بسم الله الرحمن الرحيم

سوف أقوم بإذن الله تعالى بتقديم مرشد تعليمى لتعليم كيفية كسر حماية البرامج (كراك) ، وذلك لكى نقوم نحن بصنع الكراك ولا ننتظر أن يقوم غيرنا بذلك ، حتى تعم الفائدة بيننا وحتى نتشارك بالمعلومة ، وحتى لا يحتكر الغرب كل تقنيات المعلومات ، فنتعلم منهم ونطور أنفسنا مثلما فعلوا هم معنا سابقا .

للأسف لن أستطيع أن أقوم بالشرح بالصور فى أغلب الحالات لأن الأدوات المستخدمة فى صنع الكراك لا أستطيع معها أخذ صورة لسطح المكتب ، فضلا عن أن الصور تأخذ حجما كبيرا نوعا ولذلك سأكتفى بالوصف ، وأيضا لن أعدكم بتقديم هذه السلسلة على نحو متصل وذلك لأننى مشغول هذا1 الشهر بامتحاناتى ولذلك لن يكون هناك ميعاد محدد لتقديم الدرس الجديد ولذلك أعتذر لكم اعتذارا شديدا .

كل ما أرجوه من هذه السلسلة أن يستفيد أى من أخوانى الكرام فى هذا الموضوع لأنه مهم حقا .

ولأننى لست بارعا جدا فى هذا العالم وصادفتنى الكثير من البرامج التى لم أستطيع كسر حمايتها لذلك أعذرونى إن أخطأت أو قصرت .

الدرس الأول

البرنامج : برنامج مرفق صغير ، قمت بتعريبه يقوم بتنظيف الجهاز من الاختصارات الملغية والمجلدات الفارغة ، عند بداية هذا البرنامج تظهر رسالة مزعجة تطلب منك التسجيل والتى يسميها عالم الهاكرز **nag-screen**.

الأدوات : إن عمل الكراكر و الهاكر مثل عمل الجراح أو المهندس ، فهم يحتاجون لأدوات للقيام بالعملية الجراحية أو للتصميم ، وإن كنا هنا نشبه أكثر الجراح حيث أننا نفتح معدة البرنامج ونقوم بإزالة الرسالة المزعجة والعد التنازلى الممل :) ، وأدواتنا هنا لن تزيد على أداتين هم **RegMonitor** وهو برنامج يراقب التسجيل **Registry** الخاص بالويندوز وسوف نستخدمه لكى نصنع كراك وسيكون عبارة عن ملف تسجيل ، أما البرنامج الأهم والذى سوف نجد به كلمة السر سيكون بإذن الله تعالى **SoftICE v4.5** ، وهذا برنامج مهم جدا لاستغنى عنه أى هاكر أو كراكر .

الخطوة الأولى : سنقوم بفتح البرنامج عندها سوف تظهر الرسالة المزعجة **nag-screen** وفيها زر يدعى تسجيل قم بالضغط عليه ثم قم بإدخال الاسم والكود تأكد من أنهما خاطئين :) ، ستظهر لك رسالة تخبرك ويا للعجب أن الكود خاطئ :) ، حسنا اضغط OK .

الخطوة الثانية : قم بإدخال الاسم الذى تفضله (أنا عن نفسى أدخلت **IDE the Cracker**) ثم أدخل أى كود مرة أخرى (لقد أدخلت 1981214) ولكن لا تضغط زر موافق قم أولا بتشغيل SoftICE (أداتنا العزيزة :)) بواسطة الضغط على Ctrl + D سوف تظهر لنا النافذة الاعتراضيه سوف نكتب الأمر التالى BPX lstrcmpa حيث BPX هو أمر لعمل نقطة توقف(Breakpoint) يقوم فيها البرنامج بوقف عمل الجهاز عند أمر تنفيذ معين أو (دالة معينة) ، أى عند تنفيذ الجهاز لوظيفة معينة ، أما lstrcmpa فهو روتين يستخدمه البرنامج لعمل دالة مقارنة بين مدخل وعملية حسابية مسبقة موجودة فى البرنامج ، ثم نقوم بالضغط على إنتر ، ثم نخرج من البرنامج بالضغط على Ctrl + D مرة أخرى .

ماذا حدث حتى الآن :- الذى حدث حتى الآن هو أننا أعطينا البرنامج اسم قام هو بتسجيله وحساب دالته ثم أعطينا كود وقبل أن يقوم بالمقارنة بين الكود المدخل والكود المسجل لديه (ذلك يحدث عند الضغط على إنتر) قمنا نحن بعمل نقطة توقف Breakpoint لكى يوقف SoftICE عمل الجهاز كاملة لنتطلع إلى سطور الذاكرة .

الخطوة الثالثة :- سوف نعود مرة أخرى سريعا إلى SoftICE بمجرد الضغط على زر موافق فى البرنامج المرغوب كسر حمايته ، وستجد نفسك عند نظام الذواكر المحمى 16 بت ، سوف نضغط F12 حتى نصل إلى نظام الذواكر 32 بت (لقد وصلت إليها عن نفسى بعد ضغطة واحدة).

0167:9EA6 < --- هذا جزء من عنوان 16 بت كمثال.

0187:004011B3 < --- هذا مثال على عنوان ال 32 بت .

الخطوة الرابعة :- عند الوصول إلى نظام 32 بت ، سنجد سطور تشبه هذه .....

