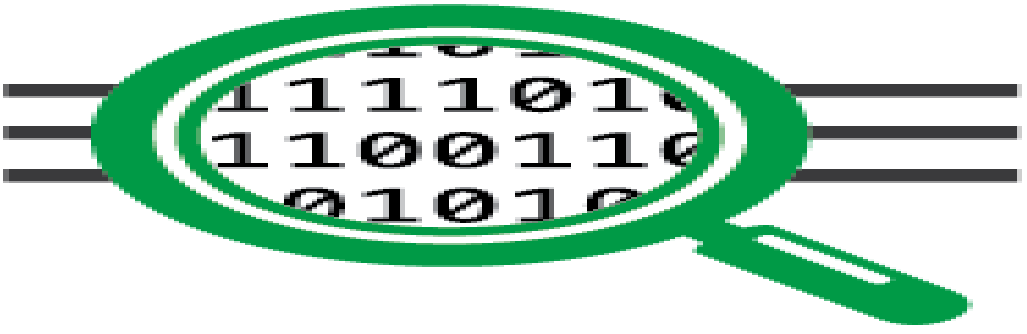
التشفير هو ترميز البيانات كي يتعذر قراءتها من أي شخص ليس لديه كلمة مرور لفك شفرة تلك البيانات. ويقوم التشفير بمعالجة البيانات باستخدام عمليات رياضية غير قابلة للعكس. ويجعل التشفير المعلومات في جهازك غير قابلة للقراءة من قبل أي شخص يستطيع أن يتسلل خلسة إلى جهازك دون إذن. ومن أشهر برامج التشفي

يستخدم التشفير في الحاسوب لغرض حماية المعلومات أثناء نقلها عبر شبكات الحاسوب , حيث يجري تشفيرها بطريقة يتفق عليها المرسل والمستقبل , لتحويل النص المفهوم لنص غير مفهوم . فقد كان قصدهم من استخدام التشفير هو إخفاء الشكل الحقيقي للرسائل حتى لو ... مثل الإنترنت- وعليه لا يمكن قراءتها من قبل أي شخص ما عدا الشخص المرسل لـه. .... الحاسوب لايعلمون شيئا عن البرامج الخبيثة أنواعها، الإختلافات بينها

1/أمن شبكة الحاسب وشبكة الانترنت تأليف: ابراهيم سامي

2/ نفس المرجع

● نظام التشفير[2]



عُرف علم التشفير أو التعمية منذ القدم، حيث استخدم في المجال الحربي والعسكري. فقد ذكر أن أول من قام بعملية التشفير للتراسل بين قطاعات الجيش هم الفراعنة. وكذلك ذكر أن العرب لهم محاولات قديمة في مجال التشفير. و استخدم الصينيون طرق عديدة في علم التشفير والتعمية لنقل الرسائل أثناء الحروب. فقد كان قصدهم من استخدام التشفير هو إخفاء الشكل الحقيقي للرسائل حتى لو سقطت في يد العدو فإنه تصعب عليه فهمها. وأفضل طريقة استخدمت في القدم هي طريقة القصير جوليوس وهو أحد قياصرة الروم. أما في عصرنا الحالي فقد باتت الحاجة ملحة لاستخدام هذا العلم "التشفير" وذلك لإرتبط العالم ببعضه عبر شبكات مفتوحة. وحيث يتم استخدام هذه الشبكات في نقل المعلومات إلكترونياً سواءً بين الأشخاص العاديين أو بين المنظمات الخاصة والعامة، عسكرية كانت أم مدنية. فلابد من طرق تحفظ سرية المعلومات. فقد بذلت الجهود الكبيرة من جميع أنحاء العالم لإيجاد الطرق المثلى التي يمكن من خلالها تبادل البيانات مع عدم إمكانية كشف هذه البيانات.

ومازال العمل والبحث في مجال علم التشفير مستمراً وذلك بسبب التطور السريع للكمبيوتر والنمو الكبير للشبكات وبخاصة الشبكة العالمية الإنترنت.

يتم حماية الشبكة اللاسلكية باستخدام بروتوكول تشفير الشبكات اللاسلكية (WEP). ويعمل هذا البروتوكول بتضمين مفتاح مشترك 64 أو 128 بت بين العملاء ونقطة الدخول، ومن ثم يتم استخدام هذا المفتاح لتشفير وفك تشفير البيانات بينهم، وهذا يوفر قدر كاف من الأمن للشبكات المنزلية. عليك الرجوع إلى الوثائق الخاصة بالأجهزة اللاسلكية لديك لتعرف كيفية تمكين وإعداد بروتوكول التشفير اللاسلكي (WEP) على شبكتك. أما بالنسبة لبيئات الشركات، فيجب اعتبار هذا البروتوكول (WEP) فقط كنقطة بداية للترتيبات الأمنية، وعلى الشركات البحث جدياً في ترقية شبكاتهم اللاسلكية إلى مستوى (WPA) أكثر أماناً.

