

Cours de Cracking de la Team NCT:

Bienvenue à toi cher apprenti ;-)

Dans ce tutoriel nous allons apprendre à utiliser quelques programmes fondamentaux dans le domaine du Cracking!!!

Alors tout d'abord voici une liste des quelques programmes que tu dois te procurer ;-)

-OllyDBG v10(ou précédente :D) => Ceci est un désassembleur et un débogueur .

-Peid v0.93(perso j'utilise celle-ci mais bon tu fais comme tu veux). => Celui-ci sert à trouver l'OEP(tu verras ça plus tard avec d'autres tutos, dans le domaine de l'unpacking ;)) et quelques autres choses encore.

-UPX v?.?? (c'est pareil...)=> Ceci est un unpacker pour les logiciels packés avec UPX ;)

-Calculatrice Windows(ou bien Excalibur 32-bit) qui sont tous les deux gratuits ;)

-Un éditeur hexadécimal pour modifier des valeurs ;) ex: Winhex,...

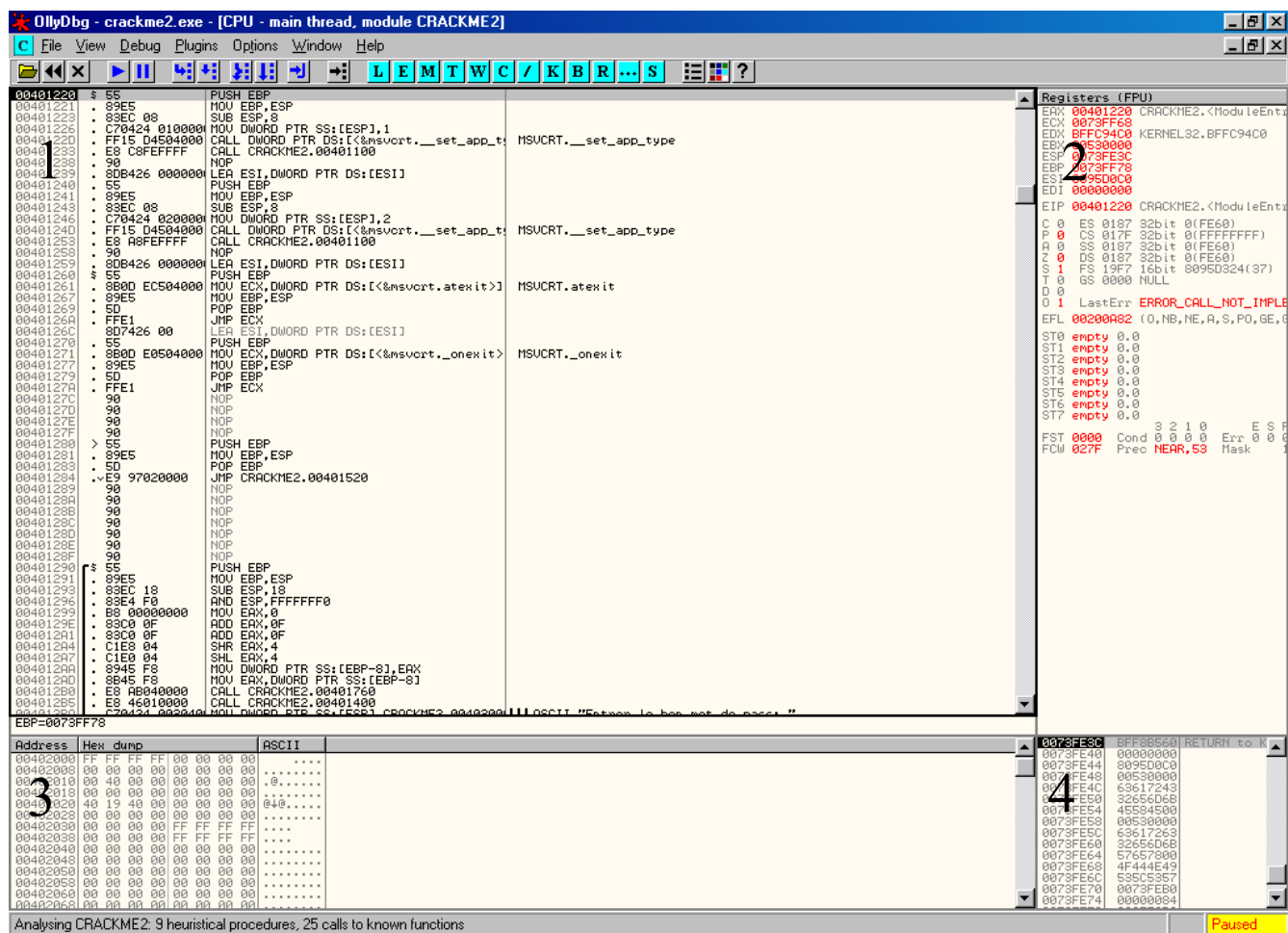
-Un cerveau si c'est possible et euh si c'est pas le cas je te conseille pas de commencer 8-)

-Un clavier, un écran, une tour, une souris,...(euh quoi ça fait pas partie de la liste? Ah ben ok -_-”)

Now je crois que tu es ready to go!!!

