Installation & Utilisation de OphCrack

Par Valérian Castel (68700)
Le 18/03/2009
Security Labs @ Caen

Sommaire

- ***Introduction***
  - *Ophcrack, c'est quoi ?*
  - *Que va-t-on apprendre dans ce tutorial ?*

- ***Téléchargement***
  - *Miroirs de téléchargement*
  - *Gravure*

- ***Installation***
  - *Ajout d'une table de scan*
  - *Lancement du logiciel*

- ***Utilisation***
  - *Exemple d'utilisation*

- ***Principe de fonctionnement***
  - *Où sont stockés mes mots de passe ?*
    - *LM Hash*
    - *NT Hash*
  - *Les tables Arc-en-Ciel (Rainbow Tables)*
    - *Introduction et description*
    - *Méthode de recherche d'un mot de passe*
    - *Un petit exemple concret ?*

- ***Conclusion***
  - *Contre mesures*

Introduction

Ophcrack c'est quoi ?

Ophcrack est un logiciel libre, conçu pour récupérer les mots de passe utilisateurs de Windows. La quasi-totalité des mots de passe pouvant être récupérés par cette méthode, selon quelques restrictions. Tout d'abord, les mots de passe doivent êtres de taille inférieur ou égal à 14 caractères alphanumériques. Ensuite, Ophcrack est utilisable de deux façons différentes : avec le LiveCD ou par un exécutable.

Attention, ce tutorial a pour but de vous expliquer comment tester vos mots de passe, et non comment cracker les mots de passe du voisin.

Que va-t-on apprendre dans ce tutorial ?

Dans ce tutorial, on va apprendre à utiliser ce logiciel. On va aussi voir le principe de fonctionnement, qui se rapproche plus ou moins d'un brute forcing, mais qui ne l'est pas [*Le brute forcing est une méthode qui permet de trouver un mot de passe en testant toutes les entrées contenues dans une bibliothèque prédéfinie.*] Grâce à ce tutorial, il est possible de récupérer les mots de passe utilisateurs sans avoir de connaissances approfondies en informatique. Vous allez voir, c'est très simple d'utilisation.

Néanmoins le principe de fonctionnement reste assez complexe. Mais nous allons quand même voir comment fonctionne ce petit logiciel.

Vous êtes prêts ? C'est parti !

Téléchargement

Pour récupérer ce logiciel, rien de plus simple. Voici l'adresse où vous pourrez le télécharger.

http://ophcrack.sourceforge.net/

Ici, vous pourrez trouver le LiveCD ainsi que l'exécutable. Pour l'exécutable, il prend en charge Windows XP et Windows Vista. Pour le LiveCD, il y a le choix entre XP ou Vista. Tout dépend sous quel système vous souhaitez tester vos mots de passe. Un LiveCD se présente sous forme d'image ISO.

Une image ISO ?

Oui, c'est une image CD généralement d'un logiciel, ou d'un système d'exploitation. C'est un fichier directement gravable sur un CD, ou un DVD, grâce à un logiciel de gravure. Il suffit de graver le CD en sélectionnant « Graver une image » dans votre logiciel de gravure préféré.

Quelques liens pour des logiciels de gravure gratuit capable de graver des images CD :

- **Free Create-Burn ISO 2.0** qui est conçu spécialement pour graver des images ISO :

  http://www.clubic.com/telecharger-fiche186590-free-create-burn-iso.html

- **Free easy CD-DVD burner**, qui est un logiciel de gravure gratuit, classique et efficace :

  http://www.clubic.com/telecharger-fiche55986-free-easy-cd-dvd-burner.html

Une fois le CD gravé, il vous reste plus qu'a passer à l'installation et au lancement de l'application.

Installation

Ajout d'une table de scan.

Note : L'ajout d'une table de scan est réservé à des utilisateurs un minimum expérimentés.

Ophcrack est un logiciel qui utilise des tables appelées tables arc-en-ciel. Pour augmenter l'efficacité du logiciel, on peut avoir une table de scan plus grande.

On peut notamment trouver la version SSTIC04-5k, en cherchant rapidement sur Google. Mais pour la plupart des liens, il faudra passer par bitorrent. A vous de trouver votre bonheur sur internet, néanmoins la plus part des tables plus importante ne sont pas gratuites.

