الفصل الثاني :

التهديدات و نقاط الضعف والهجمات

مقدمه : الآن بعد أن استعرضنا أساسيات بروتوكول Tcp /IP يمكننا المضي قدماً في مناقشتنا للتهديدات ونقاط الضعف والهجمات .

ومن المهم أن نفهم الفرق بين التهديد، نقاط الضعف او الهجوم في سياق أمن الشبكة .

• التهديدات :

التهديد أي شيء يمكن أن يعطل العمل ، الوظائف ، سلامه المعلومات ، أو توافر الشبكه أو النظام . ويمكن هذا أن يأخذ أي شكل ويمكن أن يكون فعل متعمد - عرضي - أو نسبا عن فعل الطبيعه .

• نقاط الضعف " الثغرات "

الثغره " نقطه الضعف " : هو الضعف المتأصل في التصميم أو التكوين او التشغيل أو إداره الشبكه أو النظام الذي يجعله عرضه للتهديد .

نقاط الضعف هو كل شيء يجعل الشبكات عرضه لقتراب المعلومات. والتوقف

كل شبكه وكل نظام به نقاط ضعف من نوعاً ما .

• الهجمات :

الهجوم هو تقنيه معينه تستخدم لاستغلال الثغرات ، على سبيل المثال يمكن أن يكون التهديد الحرمان من الخدمه ، على سبيل المثال ثغره في تصميم نظام التشغيل ، ومثال الهجوم يمكن أن يكون من نوع " الاتصال القاتل "

هنا لك فئتين عامتين من الهجمات :

* هجمات سلبيه * هجمات نشطه

+ الهجمات السلبيه : من الصعب جداً اكتشافها ، لأنه لا يوجد نشاط واضح يمكن مراقبته أو الكشف عنه ، من امثله الهجمات السلبيه تحسس حزمه البيانات أو تحليل البيانات عبر الشبكه .

لقد صممت هذه الأنواع من الحيات لمراقبة حركة المرور للبيانات في الشبكة وتسجيلها، وعادة ما تستخدم لجمع المعلومات التي يمكن استخدامها في وقت لاحق في الهجمات النشطة.

+ الحيات النشطة: كما يوحي الاسم، فإنها تتخذ إجراءات أكثر وضوحًا في الشبكة أو النظام، ونتيجة لذلك فإنه من السهل اكتشافها، ولكنها في الوقت نفسه فإنها يمكن أن تكون أكثر تدميرًا للشبكة. ومن الأمثلة على هذا النوع من الهجوم هو هجوم الحرمان من الخدمة.

الشبكات والأنظمة تواجه العديد من أنواع التهديدات والهجمات مثل: الفيروسات - الديدان - أحصنة طروادة - فخ الأبواب - الاحتيال - التنكر - كسر كلمة المرور - الهندسة الاجتماعية - المسح - التجسس - القنابل الحرب - هجمات الحرمان من الخدمة - الهجمات الأخرى على البروتوكول.

ويبدو أنه يتم تطوير أنواع جديدة من التهديدات كل شهر

* بعض مخاطر الشبكة:

كما قلنا تحدث الشبكة الأمنية عندما يتم اختراق النظام من خلال أحد الهجمات أو المتسللين (الهاكر) أو الفيروسات أو نوع آخر من أنواع البرامج الخبيثة، إن أكثر الناس المستهدفين في الاختراقات الأمنية هم الأشخاص الذين يقومون بتصفح الإنترنت، حيث يتسبب الاختراق في مشاكل مزعجة مثل: البطء في حركة التصفح وانقطاعه على فترات متقطعة، ويمكن أن يتعذر الدخول إلى البيانات. وفي أسوأ الأحوال يمكن اختراق المعلومات الشخصية للمستخدم. وفي حالة وجود أخطاء برمجية أو إعدادات خاطئة في نظام التشغيل، فمن الجائز أن تسمح بدخول المستخدمين الغير مصرح لهم من قبل إلى الوثائق السرية المحتوية على معلومات شخصية أو الحصول على معلومات حول الجهاز الخاص بالمخادم مما يسمح بحدوث اختراق للنظام.

كما يمكن لهؤلاء الأشخاص تنفيذ أوامر على جهاز الخادم المضيف مما يمكنهم من تعديل النظام وإطلاق هجمات إغراقية مما يؤدي إلى تعطيل الجهاز مؤقتاً.

إن الهجمات الإغراقية تستهدف إبطاء أو شل حركة مرور البيانات عبر الشبكة، كما أنه في حالة الهجمات الإغراقية الموزعة، فإن المعتدي يقوم باستخدام عدد من الكمبيوترات التي يسيطر عليها للهجوم على كمبيوتر أو أكثر من شبكة ما.

مع ملاحظة أنه يتم تركيب البرنامج الرئيسي للهجمات الإغراقية الموزعة في أحد الأجهزة وذلك باستخدام حساب مسروق.

إن التجسس على بيانات الشبكة واعتراض المعلومات التي تتنقل بين الخوادم واستعراضها يمكن أن يصبح أمراً ممكناً إذا تركت الشبكة أو الخوادم مفتوحة ونقاط ضعفها مكشوفة.

فيما يلي سيتم مراجعة أنواع التهديدات العامة التي تواجه مسؤولي الشبكة كل يوم، بما في ذلك وصف محدد لعدد محدد من الهجمات المعروفة على النحو التالي:

(A) الفيروسات The Virus

وفقاً لاقتصاديات الحاسوب الأمريكية ComputerEcomomics "مجموعة متخصصة في تحليل وأبحاث الحاسوب" فإن الأثر 12 مليار دولار المنفقة على مستوى العالم في عام 1999 نتيجة لفيروسات الحاسوب.

الفيروس هو برنامج غير مرغوب فيه يدخل إلى الجهاز أو النظام دون إذن ويقوم بإدخال نسخ منه في برامج الشبكة.

والفيروس هو أحد البرامج الخبيثة أو المتطفلة. والبرامج المتطفلة الأخرى تشمل الديدان أو أحصنة طروادة أو برامج الدعاية أو برامج التجسس.

إن الفيروس لا يمكن أن يعمل بشكل مستقل، فهو برنامج أو جزء من تعليمات برمجية تتمتع بخاصية الانتشار الذاتي.

٩

ويطلق عليه اسم فيروس لأنه شل نظرية البيولوجي فيما يخص التصنيف لكي يعمل. في حالة فيروس الكمبيوتر فإن الملف هو بمثابة البرنامج الذي يثبت الفيروس نفسه فيها.

عادة ما ينتشر الفيروس عن طريق تنفيذ برنامج مصاب أو عن طريق إرسال ملف مصاب إلى شخص آخر، وعادة ما يكون ذلك عن طريق البريد الإلكتروني.

ومن أهم الفيروسات التي تتمثل برامج خبيثة أكثر انتشارًا نوعين:

- الأول: هي برامج خبيثة التي تكون هدفها الإضرار بمن الأشخاص والإضرار على استخدامات الجهاز وتعطيله وتسبب في إحداث انقطاعات وأعطال في أوقات منتظمة، وتعدل البرامج والمواقع المختلفة التي قد يرغب المستخدم في الدخول إليها.
- الثاني: هي برامج خبيثة الأكثر خطورة التي تعتبر أدق أصعب شكل أمنية من خلال الحصول على معلومات الشخصية من رسائل البريد الإلكترونية والبيانات الأخرى المخزنة بجهازك.

← أما بالنسبة لبرامج الدعاية وبرامج التجسس فهي مزعجة بالغالب وتؤدي إلى ظهور نوافذ دعائية منبثقة على الشاشة، كما أن برامج التجسس تجمع معلوماتك الشخصية وتقدمها إلى جهات أخرى تطلب الحصول عليها لأغراض تجارية.

