الانترنت
تعريفه، بدايته، واشهر جرائمه

ورقة بحثية
محمد عبدالله منشاوي
مكة المكرمة 1423هـ

إهداء

إلى كل من يسعى إلى تنمية ثقافته ومعلوماته .....

إلى من سمع بمصطلح الانترنت ورغب في معرفة المزيد منه.....

إليكم جميعاً هذه العمل المتواضع جداً لعله يكون الشمعة الأولى لإنارة الطريق في عالم الانترنت.

أخوكم

/ محمد عبدالله منشاوي

مكة المكرمة 24/12/1423هـ

مقدمة:

لا يخفى على احد ما تمثله الثقافة العامة من أهمية للأشخاص بشكل عام، ولرجل الأمن بشكل خاص، و نظراً لانتشار تقنية الانترنت بشكل سريع وواسع استلزم معه الإلمام بشيء بسيط عن هذه التقنية تمهيدا للأخذ بها واستغلالها في خدمة الأهداف الأمنية.

ومن هنا جاءت هذه الورقة البحثية الموجزة كمحاولة مختصرة لتبسيط مفهوم الانترنت وتعريف الفيروسات الحاسوبية والاختراقات كوتهما من أهم الجرائم التي ترتكب في شبكة الانترنت، وان كانت هناك العديد من جرائم الانترنت التي ظهرت كنمط حديث أفرزته التقنية الحديثة، والتي لا يسع المجال هنا للتطرق لها، ولعلنا نفرد لها بحث آخر إن شاء الله وسيكتفى هنا بالتعريف بالانترنت وبداياته وكيفية عمله ومستلزمات استخدامه ومن ثم التطرق إلى تعريف بأشهر جرائمه وهي جرائم الفيروسات الحاسوبية وجرائم الاختراقات.

تعريف الإنترنت وبداياته واستخداماته :
يمكن الدخول إلى الشبكة العالمية والمعروفة بالانترنت بواسطة جهاز الحاسب الآلي، فما هو تعريف الإنترنت وكيف بدأ :

أولا ما هي الشبكة : وظيفة أي شبكة هي تيسير المشاركة في المعلومات والبرامج وغيرها من موارد النظام بين عدد كبير من المستخدمين والشبكات علي نوعين :

1- الشبكات المحلية (LAN) (LOCAL AREA NETWORKS) تستخدم داخل منطقة معينة أو حيز معين.

2- الشبكات علي نطاق واسع (WAN) (WIDE AREA NETWORKS) تربط بين عدة شبكات محلية معا في إطار واحد باستخدام التلفون أو القمر الصناعي أو الميكروويف.

ثانيا : تعريف الإنترنت : "الإنترنت هو جزء من ثورة الاتصالات ويعرف البعض الإنترنت بشبكة الشبكات في حين يعرفها البعض الآخر بأنها شبكة طرق المواصلات السريعة، ويمكن تعريف الإنترنت بشبكة الشبكات" (ابوالحجاج، 1998م، ص 18)

بداية الإنترنت: بدأ الإنترنت في 2/1/1969 عندما شكلت وزارة الدفاع الأمريكية فريقا من العلماء للقيام بمشروع بحثي عن تشبيك الحاسبات وركّزت التجارب علي تجزئة الرسالة المراد بعثها إلى موقع معين في الشبكة ومن ثم نقل هذه الأجزاء بشكل وطرق مستقلة حتى تصل مجّمعة إلى هدفها وكان هذا الأمر يمثل أهمية قصوى لأمريكا وقت الحرب ففي حالة نجاح العدو في تدمير بعض خطوط الاتصال في منطقة معينة فان الأجزاء الصغيرة يمكن أن تواصل سيرها من تلقاء نفسها عن أي طريق آخر بديل إلى خط النهاية. ومن ثم تطور المشروع وتحول إلى الاستعمال السلمي حيث انقسم عام 1983 إلى شبكتين احتفظت الشبكة الأولى باسمها الأساسي (ARPANE) كما احتفظت بغرضها الأساسي وهو خدمة الاستخدامات العسكرية . وسميت الشبكة الثانية باسم (MILNET) للاستخدامات المدنية أي تبادل المعلومات وتوصيل البريد الإلكتروني ومن ثم ظهر المصطلح " الإنترنت " حيث أمكن تبادل المعلومات بين هاتين الشبكتين. وفي عام 1986 أمكن ربط شبكات خمس مراكز للكمبيوترات العملاقة وسميت (NSFNET (والتي أصبحت العمود الفقري وحجر الأساس لنمو وازدهار الإنترنت في أمريكا ومن ثم دول العالم الأخرى.

