تمهيـــد

تمهيد

الكراك هو مصطلح يعبر عن اختراق حماية البرنامج وجعله يعمل بصوره كاملة بدون الحاجة إلى رخصه من الشركة المنتجة وقد تكون الرخصة هي عبارة عن إدخال رقم معين (Serial) في احد خانات البرنامج ليعمل

بصوره كاملة أو ضرورة إدخال السي دي عند فتح البرنامج أو وجود جهاز يتم تركيبه في منفذ الاتصال المتوازي (parallel) أو منفذ الاتصال (USB) ويسمى الجهاز دونجل أو Dongle

و في كل الطرق السابقة الفكرة واحده هو التأكد من وجود الرخصة الخاصة بالبرنامج قبل تشغيل البرنامج أو اللعبة ولا يجب أن تعرف الكثير من لغات البرمجة لتقوم بفك حماية البرامج ولكن بعض المعرفة يسهل عليك كثيرا أن تفهم بعد ذلك حتى طرق الحماية الجديدة التي قد تظهر بعد ذلك

يقوم هذا الكتاب بتعريفك الأساسيات الهامة لفك حماية أي برنامج ولكن يجب عليك أن تعرف أن شركات البرامج والألعاب تتكلف مبالغ باهظة لإنتاج هذه البرمجيات فإذا حصلت على برنامج وأعجبك فيجب عليك شراء النسخة الكاملة فورا أو حذف النسخة التي بحوزتك فهذا يضر بالشركة بصوره مباشره وبصوره غير مباشره باقتصاد الدولة والغرض هنا هو مجرد متعه اختراق الحدود التي يضعها أمام ك الكمبيوتر فهو مجرد برنامج وترميزات معينه ويجب التعامل معه على هذا الأساس ولا تنس انك إذا اعتقدت انك تملك بعض المعلومات عن الاختراق أو الهاك أن هذا مجرد نقطه في بحر المعرفة الذي لن يكون له نهاية فلا تفعل ضرر بأحد لا تريد لأحد أن يفعله بك أو ببلدك.

وإذا أتقنت اختراق حماية البرامج فيمكنك أن تستخدم هذا لعمل بناء وهو إعلام الشركات المنتجة للبرامج عن نقط الضعف سواء في الحماية أو في البرنامج نفسه وقد تحصل على مكافئه مجزيه !!

لغير المبرمجين

سنعبر عن البرامج التقليدية والألعاب بمصطلح برامج فكلاهما برنامج فيما عدا أن الألعاب لا تنتج شيئا غير الترفيه ويقوم المبرمج في الحالتين بكتابة تعليمات وأوامر معينه بأحد لغات البرمجة مثل لغة C أو Delphi أو Visual

Basic وبعد ذلك يقوم مترجم هذه اللغة بتحويل ملفات الأوامر إلى ملف تنفيذي له الامتداد exe

و يحتوى هذا الملف على نفس التعليمات التي كتبها المبرمج ولكن ليس باللغة الانجليزية ولكن برموز يفهمها الكمبيوتر وقد نستطيع فهم محتويات ملف exe إذا قمنا بترجمته إلى لغة الاسمبلى (Assembly Language) وهي أول لغة كمبيوتر فعليه في العالم وأقوى لغة في التعامل مع محتويات جهاز الكمبيوتر مباشره مثل المعالج أو احد منافذ الاتصال أو الهارد الديسك

ونستطيع أيضا تحويل تعليمات الملف exe إلى اللغة الأصلية التي كتب بها عن طريق أداوت تحتوى على محركات خاصة بإعادة هندسه الملف إلى أوامر باللغة الانجليزية (Reverse Engineering) ولكن يجب أولا أن تعرف اللغة التي كتب البرنامج فعملية إعادة الترجمة تختلف من لغة لأخرى باختلاف معالج اللغة الذي أنشئ الملف exe

و لكن عمليه إعادة الترجمة لا تعمل الآن بصوره 100 % لان هناك الكثير من البرامج التي تقوم بتشفير الملف التنفيذي exe بعد إنشاؤه فلا يمكن إعادة الترجمة ولكن يكون الاعتماد هنا على معرفه أسلوب البرنامج الذي انشأ الحماية نفسه وإيجاد نقطة ضعف له فلا يوجد للآن في العالم كله برنامج بدون نقاط ضعف وقد يستثنى من هذه القاعدة بعض التشفيرات الخاصة القوية وغيرها التي تتميز بتشفير 256 بت وبطرق غير معروفه إلا للجهات الحكومية والتي لا يمكن فكها إلا عن طريق عدد كبير من أقوى أجهزة الكمبيوتر يعملوا بطريقة متوازية ولعدد من السنوات !!

يحتوى الملف التنفيذي أيضا على تعليمات خاصة يجب أن يقوم بتحميلها عند التشغيل بذاكرة الكمبيوتر ويمكننا هنا مثلا إيقاف البرنامج في مرحله معينه من احد مراحل التنفيذ واختبار تعليمات معينه خاصة بالملف في الذاكرة وهي احد الطرق المعروفة لاختبار البرامج عموما وتسمى (debugging) ويوجد برامج شهيرة تستخدم لعملية الديبج مثل softice و W32Dasm وغيرها .

وحتى يمكنك أن تتابع هذا الكتاب فلابد أن تحصل على بعض البرامج التي تعتبر هي الأدوات لعمليه الكراك ويمكنك دائما الحصول على احدث إصدار لهذه البرامج عن طريق البحث عنها في الانترنت خصوصا عن طريق الموقع www.google.com

- برنامج TASM وهو اختصار لمعالج الاسمبلى الأقوى والأقدم Borland Turbo Assembler ويمكنك من خلاله ترجمه كود الاسمبلى إلى ملفات تنفيذيه
- برنامج NuMega SoftIce Debugger وهو من أقوى برامج الديبجر ويوجد منه الإصدار 3.22
- برنامج C Compiler Power من البرامج الصغيرة جدا ويقوم بترجمة تعليمات C إلى ملف تنفيذي ويمكن الوصول
- برنامج Sourcer Disassembler من البرامج الجيدة لأعاده هندسه الملفات التنفيذية إلى الملف المصدر بلغة التجميع Assembly
- برنامج Wdasm32 Windows Disassembler من البرامج السهلة التي يمكن للمبتدئين استخدامها لإعادة هندسه الملفات التنفيذية للويندوز
- برنامج IDA Interactive Disassembler هو أفضل احترافية من