ما هو التشفير أو التعمية (Cryptography) :

التشفير هو العلم الذي يستخدم الرياضيات للتشفير وفك تشفير البيانات. التشفير يُمكّنُك من تخزين المعلومات الحساسة أو نقلها عبر الشبكات غير الآمنة- مثل الإنترنت- وعليه لا يمكن قراءتها من قبل أي شخص ما عدا الشخص المرسل لـه. وحيث أن التشفير هو العلم المستخدم لحفظ أمن وسرية المعلومات، فإن تحليل وفك التشفير (Cryptanalysis) هو علم لكسر و خرق الاتصالات الآمنة.

التشفير هو ترميز البيانات كي يتعذر قراءتها من أي شخص ليس لديه كلمة مرور لفك شفرة تلك البيانات. ويقوم التشفير بمعالجة البيانات باستخدام عمليات رياضية غير قابلة للعكس. ويجعل

التشفير المعلومات في جهازك غير قابلة للقراءة من قبل أي شخص يستطيع أن يتسلل خلسة إلى جهازك دون إذن. ومن أشهر برامج التشفير (PGP)

أهداف التشفير:
يوجد أربعة أهداف رئيسية وراء استخدام علم التشفير وهي كالتالي:
1. السرية أو الخصوصية (Confidentiality) :
هي خدمة تستخدم لحفظ محتوى المعلومات من جميع الأشخاص ما عدا الذي قد صرح لهم الإطلاع عليها.
2.تكامل البيانات (Integrity) :
وهي خدمة تستخدم لحفظ المعلومات من التغيير (حذف أو إضافة أو تعديل) من قبل الأشخاص الغير مصرح لهم بذلك.
3.إثبات الهوية (Authentication) :
وهي خدمة تستخدم لإثبات هوية التعامل مع البيانات (المصرح لهم).
4.عدم الجحود (Non-repudiation) :
وهي خدمة تستخدم لمنع الشخص من إنكاره القيام بعمل ما.
إذاً الهدف الأساسي من التشفير هو توفير هذه الخدمات للأشخاص ليتم الحفاظ على أمن معلوماتهم.
أنواع التشفير :
حالياً يوجد نوعان من التشفير وهما كالتالي :
1. التشفير التقليدي. (Conventional Cryptography).
2. تشفير المفتاح العام. (Public Key Cryptography).

<u>تشفير الأقراص والملفات:</u>

برامج تشفير الأقراص هي برامج مصممة لحماية المعلومات الموجودة على الأقراص عبر تقنية تجعل المعلومات المخزنة على القرص مشفرة. تقوم هذه البرامج بإظهار محتوى الملفات المشفرة الموجودة على القرص المشفر عبر فك تشفيرها عند طلبها من قبل مستخدم يملك كلمة السر الصحيحة التي استخدمت لحماية المعلومات المشفرة من الوصول لغير المصرح لهم قراءة محتويات القرص.

برامج تشفير الأقراص يمكن أن تستخدم لاخفاء بيانات ضمن القرص المشفر بحيث يستطيع صاحب البيانات إخفاء حقيقة وجودها في حين لا يمكن لأحد إثبات وجود هذه المعلومات في ما يسمى الإنكار القابل للتصديق Plausible Deniability لتوضيح ذلك نفترض المثال التالي:

رامي ناشط لديه جدول بمعلومات مهمة جدا, يقوم رامي بانشاء قرص مشفر ويستخدم كلمة سر أولى لحماية هذا القرص ويضع معلومات غير مهمة جدا ضمن القرص المشفر. بعد ذلك يقوم رامي باخفاء الجدول ضمن القرص باستخدام كلمة سر ثانية. للأسف تم اعتقال رامي ومصادره حاسبه. يقوم المحقق بمعاينة الحاسب ويلاحظ وجود قرص مشفر. يقوم المحقق بتعذيب رامي للحصول على كلمة السر الخاصة بالقرص. رامي خوفا من التعذيب يقوم بذكر كلمة السر الأولى. التي يستهدمها المحقق لمعاينة

الملفات المشفرة, التي قلنا سابقا أنها غير مهمة جدا. لكن ما لا يعلمه المحقق أن القرص يحتوي معلومات مهمة مخفية لا يستطيع المحقق سؤاله عنها لعدم وجود دليل على وجودها. ويمكن لرامي أن ينكر وجودها في حال سؤل عنها دون أن يكون للمحقق أي دليل يشير إلى وجودها. ربما بقليل من الحظ تنقذ هذه الخاصية حياة رامي. أحد أكثر برامج تشفير الأقراص التي تملك هذه الخاصية هو برنامج تروكريبت TrueCrypt. ترو كريبت برنامج تشفير أقراص يعمل على أنظمة تشغيل متعددة, سهل الاستخدام وله سمعة طيبة. ويعطي مستخدمه امكانية تشفير المجلدات وأيضا تشفير الأقراص الصلبة والمحمولة. بالإضافة لذلك يوفر تروكريب أيضا امكانية الإنكار القابل للتصديق Plausible Deniability عبر المجلدات المخفية ضمن القرص المشفر. للمزيد حول البرنامج وطريقة استخدامه اتبع الرابط إلى صفحة برنامج تروكريبت TrueCrypt. هناك أيضا برامج أخرى لتشفير الملفات مثل برنامج AES Crypt. وهو برنامج سهل الاستخدام متوفر على أنظمة تشغيل متعددة يعتمد على معيار Advanced Encryption Standard AES لتشفير الملفات. لمزيد من المعلومات عن البرنامج وطريقة استخدامه اتبع الرابط إلى صفحة برنامج AES Crypt.