من يملك الإنترنت؟؟ لا أحد في الوقت الراهن يملك الإنترنت ففي البداية يمكن القول بان الحكومة الأمريكية ممثلة في وزارة الدفاع ثم المؤسسة القومية للعلوم هي المالك الوحيد للشبكة ولكن بعد تطور الشبكة ونموها لم يعد هناك مالك لها واختفي مفهوم التملك ليحل محله ما أصبح يسمي بمجتمع الإنترنت كما أن تمويل الشبكة تحول من القطاع الحكومي إلى القطاع الخاص. ومن هنا ولدت العديد من الشبكات الإقليمية ذات الصبغة التجارية حيث يمكن الاستفادة من خدماتها مقابل اشتراك. (أبو الحجاج 1998م).

توسع الشبكة: في عام 1985م كان هناك اقل من ألفي حاسوب آلي مرتبط بالشبكة وفي عام 1995م وصل العدد إلى (5) مليون حاسوب وفي عام 1997م تتجاوز حاجز الـ (6) مليون وتستخدم ما يزيد علي (300) ألف خادم (SERVER) أي شبكة فرعية متناثرة في أرجاء العالم,ويمكن القول بان عدد المستخدمين الجدد يبلغ (2) مليون شهريا أي ما يعني انضمام (46) مستخدم جديد للشبكة في كل دقيقة (السيد ، 1997 م).

وفي استطلاع أجرته شبكة (NUA) الأمريكية قدر عدد مستخدمي الشبكة عالميا بحوالي (134) مليون مستخدم في العام 1998م وتصدرت الولايات المتحدة الأمريكية وكندا الصدارة حيث من حيث عدد المستخدمين الذي بلغ (70) مليون مستخدم (NUA , 1998)

وفي تقرير أخير صدر بتاريخ 26 أكتوبر 2000 م قدّر عدد المستخدمين للشبكة عام 2005 بحوالي (245) مليون مستخدم وان غالبية هذه الزيادة ستكون خارج الولايات المتحدة الأمريكية (NUA ,10. 2000)

كما أوضح مسح ميداني اجري بتاريخ 6 نوفمبر 2000 على (2500) مستخدم للانترنت في كلا من أمريكا وبريطانيا وألمانيا واستراليا وفرنسا أن متوسط استخدام الإنترنت (4.2) ساعة أسبوعيا في أمريكا و (3.2) ساعة في أوروبا و (3.6) ساعة في استراليا . وان (44٪) من مستخدمي الشبكة في أمريكا يتصلون بها من منازلهم مقابل (38٪) في استراليا و (31٪) في بريطانيا وألمانيا في حين تبلغ النسبة في فرنسا (16٪) (NUA ,11. 2000)

وقد أشار الرئيس الأمريكي إلى أن هناك مشروع مستقبلي لتطوير شبكة الإنترنت باسم (الإنترنت 2) أو الجيل الثاني من الإنترنت فكان مما قاله " لا بد من أن نبني الجيل الثاني لشبكة الإنترنت لتتاح الفرصة لجامعاتنا الرائدة ومختبراتنا القومية للتواصل بسرعة تزيد ألف مرة من سرعات اليوم، وذلك لتطوير كل من العلاجات الطبية الحديثة ومصادر الطاقة الجديدة، وأساليب العمل الجماعي " (أفاق الإنترنت ، 1997)

وقد ظهر حديثا ما يشير إلى أن هناك في هذه الأيام سباق فضاء من نوع آخر حيث استطاعت شركة ستارباند (Starband) في تجربه أجرتها في شمال أميركا من إكمال مشروع انترنت أقمار اصطناعية ذو اتجاهين وسرعته كما أوردته الشركة هي (500) ك.ب في الثانية من الإنترنت إلى الحاسوب وسيبدأ تسويقه إلى المستهلك ويذكر انه يقف وراء هذه المشروع أكثر من شركة متخصصة في هذا المجال وهي: (Microsoft ,Echostar and Ing Furman Selz Investments)

بروتوكولات الإنترنت :

حتى تستطيع إقامة اتصال بين الحاسوبات المختلفة فان الأمر يتطلب وجود مجموعة من القواعد المتفق عليها والمعروفة باسم البروتوكولات، وقد تنوعت أسماء هذه البروتوكولات بين الأسماء الطريفة مثل جوفر (Gopher) والأسماء الطويلة المزعجة التي تم اختصارها مثل بروتوكول نقل النص المتشعب HTTP)) بدلا من(Hypertext Transfer Protocol) أو بروتوكول التحكم في النقل (TCP/IP) بدلا عن مسماه الطويل (Transmission Control Protocol/Internet Protocol)

فما هي هذه البرتوكولات وما هي وظائفها :