⊛ أنواع أو أنماط الفيروسات:

- الفيروسات التقليدية Classic virus: وهي برامج صنعت تخريب لبيانات ومعلومات أعطال أو أخطار فيه بشكل روتيني.
- فيروسات تقدم باستخدام أسلوب الاختفاء بالملفات: حيث أنه يقتبس جزء من الكود البرمجي إلى الملف فيصبح ويصبح جزء منه، وبشكل عام تصنع الفيروسات فيروسًا وتعديلات في التركيب بشكل

تمنع المستخدم من استخدام ادارة المهام واظهار الملفات المخفية و
ملفات النظام.

- فيروسات الملفات File Viruses

هذه الفيروسات تتبع واحداً على الأقل من هذه الأساليب لإصابة النظام.

١- فيروسات مختصة تصيب الملفات التنفيذية، وفي هذه الحالة عندما
يتم اكتشافه من قبل مضاد الفيروس فإنه يعطيك خيارات التصليح:
(Disinfect, Cure, Repair,... etc
حيث يختلف حسب نوع مضاد الفيروسات الذي تستخدمه.
ومن أشهر هذه الفيروسات المختصة هو فيروسات سالتي أو المسمى
sality وفيروس Mabezat، وللأسف أكثر الفيروسات من هذا النوع.

٢- فيروسات تكرر الملفات الموجودة على الجهاز Duplicate Files
حيث تملئ ذاكرة الجهاز بسبب تكرار الملفات "تخيل لديك ملفات
وبيانات مشتركة وتملئ 75% من ذاكرة الجهاز، فإذا أعدنا الفيروس
بنسخ كل ملف مرة واحدة فقط تكون النتيجة الجهاز لا يملك ذاكرة كافية!!
وكمثال لبعض الفيروسات لفيروسات الشركات مثل فيروس Temp.exe

٣- فيروسات تقوم بنسخ نفسها في مسارات مشهورة بالجهاز
systemdrive%، SystemRoot%، Temp%، %
etc ...، Userprofile%

٤- فيروسات تستخدم ميزات ملفات النظام

أ- Viruses Boot Sector: وهي فيروسات تصيب الملفات المسؤولة عن
اقلاع الجهاز والنظام، فتقوم بنسخ نفسها إلى ملفات الإقلاع، وقد تغير
مسار تلك الملفات. ولا تصيب إلا الأقراص المرنة.
وهذه الفيروسات انتشرت في الثمانينات من القرن الماضي، ولكن مع تقدم
معالجات 32bits وتناقص استخدام الأقراص المرنة تضاءل عدد هذا النوع
إلا أنه من الممكن عكسه أثناء هذا فيروسات تصيب الـ CD وعلى
العلامات.

6

ب- Viruses Macro : وهذه الفيروسات تصيب ملفات محررات النصوص مثل Ms worde - MsExel - Point Pwer

وهذا النوع غير منتشر ونادر

مثال عليه : أحد الفيروسات ما إن تفتحه بالجهاز حتى يمحي كل ملفات الاوفس التي تعمل بالجهاز حتى ولو كانت محزنه.

ج- Script Viruses : وهي فيروسات تستخدم الاكواد واللغات زمرية دد جافا سكريبت - فيجوال بيسك سكريبت ، php ، ملفات باتش ....) وهي تصيب النظام وتؤدي إلى تحويل الاكواد إلى عمليات تخل بالنظام.

(B) - الدوده

الدوده هو برنامج قائم بذاته ومستقل وعاده ما يكون مصمم لينتشر أو يولد نفسه على الأنظمه المصابه ويسعى إلى أنظمه أخرى عبر الشبكات المتاحه. الفرق الرئيسي بين الفيروس والدوده هو أن الفيروس برنامج غير مستقل.

عموماً، هناك سلالات جديده من الحشرات، التي تم فيها طمس الفرق بين الفيروسات والديدان. مثال على ذلك الهجين الجديد: فيروس ميليسا.

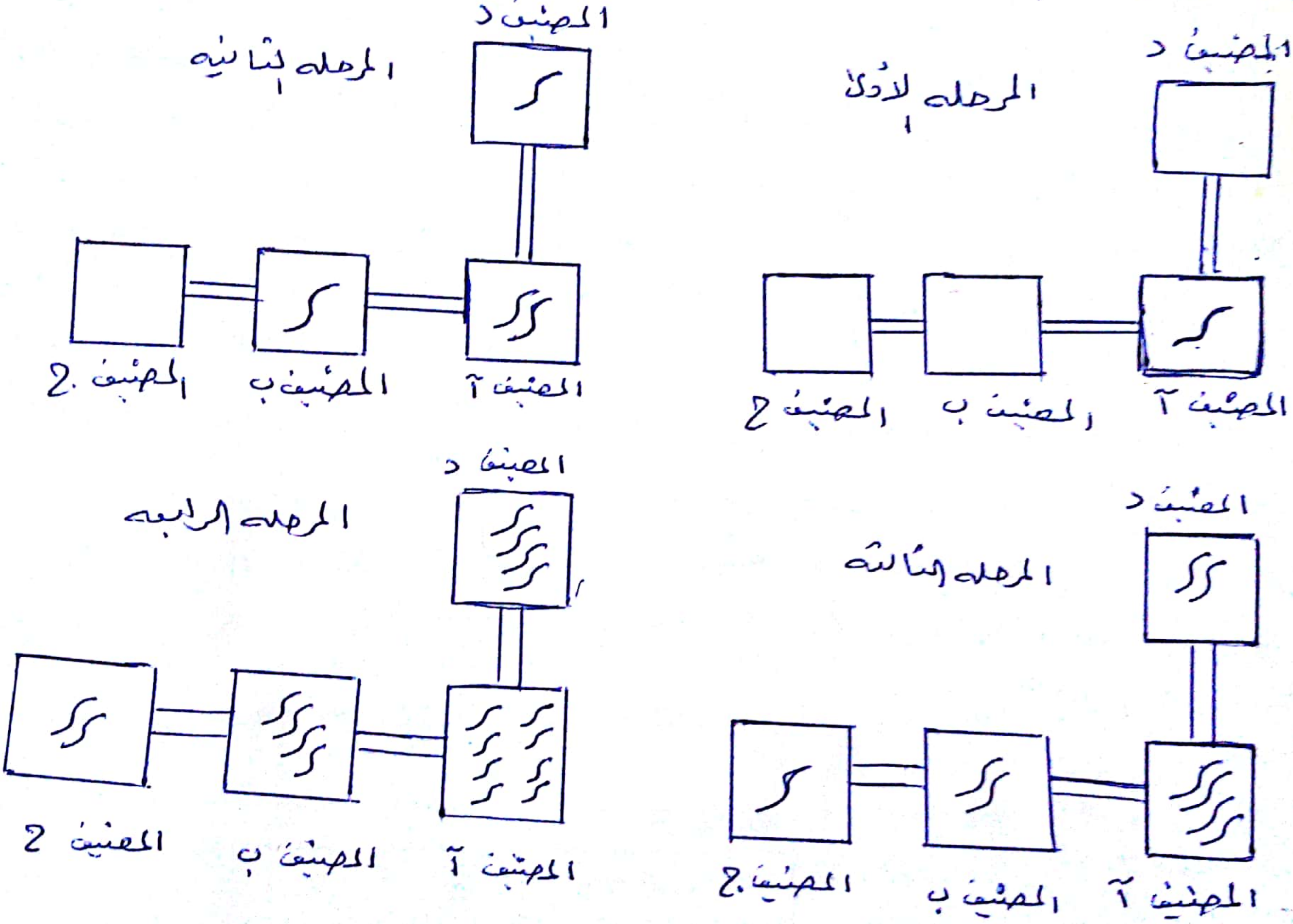
في عام 1999 هاجم فيروس ميليسا العديد من مستخدمي منتجات مايكروسوفت وقد انتشر في البدء كفيروس، ولكن الفيروس واصل الانتشار كعمليه نشطه بدأها الفيروس بنفسه.

