المديرية العامة للاتصالات والمعلوماتية
مديرية تكنولوجيا المعلومات
قسم نظم المعلومات
شعبة أمنية المعلومات

COMPUTER HACKERS

قراصنة الحاسوب

قراصنة الحاسوب

تاريخ القرصنة

في مطلع عام ١٩٨١ أنتجت شركة IBM جهاز الكمبيوتر الشخصي والذي يتميز بصغر حجمه و سهولة استخدامه وتزامن ظهور قراصنة المعلومات مع انتاج هذا النوع من الأجهزة إذ كان في باديء الأمر عمل تطفلي لمعرفة أسس ومباديء عمل هذه الأجهزة ، ومن ثم تطور الى مجاميع هدفها العبث والتخريب لمختلف المعلومات في أجهزة المؤسسات التجارية والمصرفية.

من هم القراصنة : هم اشخاص هواة في بادئ الامر ومن ثم إت خذت حرفة لتحقيق اغراض معينة من اجل سرقة او اتلاف او التنصت على معلومات ووثائق مهمة بالنسبة لهم .

مقومات اختراق الحواسيب

يجب ان تتوافر الامور التالية للمخترق لكي يتمكن من اختراق حاسوب ما :

١ -ان يكون الحاسوب مزود بخدمة شبكة الانترنت

٢ -ان يكون المخترق على علم بعنوان الشبكة (IP) الخاص بالحاسوب المعني

٣ -ان يحوي الحاسوب المعين على الملف الخاص (patch file) و المرسل مسبقاً من قبل المخترق

٤ -ان يقوم العامل على الحاسوب بقبول ملف او رابط او بفتح الرسائل عبر البريد الالكتروني من قبل المخترق وبذلك يكون قد قام بتفعيل الملف المصاب او الباتش فايل وفتح جلسة معه .

ومن أهم أهداف المخترق :

الاختراق

هي القدره على الوصول لهدف معين بطريقة غير قانونية والدخول الى اجهزه الآخرين دون علم منهم بغض النظر عن الاضرار التي قد يحدثها .

الاستراق

هي القدره على الوصول لهدف معين بطريقة غير قانونية وأخذ نسخة من وثائق مقصودة مع إخفاء جميع الأثار الدالة على تلك السرقة .

العبـث

هي القدره على الوصول لهدف معين بطريقة غير قانونية والدخول الى اجهزه الآخرين والقيام باتلاف وثائق معينة دون هدف منشود.

الاحتياطات المتخذه و طرق الحماية من قراصنة الحاسوب

١. استخدام برامج مكافحة الفيروسات و برامج الجدار الناري وتحديثها بشكل دوري.
٢. تجنب التعامل مع المواقع الغير معلومة لديك ، أو تفعيل الملفات المرسلة اليك من جهة غير معلومة عن طريق المحادثة أو البريد الألكتروني .
٣. تغيير كلمات المرور بشكل دوري وصياغتها بشكل معقد كونها عرضة للأستراق .
٤. عدم تحميل ملف ما وخزنه على القرص الصلب في حاسوبك مالم تعرف مصدره .

الآثار الناتجة من الاختراق

١. تغيير محتويات المواقع الالكترونية بمعلومات غير صحيحة او اعطاء آراء مخالفة لما يتبناه ويطرحة الموقع .
٢. تزييف الحسابات المالية بقصد الكسب المادي من خلال مواقع البنوك وبطاقة الائتمان المصرفية .
٣. انتحال الشخصية من خلال سرقة كلمات المرور للمواقع والبريد الالكتروني وما ينجم منه من مخالفات قانونية ومشكلات اجتماعية .