أولا : بروتوكول الإنترنت (Internet Protocol) (IP) أحد أهم البروتوكولات الأساسية والـ (IP) عبارة عن رقم مكون من أربعة أجزاء، يعرّف الجزء الأول من الرقم بدءاً من اليسار المنطقة الجغرافية، والجزء الثاني يحدد المنظمة أو الحاسوب المزود، أما المجموعة الثالثة من الأرقام فتحدد مجموعة الكمبيوترات التي ينتمي إليها الجهاز، والمجموعة الرابعة يحدد الجهاز المستخدم. ويمكن اعتبار الـ IP)) نوع من الخرائط الخاصة بالانترنت، حيث يمكن الاتصال بأي حاسوب أو بأي موقع من خلال نقطة معينة على هذه الخريطة.

ثانيا : لغة ترميز النص التشعبي وبروتوكول نقل النص التشعبي

Language and HTML Hypertext Markup and hypertext Transfer Protocol)
(HTTP)

يتحكم HTML)) و (HTTP) معا في الشبكة العنكبوتية (WWW) فـ الـ(HTML) طريقة لإضافة تنسيق إلى ملفات النصوص بحيث يمكنك رؤية أشياء مثل العناوين، والكلمات المراد تحديدها للفت الانتباه، والفقرات التي يتم توسيطها بالصفحة، والصورة المدرجة داخل النص، وذلك عند استخدامك لمستعرض ويب (HTML)أما (HTTP) فهو بروتوكول يقوم بتعريف كيفية إرسال و استقبال ملفات HTML))

ثالثا: بروتوكول التحكم في النقل(Transmission Control Protocol) أو ما يعرف اختصارا بـ(TCP) هو البروتوكول الذي يعرِّف البناء الخاص بالبيانات وكيفية إرسالها بين الحاسوبات،وعادة يتم تقسيم هذه البيانات إلى أجزاء عند إرسالها، ومن ثم يعمد إلى إعادة تجميعها وإعادتها إلى ترتيبها الأصلي عند وصولها إلى نقطة النهاية. ونظرا لاشتراك البروتوكول ((TCP و IP)) فقد جرى العمل عادة إلى الإشارة إليهما مجتمعين بـ (TCP/IP)

رابعا: تلنت Telnet)) : هو بروتوكول يقوم يتيح لك تشغيل جهاز آخر من خلال جهازك. فعندما تستخدم برنامج (Telnet) يمكنك الدخول إلى كمبيوتر آخر وتشغيل برامج كما لو كنت تجلس أمامه.

خامسا: جوفر (Gopher) يتم عرض محتويات الجهاز الخادم الذي يستخدم بروتوكول (Gopher) على هيئة قوائم فرعية ويمكنك اختيار أي عنصر من عناصر هذه القوائم. وما يميز هذا البروتوكول هو إعطاء المستخدم إمكانية اختيار أي عنصر من عناصر هذه القوائم ولو كانت على خادم (Gopher) آخر يختلف عن الخادم الذي قدم لك القائمة الأولى.

سادسا : بروتوكول نقل أخبار الشبكة: (Network News Transfer Protocol) والمعروف اختصارا بـ((NNTP تقوم أجهزة الخادم الخاصة بـيوزنت (UseNet) بتخزين الرسائل وتبادلها باستخدام بروتوكول (NNTP) وبهذه الطريقة يستطيع

العديد من الأفراد قراءة و إرسال الرسائل إلى هذه الأجهزة الخادمة باستخدام برنامج لقراءة الأخبار.

مستلزمات الاتصال بالشبكة:
حاسب إلى 2- مودم 3- الاشتراك في الخدمة 4- برامج تصفح الشبكة

خدمات الإنترنت:
1- البريد الإلكتروني :لإرسال واستقبال الرسائل ونقل الملفات مع أي شخص له عنوان بريدي بصورة سريعة جدا لا تتعدى دقائق .

2- قوائم العناوين البريدية : تشمل إنشاء وتحديث قوائم العناوين البريدية لمجموعات من الأشخاص لهم اهتمامات مشتركة .

3- خدمة المجموعات الإخبارية: تشبه خدمة القوائم البريدية باختلاف أن كل عضو يستطيع التحكم في نوع المقالات التي يريد استلامها.

4- خدمة الاستعلام الشخصي : يمكن الاستعلام عن العنوان البريدي لأي شخص أو هيئة تستخدم الإنترنت والمسجلين لديها.

5- خدمة المحادثات الشخصية : يمكن التحدث مع طرف آخر صوتا وصورة وكتابة.

6- خدمة الدردشة الجماعية : تشبه الخدمة السابقة إلا انه يمكن التحدث مع أكثر من شخص في نفس الوقت حيث يمكن تنظيم مؤتمر لعدد من الأفراد.