Commençons avec OllyDBG!!!

Voici tout d'abord la présentation générale de Olly:



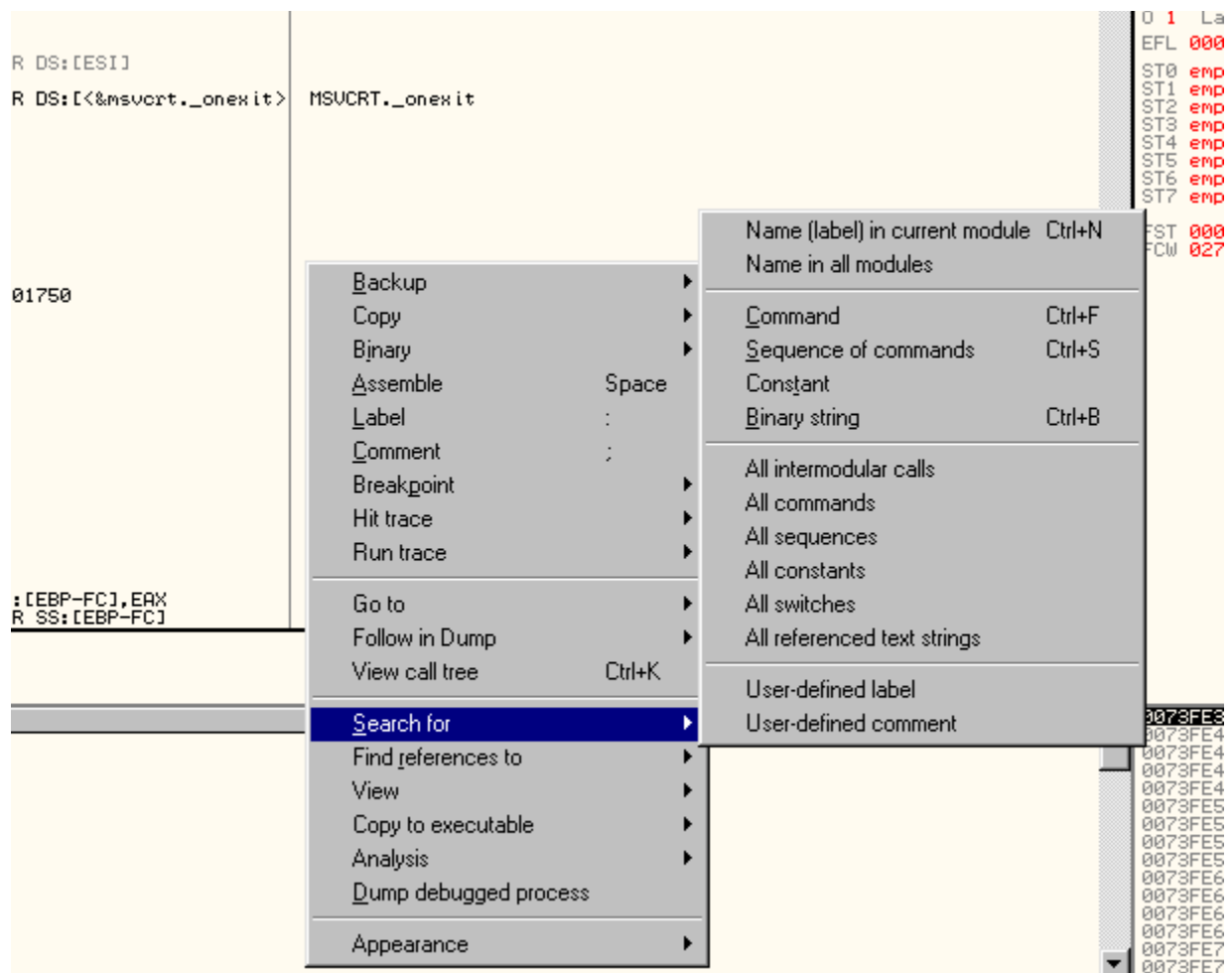
Donc voici la pitite analyse de la fenêtre ;)

1. C'est la fenêtre où se trouve le code que vous avez désassemblé ;)
2. C'est la fenêtre des registres ;) EAX,EBX,ECX,EDX & co.
3. C'est l'analyse du code en hexa.
4. C'est la fenêtre de la pile ;)