0187:525258EE PUSH EAX □ هذا هو الكود الخاطئ الذى أدخلته

0187:52528754 PUSH 406030 □ (: هنا ستجد رقمك السرى

0187:52524545 CALL [……] □ هنا يقوم البرنامج بالمقارنة بين الرقمين

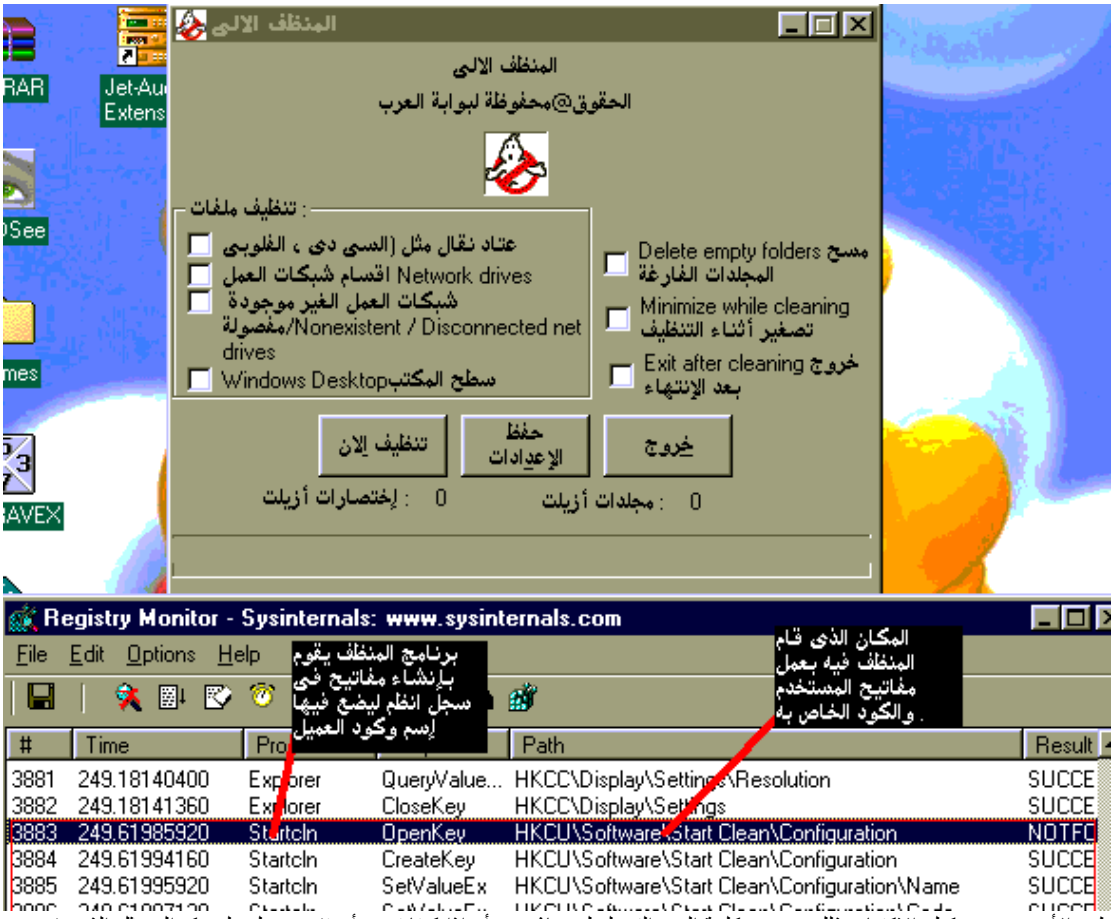
0187:5252RT6 TEST EAX,EAX □ هنا يقوم البرنامج بمعرفة صحة الكود المدخل من خطئه

0187:525ETB3 JNZ 004001271 □ يأمر الروتين الذى قمنا بعمل نقطة كسر عليه البرنامج بالقفز إلى سطر ذاكرة آخر .

على أساس المثال السابق ستقوم بعمل إظهار لموقع الذاكرة الذى يحتوى على الكود الحقيقى وأمر الإظهار هذا هو D ، وعلى هذا سيكون الأمر كذلك :=D 406030

سوف يظهر لك بأعلى (حسب إعدادات SoftICE لديك) الرقم السرى ، مبروك لقد قمت بكسر البرنامج بنجا ح :) .

لقد وجدت كلمة السر الخاصة بى (485-2509-25986-2694) .



الخطوة الأخيرة :- يمكنك الاكتفاء بذلك ووضع كلمة السر التى لديك مباشرة ، أو إذا كنتا تحب أن تقوم بعمل ملف كراك مثل الذى نقوم بتحميله من مواقع الهاكر ، سنقوم الآن باستخدام الأداة التالية وهى برنامج REGMON وهو برنامج يراقب مسجل النظام فى الويندوز كما أوضحنا سابقا ، قم بفتح البرنامج ثم قم بوضع كلمة السر الصحيحة فى برنامج المنظف الآلى (راقب برنامج REGMON جيدا قبل أن تضغط موافق) ستجد مثل الآتى فى الصورة :=

قم الآن بفتح محرر النظام Registry Editor (بالضغط على Start ثم Run ثم كتابة Regedit) ، ثم قم بالذهاب إلى مكان التسجيل وهو فى هذه الحالة :=

HKEY_CURRENT_USER
!
!---------- Software
!
!---------- Start Clean
!
!---------- configuration .

ثم قم بالضغط على Registry ثم اختر Export registry file وقم بتسمية الملف كما تحب ، للتأكد من صحة عمل الملف قم بمسح المفتاح المسمى Start Clean من محرر النظام ثم قم بفتح البرنامج (المنظف) ، سوف تجده أنه يطلب الكود مرة أخرى (إن شاء الله) ، اضغط على الملف الذى أنشأته من محرر النظم ليقوم بعمل المفتاح مرة أخرى ، شغل البرنامج (المنظف) ستجده يعمل دون طلب التسجيل إن شاء الله :) .

أرجو أن تأخذوا من هذا الشرح استفادة ما ، واعذرونى إن أخطأت أو نسيت .

و