7- خدمة تحويل أو نقل الملفات : لنقل الملفات من حاسب إلى آخر ((FTP وهي اختصار (FILE TRANSFER PROTOCOL).

8- خدمة الأرشيف الإلكتروني :ARCHIE)) يمكن البحث عن ملفات معينة قد تكون مفقودة في برامجك المستخدمة في حاسبك .

9- خدمة شبكة الاستعلامات الشاملة : GOPHER)) يسمح للمستخدم بتشغيل والاستفادة من خدمات الكثير من الموارد الأخرى مثل خدمة نقل الملفات وخدمة المشاركة في قوائم العناوين البريدية حيث يفهرس المعلومات الموجودة علي الشبكة

10- خدمة الاستعلامات واسعة النطاق : (WAIS) تسمي هذه الخدمة باسم حاسباتها الخادمة نفسها وهي أكثر ذكاء ودقة وفاعلية من الأنظمة الأخرى حيث تبحث داخل الوثائق أو المستندات ذاتها عن بعض الكلمات المحورية أو الدالة التي يحددها المستخدم ثم تقدم نتائج البحث في شكل قائمة بأسماء المواقع التي تحتوي علي المعلومات المطلوبة.

11- خدمة الدخول عن بعد : TELNET)) تسمح باستخدام برامج وتطبيقات في الحاسب الآلي الآخر .

12- الصفحة الإعلامية العالمية : (WWW) (WORLD WIDE WEB) وتسمي أيضا الويب (WEB) : تجمع معا كافة الموارد المتعددة التي تحتوي عليها الإنترنت للبحث عن كل ما تريد في الشبكات المختلفة وإحضارها بالنص والصوت والصورة و الويب نظاما فرعيا من الإنترنت لكنها النظام الأعظم من الأنظمة الأخرى فهي النظام الشامل باستخدام الوسائط المتعددة

برامج التصفح المتوفرة :
هناك العديد من برامج تصفح الانترنت، أهمها:

1- NETSCAPE

2- INTERNET EXPLORER
3- MOSAIC

الفيروسات الحاسب آلية :
الفيروسات الحاسب آلية هي إحدى أنواع البرامج الحاسب الآلية، إلاّ أنّ الأوامر المكتوبة في هذه البرنامج تقتصر على أوامر تخريبية ضارة بالجهاز ومحتوياته، فيمكن عند كتابة كلمة أو أمر ما، أو حتى مجرد فتح البرنامج الحامل للفيروس، أو الرسالة البريدية المرسل معها الفيروس، إصابة الجهاز به ومن ثَمّ قيام الفيروس بمسح محتويات الجهاز أو العبث بالملفات الموجودة به. وقد عرّفها أحد خبراء الفيروسات (Fred Cohen) بأنّها نوع من البرامج التي تؤثّر في البرامج الأخرى، بحيث تعدّل في تلك البرامج لتصبح نسخة منها، وهذا يعنى ببساطة أنّ الفيروس ينسخ نفسه من حاسب آلي إلى حاسب آلي آخر، بحيث يتكاثر بأعداد كبيرة (Highley,1999).

ويمكن تقسيم الفيروسات إلى خمسة أنواع :

الأول: فيروسات الجزء التشغيلي للاسطوانة كفيروس Brain)) و(Newzeland).

الثاني: الفيروسات المتطفلة كفيروس (Cascade) وفيروس (Vienna).

الثالث: الفيروسات المتعددة الأنواع كفيروس (Spanish-Telecom) وفيروس (Flip).

الرابع:الفيروسات المصاحبة للبرامج التشغيلية (exe) سواء على نظام الدوس أو الوندوز.

الخامس: يعرف بحصان طروادة، وهذا النوع يصنّفه البعض كنوع مستقّل بحد ذاته، إلاّ أنّه أدرج في هذا التقسيم كأحد أنواع الفيروسات، وينسب هذا النوع إلى الحصان اليوناني الخشبي الذي استخدم في فتح طروادة حيث يختفي الفيروس تحت غطاء سلمي إلا أنّ أثره التدميري خطير.

وتعمل الفيروسات على إخفاء نفسها عن البرامج المضادة للفيروسات باستخدام طرق تشفير لتغيّر أشكالها، لذلك وجب تحديث برامج مكافحة الفيروسات بصفة دائمة (عيد،1419هـ : 63-66).

ويختلف الخبراء في تقسيمهم للفيروسات، فمنهم من يقسمّها على أساس المكان المستهدف بالإصابة داخل جهاز الكمبيوتر، ويرون أنّ هناك ثلاثة أنواع رئيسة من الفيروسات هي: فيروسات قطاع الإقلاع(Boot Sector) وفيروسـات المـلفات(File Injectors)وفيروسـات الماكرو(macro Virus).