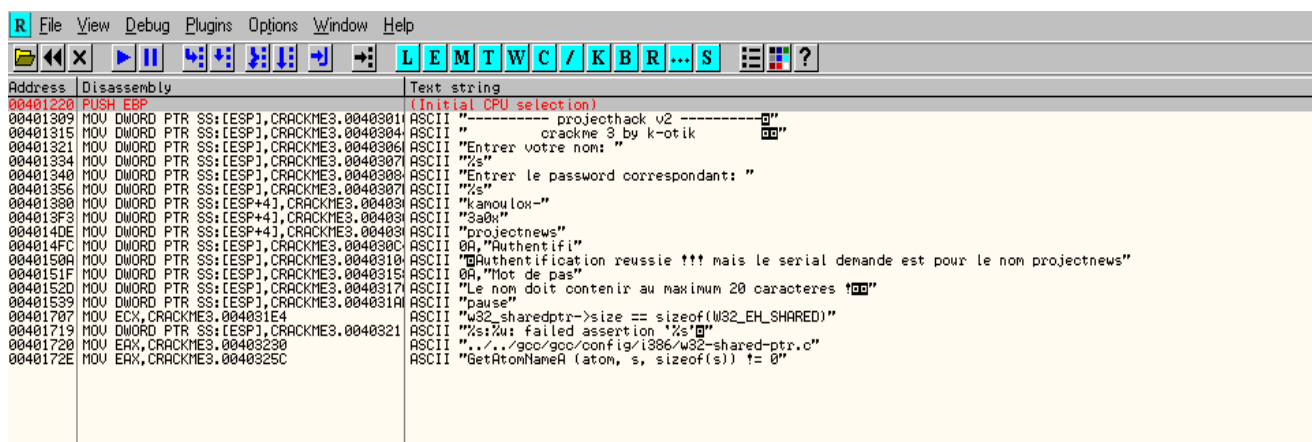
Voici donc les fenêtres principales de Olly ;)

Maintenant on va passer à certains éléments plus précis...

1. Q: Mais dis moi, comment on trouve les SDR(String Data Reference, c'est-à-dire les différents affichages de texte que l'on retrouve dans le programme.)
R: Et bien tout simplement en faisant Clic-droit => Search For => All referenced text strings... Et là... paf , plein de phrases partout... aie aie aie... enfin voici comment tu dois rechercher certaines données ;) Pour ceux qui n'ont pas compris, voici une image ;)



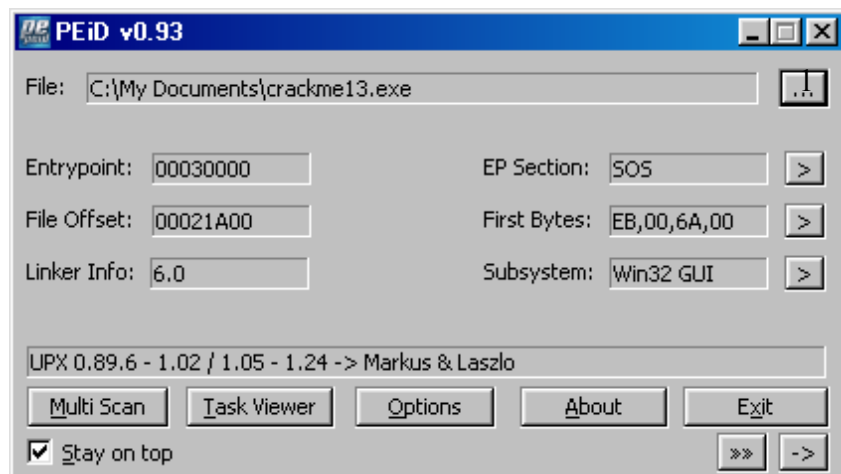
Ensuite après avoir cliqué sur All referenced text strings,
tu auras ceci...



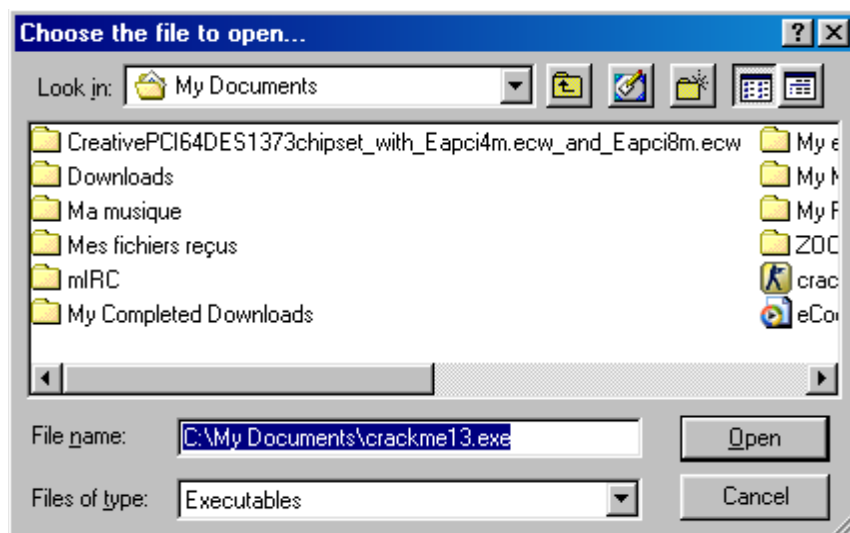
Dam Dam Dam Dam!!!!

