Lang. : asm32
Tools : OllyDBG , PEiD , UN FSG 2.0
Cracker: allko

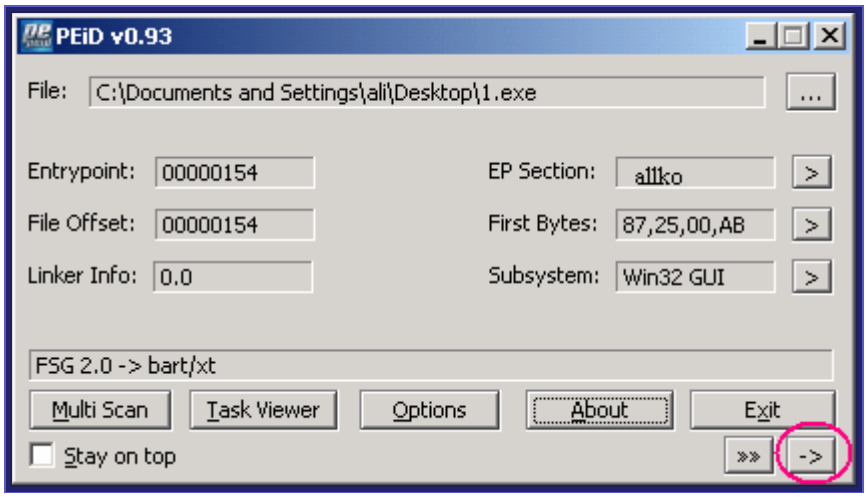
Learn Reverse Engineering Series- lesson four
RE techniques (I)

Introduction :

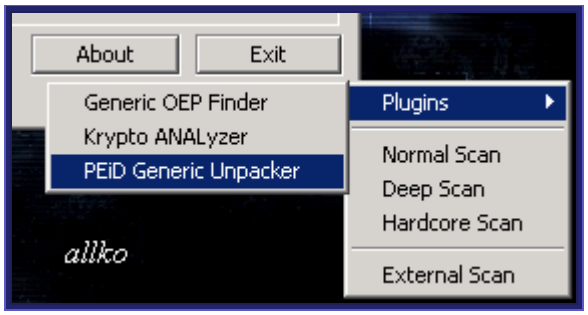
لا أعرف لماذا لا يوجد لدى الغرب (اعني المواقع الأجنبية عامة ومواقع الـ **RE** خاصة) درس واحد يحتوي على صور!!
جميع الدروس (**tutorials**) لديهم عبارة عن ملف **.txt** بحجم لا يزيد عن **10kb** ومليء بالكلام!! أعرف ان دروسهم غنية بالمعلومات لكن تخيل مثلا أن هذا الدرس الذي تقرأه لا يحوي أي صورة توضح لك في أي مكان في العالم أنت!!
لن أطيل عليكم...في هذا الدرس سنتعلم بعض التقنيات – البسيطة - الخاصة بالهندسة العكسية...

Technique one : automatic unpacking

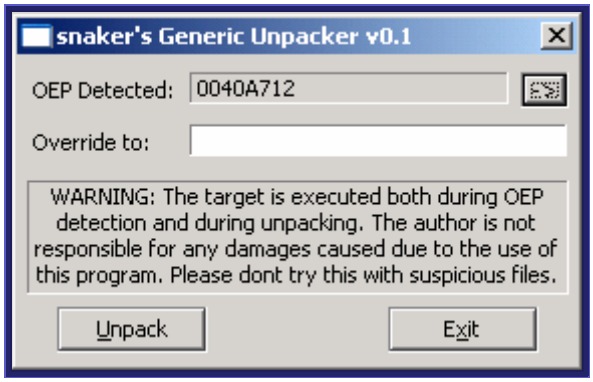
التقنية الأولى هي فك الضغط...
بداية هناك **plug in** يجب ان تكون لديك...وقد قمت بارفاقهما وهما **GenOEP.dll** و **ZDRx.dll** قم بنسخهما وضعهما في مجلد
Plug in ضمن المجلد الاساسي لـ **PEiD** ... قم بفحص الملف المسمى (1) بواسطة **PEiD** لتشاهد التالي