ميكانيكية الاختراق

ان الاختراق يعتمد على السيطره عن بعد Remote ويتم ذلك بتوفير برنامج في كل من جهازي المخترق والضحية ففي جهاز الضحية يوجد برنامج الخادم server وفي جهاز المخترق يوجد برنامج العميل client .
وتختلف طرق اختراق الاجهزه بأختلاف وسائل الاختراق وهناك عده وسائل لتنفيذ ذلك والموضحه ادناه :

١. عن طريق ملفات أحصنة طروادة Trojan : لابد من توفر برنامج تجسسي (ضروري لتحقيق نظرية الاختراق) وهو ملف الباتش patch ويكون صغير الحجم ويعرف احياناً بالملف اللاصق (الصامت) حيث يتم ارساله وزرعة من قبل المستفيد (المخترق)وتكون مهمته الاساسية المبيت بجهاز الضحية الخادم وكذلك يعتبر حلقة الوصل بينه وبين المخترق وسمي بهذا الاسم نسبة الى الحصان الخشبي الشهير في الأسطورة المعروفة الذي ترك امام الحصن وحين ادخله اليه الناس خرج من داخلة الغزاة فتمكنوا من السيطرة والإستيلا على الحصن .

كيفية الأرسال:

تتم عملية إرسال برامج التجسس بعدة طرق من اشهرها البريد الألكتروني حيث يقوم الضحية بفتح المرفقات من الرسائل الالكترونية والتي غالباً ماتكون غير معروفة المصدر فيجد ملف الباتش المرسل و يفتحه الضحية معتقداً انه برنامج مفيد او من عامل الفضول ويتفاجئ بانه لا يعمل بعد فتحه ويهمل الموضوع في حينها يكون المخترق قد وضع قدمه الأولى بداخل الجهاز (يقوم بعض الأشخاص بحذف الملف مباشرة عند إكتشافهم بأنه لايعمل ولكن يكون قد فات الأوان لأن ملف الباتش من هذا النوع يعمل فورا بعد فتحة وإن تم حذفه) .

كيفية الإستقبال:

عند زرع ملف الباتش في جهاز الضحية (الخادم) فأنه يقوم مباشرة بالأتجاه الى ملف تسجيل النظام Registry لأنه يؤدي ثلاثة امور رئيسية في كل مرة يتم فيها تشغيل الجهاز :
(أ) فتح بوابة او منفذ ليتم من خلالها الاتصال داخل الجهاز المصاب تمكن المخترق من النفوذ .
(ب) تحديث نفسه وجمع المعلومات المحدثة بجهاز الضحية إستعدادا لأرسالها للمخترق فيما بعد .
(ج) تحديث بيانات المخترق (المستفيد) في الطرف الأخر .

٢. عن طريق الـIP Address Internet Protocol كل جهاز متصل بالشبكة يكون له رقم معين خاص به يعرف بأسم الـ IP Address وكل عنوان لموقع على الأنترنت يترجم الى IP Address الخاص بمزود الخدمة ويعتبر الـ IP هو رقم هوية خاص بكل من يعمل على الأنترنت،وعندما يقوم المخترق من معرفة IP يستطيع بسهولة الولوج الى الجهاز والسيطرة عليه فقط للفترة التي يكون فيها الضحية متصل بالشبكة ولكن هذا الخيار لايخدم المخترق كثيرا لأن السيرفر الخاص بمزود الخدمة يقوم بتغيير رقم الـ IP الخاص بالمشترك تلقائيا عند كل عملية دخول للشبكة .

٣. عن طريق الكوكيز Cookies :

وهي عباراة عن ملف صغير تضعه بعض المواقع التي يزورها المستخدم على قرصه الصلب وفق آليات تمكن الموقع الذي يتبع له جمع وتخزين بعض البيانات عن الجهاز وعدد المرات التي زار المستخدم فيها الموقع كما وأنها تسرع عمليات نقل البيانات بين جهاز المستخدم والموقع فالهدف الأساسي منها هو تجاري ولكنه يساء إستخدامه من قبل بعض المبرمجين المتمرسين بلغة الجافا فهذة اللغة لديها قدرات عالية للتعمق اكثر لداخل الأجهزة والحصول على معلومات اكثر عن المستخدم، لايفضل منع الكوكيز كليا ولكن يمكن فلترتها من خلال المتصفح او ببعض البرامج .