Après avoir récupéré la table souhaitée, il vous faudra un logiciel qui décompresse l'image ISO du liveCD, UltraISO est le logiciel qu'il vous faut.

Vous pourrez trouver la version d'évaluation ici : http://www.clubic.com/telecharger-fiche42685-ultraiso.html

Après avoir installé ce logiciel, il faut ouvrir l'image ISO avec ce logiciel (clic droit sur l'ISO puis ouvrir avec… et sélectionnez UltraISO.)

Une fois arrivé dans le logiciel, il vous faut trouver le dossier 10000 et remplacer l'intégralité de son contenu par le contenu du zip téléchargé auparavant. La nouvelle table remplacera l'ancienne qui est moins complète. Une fois cette manipulation effectuée, vous n'avez plus qu'à enregistrer l'image ISO.

Attention : dans la plupart des cas, la table étant importante, l'ISO prendra plus de place qu'auparavant, et du coup, il faudra utiliser un DVD et non un CD.

Voilà le tour est joué, vous avez maintenant une table de scan plus importante !

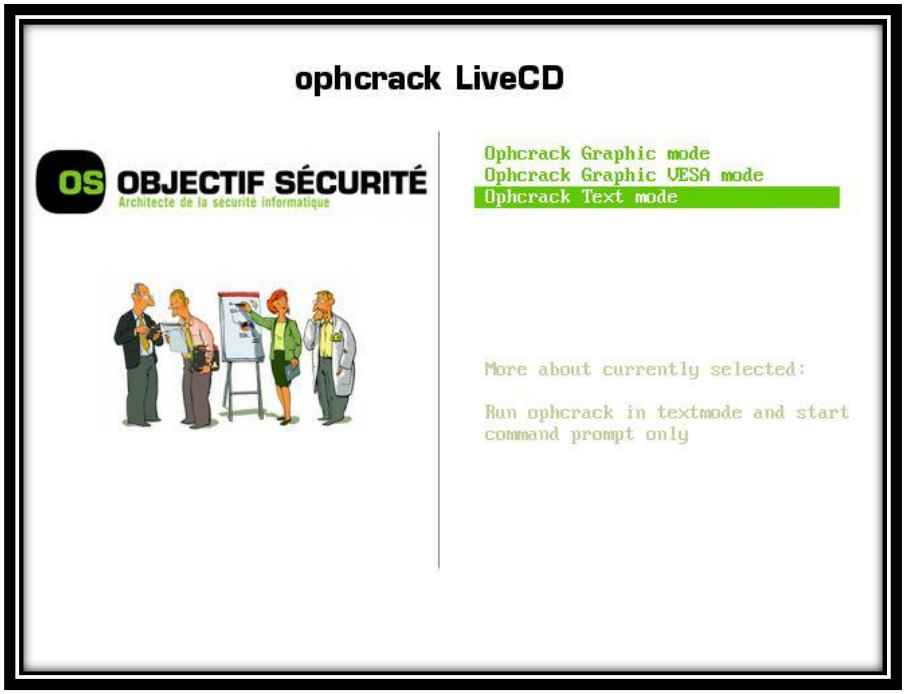
Lancement du logiciel

Et voilà, ça commence, on va enfin lancer la bête !

Pour l'exécutable, il suffit de le lancer et de suivre les instructions d'installation. Vous devez être connecté à internet afin de récupérer les tables de scan. C'est lors de l'installation que vous choisissez les tables à installer. Vous avez le choix entre small WinXP tables, fast WinXP tables, et free Vista tables. Bien entendu, cela ne sert à rien de tout prendre. Si vous tournez sur Vista, le choix est vite fait. Par contre si vous êtes sur XP, l'idéal est de prendre la version fast. En effet, cette table est plus grande [703MB] que la small WinXP tables [380MB].

Pour le LiveCD, il n'y a pas d'installation à effectuer. Il vous suffit de booter directement sur le CD. Pour cela il vous faut modifier la priorité de boot dans le BIOS. Pour accéder au BIOS, lorsque vous allumez votre ordinateur, il faut appuyer sur une touche dès le démarrage, celle-ci diffère selon les machines. Parfois ce sera F2, parfois Suppr. Soit vous avez de bons yeux, et dans ce cas il faut voir ça dès le démarrage, soit vous faites plusieurs essais, et vous finirez bien par trouver la touche correspondante !