واحده من الديدان الأولى وربما الأكثر شهرة هي دوده الانترنت التي صممت واطلقت بواسطه روبرت موريس عام 1986.

كتب موريس برنامج دوده اطلقه في الانترنت. كانت عمليات الدوده جديده نسبياً، لكنها لا تزال لها تأثير مدمر على الانترنت. وقد تم تصميم الدوده لتقليد نسخ نفسها ولتصيب الأنظمه الأخرى.

طالما يتطلب البرنامج فإنه يقوم بتوليد ~~[crossed out]~~ وإجراء عمليه أخرى، وبواسطه العمليه الأخرى هو عمل وتشغيل نسخه أخرى من البرنامج، ثم يقوم البرنامج بالبحث عن أنظمه أخرى متصله بالنظام المصاب وينشر نفسه إلى الانظمه الأخرى في الشبكه.

نمو عدد العمليات الجارية حتى يصبح هناك "عدد لا نهائي". والشكل التالي يوضح كيف تنمو دودة الانترنت وتنتشر.



عملية واحدة تتوالد لتصبح عمليتين ، عمليتين تتوالد لتصبح أربع عمليات ، أربع عمليات تتوالد لتصبح ثمانية.

ان ذلك لن يستغرق وقتاً طويلاً جداً حتى يتم استهلاك وحدة المعالجة المركزية وموارد الذاكرة ثم يتعطل النظام. وبالاضافة لذلك ، في كل مرة تتوالد العمليات مرة أخرى ، فان الدودة "العمليات" تبحث عن وصلة خارج الشبكة وقد تم تصميم الدودة لتنتشر وتبحث عن أنظمة أخرى لتصيبها ثم تكرر العملية. وقف العمليات من التكاثر مسألة بسيطة وهي اعادة تشغيل النظام ، ومع ذلك وجد مسؤولو النظام انه يمكنهم عمل أي شيء ثم تعمل بصورة طبيعية عند اعادة تشغيلها ، إلا أنها تصاب بالعدوى مرة أخرى من قبل جهاز آخر مصاب في الانترنت. ولوقف الدودة من اصابة الأنظمة على الشبكة كان لابد من إغلاق جميع الاجهزة في الوقت نفسه أو فصلها عن الشبكة ، وقدرت تكلفة تنظيف دودة الانترنت بعشرات الملايين من الدولارات. اعتقل موريس وقدم للمحاكمة وكانت ادانته.

C- أحصنة طروادة

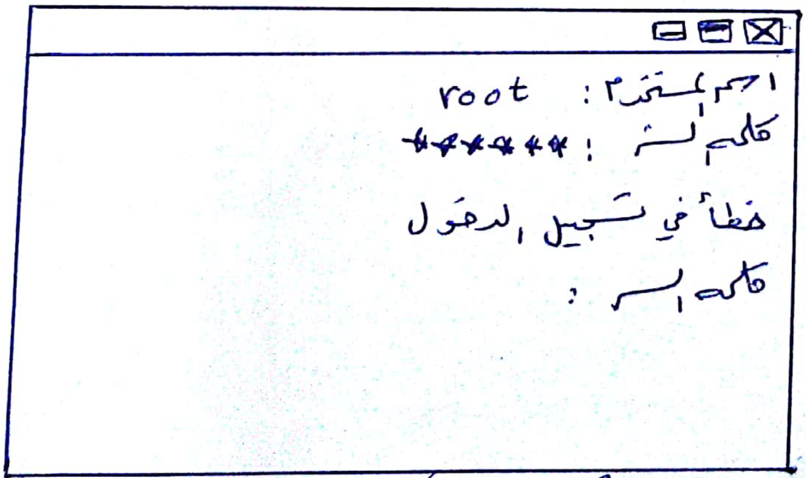
• حصان طروادة هو برنامج أو جزء من شيفرة برنامج يختفي داخل البرنامج الاساسي وينفذ وظيفته، هذا النوع من التهديد حصل على اسمه من الاساطير اليونانية وقصة حصان طروادة تحكي القصة كيف غزى أوديسيوس ورجاله طروادة عن طريق الاختفاء داخل حصان خشبي عملاق.

يختفي حصان طروادة نفسه داخل برنامج آخر أو يختفي في هيئة برنامج آخر ويتم ذلك عن طريق تعديل البرنامج الحالي أو ببساطة عن طريق استبدال البرنامج القائم بواحد آخر جديد.

يعمل حصان طروادة بنفس الطريقة التي يعمل بها البرنامج الحالي المشروع. ولكنه عادة مايؤدي وظائف الأخرى أيضاً مثل تسجيل المعلومات لحسابه أو لغرض مخرب.

مثال ذلك: برنامج سرقة كلمة السر: برنامج سرقة كلمة السر هو برنامج صمم ليظهر وكأنه واجهة المستخدم الطبيعية لادخال كلمة السر التي تكفل للمستخدم عند بدء النظام.

مثال لذلك: في شاشة البيئة أدناه أدخل المستخدم اسم المستخدم وكلمة السر الصحيحة ومع ذلك النظام أخبر المستخدم أن معلومات الدخول غير صحيحة. عندما يحاول المستخدم مرة ثانية استعملت كلمة السر واستطاع هو ان تسجيل الدخول للنظام.



تسجيل الدخول عن طريق حصان طروادة

الحقيقة في هذا المثال حصان طروادة صمم لسرقة كلمات السر، حيث يتم استبدال برنامج الدخول التنفيذي Login.exe ببرنامج حصان طروادة. حيث يبدو مثل شاشة الدخول الاساسية، ولكن ما حدث في الواقع أن شاشة الدخول الاولى كانت حصان طروادة وعندما تم ادخال اسم المستخدم وكلمة المرور تم تسجيل المعلومات وتخزينها ثم عرض برنامج حصان طروادة على رسالة "معلومات الدخول غير صحيحة" ثم وجه بعدها المستخدم إلى برنامج تسجيل الدخول الحقيقي. وببساطة يفترض المستخدم انه اخطأ في كتابة كلمة السر بالمرة الاولى ولا يعلم أبداً أن اسم المستخدم وكلمة المرور للتو قد سرقت.

٥) فتح الابواب : Backdoors : وهي الأخطر لأنها تأخذ صلاحيات مدير نظام وتعمل بسرية تامة وبدون علم المستخدم . وتستخدم بشبكة محلية أو بشبكة الانترنت للتحكم بجهاز الضحية وتتبع سلوك أدوات مدير النظام .

RAT = Remote Administrator Tool

الفرق الاساسي والوحيد بين التروجانات (Trojans) وبرامج الادارة هو أن التروجانات تنزل وتعمل بدون علم المستخدم بينما أدوات الادارة تكون واضحة وتطلب رسالة أنها تراقب النظام . وهذا النوع يستخدم للتحكم ببروتوكول TCP/IP وهو نفس البروتوكول المستخدم بالمتصفح وإدارة مقاهي الانترنت .

