Menu

News

Forum

Liens

Outils

Livre d'or

Tutoriaux

Flash Decompiler

Cracking

Photoshop

Cracking : le .net, incrackable ?! Land-Of-Bork0

Salut à tous !

Dans ce tuto, on va s'attaquer a une protection reputée pour etre incrackable...le .net (dotNet).

Euh, le .net c'est une extension de site web ?! Et puis pourquoi dotnet, .net ?

Le dotnet (dot veut dire point '.' in english) est la nouvelle génération d'application multiplateforme microsoft Simple non.. Bon ok, je refais Je vais pas vous faire un cours détaillé sur le .net et le frameworks, on va s'interesser à la partie languages de programmation. Vous devez surement connaitre (au moins de nom) les languages de programmation basiques comme le C, C++, Visual Basic, Delphi, Java, PHP, ASP ? Et bien, microsoft a développé des nouveaux languages de programmation tel le C#.net (prononcez Csharp, sharp = #), le C++.net, le Visual Basic.net, l'ASP.net, le Delphi.net, etc... qui fonctionne à condition d'avoir installer ce qu'on appelle le FrameWorks, c'est une 'plate-forme' qui permet de faire fonctionner toutes les applications programmées dans n'importe quel language .net, vous pouvez telecharger la dernière version du frameworks sur le site de microsoft. Pour faire des applications dans les languages .net (à noter que le language .net le plus utilisé par microsoft est le C#) vous devez disposer soit de microsoft visual studio 2005 (ou 2003) mais vous pouvez aussi prendre les versions express (gratuites) qui permettent de programmer dans un seul language et sont un peu limités (enfin, limité, vous avez quand meme énormément de possibilités encore !). N'oubliez pas de telecharger le frameworks !

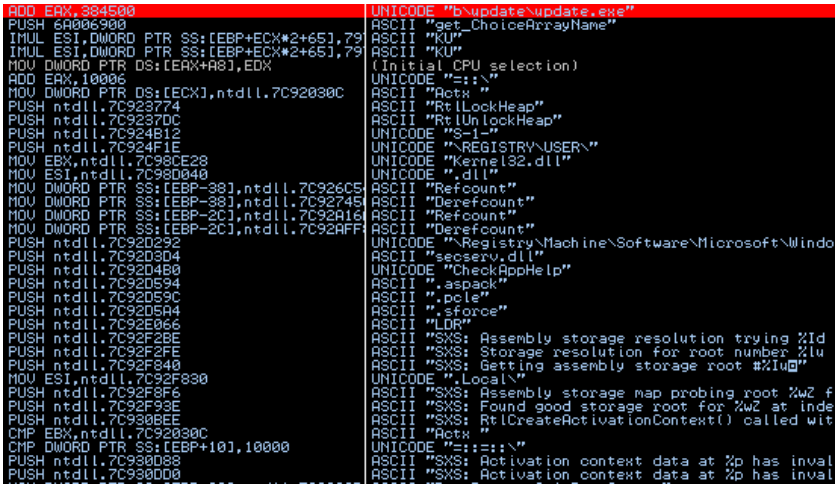
Je vous ai concocté un petit crackme en C#.net

Telecharger le crackme (140 Ko)

On le lance, il nous demande un joli password, on en met un bidon et hop :

Vous pouvez le scanner avec PEid, il vous dira "Microsoft Visual C# / Basic .NET"

Bon, on va d'abord tester avec Olly Lancez le, après un long moment d'attente, on voit du code apparaitre, allez voir dans les SDR :



