Hacker Highschool
SECURITY AWARENESS FOR TEENS

LEÇON 11
LES MOTS DE PASSE

Hacker Highschool
SECURITY AWARENESS FOR TEENS

ISECOM
INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES

"License for Use" Information

The following lessons and workbooks are open and publicly available under the following terms and conditions of ISECOM:

All works in the Hacker Highschool project are provided for non-commercial use with elementary school students, junior high school students, and high school students whether in a public institution, private institution, or a part of home-schooling. These materials may not be reproduced for sale in any form. The provision of any class, course, training, or camp with these materials for which a fee is charged is expressly forbidden without a license including college classes, university classes, trade-school classes, summer or computer camps, and similar. To purchase a license, visit the LICENSE section of the Hacker Highschool web page at www.hackerhighschool.org/license.

The HHS Project is a learning tool and as with any learning tool, the instruction is the influence of the instructor and not the tool. ISECOM cannot accept responsibility for how any information herein is applied or abused.

The HHS Project is an open community effort and if you find value in this project, we do ask you support us through the purchase of a license, a donation, or sponsorship.

All works copyright ISECOM, 2004.

Conditions d'utilisation de ce support

Ces leçons et supports sont gratuits et disponibles pour le public sous les conditions suivantes d'ISECOM:

Tous les travaux menés dans le cadre du "Hacker HighSchool" sont disponibles à usage non commercial auprès d'élèves du collège, du lycée, dans le cadre d'écoles publiques ou privées, ou encore lors de scolarisations à domicile. Ces supports ne peuvent être reproduits en vue d'un usage commercial. Il est expressément interdit d'utiliser ces supports dans le cadre de cours, leçons et/ou stages payants, à moins d'obtenir une licence pour cela (dans ce cas, veuillez aller sur *www.hackerhighschool.org/license*).

Le projet HSS (Hacker HighSchool) est un outil de travail et d'apprentissage, et en tant que tel, son utilisation relève de la personne qui l'utilise, et non de l'outil lui-même. ISECOM ne peut être mis en cause si cet outil est utilisé à mauvais escient ou de manière illégale.

Le projet HSS est aussi le fruit de l'effort de toute une communautés, et si vous trouvez ce projet intéressant, nous vous serions plus que reconnaissants de votre aide, soit par l'achat d'une licence, soit par un don, soit encore par un quelconque parrainage.

Table des matières

Personnes ayant contribué à ce projet

Kim Truett, ISECOM

Chuck Truett, ISECOM

J. Agustín Zaballos, La Salle URL Barcelona

Pete Herzog, ISECOM

Jaume Abella, La Salle URL Barcelona - ISECOM

Marta Barceló, ISECOM

Traduction

Bénoni Martin

ISECOM
INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES

LA SALLE
Enginyeria
Arquitectura
Universitat Ramon Llull

11.0 Introduction

Un des personnages principaux dans le film Matrix est le Maître des Clés. Protégé par la matrice et recherché par Neo, c'est effectivement un personnage important car il fait et détient les clés de la plupart des portes de la Matrice: cette dernière est un monde créé par ordinateur et ces fameuses clés sont des mots de passe. Dans ce film, il possède des mots de passe simples, des mots de passe pour les backdoors et des clés maîtres, en fait des mots de passe pour tout.

Les mots de passe sont des clés qui gèrent les accès, qui vous les autorisent alors qu'elles les refusent à d'autres, qui permettent de contrôler les accès aux informations (documents protégés par des mots de passe) ou les autres accès (des pages web protégées par mots de passe), ou encore qui gèrent les authentifications (prouver que vous êtes bien celui que vous prétendez être).

11.1 Les différents types de mots de passe

Il y 3 types principaux de mots de passe:

11.1.1 Chaînes de caractères

Les mots de passe les plus simples sont constitués de chaînes de caractères alphanumériques et de symboles qui sont fournis à partir d'un clavier. Ils vont du simple code à 3 chiffres utilisé pour ouvrir les portes de certains garages aux combinaisons complexe de caractères alphanumériques et de symboles recommandés pour protéger des applications hautement sensibles.

11.1.2 Chaînes de caractères avec un jeton

En passant à la vitesse supérieure, nous avons des mots de passe composés de notre chaîne de caractères précédente à laquelle on rajoute un jeton. Un bon exemple est l'ATM, qui nécessite à la fois une carte (notre jeton) et la connaissance du PIN -Personal Identification Number-. Cette méthode est considérée comme plus sécurisée que la précédente car il est nécessaire d'avoir les deux pour être authentifié.