وهذا النوع يتكون من جزئين : - الأول جهاز الضحية الذي يتلقى الاوامر من المخترق
- الثاني عند المخترق الذي يبعث التروجان

الخطورة بهذا النوع تكمن في :
- ارسال واستقبال الملفات من وإلى جهاز الضحية
- الدخول للملفات الخاصة ومعاينتها حذفها أو تعديلها
- توجيه المستخدم الضحية الى موقع انترنت بدون إرادته وتغيير الصفحة الرئيسية .
- سرقة المعلومات الخاصة وكلمات السر
- تشغيل البرامج والاجهزة المرتبطة بالجهاز كالطابعة أو كاميرا ...)
- اعادة تشغيل الجهاز واطفاؤه .

٦) قنابل المنطق : القنبلة المنطقية هي برنامج أو جزء من برنامج صمم حسب نوايا سيئة ، ويشار إليه بقنبلة المنطق لأنه يتم تشغيل البرنامج عند حدوث بعض الظروف المنطقية . تقريباً هذا النوع من الهجوم يرتكب من الداخل من شخص حاصل على إذن الدخول للشبكة .
الجاني ممكن أن يكون مبرمجاً أو بائع يزود بالبرامج

٧) مسح المنافذ : مثل لص يرصد هدفاً يخطط للسرقة ((مرقبة)) غالباً ما يرصد القراصنة حالة نظام ما لجمع معلومات ممكن أن يستخدمها لاحقاً في مهاجمة النظام .
أحدث الأدوات التي غالباً ما يستخدمها القراصنة لهذا النوع من الاستطلاع هو ماسح المنافذ .

برنامج ماسح المنافذ هو برنامج يتصنت على منافذ ذات أرقام معروفة للكشف عن الخدمات التي تعمل حالياً في النظام والتي يمكن استغلالها لاقتحام النظام.
هناك العديد من برامج مسح المنافذ متاحة على شبكة الانترنت في مواقع مختلفة، والحصول عليها أمر يسير.
ويمكن للمنشآت مراقبة ملفات سجل النظام من أجل كشف مسح المنافذ كمؤشر تمهيداً للهجوم. معظم برمجيات كشف التسلل تعمل على مراقبة مسح المنافذ. إذا اكتشفت أن منافذ النظام الخاص بك تم مسحها، فيمكنك تتبع المسح إلى نقطة نشأته.
ولكن بعض برامج مسح المنافذ تأخذ شكلاً أو نمطاً أكبر للتخفي للمسح، لذلك من الصعب جداً كشفها "ومثال ذلك استخدام مسح تزامن SYN"

- الانتحال "التحايل":
الانتحال أو التحايل يغطي أنواع واسعة من التهديدات. والصورة عامة الانتحال يستلزم تزوير هوية فرد أو التنكر في هيئة فرد أو كيان آخر من أجل الدخول في النظام أو الشبكة للحصول على معلومات من أجل بعض الأهداف غير المسموح بها.
هناك العديد من أنواع الانتحال المختلفة: ● هذا هو عنوان الانترنت IP
● اختطاف طلب اتصال ● محاكاة تسلسل الأرقام ● محاكاة خدمة اسم النطاق DNS
● محاكاة عنوان الانترنت IP

لكل جهاز في شبكة الـ TCP / IP عنوان انترنت فريد من نوعه IP
عنوان الانترنت (IP) هو عنوان فريد من نوعه للتعرف على الجهاز ولا يمكن أن يكون لجهازين في الشبكة نفس العنوان IP.
يتم تنسيق عناوين الانترنت IP على هيئة أربعة أرقام عشرية مفصولة بنقاط على سبيل المثال 147.34.28.103.
انتحال عنوان الانترنت IP يستفيد من الأنظمة والشبكات التي تعتمد على عنوان الانترنت IP لربط الأنظمة والأجهزة والمصادقة على سبيل المثال: أجهزة التوجيه الخاصة بتصفية حزم المستخدمة أحياناً لحماية الشبكات الداخلية من الشبكات الخارجية الغير موثوق بها.

هذه الموجهات تسمح فقط للعناوين انترنت IP محددة لحزم الشبكة الخارجية إلى الشبكة الداخلية، إذا استطاع القرصان تحديد عنوان انترنت IP مسموح له بالعبور من خلال جهاز التوجيه، فإنه يقدر على انتحال عنوان انترنت الشبكة الخارجية للوصول للشبكة الداخلية ومن الواضح استطاع الهاكرز تقمص الشخصية لشخص آخر.

- انتحال الأرقام التسلسلية
الشبكات TCP/IP تستخدم أرقام متسلسلة. الأرقام التسلسلية هي رمز لكل عملية نقل ويتم تبادلها مع كل معاملة. ويستند رقم التسلسل على الساعة الداخلية لكل كمبيوتر، ويمكن التنبؤ بالعدد لأنه يقوم على مجموعة من الخوارزميات.
من خلال رصد اتصال الشبكة، يمكن للقرصان تسجيل الأرقام التسلسلية المتبادلة وتوقع المجموعة التالية من الأرقام التسلسلية. ومع ذلك ومع هذه المعلومات يمكن القرصان من إدخال نفسه في اتصال الشبكة وعلى نحو فعال يمكنه التحكم أو إدراج معلومات خاطئة.
هو أفضل وسيلة للدفاع ضد انتحال أرقام التسلسل هو تشفير الاتصال حيث يمنع أي شخص قد يكون مراقب الشبكة من التعرف على تسلسل الأرقام أو أي معلومات مفيدة أخرى.

- قرصنة طلب الاتصال:
خطف طلب الاتصال مشابه لانتحال على أرقام التسلسل.
في هذه العملية يتولى القرصان على طلب الاتصال، عادة تكون بين مستخدم وخادم ملفات، وغالباً ما يتم هنا عن طريق الوصول إلى جهاز توجيه أو بعض الأجهزة الشبكة الأخرى التي تعمل كبوابة بين المستخدم الشرعي وخادم ملفات عن طريق احتيال عنوان الانترنت IP
بما أن قرصنة الطلب عادة ما يتطلب من القرصان الحصول على امتياز الدخول إلى جهاز الشبكة. أفضل وسيلة دفاع يمكن اتخاذها هي تأمين جميع الأجهزة في الشبكة بشكل جيد.

- خدمة اسم النظام DNS
خدمة اسم النظام DNS هي خدمة هرمية تستخدم مع مجموعة بروتوكول TCP/IP ويتم توزيعها وتكرارها على الخوادم عبر الانترنت

وتستخدم في شبكة الانترنت وكذلك الشبكات الداخلية Intranet وذلك لتوجيه عناوين الانترنت IP إلى اسماء وصفية.
كما يمكن التفكير في اسم النطاق DNS كجدول بحيث يسمح للمستخدمين بتحديد أجهزة الحاسوب الذاتية بواسطة اسماء الوصفية بدلاً من عناوين الانترنت IP.
وميزة DNS في أنه ليس من الضروري أن يكون لديك معرفة لعناوين الانترنت IP لجميع مواقع الانترنت للوصول إليها.
كما يتم تهيئة اسم النطاق DNS لاستخدام سلسلة من أسماء الخوادم استناداً إلى النطاقات في الاسم المقصود، حتى يتم العثور على اسم مطابقة.
برنامج خادم اسم النطاق DNS الشائع الاستخدام في شبكة الانترنت هو BIND DNS، ويخضع لعدة عمليات احتيال، أنتشرهما شائعتا الاستخدام من هذه العمليات: ١- الرجل في المنتصف
٢- تسميم اسم النطاق DNS
وهناك عملية أكثر شيوعاً وهي اعادة توجيه رحلة الانترنت URL