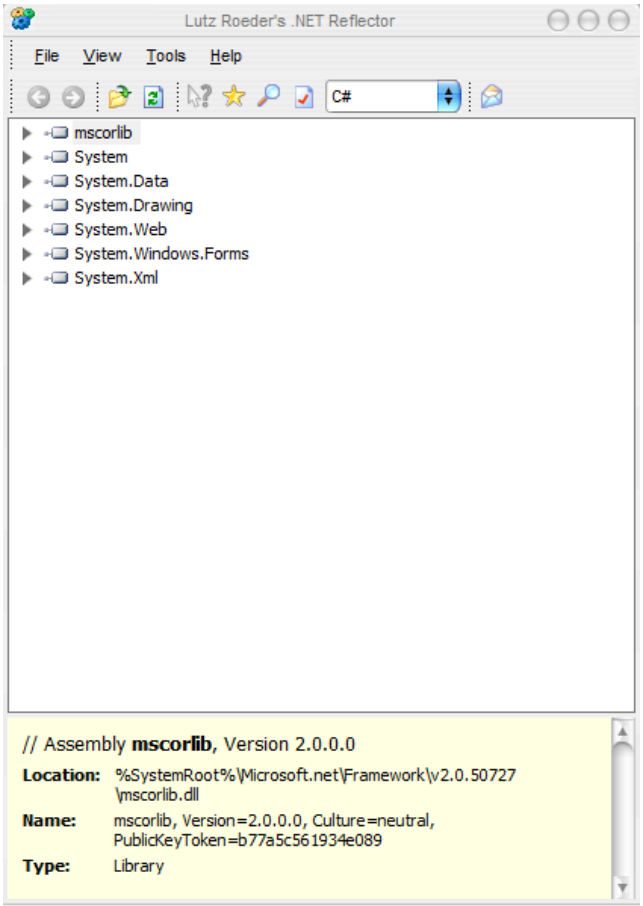
Si vous etes suicidaire, vous pouvez tout regarder ligne par ligne en éspérant trouver une information que vous ne trouverez pas... Pour les autres, fermez Olly, il ne sera pas de la partie aujourd'hui !

 Et on fait quoi alors ?!

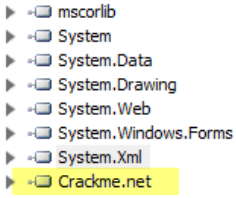
Le frameworks ayant un compilateur spécial (le meme pour tout les languages donc exactement la meme vitesse), il est possible de voir le code, après compilation, presque intact ! Il existe plusieurs logs, j'ai choisi "reflector qui est simple et petit...

Telecharger reflector

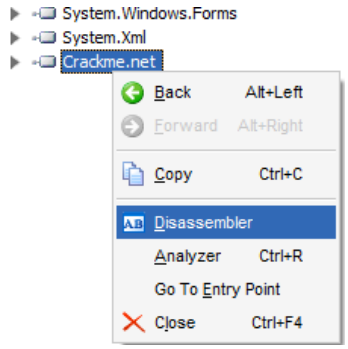
Après l'avoir extrait n'importe ou, lancez le :



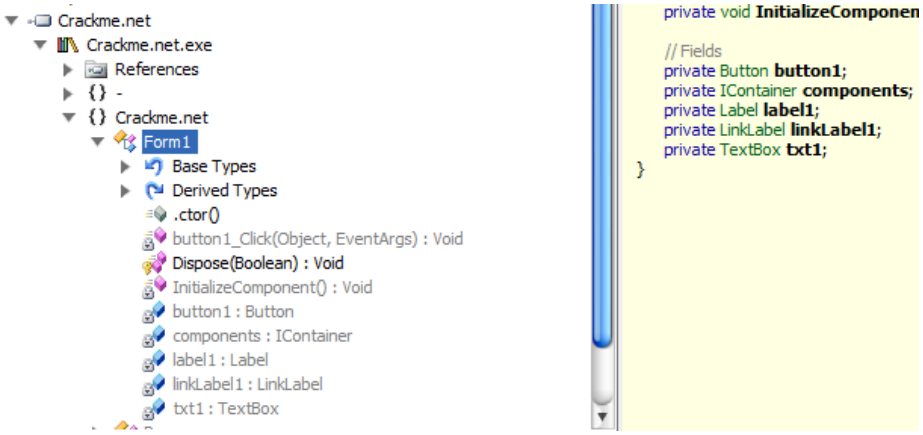
ne nous occupons pas du coeur, mais regardons les menu, on voit "File", soyons fou, essayons d'ouvrir notre petit crackme ! (File » Open » crackme.exe)