تشفير رسائل البريد الالكتروني:

تشفير رسائل البريد الالكتروني أمر ضروري جدا وأمر أساسي لضمان الخصوصية. لتشفير رسائل البريد الالكتروني يتم الاعتماد على بروتوكول PGP وهي الأحرف الأولى للكلمات Pretty Good Privacy التي تعني بالعربية: خصوصية جيدة جدا. يتيح بروتوكول PGP امكانية توقيع رسالة ما الكترونيا وتشفيرها. بحيث لا يستطيع فك تشفيرها إلا الشخص الموجهة إليه تلك الرسالة. تجري عملية التشفير على جهاز المرسل وعملية فك التشفير على جهاز المستقبل باستخدام ما يسمى المفاتيح. بروتوكول PGP يقوم بتشفير محتوى الرسالة لكنه للأسف لا يشفر عنوان البريد الالكتروني ولا حساب صاحب البريد الالكتروني ولا حساب المستقبل. للمزيد حول بروتوكول PGP واستخدامه اتبع الرابط: بروتوكول PGP من المهم جدا الانتباه أنه قد يتمكن الأشخاص المتطفلون على الخصوصية من ملاحظة وجود رسالة مشفرة أو أكثر (إذا استطاعوا اختراق حساب البريد الالكتروني مثلا أو إذا كان لديهم الإمكانية لمراقبة وارد البريد كأن يكون حساب بريدك الالكتروني ملكا لمزود خدمة تحت سلطة جهاز أمني استبدادي). وربما قد يدفهم ذلك لمزيد من التطفل أو حتى الانتقال إلى مستوى الملاحقة الجسدية حسب الوضع والقوانين والامكانيات والمعلومات المتوفرة لدى المتطفلين على الخصوصية مهما كانوا. لذلك قد يكون استخدام بروتوكول التشفير مضرا

✔ **-استخدام برامج التشفير واخفاء الهوية وحماية المجلدات[1]**

مثل Easy File & Folder Protector. Steganos Security Suite

ولإخفاء هويتك على الانترنت استخدم Steganos Internet Privacy برنامج Free Hide IP او proxy

---

Bill's Security Site.com – Encryption/1

الشهادة الرقمية[1]

● تعريف الشهادة الرقمية :

هي وثيقة رقمية تحتوي على مجموعة من المعلومات التي تقود إلى التحقق من هوية الشخص أو المنظمة أو الموقع الإلكتروني و تشفر المعلومات التي يحويها جهاز الخادم (server) عبر ما يسمى بتقنية
(Secure Sockets Layer //SSL]. طبقة مآخذ التوصيل الآمنة

مفاهيم أساسية:

✔المفتاح الخاص:

مفتاح سري يستخدمه صاحبه لفك تشفير الرسائل المرسلة له. وكذلك يستخدمه للتوقيع الالكتروني. ومن مسؤولية صاحبه المحافظة على سريته

✔المفتاح العام:

.مفتاح ليس سري يستخدم لتشفير الرسائل المرسلة لصاحب هذا المفتاح. وكذلك للتحقق من توقيعه

هيئة التوثيق (Certification Authority):

هي الجهة التي تقوم بإصدار الشهادة الرقمية والتوقيع عليها. قبل أن تقوم الهيئة بالتوقيع على الشهادة تتأكد من هوية الشخص (صاحب الشهادة) وتتم عملية التأكد من الهوية على حسب استخدامات الشهادة الرقمية فإذا كانت ستستخدم لحماية البريد الإلكتروني فيتم التأكد من هويته بعنوان البريد الإلكتروني فقط أما إذا كانت لاستخدامات حساسة مثل: إرسال مبالغ كبيرة من المال عن طريق الانترنت فهذه تتطلب حضور الشخص (صاحب الشهادة) إلى هيئة التوثيق للتأكد من هويته وتوقيع الشهادة. وكذلك من خلال هيئة التوثيق يستطيع الشخص أن يجدد شهادته المنتهية.
. وهي مواقع موجودة على الانترنت thwat و verysign و comodo ومن الهيئات

هيئة التسجيل (Registration Authority):

هي هيئات تساعد هيئة التوثيق وتخفف الضغط عنها في عمل بعض الوظائف مثل التحقق من .الهوية وإصدار التوقيع الإلكتروني

مخزن الشهادات الرقمية (Certificate Repository):

هو دليل عام متاح للكل تخزن فيه الشهادات الملغاة والفعالة بحيث يستفيد

الأشخاص من هذا الدليل للبحث عن المفتاح العام للشخص المراد التعامل معه سواء لتشفير الرسائل المرسلة له بمفتاحه العام لضمان السرية أو لفك التوقيع للتأكد من هوية المرسل