٣- رجل في المنتصف
في هجوم الرجل في المنتصف فإن القراصنة يضع نفسه بين برنامج المستخدم وخادم الشبكة.
وبذلك يمكن للقرصان اعتراض المعلومات التي تم ادخالها من قبل المستخدم مثل:
أرقام بطاقات الائتمان، كلمات السر، معلومات الحسابات.
عند تنفيذ مخطط واحد من هذه الاصناف فإن القرصان يضع نفسه بين المتصفح وخادم الانترنت وعادة ما يتم هجوم رجل في المنتصف والذي يسمى أحياناً بالتحايل على الانترنت من خلال اسم النطاق DNS أو بالتحايل مع الارتباط التشعبي.
هناك عدة طرق يمكن للقرصان أن يشن هجوم رجل في المنتصف من خلالها، احدى هذه الطرق تسجيل عنوان انترنت مشابه جداً لعنوان انترنت موجود، وبالتالي عندما يقوم شخص ما يرغب باستخدام هذا الموقع في شبكة الانترنت ويقوم بوضع عنوان هذا الموقع فإنه سوف يتم تحويله للموقع المزيف الذي تم تصميمه بواسطة القرصان لهيدو وكأنه الموقع الحقيقي.
لمتصفح الانترنت يبدو كل شيء طبيعي، فإنه يتفاعل مع الموقع المزيف تماماً كما يتفاعل مع الموقع الحقيقي، عندما يدخل الشخص المتصفح بعض المعلومات والخيارات قد يقوم القرصان بتمرير هذه المعلومات للموقع الحقيقي وتعيين شكل المتصفح للموقع الحقيقي ويظهر له الشاشات الحقيقية للموقع.

*- تسميم اسم النطاق DNS

تسميم اسم النطاق DNS يستغل ثغرة أمنية للإصدارات الأولى لـ BIND «بيركلي انترنت نيم دومين» وهو برنامج اسم النطاق الأكثر انتشاراً في شبكة الإنترنت، وقد طور هذا الإصدار ليتم استخدامه في نظام يونكس «BSD UNIX».

تقوم شبكة خدمات BIND للإنترنت بترجمة عناوين الـ IP الأساسية «الأرقام» إلى أسماء شائعة الاستخدام مثل www.ggu.edu لجامعة كولدن جيت.

قبل الإصدار 8.1 من BIND كان من الممكن أن يتم تسميم مدخلات جدول مخدم النطاقات DNS بمعلومات خاطئة.

حيث إنه يمكن أن تشمل هذه المعلومات عنوان انترنت IP كاذب تدخل في جدول المخدم، وبالنتيجة عندما يستخدم الشخص ذلك المخدم DNS للوصول إلى عنوان انترنت URL يتم توجيهه إلى عنوان انترنت IP غير صحيح.

بالتحايل على اسم مخدم النطاق DNS يمكن أن يصنع القرصان عنوان انترنت URL مشروع للموقع في شبكة الانترنت

مثلاً: يقوم متصفح شبكة الانترنت بكتابة www.amazon.com ويتوقع أنه يدخل الموقع Amazon.com لشراء كتب. في نظام الانترنت فإنه يشار للعنوان www.amazon.com بـ xxx.xxx.xxx.xxx ولكن القرصان قد قام بالتحايل على مخدم النطاقات DNS لكي يشير إلى الموقع الخاص به، ونتيجة لذلك يتم توجيه متصفح الانترنت إلى موقع القرصان وليس لموقع amazon.com

*- إعادة التوجيه:

في هذه الحالة يقوم القرصان بخداع وصلة على صفحة شخص آخر أو إنشاء صفحة خاصة به مع وصلات كاذبة.

وفي كلتا الحالتين يشير الرابط على أنه موقع تجاري، لكن في واقع الأمر الرابط يجلب متصفح الانترنت إلى موقع تم تصميمه ويتم التحكم به بواسطة قرصان ويبدو مثل الموقع الذي يتوقعه الشخص المتصفح.

في الحالتين: عند استخدام هجوم رجل في الوسط «المنتصف» في الواقع يمكن أن يمرر موقع القرصان طلبات العميل إلى الموقع الحقيقي ويظهر للعميل الصفحات المطلوبة من الموقع الحقيقي، في حين أن القرصان يرصد ويسجل جميع العمليات بين العميل والمخدم.

هناك إجراء مضاد فعّال لهجوم رجل في المنتصف، يمكن لهذا الهجوم أن يكون ناجحاً حتى في ظل استخدام نظام تشفير مثل «SSL». فإنه يتطلب من المرصاد الحصول على شهادة رقمية صالحة لتحميلها على جهاز الخادم الخاص به، بحيث يمكن تفعيل نظام التشفير SSL.

يجب على مستخدمي شبكة الانترنت أن يكونوا حذرين حول أمن اتصالاتهم، ويجب أن يتأكدوا من الروابط التي يزورونها والتنقل فقط ضمن الروابط من مواقع آمنة.

⊛ - إعادة الهجوم

لينفذ المهاجم إعادة الهجوم عن طريق اعتراض وتخزين معلومات مرسلة بصورة شرعية بين نظامين ويقوم بإعادة بثها في وقت لاحق نظرياً.

يمكن لهذا الهجوم أن يكون ناجحاً حتى في حالة الإرسال المشفر.

أفضل وسيلة دفاع ضد هذا الهجوم هو استخدام مفاتيح الجلسة والتحقق من الطابع الزمني على كل الإرسالات، وتوظيف رسالة لتعتمد على الرقم المتزايد.

⊛ - كسر كلمة السر:

برامج كسر كلمة السر هي برامج تقوم بفك شيفرة ملف كلمات السر، وهذه البرامج متوفرة لمعظم نظم الشبكات ونظم تشغيل الحواسيب. وهي قادرة على فك تشفير ملفات كلمات السر عن طريق استخدام نفس الخوارزمية المستخدمة لإنشاء كلمة السر المشفرة.

بصورة عامة تستخدم قاموس من الكلمات أو العبارات المعروفة والتي تم تشفيرها أيضاً بخوارزمية كلمة المرور.

تقوم برامج كسر كلمة المرور بمقارنة كل جمل من ملف كلمة المرور مقابل كل جمل في القاموس لإيجاد الكلمة المطابقة، وعندما يتم التطابق يكون قد تم العثور على كلمة السر.

يمكن العثور على شيفرة المصدر لبرامج كسر كلمة السر لمعظم الحواسيب وأنظمة التشغيل للشبكات بسهولة على شبكة الانترنت في مواقع مثل www.L0pht.com

لبعض من البرامج المتاحة على الشبكة مثل Brute، CrackerJack، New Hak...

⊛ - الهندسة الاجتماعية:

الهندسة الاجتماعية عادة ما تشير إلى عملية إقناع شخص للكشف عن معلومات "دون علمهم" التي تمكن المرصاد من الوصول إلى النظام أو الشبكة.

مثال ذلك: يمكن للمرصاد أن يحصل على دليل الهاتف الخاص بالشركة ومن ثم ينتحل موظف من غير المكتب

إدارة نظم معلومات الشركة، وربما يستخدم القراصنة اسم شخص ما من
مدعياً أنه يتصل من إدارة الشركة «إدارة نظم المعلومات» وقد يقول أن هناك مشكلة ويطلب من الموظف
إدخال سلسلة طويلة من الأوامر الغامضة للتحقق من المشكلة، يدخل الموظف الأوامر
التي يبدو أنها تعمل، في حين أن موظف نظم المعلومات المضلل يدعي التواصل كما
تكون متزامنة مع الموظف. الموظف المستهدف يشعر بالضغط عليه نتيجة المشكلة
على ما يبدو وفي إدخال الأوامر بشكل صحيح، وأخيراً يقول موظف إدارة نظم المعلومات
المزيف شيئاً من هذا القبيل «فقط أعطني كلمة السر الخاصة بك حتى أستطيع التحقق
من ذلك بنفسي وتتمكن من حل المشكلة» وربما لا يكتشف الموظف كلمة السر الخاصة
بالقراصنة معتقداً أن القراصنة موظفو نظم المعلومات للشركة. وبهذه البساطة الآن
حصل القراصنة على اسم المستخدم وكلمة المرور والمفاتيح للوصول إلى نظام الشركة.

