Piratage d'utilisateurs - 1/2

Ici, je vais tenter d'expliquer deux méthodes simples (et me paraissant intéressantes) de piratage de comptes d'utilisateurs : la force brute, et le keylogger.

Cet article a pour but de vous expliquer deux méthodes particulièrement intéressantes dans le piratage informatique des comptes d'individus. La première est la technique de force brute, pouvant être utilisée n'importe quand sur n'importe quel compte présent sur un serveur sur le net. Elle ne nécessite pas de toucher au PC de l'individu, mais elle est très lente, et parfois contrée. La seconde est une technique plus subtile : l'utilisation d'enregistreurs de frappes, ou de keyloggers. Il s'agit de s'infiltrer dans le PC de l'individu en lui envoyant un quelconque keylogger et en le faisant lui accepter, puis de récupérer facilement ses données grâce à ce logiciel. L'avantage est ici la rapidité et l'efficacité ; mais le problème principal est qu'il faut faire en sorte que l'individu accepte de l'ouvrir une première fois, sans éveiller les soupçons.

Le but n'est ici pas d'initier quiconque au hacking, mais on dit qu'on se protège mieux de ce qu'on connaît bien ; et l'être humain ayant peur de l'inconnu, mieux vaut connaître ses ennemis potentiels.

Technique de forcing : la force brute

Le principe de la force brute est extrêmement simple, et est aussi aléatoire que son nom. C'est très simple : le logiciel est exécuté à partir de la machine de celui qui veut le code de l'autre, et il s'agit d'envoyer des requêtes de connexion à un serveur, connaissant uniquement son nom de compte. L'astuce est qu'en une seconde, un nombre important de combinaisons de mots de passe est essayé. Par exemple, le logiciel peut se connecter sur le serveur POP d'un hébergeur mail, et de tester avec un même compte un nombre important de mots de passe, jusqu'à ce que la requête de connexion soit acceptée ; auquel cas, le logiciel s'arrête et a trouvé le mot de passe.

On suppose qu'un compte soit nommé "azerty", et qu'on veuille découvrir son mot de passe sur un serveur POP mail. On envoie donc une requête au serveur "pop. Servermail. Com" avec "azerty" comme nom de compte, et "a" comme mot de passe. Tout de suite après, on envoie une autre requête avec "azerty" comme nom de compte et "b" comme mot de passe. Et ainsi de suite. A chaque requête refusée, on reçoit une réponse négative du serveur, le logiciel sachant l'interpréter. Puis, on arrive à "z". On teste alors les chiffres, les majuscules, la ponctuation acceptée par le serveur (parfois les points, les espaces, etc...). Arrivé à la dernière possibilité, qui est par exemple un points : ". ", on recommence, mais avec deux caractères. Cela donne "aa", puis "ab", puis "ac", jusqu'à "... ", et ainsi de suite jusqu'à trouver le bon mot de passe, qu'on connaîtra lorsque le serveur nous enverra une réponse positive.

Programmer un tel logiciel n'est pas si simple que cela : cette technique n'est pas totalement efficace. Par exemple, une requête peut facilement se perdre, et ça peut faire bugger le logiciel. Certains serveurs peuvent aussi bloquer les requêtes à partir d'un certain nombre, par reconnaissance de l'IP. De plus, cela requiert beaucoup de temps, surtout si le mot de passe est long. Un vrai logiciel logiciel de force brute prend compte de tous ces paramètres, et certains vérifient d'abord les mots de passe les plus courants avant de vérifier aléatoirement les mots de passe.

Par extension, cette technique peut servir n'importe où lorsqu'il faut déverrouiller un système quelconque grâce à un mot de passe.

Technique subtile : le keylogger

Piratage d'utilisateurs - 2/2

Tout d'abord, qu'est-ce qu'un keylogger ? En fait, un keylogger est un logiciel capable de s'ouvrir en arrière-plan dans un système d'exploitation et de récupérer toutes les touches tapées par l'utilisateur, tout cela sans se faire repérer, évidemment. Puis il l'envoie par mail, ou d'une autre façon le communique à celui qui est intéressé (souvent par connexion directe avec l'IP de l'expéditeur du trojan).

Les keyloggers sont nombreux. Certains sont efficaces, d'autres pas trop. Ce qu'il faut savoir, c'est que certains trient les touches de sorte à savoir quand l'utilisateur tape le mot de passe (et donc quel est le mot de passe). Evidemment, les plus connus sont aujourd'hui démasquer par les antivirus. Cependant, il est facile d'effacer et de recoder ou de coder directement un keylogger. Bien sûr, il faut se baser sur le système d'exploitation de la cible pour pouvoir avoir un logiciel optimal... Pour cela il suffit de passer par l'une des nombreuses failles du système ; plus un système est libre, plus il a de failles.

Les keyloggers peuvent être inclus dans des trojans, ou chevaux de Troie. Il suffit, pour qu'un keylloger (ou un trojan) soit efficace, qu'on envoie la partie client à la cible, et qu'on ouvre la partie serveur chez soi. Ainsi, toutes les données que peut fournir le client sont envoyées au serveur ; et l'utilisateur n'a plus que l'embarras du choix dans l'utilisation de ces données. Fichiers, touches, images à la webcam... Tout cela peut être récupéré. Pour cela, il faut que la cible ouvre la partie client. Il faut donc faire passer ça pour un autre logiciel, ou combiner cela à une image (pour camoufler le logiciel derrière).

N'oubliez pas : si vous refusez les fichiers qui peuvent vous nuire, (presque) rien ne peut vous arriver. Tout dépend donc de votre méfiance. Mais avant tout, il faut posséder un bon antivirus. Tout fichier exécutable inconnu ne doit être ouvert.

Mais avant tout... HAVE FUN !