أهم المعلومات الموجودة في الشهادة الرقمية:

- الرقم التسلسلي: وهو الذي يميز الشهادة عن غيرها من الشهادات.
- خوارزمية التوقيع: الخوارزمية المستخدمة لإنشاء التوقيع الالكتروني.
- صالحة – من: تاريخ بداية صلاحية الشهادة.
- صالحة – إلى: تاريخ نهاية صلاحية الشهادة.
- المفتاح العام: المفتاح العام المستخدم لتشفير الرسائل المرسلة إلى صاحب الشهادة.
- مصدر الشهادة: الجهة التي أصدرت الشهادة.
- أسم مالك الشهادة: سواء كان شخص أو منظمة أو موقع الكتروني

a) **أنواع الشهادات الرقمية[2]:**

- **شهادات هيئة التوثيق:**

هذا النوع من الشهادات يصدر من هيئة التوثيق مباشرة وعادة ما يكون لحماية البريد الإلكتروني.

- **شهادات الخادم:**

هذا النوع من الشهادات يصدر من خادم الشبكة (web server) أو خادم البريد (mail server) للتأكد من أمان إرسال واستقبال البيانات.

- **شهادات ناشر البرامج:**

تستخدم للتأكد من أن البرامج الخاصة بناشر معين برامج آمنه.

b) معيار الشهادة الرقمية (X.509):

هو معيار عالمي أصدره اتحاد الاتصالات الدولي (ITU) لتوحيد شكل وبنية (format) الشهادة الرقمية. أكثر الشهادات الرقمية حاليا تتبع هذا المعيار .[3]
الفرق بين التوقيع الرقمي والشهادة الرقمية:
في التوقيع الرقمي لا يوجد ضمان أن المفتاح العام هو لهذا الشخص بالفعل مثلا يستطيع خالد أن ينشئ له مفتاحين عام وخاص ثم ينشر مفتاحه العام على أساس أنه أحمد فلو أراد شخص أن يرسل رسالة سريه لأحمد سوف يشفرها باستخدام المفتاح العام الذي نشره خالد وبالتالي سوف يستطيع خالد فك تشفير الرسالة والاطلاع عليها . أي أنه في التوقيع الرقمي لا يوجد ربط بين الشخص بالفعل ومفتاحه العام لذلك ظهرت الشهادة الرقمية والتي تربط بين الشخص ومفتاحه العام حيث تحتوي الشهادة على صاحب الشهادة ومفتاحه العام وموقعه من طرف موثوق فيه يثبت ذلك .

من المعروف للجميع ان التوقيع الرقمي او الشهاده الرقميه تحمي البرامج والملفات من التعديل عليها سواء كان ذلك من المستخدمين او من البرمجيات الخبيثه

لكن هناك بعض المستخدمين بمجرد رؤية التوقيع الرقمي في خصائص الملف يتم الحكم عليه بانه سليم ونظيف بدون التحقق من سلامة الشهاده الرقميه كهذه الملفات مثلا

وعند فحص الشهادة الرقميه هل هي فعلا سليمه ام لا

التوقيع غير صالح اي ان الشهاده تم ابطالها
لذا يجب التحقق من الملفات التي تحمل توقيع رقمي وخاصه ان هناك ملفات كانت من العينات التي نجري عليها اختبارات وتم الحكم عليها بانها سليمه ولم نتحقق من توقيعها الرقمي على انه صالح
الملفات التي تحتفظ بالتوقيع الرقمي عند فحص الشهاده الرقميه ان كانت التوقع صالح او لا بأس به فهنا يمكن الحكم على ان الملف سليم 100%

الجانب التطبيق

دورة حياة الشهادات الرقمية:

هناك بعض الأحداث التي تؤثر على فعالية الشهادة الرقمية مثل إضافة جهاز (hardware) جديد على الكمبيوتر أو تحديث برنامج وغيره لذلك أصبح للشهادة الرقمية حالات تمر فيها منذ إصدارها.

- الإصدار:

وهي أول مرحلة وتشمل التأكد من هوية الشخص قبل الإصدار. ويعتمد التأكد على نوع الشهادة المصدرة ففي الشهادات الرقمية التي تصدر للبريد الالكتروني يتم التأكد من هوية الشخص بطلب إرسال رسالة من بريده الالكتروني فقط أما الشهادات الرقمية المستخدمة للعمليات المالية فتتطلب إجرآت اخرى للتأكد من الهوية . بعد التأكد من الهوية يتم إرسال الطلب لهيئة التوثيق وتوافق على إصدار الشهادة.

- الإلغاء:

يستطيع الشخص أن يلغي شهادته قبل تاريخ انتهائها عندما يفقد المفتاح الخاص بالشهادة أو ينتشر لأنه بعد انتشار المفتاح الخاص تبطل فعالية الشهادة وهي الثقة بالطرف
الآخر.(Authentication) ويتم إضافة الشهادة الملغاة إلى قائمة الشهادات الملغاة.