من المهم أن يكون لكل منشأة سياسة بخصوص الكشف عن كلمات السر، عموماً يجب أن تكشف
السياسة بأنه غير مسموح بكشف كلمات السر لأي شخص بما في ذلك موظفو نظم المعلومات
ويجب إبلاغ هذه السياسة لكل موظفي الشركة.

* الغوص بالقمامة:

هي تقنية غير متقنة، يعرف الغوص بالقمامة بعملية جمع المعلومات عن طريق البحث في القمامة
عن مطبوعات أو حواسيب ذات قيمة وتتميز هجوم الغوص بالقمامة.
هنا يبحث القراصنة على معلومات مثل أسماء حسابات النظام وشيفرة المصدر «وخاصة
إذا كانت تحتوي على كلمات سر مضمنة» أو أرقام حسابات العملاء «للمؤسسات المالية»
لذلك من المهم أن يكون لدى المنشأة معدات مناسبة للتخلص من السجلات والملفات
الورقية.

* - التجسس:

تجسس شبكة الحاسوب أو تجسس حزم البيانات هي عملية رصد للشبكة في محاولة لجمع
المعلومات التي قد تكون مفيدة للهجوم.
يمكن للقراصنة مراقبة حزم البيانات للشبكة للحصول على كلمات السر أو عناوين الانترنت IP
العديد من البائعين يصنعون الأجهزة والبرمجيات لأغراض مشروعة ولكن يمكن أن
يساء استخدامها من قبل القراصنة.
الحقيقة الوحيدة المريحة عن هذه المنتجات هي أن القراصنة لا يستطيعون تحمل
نفقاتها شرائها. ومع ذلك عليهم سرقتها، وهناك بعض الأدوات المجانية والبرامج
العامة متاحة للتنزيل من مواقع القراصنة مثل Tcp DUMP ، Tcpmon
gobbler، برامج Sniffer pro .

هناك العديد من الأدوات المتوفرة للحد من مخاطر تحسس الشبكة مثل الصدفة المحمية SSH والشبكات الخاصة الافتراضية VPN،

في بعض الأحيان تحليل بسيط لحركة البيانات يمكنه الحصول على معلومات مفيدة، وبالتمكن من التعرف على الأنظمة الأكثر نشاطاً يمكن أن تكون ذات قيمة كبيرة.

إن استخدام محولات الشبكة بدلاً من المحاور التقليدية يمكن أن تكون طريقة أخرى للحد من خطر رصد الشبكة.

هناك أدوات أخرى متاحة ترمي إلى الكشف عن راصدي حزم البيانات بحزم المصرح لهم في الشبكة مثال ذلك برنامج مضاد رصد الشبكات متوفر من شركة Lopht للمنظمات لتشغيله على موقع www.Lopht.com، وبالتحديد هذه المنتجات تكشف خصائص بطاقة واجهة الشبكة (NIC)

* تشويه المواقع

كثيراً من الأحيان يتم تشويه مواقع بعض الشركات من قبل قراصنة الحاسوب الذين ينشرون بعض رسائل الاحتجاج على شيء ما، وعادة يتم هجوم تشويه المواقع على شبكة الانترنيت من خلال استغلال بعض نقاط الضعف التي تصيب محكم شبكة الانترنيت أو استغلال الضعف القائم على بروتوكول آخر في نظام تشغيل محكم الشبكة.

أفضل وسيلة دفاع تتخذها الشبكة أو المنشأة ضد تشويه موقعها هو الحصول على آخر اصدارات برنامج خادم شبكة الانترنيت والنسخ المحدثة عن نظام التشغيل لخادم أيضاً ينبغي للمنشأة أن تكفل التدريب السليم لمدير النظام لديها ليكون قادراً على تثبيت وصيانة البرامج.

وبعض الشركات تقوم بنشر خوادم شبكات ثانوية تسمى cash servers التي تقوم بتحديث خوادم الانترنيت ومن ثم يقوم برنامج cash servers باعادة النسخة الاصلية عند هجوم القراصنة لتشويه الموقع.

* انتحال الحرب

يستخدم هنا المتسلل الطريقة في العثور على باب خلفي في شبكة المنشأة، هذا النوع من الهجوم فعال ضد الدفاع من محيط.

معظم المنشآت لديها أرقام هاتف ضمن نطاق محدد وتبدأ بنفس البادئة، على سبيل المثال: لنفترض لدينا شركة تبدأ أرقامها ب 595 وهناك 4000 تحويلة والتحويلة الاولى هي 1000 وبالتالي هواتف هذه الشركة تبدأ بالرقم 595-1000 وتنتهي ب 595-5000

الاتصال الحربي غالباً ما يستخدم نظام الاتصال الآلي (برنامج) للاتصال على كل هاتف من أرقام معينة، بحثاً عن تلك التي تستخدم جهاز مودم Modem

ستعمل هذا البرنامج على هاتف كاملاً والموجودة مودم وبالتالي يقوم القرصان بالبحث عن جميع الاتصالات على تلك الأجهزة المودم ومن ثم يقوم بمحاولة اقتحام النظام المتصل بجهاز المودم من أجل الدخول للشبكة.

* الحرمان من الخدمة

الحرمان من الخدمة مصمم من أجل تعطيل أو جعل النظام أو الشبكة غير قادر على العمل، والهدف من هذا الهجوم ليس الدخول إلى الشبكة أو الحصول على المعلومات، ولكن لجعل الشبكة أو النظام غير متاح للاستخدام من قبل المستخدمين الآخرين.

غالباً ما تستخدم مثل هذه الهجمات للانتقام أو المنافسة. مع العلم أنه في هذا النوع من الهجوم فانه يلزم قدراً كبيراً من الخبرة والمهارة والذكاء لكي يكون الأمر ناجحاً.

هنالك العديد من أنواع هجوم الحرمان من الخدمة مثل:

- بينغ القاتل Ping of death . ارقام التسلسل المتزامنة SYN الاغراق
- البريد الالكتروني الغير مرغوب فيه المعروف " SPAM " وغيرها.

* بعض الهجمات الأخرى

سنذكر بعض الهجمات الأخرى التي يمكن أن تواجه الشبكات والأنظمة المعلوماتية ومنها:

P - General Trojans : هذا النوع يخرب الجهاز ويسرق البيانات من الجهاز الضحية، وأغلب مبرمجي البرامج الخبيثة يصنعون أصنافاً كثيرة لهذا النوع

ب - PSW Trojans : هو سارق كلمات السر، حيث يقوم بعض المواقع التي تحفظ بها كلمات السر وبأخذها ثم يرسلها للشخص الذي يريده.