11.1.3 Mots de passe biométriques

Plus complexe encore, nous avons les mots de passe biométriques. Ils utilisent des empreintes biologiques de certaines parties de notre corps, comme nos empreintes digitales afin de nous authentifier. Un autre exemple est l'empreinte rétinienne où c'est la rétine (c'est la partie qui est à l'arrière de l'oeil, coté interne) qui est photographiée. Cette rétine est constituée d'un réseau unique de vaisseaux sanguins et c'est ce réseau qui va être utilisé. Cette catégorie de mots de passe est considérée comme la plus sure, mais en réalité un mot de passe que vous portez sur vous n'est pas plus sécurisé qu'un mot de passe complexe que vous avez en tête, en assumant que le logiciel utilisé pour vérifier ce mot de passe est … sécurisé!

11.2 Historique des mots de passe

Quelques mots à propos ce cet historique:
Dans des versions anciennes de MS Word et Excel (versions avant Office 2000), les mots de passe étaient enregistrés en clair dans les en-têtes des documents. Il suffisait donc de lire cet en-tête pour avoir accès aux mots de passe!

Windows a enregistré une fois les mots de passe dans un fichier caché. Dans ce cas, si vous aviez oublié votre mot de passe, il vous suffisait de supprimer ce mot de passe pour le réinitialiser.

Plus proche de nous, Microsoft et Adobe ont rajouté la possibilité de protéger les documents avec un mot de passe. Mais ces fichiers pouvaient être ouverts sous d'autres applications comme Notepad sans problème.

Les bases de données Access de version 2.0 pouvaient être ouvertes comme un simple fichier texte en changeant l'extension en ".txt". Ce faisant, vous aviez accès aux données.

Les documents écrits avec Adobe version 4 ou inférieur étaient tous imprimables et même souvent lisibles en utilisant Linux PDF ou Ghostview pour Windows.

Les réseaux sans fil ont aussi quelques difficultés avec le cryptage car la clé de cryptage peut être devinée si vous collectez suffisamment de données cryptées. Avec la puissance de calcul que dispose un utilisateur lambda à l'heure actuelle, la clé peut être cassée presque immédiatement pour en tirer le mot de passe.

La sécurité sous Bluetooth est aussi réputée bonne, dès qu'elle est mise en place. Le problème est que Bluetooth transmet un beau mot de passe en clair, entre les deux parties. Si ce mot de passe est intercepté, toutes les communications ultérieures sont compromises.

Exercice. Téléchargez un fichier PDF sur Internet et essayez de l'ouvrir avec d'autres programmes. Les données sont-elles lisibles?

11.3 Construction d'un mot de passe solide

Les meilleurs mots de passe:

- ✔ ne figurent pas dans les dictionnaires,
- ✔ contiennent des nombres, des lettres et de symboles
- ✔ contiennent des majuscules et minuscules,
- ✔ plus ils sont longs, plus ils sont sécurisés (en général)
- ✔

Pour un mot de passe de 2 lettres, étant donné que l'alphabet a 26 lettres et qu'il y a dix chiffres différents (sans compter les symboles), cela fait 236 combinaisons possibles (soit 687000000 possibilités). Pour un mot de passe de 8 caractères, on a 836 combinaisons possibles, ce qui nous fait 324 000 000 000 000 000 000 000 000 000000 possibilités.

Il y a toute une panoplie de générateurs de mots de passe sur Internet, mais la plupart fourniront des mots de passe impossible à se souvenir.

Essayez donc plutôt une chaîne de caractères avec un moyen mnémotechnique pour vous en souvenir.

Par exemple:

gandt3b! (goldilocks and the 3 beans!)
JJPL2c1d (John, Jill, Paul, Lucy, 2 cats, 1 d - les habitants de votre maison)

Exercices:

1. Créez un bon mot de passe dont vous pouvez vous souvenir, et qui obtient un bon score sur http://www.securitystats.com/tools/password.php
2. Regardez les sites de trois banques différentes et trouvez quel type de mot de passe est requis pour autoriser l'accès à un internaute. Es-ce que ces banques proposent également des moyens de créer de bons mots de passe?

11.4 Cryptage des mots de passe

La plupart du temps, les gens ne se posent pas de questions sur le cryptage d'un mot de passe, car il semble n'y avoir pas grand-chose à dire: le mot de passe est crypté et c'est tout. Et pourtant ce n'est pas aussi simple que cela car l'efficacité d'un bon mot de passe dépend de sa force de cryptage, cette dernière pouvant aller de très faible à très grande.

Au niveau de cryptage le plus faible, nous avons le simple encodage des mots de passe. Cela produit un mot de passe qui n'est pas facile à lire au premier abord, mais qui est facilement déchiffrable (en connaissant la clé) avec un ordinateur, un papier et un crayon, ou un anneau décodeur en plastique découpé dans une boite de céréales. Le chiffrage ROT13 en est un bon exemple: il remplace chaque lettre du texte à chiffrer par la lettre 13 places plus loin dans l'alphabet (par exemple ABC sera crypté en NOP).