Voila pour ce qui est de l'utilisation de Olly, il est vrai que tout n'a pas été abordé, mais tu peux toujours nous poser tes questions ici : <http://xtx.free.fr>

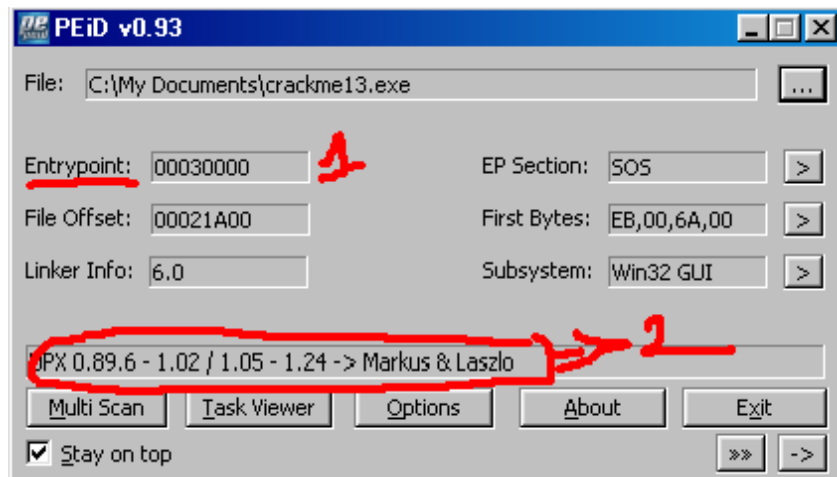
Ensuite vient Peid:



Tout d'abord, tu dois cliquer en 1, sur le bouton avec les trois petits points, tu verras apparaître une petite fenêtre comme celle-ci:



A ce moment, tu dois choisir le fichier à analyser, tu vas l'ouvrir et puis, bim bum bam, qu'est ce que tu trouveras? Tu trouveras ça:

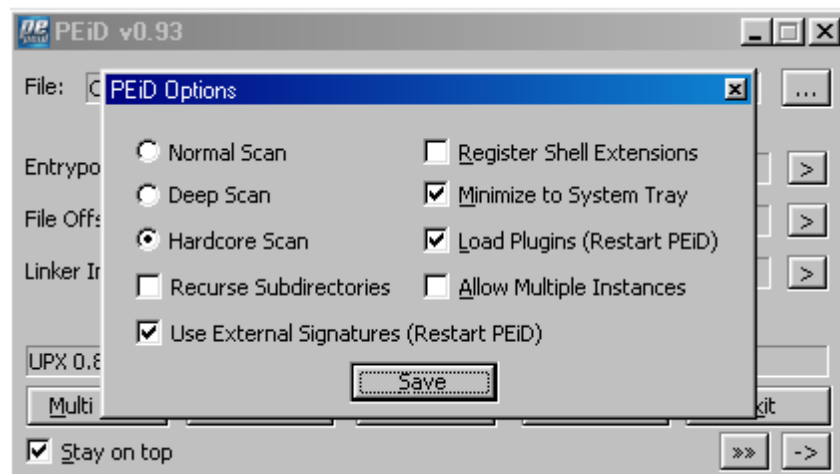


Oulla alors, qu'est ce que ça peut bien vouloir dire???

Les deux éléments importants pour l'instant se trouvent en 1 et en 2:

1. Entrypoint: Point d'entrée du programme, que tu peux modifier avec LordPE ;) , c'est bien pratique pour l'unpacking, surtout quand un programme est packé avec UPX 8-) :D
- 2.) Ici on voit avec quel protection le programme a été packé ;) Tu verras que tu pourras utiliser Google ton meilleur ami pour rechercher un unpacker ou bien trouver un tuto sur l'unpacking manuel ;).

Souvent, on n'arrive pas à detecter de signature...
donc qu'est-ce qu'on fait? On clique sur options et là...



En temps normal PeiD se met sur Normal Scan ou Deep Scan mais là on peut se mettre sur Hardcore scan si on n'arrive pas à trouver de signature ;)

THE END OF PART 1...

Merci à tous les membres de la NCT pour ce tuto.

Arch Enemy.