وهناك من يقسّمها إلى: فيروسـات الإصابة المـباشـرة (Direct action) وهي التي تقوم بتنفيذ مهمتها التخريبية فور تنشيطها، أو المقيمة (staying) وهي التي تظل كامنة في ذاكرة الكمبيوتر وتنشط بمجرد أن يقوم المستخدم بتنفيذ أمر ما، ومعظم الفيروسات المعروفة تندرج تحت هذا التقسيم، وهناك أيضاً الفيروسات المتغّيرة (Polymorphs) التي تقوم بتغيير شكلها باستمرار أثناء عملية التكاثر حتى تضلّل برامج مكافحة الفيروسات (موقع جريدة الجزيرة ،2000).

ومن الجرائم المتعلقة بإرسال فيروسات حاسوبية قيام شخص أمريكي يدعى (Robert Morris) بإرسال دودة حاسوبية بتاريخ الثاني من نوفمبر عام (1988م) عبر الإنترنت، وقد كرّر الفيروس نفسه عبر الشبكة بسرعة فاقت توقع مصمم الفيروس وأدى ذلك إلى تعطيل ما يقارب من (6200) ستة آلاف ومائتي حاسبِ آلي مرتبط بالإنترنت، وقد قدرّت الأضرار التي لحقت بتلك الأجهزة بمئات الملايين من الدولارات. ولو قُدّر لمصمم الفيروس تصميمه بحيث يكون أشدّ ضرراً، للحقت أضرار أخرى لا يمكن حصرها بتلك الأجهزة، وقد حُكم على المذكور بالسجن ثلاث سنوات بالرغم من دفاع المذكور عن نفسه أنّه لم يكن يقصد إحداث مثل تلك الأضرار(Morningstar, 1998).

كيف يتم اقتحام الجهاز؟

لتتم عملية الاقتحام يجب زرع حصان طروادة في جهاز الضحية بعدة طرق منها:

1. يرسل عن طريق البريد الإلكتروني باعتباره ملفاً ملحقاً حيث يقوم الشخص باستقباله وتشغيله، وقد لا يرسل وحده حيث من الممكن أن يكون ضمن برامج، أو ملفات أخرى.

2. عند استخدام برنامج المحادثة الشهير (ICQ) وهو برنامج محادثة أنتجته إسرائيل.

3.عـند تحميل بـرنامج من أحد المواقع غير الموثوق بها وهي كثيرة جدا.

4.طريقة أخرى لتحميله، تتلخّص في مجرد كتابة كوده على الجهاز نفسه في دقائق قليلة.

5.في حالة اتصال الجهاز بشبكة داخـلية أو شبكة إنترانت.

6.يمكن نقل الملف أيضاً بواسطة برامج (FTP) أو (Telnet) الخاصة بنقل الملفات.

7.كما يمكن الإصابة من خلال بعض البرامج الموجودة على الحاسب مثل الماكرو الموجود في برامج معالجة النصوص (Nanoart,2000).

وبصفة عامة فإن برامج القرصنة تعتمد كلياً على بروتوكول الـ ((TCP/IP وهناك أدوات (ActiveX) مصمّمه ومجهّزة لخدمة التعامل بهذا البروتوكول، ومن أشهرها (WINSOCK.OCX) لمبرمجي لغات البرمجة الداعمة للتعامل مع هذه الأدوات. ويحتاج الأمر إلى برنامجين، خادم في جهاز الضحية، وعميل في جهاز المتسلل، فيقوم الخادم بفتح منفذ محدد مسبقاً في جهاز الضحية ، في حين يكون برنامج الخادم في حالة انتظار لحظة محاولة دخول المخترق لجهاز الضحية، حيث يتعرف برنامج الخادم (server) على إشارات البرنامج المخترق، ويتم الاتصال، ومن ثَمّ يتمّ عرض كامل محتويات جهاز الضحية عند المخترق، حيث يتمكّن من العبث بها أو الاستيلاء على ما يريد منها .

فالمنافذ (Ports) يمكن وصفها ببوابات للجهاز، وهناك ما يقارب الـ(65.000) منفذ تقريباً في كل جهاز، يميّز كلّ منفذ عن الآخر برقم خاص ولكلّ منها غرض محدد، فمثلاً المنفذ (8080) يخصص أحياناً لمزود الخدمة، وهذه المنافذ غير مادية مثل منفذ الطابعة، وتعدّ جزءاً من الذاكرة، لها عنوان معين يتعرف عليها الجهاز بأنّها منطقة إرسال واستقبال البيانات، وكلّ ما يقوم به المتسلل هو فتح أحد هذه المنافذ للوصول لجهاز الضحية وهو ما يسمى بطريقة الزبون/الخادم (Client\Server)) حيث يتمّ إرسال ملف لجهاز الضحية، يفتح المنافذ فيصبح جهاز الضحية (server)، وجهاز المتسلل (Client)، ومن ثَمّ يقوم المتسلل بالوصول لهذه المنافذ باستخدام برامج كثيرة متخصصة كبرنامج ((Net Bus أو ((Net Sphere.