- الانتهاء:

لكل شهادة تاريخ انتهاء بعد هذا التاريخ تصبح الشهادة غير صالحه للاستخدام ولابد من إصدار شهادة جديدة ويمكن أن تكون الشهادة الجديدة لها نفس المفتاح العام والخاص للشهادة المنتهية.

- التعطيل المؤقت:

يمكن للشخص أن يوقف أو يعطل استخدام الشهادة لفترة زمنية لا يحتاج فيها لاستخدام الشهادة حتى لا تستغل من قبل أشخاص آخرين [3].

كيفية الحصول على الشهادة الرقمية المستخدمة لغرض حماية البريد المثالي

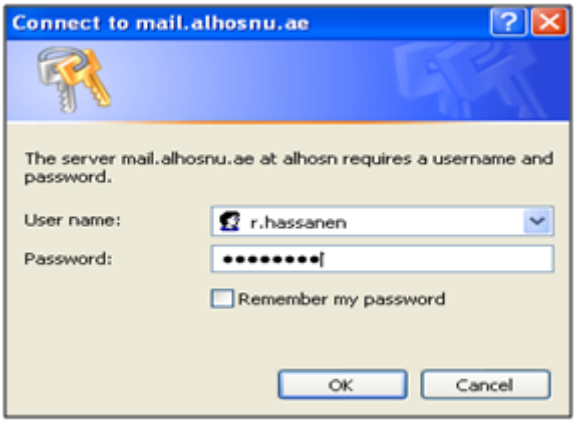
1. اذهب إلى احد المواقع الإلكترونية التي تمنح الشهادات على سبيل المثال .comodo
2. قم بتعبئة البيانات المطلوبة (الاسم الأول، الاسم الأخير، عنوان البريد الإلكتروني، البلد، الرقم السري

الخلاصة: إذا تعتبر الشهادة الرقمية من الوسائل الأمنية التي ساعدت على استخدام الانترنت سواء في التعاملات التجارية أو استخدام البريد الإلكتروني وغيرها بكل أمن

كلمات المرور Pass Words

لكل بيت مفتاح .. هكذا هي فكرة عمل كلمة المرور، فبدونها لا يمكن لأي شخص غير مخول بالدخول على شبكة المعلومات، وهي جواز مرور المستخدم إلى الشبكة، فكلمة المرور تثبت للشبكة بأنك أنت الشخص المخول للدخول إليها، وهي أبسط أنواع حماية المعلومات على شبكة المعلومات فهي تعمل على حماية معلوماتك الشخصية ومعلومات العمل الخاصة بك وسجلاتك الشخصية، وغيرها من البيانات، كما أنها في بعض الأحيان تكون حماية للأفعال مثل كلمة السر في المشتريات والحسابات البنكية وغيرها.
ومن أهمية كلمة المرور يجب علينا أن نحرص عليها وعند اختيارها يجب مراعاة ثلاثة أمور هي:-

- اختيار كلمة مرور صعبة ولا يسهل تخمينها.
- عدم إطلاع الغير عليها.
- تغييرها بشكل دوري.
- لا تجعل كلمة المرور كلمة واحدة مثل djamel.
- لا تضمن كلمة المرور بيانات شخصية عنك مثل تاريخ الميلاد.
- لا ينبغي أن تقل كلمة المرور عن عشرة خانات.
- اجعل كلمة المرور خليط بين الحروف والأرقام.



الأمن والسلامة على الإنترنت

على الرغم من الآفاق الواسعة التي فتحتها شبكة الإنترنت، وعلى الرغم من المتعة التي يعيشها المستخدم عند استخدامه لخدماتها أو حين ابحاره في صفحاتها، تبقى المشكلة العالقة هي كيفية تأمين الحماية الشخصية التي باتت هاجساً يشغل بال المستخدمين ومطوري صناعة خدمات الإنترنت على حد السواء.
تنقسم الحماية الشخصية على شبكة الإنترنت إلى قسمين هما:
1. السلامة.
2. الأمن.

1) فالسلامة هي توفير الحماية لضمان سلامة المستخدم نفسه من العرض للإستغلال أو الإبتزاز أو الإنتهاك أو الاساءة. علاوة على أنها اصطلاح يستخدم للإشارة إلى حماية الأطفال أثناء استخدامهم لشبكة الإنترنت.
2) أما الأمن فهو توفير الحمابة لضمان أمن المعلومات والبيانات والخصوصية الشخصية. وهي بذلك تشمل حماية الملفات والعتاد.

مخاطر شبكة الإنترنت:
لقد أصبح الاعتماد على شبكة الإنترنت كبيراً كواحدة من وسائل الاتصال الهامة في مختلف حقول الاستخدام بشكل أبرز أهمية التركيز على المخاطر التي قد تنتج جراء ذلك الاستخدام. فما هي مخاطر شبكة الإنترنت؟ هناك العديد من المخاطر بعضها جدي والبعض الآخر أقل جدية. وتتراوح تلك المخاطر بين الاصابة بالفيروسات المدمرة للبيانات والمعلومات المخزنة على الحاسوب. والاختراق للعبث بملفات المستخدم. أو استغلال حاسوبه بقصد الاساءة إلى آخرين. إلى سرقة البيانات الشخصية بقصد الإنتحال أو الإبتزاز. وسرقة بطاقات الإئتمان. وعلى الرقم من أنه ليست هناك ضمانات كاملة للحماية من المخاطر إلا أن هناك خطوات وقائية تحمي المستخدم من خطر الإصابة.