Même avec les meilleurs algorithmes, le cryptage sera aussi fort que le sera la clé utilisée. Par exemple pour notre ROT13 précédent, si nous considérons que le déplacement de 13 lettres constitue la clé, alors ROT13 est un algorithme très faible. Il peut cependant être renforcé en utilisant par exemple ROT10 (on remplacera alors chaque lettre par celle qui est 10 places plus loin dans l'alphabet) ou encore ROP-2 (auquel cas on prendra la lettre deux places avant dans l'alphabet). On peut le renforcer un peu lus encore en utilisant ROTpi: dans ce cas, la première lettre du texte à chiffrer sera remplacée par celle qui est 3 positions plus loin, la seconde par celle 1 position plus loin, la troisième par celle 4 positions plus loin et ainsi de suite, en prenant comme déplacement pour la $i^{ème}$ lettre du texte à chiffrer, le chiffre en $i^{ème}$ position de pi (3.14159265…).

A cause de ces possibles variations pour le cryptage, vous devez vous assurer que vous utilisez une méthode sure de cryptage et que la clé, celle qui ne dépend que de vous, vous assurera un cryptage robuste.

Pour finir, vous devez aussi vous souvenir qu'un bon système de cryptage est inutile sans une bonne clé de cryptage, de même qu'une bonne clé est tout aussi inutile sans un bon système de cryptage.

Exercices:

1. Voici une liste de fruits cryptés avec le cryptage ROT13. Essayez de les décoder:
    1. cbzzr
    2. benatr
    3. pvgeba
    4. zryba
    5. gbzngr

2. Trouvez sur Internet un site qui vous permette de décoder automatiquement le mots codés avec ROT13.

3. Il y a beaucoup de systèmes qui se disent systèmes de cryptage, mais ne sont en réalité que de simples systèmes de codage: un vrai système de cryptage nécessite une clé pour crypter et/ou pour décrypter. Parmi les propositions suivantes, lesquelles sont des systèmes de codage et lesquelles sont des systèmes de cryptage:
    1. Twofish
    2. MIME
    3. RSA

4. CAST
5. AES
6. BASE64
7. IDEA
8. 3DES
9. ROT13
10. TLS

11.5 Cassage & Récupération de mots de passe

Si vous cassez un mot de passe auquel vous n'avez pas le droit, c'est illégal. Par contre si c'est votre mot de passe qui protège vos informations et que vous l'avez oublié, vous êtes bloqué à mois de ne pouvoir le récupérer ou le casser.

Casser un mot de passe se résume à quelques techniques de base:

- Fureter autour de vous, des fois les mots de passe sont écrit sur un post-it, à coté des claviers, sous un tapis de souris, …
- Tenter une attaque par force brute, soit tester tous les mots de passe qui vous viennent à l'esprit l'un après l'autre,
- Attaque par dictionnaire. Des programmes existent pour automatiser l'attaque précédente et testent tous les mots de passe qui sont dans leur dictionnaire.

Il y a bon nombre d'outils sur Internet permettant de retrouver les mots de passe protégeant les documents. Cependant, les dernières versions de logiciels de bureautique deviennent de plus en plus sécurisées, rendant ainsi de plus en plus difficiles la récupération des mots de passe avec les techniques basiques décrites précédemment ou avec des outils de récupération de mots de passe.

Exercice. Identifiez 3 programmes différents utilisés pour créer des documents bureautiques (par exemple des fichiers texte, des tableurs, des archives, …) et qui permettent également de protéger ces documents par mot de passe. Ensuite essayer de trouver sur Internet des moyens de casser ces mots de passe.

11.6 Comment se défendre contre les cassages de mots de passe

Voici de se défendre contre ce genre d'attaques:

1. Utilisez des mots de passe solides et complexes, qui ne pourront pas se trouver dans un dictionnaire.
2. N'écrivez pas votre mot de passe à coté de votre ordinateur, là où tout le monde peut le lire.
3. Limitez les tentatives de connexion à 3 essais, puis verrouillez le compte. Ceci n'est valable pour les protections de documents, car ceux-ci ne permettent pas ce genre de verrouillage.
4. Changez régulièrement vos mots de passe.
5. Utilisez autant que possible des mots de passe différents. cela ne signifie pas pour autant que vous devez créer autant de mots de passe que vous avez de choses à protéger, vous pouvez mettre le même mot de passe pour votre site LesSIMS.com que pour votre compte dans votre magazine local, à condition d'utiliser des mots de passe bien plus solides pour des choses importantes.

Exercice. Examinez avec votre classe les recommandations listées dans ce document http://www.securitystats.com/tools/password.php

Pour en savoir plus

http://www.password-crackers.com/pwdcrackfaq.html
http://docs.rinet.ru/LomamVse/ch10/ch10.htm
http://www.securitystats.com/tools/password.php
http://www.openwall.com/john/
http://www.atstake.com/products/lc/
http://geodsoft.com/howto/password/nt_password_hashes.htm