وبالعادة يسرق معلومات عن النظام ورقم التسلسلي لنظام التشغيل وخصوصاً أن نظام التشغيل عالي الثمن في الدول المتقدم لذلك معرفة رقم التسلسل مهم جداً "

ويسرق أيضاً بيانات الدخول للانترنت "رقم البطاقة وكلمة المرور للانترنت"

ويسرق كلمات السر للألعاب في الشبكات "الالعاب التي تكون مقابل مادي"

وكلمات السر للايميل E-mail والمواقع

- Clicker Trojans : هذا النوع يقوم بتوجيه الضحيه لموقع معين بدون ارادته والهدف منه هو إما زيادة عدد الزائرين للموقع أو استنفاذ حجم التبادل الشهري لموقع أو الهجوم على موقع أو مخدم معين بواسطة DOS ATTACK . أو اخذ الضحيه لموقع حيث يكون هذا الموقع مصابا فيتم تحميل بفيروس أو برنامج آخر للمهاجم.
قد تقوم هذه البرامج بمنع المستخدم من الدخول إلى مواقع معينة

ز- Trojans Downloaders : وهي برامج تتميز بصغر حجمها ووظيفتها تحميل برامج أخرى "تروجانات أو فيروسات" إلى جهاز الضحيه

هـ- Droppers Trojans : وهي برامج هدفها اخفاء البرامج الخبيثة عن أعين المستخدم أو عن مضاد الفيروسات.

و- Trojan Proxies : وهي برامج تستخدم لتحويل جهاز الضحيه لبروكسي يمكن الشخص أو المهاجم إلى استخدامه للدخول للانترنت بشكل متخفي.

ح- Trojan Spies : وهذا النوع يستخدم للتجسس على نشاطات الضحيه "ليس فقط كلمات سر كما في PSW Trojans بل نشاطات أخرى مثل صور سطح المكتب أو صور من الكاميرا أو أي نشاطات يقوم بها المستخدم.

ط- Trojan Notifiers : وهي فقط لاعلام المخترق الذي أرسل التروجان بنجاح إصابة الجهاز بالبرنامج الخبيث، حيث ترسل للمخترق معلومات عن الجهاز و IP والمنافذ المفتوحة.

ي- الملفات المورشفه : وهذه الملفات صممت لتخريب الملفات المضغوطة، حيث تتضاعف احجامها تلقائياً أو لوف المرات فتتخرب ويمتلئ الجهاز بملفات فارغة "شي هو قنابل العوادم"
خطورتها تكمن في اصابة خوادم الانترنيت ومخدمات البريد الالكتروني.
لها ثلاث أنواع :
- الاول تحتوي الملفات المضغوطة معلومات وبيانات مكررة
- الثاني تحوي الملفات المضغوطة
- الثالث تضغط الملفات بشكل صغير جداً مثلاً حجم 5 Gbyte يصبح 200 Kbyte

* هاكر :

الهاكر هو الذي يقوم بإنشاء وتعديل البرمجيات والعتاد الحاسوبي وغيره، 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 البرمجيات وإدارة الأنظمة وما يتعلق بأمن الحواسيب والشبكات بشكل عام.

* التصيد phishing

يستخدم مصطلح التصيد phishing للتعبير عن سرقة الهوية، وهو عمل إجرامي، حيث يقوم شخص أو شركة بالتحايل والغش من خلال إرسال رسالة بريد الكتروني مدعيًا أنه من شركة نظامية، ويطلب الحصول من المستلم الرسالة على المعلومات الشخصية مثل تفاصيل الحسابات البنكية وكلمات المرور وتفاصيل البطاقة الائتمانية.

وتستخدم المعلومات للدخول الى الحسابات البنكية عبر الانترنت والدخول الى مواقع الشركات التي تطلب البيانات الشخصية للدخول الى الموقع هناك برامج لمكافحة التصيد phishing والكشف عن الهوية الحقيقي، وافضل وسيلة لحماية الشخص من نشر معلوماته الشخصية لمن يطلبها هو أن يكون الشخص متيقظًا وحذرًا ولديه الوعي الكافي فلا يوجد هناك أي بنك معروف أو مؤسسة مقبولة تطلب من عملائهم ارسال معلوماتهم الشخصية عبر البريد الالكتروني

* البريد الالكتروني E-mail

يجدر بنا أن نتذكر دائمًا أن البريد الالكتروني لا يضمن الخصوصية، فخصوصيته تشبه البطاقة البريدية، ويتنقل البريد الالكتروني من

طريقة التي استلام عبر العديد من المخدمات، حيث عليه الوصول إليه من قبل الأشخاص الذين يديرون النظام، ومن قبل الأشخاص الذين يتسللون إليه بشكل غير نظامي، والطريقة الوحيدة للتأكد أن أحد ما من خصوصية بريدك الالكتروني هو تشفيره.

* بعض سبل الحماية

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

أ - الحصول على جدار حماية ناري " Firewall "

جدار الحماية الناري هو برنامج أو جهاز يقوم بفرز وتصفية الفيروسات والديدان والمتسللين والمعتدين الذين يحاولون الوصول إلى جهازك، ويعتبر تركيب جدار حماية ناري أكثر الطرق فاعلية، وأهم خطوة أولية يمكنك اتخاذها لحماية منظومتك هو القيام بتركيب جدار الحماية الناري قبل الدخول للانترنيت للمرة الأولى والإبقاء عليه عاملاً في كافة الأوقات.

عليه الحصول على جدار حماية ناري لجهازك من محلات الكمبيوتر أو من خلال الانترنيت.

علماً أن بعض الأنظمة " أنظمة التشغيل " مثل windows xp مع الحزمة الخدمية " الاصدار 2 " " services pack2 " ونظام ماكنتوش " Mac OS X " يوجد ضمنها جدار حماية ناري

ب - الحصول على برنامج مكافحة الفيروسات

اضافة لبرنامج جدار الحماية الناري، فإن عليك الحصول على برنامج مكافحة فيروسات قبل الدخول للانترنت للمرة الأولى، حيث يقوم هذا البرنامج بفحص جهازك لمعرفة الفيروسات الجديدة التي أصيب بها ومن ثم تنظيف هذه الفيروسات بما يكفل عدم الحاقه 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 يغنيه التفاعل معه بأمر ما عكسه.
كما يقوم برنامج مكافحة الفيروسات بالكشف عن الفيروسات في الأقراص المدخلة في جهازك والبريد الالكتروني الذي تستلمه والبرامج التي تقوم بتحميلها في جهازك من الانترنت.

في حال 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 انقاذ وإصلاح أية ملفات مصابة يستطيع إصلاحها.
هذا علماً بأن بعض برامج مكافحة الفيروسات تتطلب منك إرسال الفيروس إلى شركة مكافحة الفيروسات كي يتسنى لها إدخاله ضمن قاعدة بياناتها إذا كان من الفيروسات الجديدة.

يمكننا شراء برامج مكافحة الفيروسات عبر الانترنت أو من محلات بيع البرمجيات، كما يستحسن التأكد فيما إذا كان مزود خدمات الانترنت الذي تتعامل معه يزودك بمثل هذه البرمجيات.
ومما تجدر ملاحظته، أنه في حال كون جهازك مصاباً بالفيروسات فمن الخطأ شراء برمجيات الحماية من الانترنت لأنه يمكن لبرنامج التجسس التلصص على معلومات بطاقتك الائتمانية وأرقامها حتى ولو أدخلتها في صفحة ويب آمنة.

يجب أن يكون برنامج مكافحة الفيروسات مناسباً لجهازك والبرامج التي لديك. وهناك العديد من أنواع البرامج المتوفرة التي تناسب مختلف أنظمة التشغيل ويندوز والماكنتوش Macos ...
علماً أن أكثر برامج مكافحة الفيروسات استخداماً هي البرامج المزودة من McAfee و نورتن Norton Antivirus ومن سيمانتك Symantic وأنظمة سيسكو Cisco Systems و ميكروسوفت Microsoft

ج- حافظ على تحديث برامج جهازك.