السلامة على الإنترنت:

1. اعرف جيداً مع من تتعامل قبل الكشف عن أية معلومات.
2. تجنب الافصاح عن أية معلومات شخصية في خدمات المشاركة الحية كغرف المحادثة والمنتديات.
3. احرص على استخدام اسم الاول فقط عند المشاركة في المحادثات أو المنتديات
4. احرص على عدم ارسال أية معلومات حساسة ككلمات السر وأرقام بطاقات الإئتمان عبر البريد الالكتروني، واعلم أن الجهات الرسمية لا تطلب تلك المعلومات عبر البريد الإلكتروني.

5. استخدم كلمات سر صعبة التخمين وتجنب المعلومات العامة كتواريخ الميلاد وأرقام السيارات أو الهواتف وأسماء الأبناء، وحاول المزج بين الأحرف الصغيرة والكبيرة والأرقام والرموز.
6. تجنب المنتديات المشبوهة والمعروفة بالمنتديات السفلية والتي عادة ما يجتمع فيها مخترقوا الأنظمة.
7. تجنب خاصية التخزين التلقائي للمعلومات الشخصية على الحواسيب التي لا تخصك في حال استخدامها.
9. تجنب الاحتفاظ بالصور والمعومات الشخصية على جهاز الحاسوب، واستخدم عوضاً لذلك ذاكرة التخزين المحمولة.
10. قم بفصل كاميرا الويب في حال عدم استخدامها.
11. استخدم كلمات سر للملفات الحساسة.
12. تجنب الرد على رسائل البريد الإلكتروني المشبوهة.

سلامة التعاملات التجارية:

عند القيام بعملية الشراء الإلكتروني عبر مواقع الويب، تأكد من الآتي:
1. استخدم المواقع التجارية المعروفة.
2. تاكد من أن الموقع يمتلك عنواناً فعلياً وأرقام إتصال.
3. اطلع على سياسة الموقع التجاري وشروط الخدمة.
4. عند الشروع في علمية الدفع بواسطة بطاقة الإئتمان، تأكد من ظهور صورة القفل (padlock) في أسفل الصفحة أو نافذة العنوان.
5. اضغط على القفل لتظهر لك معلومات الشهادة الإلكترونية، وتأكد أن الشهادة منحت لنفس عنوان الموقع.
6. تأكد من أن بادئة عنوان الموقع قد تغيرت من (http) الى (https).
7. تجنب العروض الترويجية غير المعروفة الواردة عبر البريد الإلكتروني.
8. يمكنك الاستعانة بميزة الدفع عن طريق طرف ثالث، كتلك التي توفرها شركات مثل (paypal) و (مونيبوكيرز money bookers).
9. استخدم بطاقات الإئتمان الإفتراضية التي تصدرها بعض المؤسسات المصرفية بدلاً من استخدام البطاقات التقليدية.

قم بتنزيل أحدث نسخة(إصدار)من المتصفح وذلك لأن الإصدارات القديمة بها العديد من الثقوب الأمنية

أمن الإنترنت

إن إمكانية الاتصال غير المسبوقة التي أتاحها عصر الإنترنت، أدت إلى فوائد اجتماعية واقتصادية هائلة، لكنها في الوقت نفسه فرضت العديد من التحديات الجديدة. وفي عالمنا المتصل تمامًا، لا تزال التهديدات المتعلقة بأمن الإنترنت تواصل تطوّرها، الأمر الذي يمنحها الأسبقية دومًا على أكثر الدفاعات تقدمًا.

خلفية

أدت تهديدات الأمن القائمة على الشبكة إلى انتشار عمليات سرقة الهوية والاحتيال المالي على نطاق واسع. ويعاني المستهلكون والشركات من مشاكل بالغة من جراء رسائل البريد غير المرغوب فيه، والفيروسات، وبرامج التجسس. كما أن الاختراق

الأمني يمكن أن يضر بالعلامة التجارية للشركات أو سمعتها بشكل يستحيل تدارك آثاره. وفي الولايات المتحدة، تعرقل المشاكل المتعلقة بأمن الإنترنت مسيرة التحول إلى استخدام السجلات الطبية الإلكترونية داخل البلاد. وفي الاتحاد الأوروبي، تشكّل ثقة المستهلكين فيما يتعلق بأمن الإنترنت وحماية البيانات عائقًا أمام التوسع السريع للتجارة الإلكترونية عبر حدود الدول الأعضاء. وتجدر الإشارة إلى أن الهجمات على المعلومات تشكّل اليوم عملاً مؤسسيًا مربحًا، ويُدار في الغالب بواسطة جماعات الجريمة المنظمة. وقد تم وضع عدد متزايد من نماذج الأعمال المتطورة القائمة على جرائم الفضاء الإلكتروني، بما في ذلك ظهور الشركات الإجرامية، بغرض بيع الأدوات والخدمات المخصصة لتنفيذ هجمات على الشبكات، بدلاً من مجرد بيع المعلومات التي يتم الحصول عليها من تلك الهجمات.