Une fois dans le BIOS, il faut trouver le paramètre du type « Boot Priority », encore cela diffère selon les machines. Une fois que vous avez trouvé, il faut mettre CD/DVD en « 1st Device » et normalement le disque dur (HDD) prendra la place du CD/DVD. Une fois cette manipulation effectuée, il faut sauvegarder et quitter, en tapant F10, puis Y pour confirmer. L'ordinateur redémarrera en bootant sur le CD (Bien sûr si celui-ci est dans le lecteur !)



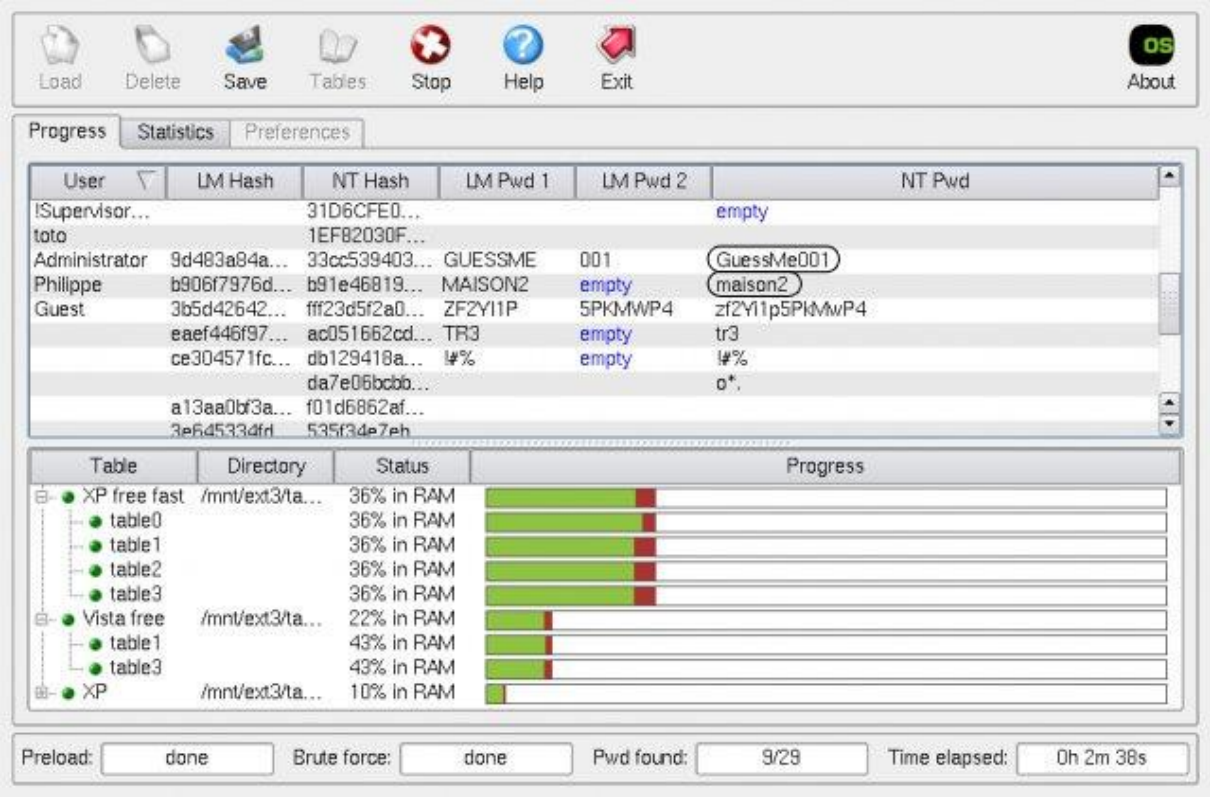
Ensuite, trois choix s'offre à vous (voir la photo ci-dessus) : Graphic mode, Graphic VESA mode, et Text Mode. Je vous conseille le Graphic mode, mais si celui-ci ne passe pas, il faut utiliser le Graphic VESA mode, qui utilise des drivers généric avec une résolution de 1024x768 de base. Le Text Mode est réservé à des utilisateurs plus expérimentés.

Vous avez réussi à lancer le LiveCD ? Voyons maintenant comment récupérer vos mots de passe !