ولعلّ الخطورة الإضافية تكمن في أنّه عند دخول المتسلل إلى جهاز الضحية فإنّه لن يكون الشخص الوحيد الذي يستطيع الدخول لذلك الجهاز، حيث يصبح ذلك الجهاز مركزاً عاماً يمكن لأي شخص الدخول عليه بمجرد عمل مسح للمنافذ (Port scanning) عن طريق أحد البرامج المتخصصة في ذلك.

خـطـورة برامج حـصان طروادة:

بداية تصميم هذه البرامج كان لأهداف نبيلة، كمعرفة ما يقوم به الأبناء، أو الموظفون، على جهاز الحاسب في غياب الوالدين، أو المدراء، وذلك من خلال ما يكتبونه على لوحة المفاتيح، إلا أنّه سرعان ما أسيء استخدامه. وتعدّ هذه البرامج من أخطر البـرامــج المستخدمة من قبل المتسللين، لأنّه يتيح للدخيل الحصول على كلمات المرور (passwords)، وبالتالي الهيمنة على الحاسب الآلي بالكامل. كما أنّ المتسلّل لن يتمّ معرفته أو ملاحظته لأنّه يستخدم الطرق المشروعة التي يستخدمها مالك الجهاز. كما تكمن الخطورة أيضاً في أنّ معظم برامج حصان طروادة لا يمكن ملاحظتها بواسطة مضادات الفيروسات، إضافة إلى أنّ الطبيعة الساكنة لحصان طروادة يجعلها أخطر من الفيروسات، فهي لا تقوم بتقديم نفسها للضحية مثلما يـقـوم الفيروس الذي دائما ما يمكن ملاحظته من خلال الإزعاج، أو الأضرار التي يقوم بها للمستخدم، وبالتالي فإنه لا يمكن الشعور بهذه الأحصنة أثناء أدائها لمهمتها التجسسية، وبالتالي فإنّ فرص اكتشافها، والقبض عليها تكاد تكون معدومة (Nanoart,2000).

أهم المنافذ المستخدمة لاختراق الجهاز:

إذن فأهمّ مورد لهذه الأحصنة هي المنافذ (Ports) التي تقوم بفتحها في جهاز الضحية ومن ثَمّ التسلل منها إلى الجهاز والعبث بمحتوياته. فما هذه المنافذ؟

سنحاول هنا التطرّق بشكل إجمالي إلى أهم المنافذ التي يمكن استخدامها من قبل المتسللين، والبرامج المستخدمة في النفاذ من هذه المنافذ :

اسم البرنامج	المنفذ
blade Runner , doly Trojan ,FTP Trojan , Invisible FTP , Larva ,WebEX , Win Crash	21
Tiny Telnet Server	23
Antigen , Email Password Sender , Haebu Coceda , Kauang 2 , Pro Mail trojan , Shtrilitz , Stealth , Tapirs ,Terminator , Win Pc ,Win Spy ,Kuang20.17A-0.30	25
Agent 31 , Hackers Paradise , Master Paradise	31
Deep Throat	41
DMSetup	58
Fire hotcker	79
Executor	80
Pro Mail trojan	110