ولا تزال تقنية أمن الإنترنت تواصل تقدَّمها، متحوّلة عن الطرق السلبية القائمة على الحلول الجزئية إلى الطرق الإيجابية القائمة على حلول شاملة توفِّر إمكانيات التعرف على الهجوم واحتوائه والحجر عليه. إضافةً إلى ذلك، يتنافس موفرو خدمة الإنترنت (ISP) في تعزيز مستويات الأمن، كما يقدِّم موفرو الخدمة للمستهلكين من الأفراد حلول أمن الإنترنت كجزء من خدمتهم. ويركِّز صانعو السياسات حول العالم على حالة البنية التحتية للمعلومات. ويسعون إلى ضمان توظيف مستخدمي الشبكات لأفضل الممارسات المتعلقة بالتقنية والعمليات، وذلك لتأمين الشبكات إلى أبعد حد ممكن. كما تعمل الحكومات والشركات بصفة مستمرة على تحديث استراتيجياتها لمنع الهجمات، وتشكلت في هذا الصدد شراكات بين القطاعين العام والخاص لوضع نُهُج طوعية قائمة على السوق فيما يتعلق بأمن الإنترنت

عناصر أمن الإنترنت:

اليك هذه النصائح لزيادة مستوي الأمن لديك
والتي ينصح بها كل خبراء الحماية بالشكل التالي :

1. استخدم برامج مكافحة الفيروسات والجدران النارية (firewalls) لتأمين جهاز الحاسوب واعمل على تحديثها باستمرار. فعل جدارك الناري
فقط للذي بستخدم ويندوز اكس بي..
يوجد جدار ناري مرفق مع (Internet Explorer)
تستطيع تشغيله
2. استخدم برامج الكشف عن الملفات الخبيثة كملفات التجسس والملفات الدعائية والملفات التي تسيطر على متصفح الإنترنت.
3. افحص الملفات المنزلة من المواقع غير المعروفة أو خدمات مشاركة الملفات أو الواردة عن طريق البريد الإلكتروني.
4. لا تفتح الملفات المرفقة بالبريد الإلكتروني المجهولة المصدر.
5. استخدم مرشحات رسائل البريد الالكتروني (filters) وخدمات مكافحة البريد غير المرغوب فيه (anti-spam).
6 قم بعمل نسخ احتياطية للملفات بشكل دوري.
7 كن حذراً أثناء استخدام برامج المحادثة الفورية، وافحص الملفات التي تردك بواسطتها قبل فتحها.
8 استخدم مواقع فحص المنافذ (ports) للتأكد من عدم وجود منافذ مفتوحة للمخترقين، وتعرف تلك المواقع باسم (online port scanners).
9 قم بعمليات التحديث الضرورية والدورية لبيئة التشغيل المستخدمة لسد الثغرات الأمنية.
10. تجنب فتح حساباتك المصرفية على الشبكة أو إرسال أرقام بطاقات الائتمان عبر الشبكات اللاسلكية (wi-fi) غير الآمنة كالموجودة في المطارات والمقاهي على سبيل المثال.

11- اشتري نسخة أصلية وحديثة من نظام التشغيل وذلك لأن نظام التشغيل هو أساس الحماية..
12- قم بتنزيل أحدث نسخة(إصدار)من المتصفح وذلك لأن الإصدارات القديمة بها العديد من الثقوب الأمنية
13- تجنب تنزيل أو تحميل أي برامج أو ملفات ذات طبيعة تنفيذية خاصة من مصادر غير موثوق بها.

14- تجنب فتح الملفات المرفقة في الرسائل الإلكترونية من مصادر غير معروفة لديك
وخاصة إذا كانت ذات امتداد الملفات التنفيذية
مثل: exe-com-bat-pif-scr
إلا بعد فحصها ببرامج الحماية المحدثة

15-استخدام برامج التشفير واخفاء الهوية وحماية المجلدات
مثل Steganos Security Suite

Easy File & Folder Protector
ولإخفاء هويتك على الانترنت استخدم Steganos Internet Privacy