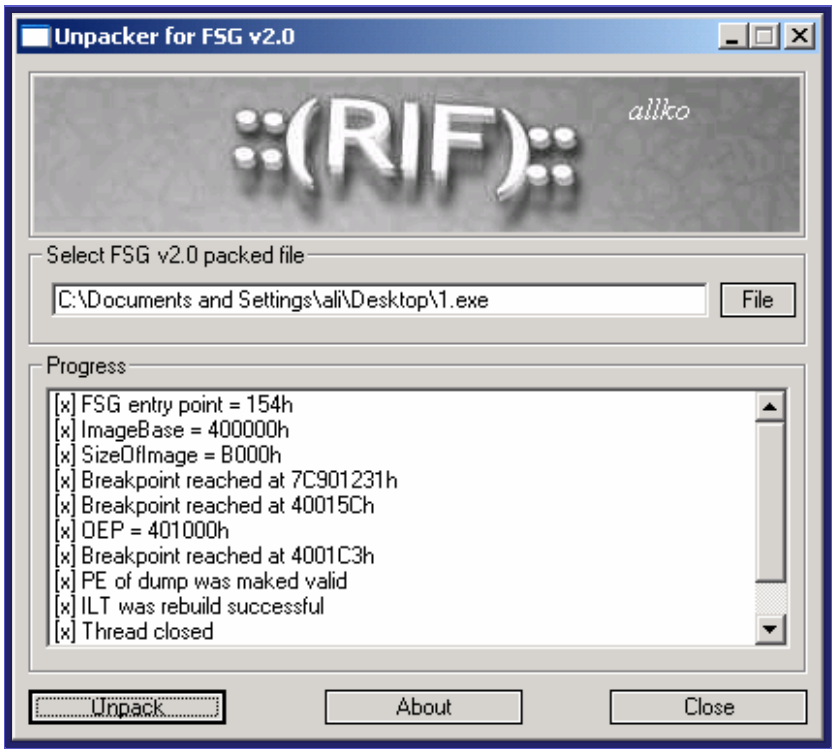
يبدوا انه مشفر بواسطة **FSG 2.0** ...حسنا والأن اضغط على الزر الموضح في الصورة ثم اختر **plug ins** ثم **PEiD Generic Unpacker**



ستظهر الصورة التالية...اضغط الزر الموضح لتحصل على **OEP : Original Entry Point** قم بنسخها...



والآن افتح البرنامج بواسطة **UN FSG 2.0** اختر **file** وحدد مكان الملف الضحية ثم اختر **Unpack** ...بعد ثوان معدودة ستخرج لك شاشة **save as** والان حدد المكان الذي تريد حفظ الملف (المفكوك تشفيره) فيه...احفظه في أي مكان ...

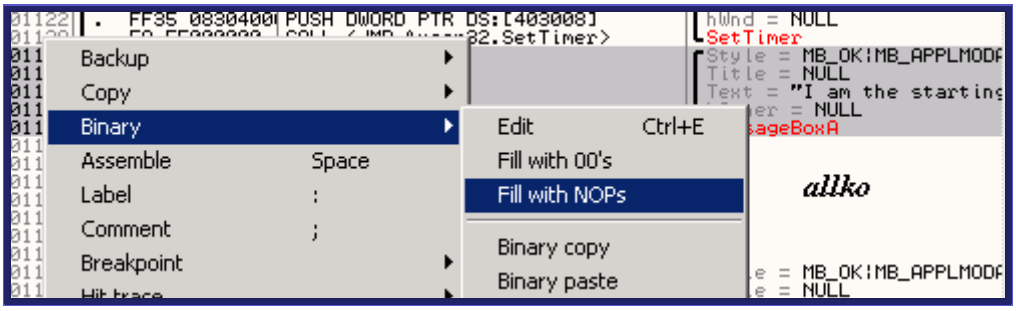


لا تنسى تغيير اسم البرنامج بحيث تضيف له امتداد **exe** فاذا سميته **allko** فغير الاسم الى **allko.exe**...

لكن لحظة!! ما الذي استنفدناه من الـ **OEP** ؟ لأننا استخدمنا **unpacker** مخصص لـ **FSG** فلم نحتج الـ **OEP** . لكن في حال استخدمت
Quick Unpack 1.0 مثلا ، فانك ستحتاج الى الـ **OEP** لان البرنامج يفشل غالبا في إيجادها.
بالإضافة إلى ذلك ، أحببت أن أعلمك – ان كنت مبتدئا – كيفية إيجاد الـ **OEP** باستخدام **PEiD** .

Technique two : Killing NAGs !!