Crackme.net est apparu dans le coeur ! Cliquez dessus, le petit menu du bas change, mais rien de bien intéressant... Faites clique droit » Disassembler :



Un ecran s'ouvre a droite. Faites un double clic sur Crackme.net dans le panneau de gauche puis cliquez sur crackme.net.exe, recliquez sur crackme.net et enfin cliquez sur form1 :



Alors, qu'est ce que c'est que tout ce charabia, pour ceu qui connaissent la programmation orientée objet ça devrait etre bien plus facile :

- Form1 = C'est la fenetre principale du programme
- button1 = le boutton "valider !"
- label1 = le texte "password"
- linkLabel = le lien vers mon site
- textBox (txt1) = la "boite a texte" ou on rentre le password

On se retrouve avec tout les éléments de la form dans le menu de droite et dans le panneau de gauche on retrouve les memes avec quelques autres trucs en plus

On va s'interesser à button1_click, qu'est ce que c'est ?! Ce sont les évènements lorsqu'on clique sur le boutton "valider" , notre routine va etre surement ici ! Cliquez dessus :

```
private void button1_Click(object sender, EventArgs e)
{
    if (this.txt1.Text == "modem")
    {
        MessageBox.Show("Identification Reussie...", "Bon Pass", MessageBoxButtons.OK, MessageBoxIcon.Asterisk);
    }
    else
    {
        MessageBox.Show("Mauvais identifiants...", "Et non !", MessageBoxButtons.OK, MessageBoxIcon.Hand);
    }
}
```

Ceux qui font de la progz auront deja compris, pour les autres, une petite explication :

private void button1_Click(...) = *indique le début des événements d'un clic sur le boutton*

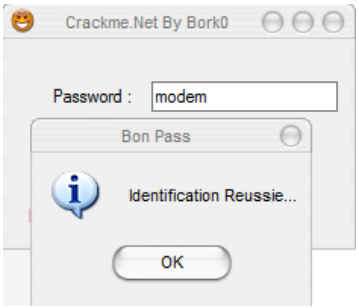
if(this.txt1.Text == "modem") = *Litéralement "Si le texte de la boite de texte txt1 est égal au mot modem alors" , c'est une condition !*

MessageBox.Show("identification réussie",...) = *Affiche une message box (boite de message contenant le message identification réussie ! C'est le bon message.*

else = *Sinon (si txt1.text n'est pas égal a modem alors)*

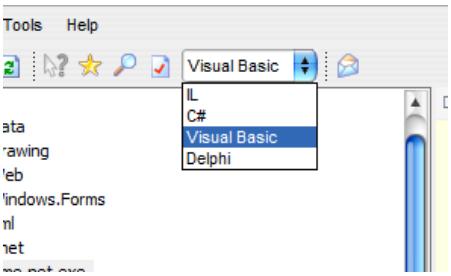
MessageBox("mauvais identifiants", ...) = *Affiche la message box d'erreur !*

Vous pouvez tster de mettre "modem" et hop :



Pour les autres crackmes en .net, c'est toujours le meme système ! Ici, ce n'est pas vos talents de crackers qui seront mis a l'épreuve mais plutot votre bonne analyse du code et une bonne connaissance des languages de programmation

Maintenant, je vais vous montrer comment changer le language de programmation affiché, imaginons que vous soyez une brêle en C# mais que vous soyez super fort en delphi ou vb, on peut changer le language ! Pour cela, faites comme sur l'image :



Et hop, le language change instantanémenent ! Pratique non ?

Vous l'aurez surement remarqué, on ne peut pas "cracker" a proprement dit, a savoir modifier les sauts conditionnels et tout le touintouin habituel quoi, ben oui, c'est l'inconvénient, vous ne pourrez pas le cracker mais vous pourrez avoir la source et donc retrouver intégralement les routines de génération du sérial, les password !

je n'ai encore jamais testé cette technique sur des programmes payants, mais à moins qu'il existe une sécurité particulière, ça doit surement marcher aussi

Enjoy

Keygenner un keymaker / Analyser le code d'un crackme

RETOUR EN HAUT / INDEX DU CRACKING / INDEX DU SITE / FORUM