Jammer Killah
121

TCP wrappers
421

Hackers Paradise
456

Rasmin
531

Ini Killer , Phase Zero , Stealth Spy
555

Attack FTP ,Satanz BackDoor
666

Dark Shadow
911

Deep Throat
999

Silencer , WEBEX
1001

Doly Trojan
1011

1012

Net Spy
1024

Rasmin
1045

Xtreme
1090

Rat
1095

1097

1098

1099

Psyber Stream Server , Voice
1170

Ultors Trojan
1234

Back Door -G , SubSeven
1243

VooDoo Doll
1245

UPD – BO DLL
1349

FTP99CMP
1492

Shivka – Burka
1600

Spy Sender
1807

Shockrave
1981

Back Door
1999

Trojan Cow
2001

Ripper
2023

Bugs
2115

Deep Throat , The Invasor
2140

Striker
2565

Win Crash
2583

Phineas Phucker
2801

Win crash
3024

Master Paradise
3129

Deep Throat , The Invasor
3150

Portal Of Doom
3700

Win crash
4092

File Nail
4567

ICQ Trojan
4590

Bubbel , Back Door Setup , Sockets de troie
5000

Back Door Setup , Sockets de troie
5001

Fire hotcker
5321

Blade Runner
5400

5401

5402

ServeMe
5555

Bo Facil

5556

5557

Robo-Hack
5569

Win Crash
5742

The Thing
6400

Deep Throat
6670

SubSeven
6711

Deep Throat
6771

Back Door-G , SubSeven
6776

Indoctrination
6939

Gate Crasher , Priority
6969

Net Monitor
7300

7301

7306

7307

7308

Remote Grab
7000

BacK Door Setup , ICKiller
7789

Portal of Doom
9872

9873

9874

9875

10067

10167

iNi – Killer
9989

Acid Shivers
10520

Coma
10607

Senna Spy
11000

Progenic trojan

11223

Hack 99 Key Logger
12223

Gaban Bus Net busPie Bill Gates , X -bill
12345

Gaban Bus Net Bus X-bill
12346

Whack – a – mole
12361

12362

WhackJob
12631

Senna Spy
13000

Priority
16969

Millennium
20001

NetBus 2 Pro
20034

Girl Friend
21544

Prosiak

22222

Evil Ftp , Ugly FTP
23456

UPD – Delta Source
26274

UPD - The Unexplained
29891

AOL Trojan
30029

NetSphere
30100

30101

30102

Sockets de Troie
30303

Baron Night , BO client ,Bo2 , Bo Facil

UPD - BackFire , Back Orifice , DeppBo
31337

NetSpy DK
31338

31339

UPD - Back Orific , Deep BO
31338

Bo Whack
31666

Prosiak
33333

Big Gluck , TN
34324

The Spy
40412

Agent 40421 , Master Paradise
40421

Master Paradise
40422

40423

40426

UPD –Delta Source
47262

Sockets de Troie
50505

Fore
50766

Remote Windows Shutdown
53001

School Bus

54321

Deep Throat
60000

Telecommando
61466

Devil
65000

المصدر موقع (http://www.nanoart.f2s.com/hack/ports3.htm)

أهم برامج الاختراق:

1. برنامج (Sub Seven) : أخطر برامج الاختراق يسمى في منطقة الخليج (الباكدور جي) ويطلق عليه البعض اسم القنبلة. تتركز خطورته في أنه يتميز بمخادعة الشخص الذي يحاول إزالته فهو يعيد تركيب نفسه تلقائيا بعد حذفه ويعتبر أقوى برنامج اختراق للأجهزة الشخصية وفي إصدارته الأخيرة يمكنه أن يخترق سيرفر لقنوات المحادثة (Mirc) كما يمكنه اختراق جهاز أي شخص بمجرد معرفة اسمه في (ICQ) كما يمكنه اختراق مزودات البريد (smtp/pop3) يعتبر الاختراق به صعب نسبيا وذلك لعدم انتشار ملف التجسس الخاص به في أجهزة المستخدمين إلا أنه قائما حاليا على الانتشار بصورة مذهلة ويتوقع أنه بحلول منتصف عام 2001 سوف تكون نسبة الأجهزة المصابة بملف السيرفر الخاص به (40-55 ٪) من مستخدمي الإنترنت حول العالم وهذه نسبة مخيفة جدا إذا تحققت فعلا وهذا البرنامج خطير للغاية فهو يمكن المخترق من السيطرة الكاملة على الجهاز وكأنه جالس على الجهاز الخاص به حيث يحتوي البرنامج على أوامر كثيرة تمكنه من السيطرة علي جهاز الضحية بل يستطيع أحيانا الحصول على أشياء لا يستطيع مستخدم الجهاز نفسه الحصول عليها مثل كلمات المرور فالمخترق من هذا البرنامج يستطيع الحصول على جميع كلمات المرور التي يستخدمها صاحب الجهاز !!! ومن أهم أعراض الإصابة بهذا البرنامج ظهور رسالة " قام هذا البرنامج بأداء عملية غير شرعية " وتظهر هذه الرسالة عند ترك الكمبيوتر بدون تحريك الماوس أو النقر على لوحة المفاتيح حيث يقوم البرنامج بعمل تغييرات في حافظة الشاشة وتظهر هذه الرسائل عادة عندما تقوم بإزالة ادخالات البرنامج في ملف(system.ini) .

2. برنامج (Back Orific) : ثاني أشهر البرامج وأقدمها يعطي المستخدم قدرة كاملة على جهاز الضحية تم الإعلان عنه من قبل جهة تدعى بجمعية البقرة الميتة (Cult of Dead Cow) والإصدارة التي صدرت في عام 1999 باسم بـ (BO2K)

3. برنامج (Hack 'a' Tack): شائع في أوروبا ونادر الاستخدام في الشرق الأوسط.