ما المقصود بكعكة الإنترنت(Internet Cookies)

مجموعة من المعلومات المخزنه والمرتبة وهي لاتشكل تهديد أمني مباشر لجهازك وذلك لعدم مقدرتها على حمل أو نقل الفيروسات كما انها لا تستطيع جمع معلومات شخصية عنك غير التي تقوم أنت بتقديمها بنفسك للمواقع أثناء تعبئة الإستمارات أو نماذج التسجيل وتتكون من ملف نصي صغير مكون عادة من ستة أجزاء وهي: اسم الكعكة ، قيمتها ، تاريخ انتهاء مفعولها ، اتجاهها ، الموقع المالك لها، درجة الأمان (التشفير) وأخيرا طبيعة المعلومات التي تقوم بجمعها .

مصدرها .

١. المواقع الالكترونية التي تقوم بزيارتها أثناء تجولك بالشبكة .
٢. البريد الإلكتروني الخاص بك حيث أنك وحال فتحك لأي رسالة قادمة من أي مصدر يقوم ذلك المصدر باهدائك كعكة من انتاجه حتى لوكان المرسل صديق لك لأن كل صفحة مرسلة لابد من احتوائها على رموز مزود الخدمة لذلك الصديق خاصة إذا كانت الرسالة من النوع المكتوب بلغة الترميز.

أشهر برامج الأختراق

ان الهدف الذي يسعى الية المخترق هو البساطة في التعامل مع برامج الأختراق والحصول على ما خف وزنه وغلاء ثمنه من جهاز الضحيه Easy to Go ، وبمعنى أخر فأن المخترق لايرغب في برنامج معقد يأخذ كثيرا من الوقت في تعلمه وكذلك لايرغب بعد تعلم البرنامج واتقانه الدخول الي جهاز خاوي لهذا السبب نجد بأن هناك ثلاثة برامج شهيرة ومعروفة يستخدمها المخترقون لبساطة تعلمها وسهولة إتقانها وفي نفس الوقت خطورة ما تقوم به هذه البرامج الثلاث :

١. برنامج Black Orifice الفجوة السوداء : يعتبر هذا البرنامج ثاني اشهر برنامج للأختراق وأقدمها يعطي سيطرة كاملة للمخترق وقد أصدرت الجمعية التي تصدرة وأسمها "جمعية البقرة الميته" Cult of Death Cow اعلانا بأطلاق اصدارة جديدة منه في نهاية الصيف السابق اسمته . Black Orifice ٢٠٠٠ .

٢. برنامج sub seven : يعتبر من اشهر واقوى البرامج واخطرها ويطلق عليه في منطقة الخليج العربي(الباكدور جي) ويسمى ايضاً بالقنبلة حيث يتميز البرنامج بانه يعيد تركيب نفسه تلقائياً بعد حذفه وكذلك يقوم بمخادعة الشخص الذي يحاول ازالته ويعتبر من اقوى برامج اختراق الاجهزة الشخصية ، و يمكن المخترق من السيطرة الكاملة على الجهاز وكأنه جالس على الجهاز الخاص به حيث يحتوي على أوامر كثيرة تمكنه من السيطرة عليه 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 .

٣. برنامج الـ Net Bus : في عام ١٩٩٨ تم إصدار نسخة تجريبيه تعمل على الويندوز ٩٥ من قبل مبرمج سويدي إسمه كارل نيكتر حيث لم يطلق عليه اسما في وقتها وتم تسميته لاحقاً باسم (اتوبيس الشبكةNet Bus) ويمكن استخدامه من تشغيله بواسطة كمبيوتر بعيد (ريموت)وصدرت بعد ذلك نسخ عديده منه اذكر منها نسخة ١,٦ و ١,٧ و Net Bus Pro وأخيرا . ٢٠٠٠ Net Bus حيث يسمح البرنامج السيطرة على جهاز الضحية عن بعد بالشكل التالي:

أ - عرض محتويات القرص الصلب بالكامل عن بعد.
ب -تشغيل برنامج معين بصورة مفاجئة .
ت -حذف اي ملف من القرص الصلب عن بعد.
ث -التقاط صور لسطح المكتب عن بعد.
ج -قفل واعادة تشغيل الجهاز Rebooting بطريقة مفاجئة .
ح -عرض صورة مفاجئة على شاشة الضحية او تغيير اعدادات الشاشة دون تدخل من المستخدم .
خ -انزال downloading اي ملف من جهاز الضحية لجهاز المخترق.
د - التجسس على المستخدم ورؤية اية كلمات يكتبها .