16- لا تقم بأي عملية شراء من شبكة الإنترنت دون التأكد من استخدام سيرفر آمن
و وجود علامة القفل المغلق في المتصفح وكذلك تغير
//:http:// To// https
وهنا تلاحظ وجود حرف (s)زيادة مما يعني انك تستخدم بروتوكول آمـن لنقل المعلومات
ولكن عليك بالتأكد من أنك تستخدم قوة تشفير 128 بت
وذلك لتوفير الأمان اللازم ويمكنك التأكد من قوة التشفير في متصفحك (إنترنت إكسبلورر)وذلك بالنقر على
Help
وهو موجود على الجانب الأيسر من شاشة المتصفح في أعلى الصفحة
ومن ثم اختيار
About Internet Explorer
وسوف تجد كلمة Cipher 128 bit
فإن لم تجد هذا الرقم ، قم بتنزيل نسخة جديدة من موقع ويندوز
17- تجنب الموافقة على حفظ اسم المستخدم وكلمات العبور في أي وقت
لأنك لو وافقت على ذلك فسوف تسهل العملية على الهاكرز؛ لأنه سوف يجدها مخزنة و جاهزة له
18- عدم زيارة المواقع المشبوهة مثل المواقع (الإباحية) فهي مرتع خصب لكل المصائب .
- قم بتحميل افضل البرامج للحماية..يعني:
- قم بتركيب أقوى جدار ناري مثل (zone alarm pro) وحدثه باستمرار .
- قم بتركيب أقوى مضادات الفيروسات مثل:
Kaspersky Antivirus Personal Pro V4 وحدثه باستمرار .
- قم بتركيب أقوى مضادات ملفات التجسس مثل The Cleanerوحدثه باستمرار .
- قم بتركيب أقوى مضادات الكوكيز مثل (AD-AWARE 6.0) وحدثه باستمرار.
19- مراقبة الاتصالات مع جهازك خلال الاتصال بالانترنت
من خلال احد البرامج المتخصصة مثل برنامج X- NETSTAT
20- الفحص الدوري للجهاز من خلال برامج الانتي فيروس
او مواقع الكشف الحي بالانترنت .
21- الاشترك في قوائم الأمن المشهورة مثل Bugtraq و NTbugtraq
22- أحذف الملفات المؤقتة للإنترنت من مجلد Temporary Internet Files
و داوم على تنظيف history للمواقع التى تتصفحها
وكذلك الحذف الدوري لمحتويات مجلد الكوكيز Cookies
23- لاتقم بتفعيل خاصية التصفح بدعم برمجيات الجافا من خلال المتصفح الا حال الحاجة القصوى لها
اذ لن يصيد أي كود دخيل مضر لجهازك وخصوصيتك أي من برامج الانتي فيروس
بالطريقة التالية:- افتح انترنت إكسبلورر قم بعملية مسح ملفات (كوكيزcookies) بين فترة وأخرى.

الخاتـــمة

من كل ماسبق ذكراه يبين لنا اهمية وضروره هذا الموضوع (أمن وحماية شبكات الحاسوب بعد معرفة وتوضيح برامج التروجان و الفيروسات تحديد أنواعها و والمخاطر والمهددات والثغرات الأمنية و تعريف خطرها على المستخدمين وكيفية الحماية منها، تبقى لنا أمر واحد مهم وهو ضرورة نشر الوعي التقني والأمني بين مستخدمي الانترنت حول هذه البرامج حتى لا يكونوا فريسة سهلة للمهاجمين. كما يجب التنبيه إلى حقيقة مؤلمة وهي أن المهاجمين يطورون أساليبهم وطرقهم باستمرار لذلك يجب الحذر منهم وإتباع وسائل الحماية الممكنة بعد التوكل على الله عز وجل أولا وأخيرا

وهكذا لكل بداية نهاية ، وخير العمل ما حسن آخره وخير الكلام ما قل ودل وبعد هذا الجهد المتواضع أتمنى أن أكون موفقا في سردي للعناصر السابقة سردا لا ملل فيه ولا تقصير موضحا الآثار الإيجابية والسلبية لهذا الموضوع الشائق الممتع ، وفقني الله وإياكم لما فيه صالحنا جميعا

وفي النهاية لا أملك إلا أن أقول أنني قد عرضت رأيي وأدليت بفكرتي في هذا الموضوع لعلي أكون قد وفقت في كتابته والتعبير عنه وأخيراً ما أنا إلا بشر قد أخطئ وقد أصيب فإن كنت قد أخطأت فأرجو مسامحتي وإن كنت قد أصبت فهذا كل ما أرجوه من الله عزوجل.

اتمني من الله العلي القدير ان اكون نلت اعجابكم فان اصبت فانه من عند الله وان اخطات فانه ومن الشيطان

تقبلوا خالص تحياتي :

الموضـــــــوع	الصفحة

فهرس المحتويات

الموضـــــــــوع	الصفحة

الفصـل الثالث:الحماية الحاسوب

مذكرة تخرج لنيل شهادة تقني سامي إعلام آلي : صيانة الأنظمة المعلوماتية و الشبكات

عنوان المذكرة: أمن وحماية شبكات الحاسوب

الجمهورية الجزائرية الديمقراطية الشعبية
وزارة التكوين والتعليم المهنيين
مديرية التكوين المهني لولاية الجلفة

بمسعد- بال

مذكرة التخرج لنيل شهادة تقني سامي
المعلوماتية: خيار صيانة الأنظمة المعلوماتية و الشبكات

تحت عنوان

أمن وحماية شبكات الحاسوب

من إعداد المتربصين:

تحت إشراف الأس

سالم بو

لدفعة
2015/2016

الشبكات الحاسوب :

الفصل الأول

فيروسات الحاسوب

الفصل الثاني

الحـــماية الحاسوب

الفصـل الثالث