4. برنامج Net bus) :) : أشهر البرامج وأكثرها انتشارا وقد يكون سبب انتشاره أنه من أوائل البرامج التي ظهرت لهذا الغرض ، ولسهولة استخدامه لقي رواجا كبيرا وعلى الرغم من أنه أنه لم يكمل العامين من عمره إلا أنه يوجد العديد من الإصدارات التي تتحسن وتزداد خـطـورة في كل إصدارة عن سابقـتها .(Nanoart, 2000)

أنواع برامج الحماية :

للحماية من الاختراق والتجسس هناك طرق تستخدمها برامج الحماية للقيام بمهماتها ومن الممكن تصنيف هذه الطرق بشكل عام إلى أربعة طرق :

وجود قاعدة بيانات مسجل فيها عدد من أحصنة طروادة المعرفة مسبقاً ، ويتم عمل مسح لكافة الملفات الموجودة في الجهاز المستخدم ومطابقتها مع الموجود في هذه القاعدة للتعرف على الملفات المتطابقة،وهذه الطريقة تحتاج إلى تحديث دوري مستمر نظراً لصدور أنواع جديدة من البرامج وظهور إصدارات أحدث للبرامج القديمة

البحث عن وجود تسلسل محدد من الرموز التي تميز كل ملف تجسسي Signature)) والتي تميز أحصنة طروادة عن غيرها من البرامج العادية وهذه الطريقة أيضاً تحتاج إلى تحديث وذلك لتجدد هذه البرامج وسلوكياتها وقد يحدث أن تعطى البرامج التي تستخدم هذه الطريقة تنبيهات خاطئة أحياناً ولكنها نادرة وذلك لاشتباهها ببعض البرامج كما حصل مع مجلة (PCMagazine) العربية في إحدى إصداراتها السابقة ، حين أظهرت بعض برامج كشف الفيروسات عن وجود فيروس في القرص المدمج الملحق بالمجلة ثم ظهر أن ذلك خطأ من البرنامج

الكشف عن التغيرات التي تطرأ على ملف التسجيل Registry)) وتوضيح ذلك للمستخدم لمعرفة إن كان التغير حصل من برنامج معروف أو من حصان طروادة

مراقبة منافذ الاتصال ((Ports الخاصة بالجهاز لاكتشاف أي محاولة غير مسموح بها للاتصال بالجهاز الهدف وقطع الاتصال و إعطاء تنبيه لذلك .

وتختلف البرامج من حيث استخدامها للأساليب المذكورة حيث أن كل برنامج يستخدم أسلوب أو أكثر . كما أن البرامج من حيث الشمول تنقسم إلى نوعين :

(أ) - نوع خاص بالحماية من اختراق معينة خصوصاً البرامج المشهورة في هذا المجال مثل (NetBus) أو برنامج ((Back Orifice فقط. وعيب مثل هذا النوع انه لا تستطيع اكتشاف الاختراق القادم من برامج أخرى إلا أن ميزة هذه الأنواع من البرامج هي قوتها في التصدي للهجمات القادمة من البرنامج المخصص له الحماية

(ب) - نوع عام حيث يقوم بالتصدي لكافة الأنواع دون تخصيص ((Nanoart,2000.

المراجع :
أولا المراجع العربية :

أبو الحجاج، أسامة.(1998 م) دليلك الشخصي إلى عالم الإنترنت . القاهرة : نهضة مصر .

السيد، سمير.(1997م). محاضرات في شبكة المعلومات العالمية . القاهرة : مكتبة عين شمس.

عيد، محمد فتحي.(141هـ). الإجرام المعاصر. الرياض : أكاديمية نايف العربية للعلوم الأمنية .

مجلة أفاق الإنترنت. (1997)، إنترنت 2، المؤلف، السنة 1 (3) ،38-41.

موقع جريدة الجزيرة (2000) http://www.al-jazirah.com

ثانيا : المراجع الأجنبية :

.NUA Internet Surveys. (1998,June). How Many Online? [Online]

.Available: http://www.nua.ie/surveys/howmayonline/index.html [15.6.1998]

.NUA Internet Surveys. (1998,June). How Many Online? [Online]

Available: http://www.nua.ie/surveys/howmayonline/index.html

.[26.10.2000]

.NUA Internet Surveys. (1998,June). How Many Online? [Online]

Available: http://www.nua.ie/surveys/howmayonline/index.html

.[6.11.2000]

.Nanoart. (2000) [Online]

/Available: http://www.nanoart.f2s.com/hack

[15/11/2000]