



Éditorial

Des empreintes trop visibles

Guillaume Lehembre 

L'article de Philippe Oechslin et Cédric Tissières sur les RainbowTables vous a certainement fait réfléchir sur la qualité de vos mots de passe. Outre le fait que la complexité d'un mot de passe est primordiale, le stockage des empreintes (*hash*) l'est tout autant. En effet, beaucoup d'administrateurs et d'utilisateurs ignorent encore la présence d'empreintes très facilement cassables au sein de leur réseau, et ce, à la fois sur leurs serveurs et leurs postes clients. La présence de ces empreintes facilite grandement la tâche d'un éventuel attaquant et permet dans de nombreux cas la compromission massive de machines si un accès administrateur (ou *root*) est obtenu sur l'équipement. Le meilleur exemple reste les empreintes *LanManager* (LM) des machines Windows qu'on retrouve quasi systématiquement sur l'ensemble des systèmes d'exploitation de Microsoft, à l'exception du dernier né : Windows Vista. La suppression de ces empreintes peut se faire à l'aide d'une politique de groupe ou en modifiant la base de registres [1]. L'outil tiers TrashLM [2] peut être utilisé, suite à l'interdiction des empreintes LM, pour ne pas avoir à demander un nouveau mot de passe aux utilisateurs. L'ensemble des systèmes d'exploitation post Windows NT SP4 supportent NTLMv2 et peuvent être configurés pour n'utiliser que ce mécanisme d'authentification lors des échanges réseaux [3]. Néanmoins dans certains environnements, des anciens systèmes ou applicatifs nécessitent de conserver les empreintes LanManager, il est alors nécessaire d'utiliser des comptes dédiés pour ces derniers et accroître la sécurité des comptes sensibles :

- en utilisant des mots de passe de 15 caractères ou plus pour empêcher le stockage des empreintes LM,
- en utilisant des caractères accentués ou des caractères spéciaux ASCII (*ALT* + *<code>*).

Les tables Rainbow en téléchargement sur Internet ([4] entre autres) ont été faites pour des caractères non accentués et les principaux caractères présents sur les claviers (ponctuations, opérateurs, etc.). Un caractère spécial ou accentué au sein du mot de passe permet donc d'empêcher sa découverte via cette méthode ... sauf bien sûr si l'attaquant a généré des tables Rainbow supportant ces caractères :-)

Les empreintes stockées en cache sont d'un type différent mais restent méconnues, elles sont au nombre de 10 (par défaut) et permettent à un utilisateur en dehors de son domaine de s'authentifier sur sa machine. Si un attaquant réussit à devenir administrateur localement sur une machine, il peut extraire les mots de passe stockés en cache grâce à l'outil *Cachedump* [5] et ensuite tenter de les casser à l'aide d'attaques par dictionnaires ou force brute. Il arrive, de temps en temps, qu'un mot de passe valide d'administrateur du domaine assez faible s'y trouve. En effet, un compte avec des droits privilégiés est nécessaire pour l'insertion de la machine dans le domaine (d'où stockage de l'accréditation en cache) et par commodité il s'agit souvent du compte administrateur du domaine alors qu'un compte dédié restreint pourrait être utilisé.

À noter que le format des mots de passe ne permet - malheureusement - pas d'utiliser les Rainbowtables. Néanmoins, il est conseillé de limiter le nombre d'accréditations en cache à 1 [6] afin de stocker uniquement l'empreinte de l'utilisateur du poste. La protection et la sécurité des empreintes des mots de passe sont donc nécessaires pour la sécurité globale d'un système, tout comme peuvent l'être l'application des correctifs de sécurité, la sensibilisation à la qualité des mots de passe et la sécurité applicative.

- <http://support.microsoft.com/kb/299656/> [1]
- <http://www.toolcrypt.org/index.html?thrashlm> [2]
- <http://support.microsoft.com/kb/147706> [3]
- <http://rainbowtables.shmoo.com/> [4]
- <http://www.off-by-one.net/misc/cachedump.html> [5]
- <http://support.microsoft.com/kb/q172931/> [6] ●

À propos de l'auteur

Guillaume Lehembre est un consultant en sécurité informatique français travaillant pour le cabinet HSC (Hervé Schauer Consultants <http://www.hsc.fr>) depuis 2004. Il a travaillé sur différents audits, études et tests d'intrusion et a acquis une certaine expérience dans la sécurité des réseaux sans fils. Il a réalisé des interventions publiques sur ce sujet et a publié plusieurs articles dont un article dans le numéro 14 de hakin9 intitulé *Sécurité Wi-Fi - WEP, WPA et WPA2*. Guillaume peut être contacté à l'adresse suivante : Guillaume.Lehembre@hsc.fr