Utilisation

Exemple d'utilisation

Passons à l'aspect pratique ! Une fois le logiciel lancé, que ce soit en LiveCD ou en exécutable, vous aurez la même fenêtre d'affichée. Il vous suffira donc de cliquer sur Crack pour que le logiciel obtienne les mots de passe utilisateurs. Cela peut prendre quelques minutes comme plusieurs dizaines de minutes. Une fois lancé, petit à petit les mots de passe seront visibles comme ceci :



Comme on le voit, on obtient le mot de passe Administrator qui est « GuessMe001 » ainsi que le mot de passe de Philippe qui est « maison2 ». On peut stopper la recherche si on veut en cliquant sur le bouton Stop. Parfois lorsque vous allez vouloir lancer le Crack, le programme n'arrivera pas à charger les tables. Dans ce cas, il faut cliquer sur Tables, puis sélectionner le dossier 10000 qui se trouve dans le répertoire du LiveCD. En ce qui concerne l'exécutable, les tables se trouve dans le dossier correspondant appelé « tables ». Comme vous pouvez le voir, ce logiciel s'utilise très simplement, et est très efficace !

Principe de fonctionnement

Où sont stockés mes mots de passe ?

LM Hash

LM hash, alias LAN Manager hash, est un format utilisé par Microsoft Windows pour stocker les mots de passe d'une taille inférieure à 15 caractères. Ce format est utilisé jusqu'à Windows Millenium. Pour les versions ultérieures, le format utilisé est NT hash, même si LM hash reste présent pour assurer la compatibilité avec les anciens systèmes (Compatibilité descendante).

NT Hash

NT hash est donc un format utilisés pour les versions de Windows utilisant Windows NT. C'est-à-dire les versions ultérieures à Windows Millenium. Ce format est aussi utilisé pour stocker les mots de passe de taille inférieure à 15 caractères.

Les Tables Arc-en-ciel (Rainbow Tables)

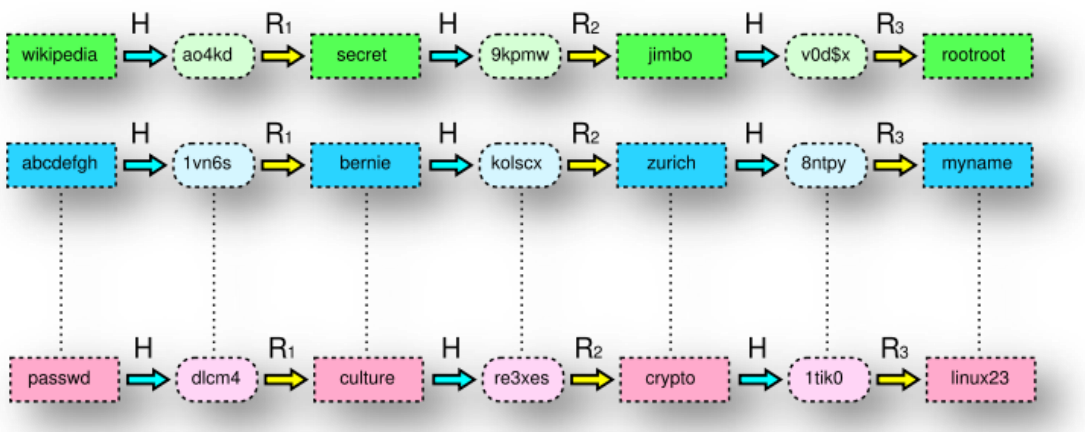
Introduction et description

Nous allons rentrer dans le vif du sujet, par quelle méthode ce logiciel récupère t'il vos mots de passe ?!

Une table arc-en-ciel c'est quoi ?

Une table arc-en-ciel est une structure de données. Elle est utilisée en cryptographie afin de retrouver des mots de passe cryptés grâce à leurs empreintes. C'est une amélioration du compromis temps-mémoire proposé par Martin Hellman et on doit cette méthode des tables arc-en-ciel à Philippe Oechslin.

Cette structure de données est constituée de lignes chaînés, avec un mot de passe de départ, et un mot de passe d'arrivé. Entre ces deux mots de passe, celui de départ subit un certain nombre de réduction à la suite, pour atteindre le dernier. Voyons cela dans un schéma, de façon plus claire :



Les fonctions de réductions ne sont pas toutes identiques, cela permet d'éviter les risques de collisions.