نظراً لأن الفيروسات تتغير باستمرار، فإنه من الأهمية بمكان قيامك بتحديث وبشكل مستمر لنظام التشغيل الموجود في جهازك وبرنامج جدار الحماية الناري وبرامج مكافحة الفيروسات المركبة في جهازك، بحيث يتم ادخال آخر تحديثات صدرت عن هذه البرامج. ومعظم برامج مكافحة الفيروسات تقوم تلقائياً بتحديث البرنامج وعليك التأكد من قيامك بالتحديث.
علماً بأن الكثير من برامج مسح الفيروسات يمكن الحصول عليها مرة كل سنة. وينصح بترقية البرنامج بعد تلك الفترة حتى تضمن جهازك آخر التحديثات.

د- لا تفتح رسائل البريد الالكتروني المشكوك فيها

تصل معظم الفيروسات إلى أجهزة الكمبيوتر عبر البريد الالكتروني، لذا لا تفتح أي مرفقات بريد الكتروني لا تعرف مصدره، وعليك التأكد من محتوياته حتى ولو كنت تستخدم برنامج مكافحة الفيروسات مع ملاحظة أنه يمكن أن تصلك رسائل بريد الكتروني مصابة بالفيروسات حتى من أصدقائك وزملائك المسجلة لديك في قائمة بريدك الالكتروني ولا يكون الفيروس خطراً إلا إذا فتحت المرفقات المصابة.
وتأكد من محتويات الرسالة تبدو منطقية قبل فتح المرفقات.
كما يجدر بك ألا تقوم بتحرير أو إحالة أي مرفقات قبل أن تتأكد من أنها آمنة، وقم بحذف أي رسالة تعتقد أنها مصابة وقم كذلك بتفريغ الرسائل المحذوفة من المجلد الذي يحتوي عليها بشكل منتظم.

هـ- الحذر عند اقفال النوافذ المنبثقة

النوافذ المنبثقة هي النوافذ التي تظهر على الشاشة لديك عند دخولك إلى مواقع الكترونية محددة، وبعض المواقع الالكترونية تحاول خداعك لتنزيل برامج تجسس أو برامج دعاية على جهازك من خلال الضغط على موافق (OK) أو قبول (Accept) الموجودة على النافذة المنبثقة. وعليك اتباع وسيلة آمنة لاقفال هذه النوافذ ألا وهي الاقفال من مربع العنوان (X) الموجود في أعلى النافذة

و- فكر ملياً قبل تنزيل ملفات من الانترنت

يمكن أيضاً أن تصاب بفيروسات وبرامج دعاية وبرامج تجسس من خلال

تنزيل برامج وملفات أخرى من الانترنت. فإذا كان برنامج مجانياً ومزوداً من قبل مطور برمجيات مجهول، فمن المرجح أنه يحتوي على برمجيات إضافية وغير مرغوب فيها، لذلك إذا كنت قد قمت بتنزيل أو شراء برنامج من مطور برمجيات مشهور وموثوق.

ويحسن حفظا بأن نظام التشفير المعمول به يستخدم في كثير من الدول والشركات يحمي مستخدمي الانترنت من الدخول لمصادر إلى معظم المواقع الالكترونية الخطرة.

٣- برامج مراقبة بيانات الشبكة Packet Sniffers

طريقة فعالة لمراقبة الحركة المرورية عبر الشبكة باستخدام أحد برامج مراقبة بيانات الشبكة، حيث يتم تجميع البيانات الداخلة والخارجة، وهي طريقة يمكن أن تكون مفيدة في الكشف عن محاولات التسلل عبر الشبكة وكذلك يمكن استخدامها لتحليل مشاكل الشبكة وتصفيته وحجب الحواسيب المشكوك فيه من الدخول للشبكة.

٥- عمل نسخ احتياطيه من ملفاتك

لتفادي فقدان الملفات في حال تعرض الجهاز للإصابة بفيروسات، عليك التأكد من عمل نسخ احتياطيه لملفاتك، وخصوصاً المهمة.
وإذا كنت تقوم بشكل منتظم بعمل نسخ احتياطيه للمعلومات الموجودة في جهازك على أقراص صلبه خارجيه أو أقراص ضوئيه قابلة للكتابة أو أقراص مرنة، فلا تضع أقراص نسخ الاحتياطيه المساندة في جهاز الكمبيوتر لديك إذا كنت تعتقد أنه لديك فيروساً، لأنه يمكن للفيروس الانتشار إلى تلك الأقراص.

٦- التحديثات

حافظ على تحديث جميع برامجك بما في ذلك أحدث نسخة من برنامج التشغيل الذي تستخدمه، وإذا كنت تستخدم التحديث التلقائي الذي يقوم بالبحث يومياً عن التحديثات عند بدء تشغيل الجهاز، فعليك إعادة تشغيل جهازك يومياً.

٤- التشفير
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 قابله للقراءة من قبل أي شخص يستطيع التسلل إلى جهازك دون إذنه

التشفير Cryptography

عرف علم التشفير او التعمية منذ القدم، حيث استخدم في المجال العسكري، فقد ذكر ان أول من قام بعملية التشفير للتراسل بين قطاعات الجيش هم الفراعنة.
وكذلك فإن العرب لهم محاولات قديمة في مجال التشفير، واستخدم الصينيون طرق عديدة في علم التشفير والتعمية لنقل الرسائل أثناء الحروب.
أما في عصرنا الحالي فقد باتت الحاجة ملحة لاستخدام هذا العلم «التشفير» وذلك لارتباط العالم ببعضه عبر شبكات مفتوحة. حيث يتم استخدام هذه الشبكات في نقل المعلومات الكترونياً سواء بين الأشخاص العاديين أو بين المنظمات الخاصة أو العامة، عسكرية كانت أم مدنية. فلا بد من طرق تحفظ سرية المعلومات.

* ما هو التشفير أو التعمية Cryptography

التشفير هو العلم الذي يستخدم الرياضيات للتشفير وفك تشفير البيانات إن التشفير يمكنك من تخزين المعلومات الحساسة أو نقلها عبر الشبكات غير الآمنة. مثل الانترنت، وعليه لا يمكن قراءتها من قبل أي شخص ما عدا الشخص المرسل له. حيث أن التشفير هو العلم المستخدم لحفظ أمن وسرية المعلومات إن تحليل وفك التشفير Cryptanalysis هو علم لكسر وخرق الاتصالات الآمنة.

وبشكل آخر: علينا القول أن التشفير هو ترميز البيانات كي يتعذر قراءتها من قبل أي شخص ليس لديه كلمة مرور لفك شيفرة تلك البيانات، ويقوم التشفير بمعالجة البيانات باستخدام عمليات رياضية غير قابلة للعكس. ويجعل التشفير المعلومات في هيئة غير قابلة للقراءة من قبل أي شخص يستطيع أن يتسلل منه إلى هيئتك دون إذن.

* أهداف التشفير

يوجد أربعة أهداف رئيسية وراء استخدام علم التشفير وهي:
1- السرية أو الخصوصية Confidentiality: هي خدمة تستخدم لحفظ محتوى المعلومات من جميع الأشخاص ما عدا الذي قد صرح له الاطلاع عليها.
2- تكامل البيانات Integrity: هي خدمة تستخدم لحفظ المعلومات من التغيير (حذف، إضافة، تعديل) من قبل أي شخص غير مصرح له.
3- اثبات الهوية Authentication: وهي خدمة تستخدم لإثبات هوية التعامل مع البيانات
4- عدم الانكار أو الجحود Non-repudiation: وهي خدمة لمنع الشخص من انكاره القيام بعمل ما.
أنواع التشفير: حالياً يوجد نوعان من التشفير:
1- تشفير تقليدي Conventional Cryp   2- تشفير المفتاح العام Public key Cryp.