

My submission to the Honeynet Project Forensic challenge 2010/3

publié par malphx le vendredi, mai 14 2010 - 22:23



The Honeynet Project's team has published the results for [their last forensic challenge](#).

Congratulations to the Winners !

This time, luck was not with me and I was not in the top 3, but came only in 4th position.

Because only the winners submissions are published on the Challenges official site, I publish mine here for review and comments.

Unfortunately, I misunderstood question 5...

This challenge was really good and again taught me a lot of new things and new tools.

My official results:

For this 3rd challenge, we received a total of 22 submissions. With your score of 41, you came into position 4. You placed into the top third. With the many great submissions and the competitive field, this is a great accomplishment. Congratulations.

Below you will find your score per answer:

- Answer 1: 2 points
- Answer 2: 4 points
- Answer 3: 2 points
- Answer 4: 4 points
- Answer 5: 1 points
- Answer 6: 8 points
- Answer 7: 2 points
- Answer 8: 6 points
- Answer 9: 4 points
- Answer 10: 5 points

In addition, you have received 3 bonus points.

You could find my submission here:

[franck_dot_guenichot_at_orange_dot_fr_Forensic_Challenge_2010_-_Challenge_3.pdf](#)

Feel free to leave a comment !

Crackme#4: le dernier pour l'instant

publié par malphx le dimanche, novembre 25 2007 - 17:57

Toujours écrit en ASM et packé avec mon protector perso.
D'ailleurs c'est la partie qui m'intéresse le plus dans cette discipline, je parle de la partie protection de PE
Car vous le verrez, une fois unpacké, le crackme en lui-même est facile.
[Publication et solution sur crackmes.de](#)

Le readme:

```
It's time for crackme4.
I wish that you will have fun defeating it ! If U can :p
=====
Code: ASM
Protection: Custom
Level: 3 (i think)
=====
Objectives:
Required: Make a keygen or patch (but a keygen is better)
Required: submit a tuto on crackmes.de
Required: Rate it !
Optional: Unpack
Optional: Describe the protector.
=====
Rules:
>>> everything is allowed but,
>>> serial fishing is not a valid solution
=====
tested on WinXP PRO SP2, WinXP Home SP1, and Win2K3 server
Entreprise Edition.
You could send me your solution or bug report (email is in my
crackmes.de profile)
Good work !
Znycuk
```

[znycuk crackme#4](#)

Pour l'instant c'est le dernier de la série, j'espère bien continuer et sortir #5 pour lequel j'avais quelques idées, cependant le temps me fait défaut.
Plus tard peut-être...

Crackme#3

publié par malphx le dimanche, novembre 25 2007 - 17:46

Le 3eme de la série, celui ci est aussi protégé par un packer custom

[Diffusé en juin 2006 sur crackmes.de](#)

Il a évidemment été solutionné par les reversers du site mentionné plus haut.

Voici le readme original:

Hi,

Here is crackme#3, i think this one will be hard for real newbies.
But not for the good reversers from crackmes.de :-)

I wish that you will have fun defeating it !

Note: My RDG Packer Detector seems to have a false positive on it.

```
=====
Code: ASM
Protection: Custom
Level: 2 (maybe)
=====
```

Objectives:

- _ Unpack if needed
- _ Make a keygen
- _ submit a tuto (it should also describe the protector)

```
=====
Rules:
>>> Patching the goodboy jump is not allowed
As a Keygen is required: no serial fishing
```

Crackme#2 "Find my passw0rd"

publié par malphx le dimanche, novembre 25 2007 - 17:37

Celui ci aussi a bien évidemment été [publié sur crackmes.de](#),
en mai 2006.

Le readme:

Hi,
This is my crackme # 2 Find my passw0rd.
In this one, i've try to make the job a little harder.

Code: ASM
Protection: Custom
Level: 2

Objectives:
_ Unpack if needed
_ Find the password
_ submit a tuto

Rules:
Patching not allowed...

tested on WinXP SP2 but should work on SP1 and Win2K.

Good work !
Znycuk

[znycuk crackme2 Find my Passw0rd](#)

Pour celui là, j'avais commencé un projet de packer/protector très simple.

Crackme#1

publié par malphx le dimanche, novembre 25 2007 - 17:13

Le fichier readme original, posté sur le site crackmes.de

Hi all,
This is my first Keygenme, written in ASM.
_ Find the solution
_ make a keygen
_ And submit a tuto
tested on WinXP SP2 but should work on SP1 and Win2K.
Good work !
Znycuk

Ah oui, je poste sous le pseudo znycuk sur le site crackmes.de,

je vous laisse trouver le lien avec mon pseudo original...

[znycuk keygenme#1](#)

[La solution pour ce crackme](#) peut être trouvée sur le site crackmes.de.

a+