قم بفتح البرنامج الذي ففكنا تشفيره للتو...كما تلاحظ هناك **nag** عند بداية التشغيل وثانية عند الضغط على الزر وثالثة زمنية ورابعة عند الخروج من البرنامج...افتح الهدف بـ **olly** ...اثناء بحثنا عن شيئ مثير للانتباه يلفت نظرنا دالة **SetTimer** يبدوا انها ذات علاقة بالـ **nag** الزمنية...اسفل منها هناك **MessageBoxA** الخاصة بـ **starting nag** ...حدد الدالة بالكامل (أي مع جميع بارامتراتها) ثم اضغط باليمين واختر
Binary ➔ fill wigh NOPs



ستجد انها اصبحت بهذا الشكل...

ثم كرر ذلك مع بقية الـ **nags** ...
وبعد الانتهاء من الاربعة اضغط باليمين واختر **copy to executable ➔ all modifications**

ثم

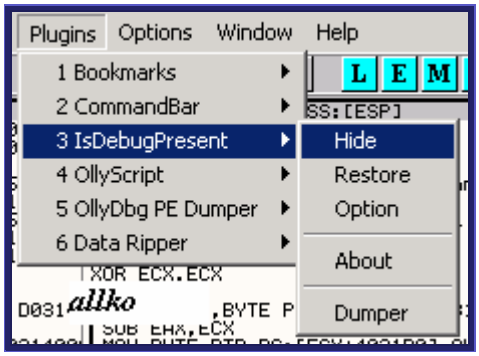
ومن النافذة الجديدة اختر **save file** ثم احفظه في أي مكان...والان قم بتشغيله...رائع!!! لم تظهر أي واحدة!!

Technique three : hiding OllyDBG !!

إخفاء **olly** ؟؟ نعم...هناك في عالم الهندسة العكسية والحماية ما يسمى بـ **unti debugging techniques**
وهي حيل تستخدم لمنع الكراكرز الطيبين – أمثالنا :) – من استخدام برامج الـ **debugging** مثل **olly** وغيره...في
مثالنا هذا (الملف المسمى 2) فان البرنامج يستخدم دالة **API** تسمى **IsDebuggerPresent** ...
افتح الملف المسمى **self destructed** لكن قبلها قم بعمل نسخة احتياطية او اكثر منه!! والان باستعراض سريع
للملف تجد هناك دالة تثير الانتباه...

كما ترى فان دالة **CreateFileA** تقوم بانشاء ملف اسمه **ERASER.BAT** لكن ما وظيفته؟ شغل الملف بالضغط
على **F9** لترى التالي

مالذي حصل؟ اكتشف البرنامج وجود **olly** فقام بإنشاء الملف **ERASER.BAT** وتنفيذه فحذف الملف **self destructed** !! لهذا قلت لك اعمل نسخة احتياطية...حسنا ما العمل؟ الحل بسيط هناك **plug in** تسمى **IsDebugerPresent** تجدها مرفقة مع الشرح...قم بوضعها في مجلد **plug ins** لـ **olly** والان حمّل الملف الضحية من جديد لكن قبل الضغط على **F9** اذهب الى **plug ins** واختر **IsDebugerPresent** ثم اختر **hide**



والان اضغط **F9** ..رائع!! لم تستطع الضحية اكتشاف وجود **olly** ...حسنا يمكنك إكمال فك الضحية اذا أحببت لكننا هنا لن نتطرق لذلك فقد عرفنا هذه الأساليب في الدروس الماضية...

Do You Know ?

هل تعلم أن أنظمة Unix-Like هي انظمه شبيهه بنظام Unix (الذي لا وجود له الآن) و تعتمد على مقاييسه في العمل , بعدما تحول نظام التشغيل Unix إلى نظام تجاري بدأت أنظمة Unix-Like بالظهور لأنه يعتبر احد الأنظمة العريقة .
جدير بالذكر أن جميع أنظمة Unix-Like كُتبت من الصفر , أي أن أي نظام Unix-Like تم كتابته من الصفر و لم يتم الاستعانة بالشفرات التي كانت موجودة في Unix الأصلي , أنظمة Unix-Like تسمى أحيانا بـ Unix-Clone . من أشهر أنظمة Unix-Like نظام Linux و UnixOS2 .

Notes :

Okay let me see...mmm...there are no note for today!!!

Outroduction :

Nothing to say , but thx a lot for reading my tutorial. Your e-mails are welcomed.

Greetings :

DiDi