Nous voyons donc que chaque ligne est une succession de fonctions. Le dernier mot de passe de la ligne est donc une composée d'un certain nombre de fonction. Cela pourrait se visualiser comme cela :

P -> H(P) -> R1(H(P)) -> H(R1(H(P))) -> R2(H(R1(H(P))) -> … Et ainsi de suite.

P : Mot de passe
H : L'empreinte du mot de passe
Rx : La fonction de réduction

METHODE DE RECHERCHE D'UN MOT DE PASSE

Alors nous allons voir un petit exemple afin de mieux comprendre le fonctionnement des tables arc-en-ciel. Ophcrack récupère donc une empreinte appelé H dans NT hash ou LM hash.

Tout d'abord, Ophcrack va prendre H et lui appliquer la dernière fonction de réduction. Le logiciel va ensuite comparer le résultat avec les mots de passe de la fin de chaque ligne de la table. Si une correspondance est trouvée, on reprend le premier mot de passe de la ligne, on génère cette chaîne, et on compare chaque empreinte de la ligne avec l'empreinte cherchée.

Si aucune correspondance n'est trouvé dans lors de la première recherche, on utilise une seconde réduction sur l'empreinte H, et on relance la recherche entre le mot de passe trouvé et ceux de la dernière colonne. Si cette recherche réussi, on effectue la même manipulation : génération de la chaîne puis comparaison avec différentes empreintes de la ligne.

Si la recherche échoue, on réalise une troisième réduction, et ainsi de suite jusqu'à ce que la recherche soit concluante.

UN PETIT EXEMPLE CONCRET ?

Soit l'empreinte H contenant « kolscx ». Nous allons donc utiliser une dernière fonction de réduction de la table, R3, qui nous donnera par exemple « jacques ». En comparant ce mot de passe avec tous les mots de passe en fin de chaque ligne, on remarque que « jacques » n'y figure pas.

On va donc utiliser l'avant dernière fonction de réduction, R2, et là on va trouver « zurich » puis on effectue une fonction H, et encore la fonction R3, pour arriver à « myname ».

En comparant « myname » avec les dernières occurrences de chaque ligne, on se rend compte que « myname » est présent. On prend P, le mot de passe de base et on génère la ligne chaînée. Ensuite, on effectue les fonctions de réduction une à une, et on compare chaque empreinte trouvée avec celle recherchée « kolscx ». Une fois trouvé, c'est donc le mot de passe précédant l'empreinte qui est le mot de passe recherché. En l'occurrence il s'agit de « bernie ».

Conclusion

Contres mesures

Tout d'abord, l'idéal est d'utiliser un mot de passe d'au moins 15 caractères. Cela fait un peu long, mais au moins vous passerez au travers de ce risque.

Ensuite il existe une méthode plus sécurisé, qui permet de passer au travers des mailles du filet aussi ! En effet, on peut rajouter ce qu'on appelle un « sel » au mot de passe. Un sel peut être par exemple les premiers caractères de l'identifiant de l'utilisateur. Cela permet de différencier deux utilisateurs qui auraient les deux mêmes mots de passe aussi et donc éviter les risques de collisions.

Cette méthode de sel est nettement plus efficace néanmoins en rajoutant des caractères autres qu'alphanumérique. En effet, les tables arc-en-ciel sont prévues pour des mots de passe à caractère exclusivement alphanumérique. Ainsi, grâce à cette méthode, on pourra sécuriser au maximum ses mots de passe.

Bien entendu cette méthode de sel va au-delà des mots de passe utilisateurs Windows puisqu'elle n'est pas utilisée par ce système d'exploitation. Néanmoins, sur GNU/Linux, cette méthode est utilisée.

A savoir que les tables arc-en-ciel sont utilisées pour beaucoup de cryptages, tels que MD5, SHA-1 et bien d'autres encore. Sans la méthode du sel, le cryptage deviendrait complètement obsolète. Ce qui est le cas pour les systèmes d'exploitation Windows, dont les mots de passe sont crackables au maximum en une demi heure.

Pour conclure, les tables arc-en-ciel sont des armes redoutables pour les systèmes qui n'utilisent pas de sel. Les systèmes tels que Windows XP ou Windows Vista ne sont absolument pas sécurisés pour ce genre d'attaque par exemple.

Merci à Wikipédia pour les Rainbows tables.