

Mot de passe
JFC du 2 février 2016

Philippe Aymar – expert près la cour d’appel de Paris
Antoine Laureau - expert près la cour d’appel de Versailles

Casser les mots de passe – Quels mots de passe, pourquoi faire?

▶ Fichiers

- ▶ Un zip, un rar ,un docx, un PDF
- ▶ → accéder au contenu

▶ Environnements

- ▶ Un iPhone, un BB, un Android, un ...
- ▶ Un compte PC, un Mac, un Linux,...
- ▶ Un disque chiffré, Bitlocker, Filevault, TrueCrypt,...
- ▶ Un compte Gmail, un compte Hotmail, un compte Exchange, ...
- ▶ → accéder au contenu,
- ▶ → accéder aux paramètres d'environnements (organisation bureau,...)
- ▶ → accéder aux éléments de l'environnement qui sont perdus à la réinitialisation mot de passe (limite KonBoot)

▶ Trousseau – Coffre fort à mots clés

- ▶ La mémoire de tous les mots de passe (password safe, keepass, Apple Keychain, ...)

Les principes du mots de passe

- ▶ **Le principe**
 - ▶ Saisie du mot de passe
 - ▶ Transmission au système de vérification
 - ▶ Réponse matérialisée par un jeton d'accès
- ▶ **Système de vérification**
 - ▶ Local
 - ▶ Comparaison avec un hash du mot de passe stocké localement
 - ▶ Déporté
 - ▶ Comparaison avec hash du mot de passe ou le mot de passe stocké sur un serveur
- ▶ **Jeton d'accès**
 - ▶ Parfois persistant pour certains services en ligne

Stratégies

- ▶ **Système de vérification local**
 - ▶ Extraire le hash si c'est possible
 - ▶ Un en-tête du fichier protégé
 - ▶ Contenu dans fichier de l'environnement lui-même éventuellement protégé par un mot de passe
 - ▶ Trouver une collision
 - ▶ Dictionnaire
 - Bases de données en ligne
 - ▶ Attaque du hash
 - Méthodes de collision
 - Force brute, éventuellement orientée
- ▶ **Système de vérification déporté**
 - ▶ Force brute - parfois impossible
 - ▶ « ingénierie humaine » si on a le temps ou le post-it
 - ▶ Tenter de rechercher le jeton si on a accès à un environnement qui a accès
 - ▶ Contourner avec un hacker – pour ceux qui savent et ... qui ont le droit

La récupération des jetons














- ▶ Les téléphones mobiles conservent des jetons d'accès aux services Dropbox, ...
- ▶ Les ordinateurs conservent des jetons d'accès aux téléphones (backup) et aux services en ligne
 - ▶ Ex. ElcomSoft Phone Breaker – sur session live ou sur image disque dur
- ▶ Fonction offerte par ??
 - ▶ Cellebrite
 - ▶ Xry?
 - ▶ Oxygen Forensics – version « detective » (token Google)
 - ▶ Elcomsoft iOS Forensic Toolkit (pour iOS)?

Les mots de passe locaux

- ▶ **Logiciels clés en main spécialisés sur des applications**
 - ▶ OphCrack, JtR, Hashcat, Oclhashcat → Windows,
 - ▶ JtR, Hashcat → Mac
 - ▶ Elcomsoft, passware → Office, Acrobat, Zip, backup iPhone/BB/...
- ▶ **Boîte à outils John the Ripper (JtR)**
 - ▶ Jumbo patch– une série de scripts (office2john.py, ml2john.py,...) pour extraire le hash (keepass...)
 - ▶ John pour casser renverser le hash
- ▶ **Si on est perdu: <https://forum.insidepro.com>**

John

- ▶ L'exécutable
 - ▶ Rechercher la dernière version sur OpenWall
- ▶ Les utilitaires perl et python d'extractions de hash
 - ▶ <https://github.com/magnumripper/JohnTheRipper/tree/bleeding-jumbo/run>

 ml2john.py	Remove unused code from ml2john.py	3 years ago
 mozilla2john.py	mozilla2john.py helper script	a year ago
 netntlm.pl	john-1.7.9-jumbo-1 (1.7.8-jumbo-8 equivalent)	4 years ago
 netscreen.py	john-1.7.9-jumbo-6 as released by Solar	4 years ago
 odf2john.py	Added ability to odf2john to generate a gecoc field for meta data of ...	3 years ago
 office2john.py	Update olefile to 0.42.1 (released 2015-01-24)	5 months ago
 openbsd_softraid2john.py	Add script to extract OpenBSD softraid hashes from disk image	a year ago
 openssl2john.py	Change optparse to argparse in efs2john.py and openssl2john.py	9 months ago
 pass_gen.pl	dynamic: added McAfee master unlock password	21 days ago
 password.lst	State that this list "is assumed to be in the public domain"	3 years ago
 pcap2john.py	Remove a debugging statement from the HSRP v2 parser	4 months ago
 pdf2john.py	pdf2john: Fix AttributeError	a year ago
 pem2john.py	[pem] false positives shouldn't happen now	3 months ago

Récupérer un mot de passe Mac

- ▶ 1) Trouver le fichier qui contient les hash
 - ▶ OSX <= 10.7
 - ▶ /private/var/db/dslocal/nodes/Default/users/.plist
 - ▶ OSX >= 10.8
 - ▶ /var/db/dslocal/nodes/Default/users/<accountname>.plist
- ▶ 2) avec DaveGrohl (davegrohl.com)
 - ▶ Sudo ./dave --plist pauldupond.plist
- ▶ 3) avec John
 - ▶ perl lion2john.pl user.plist
 - ▶ python ml2john.py ../user.plist > hash.txt (attention python 2.x)
 - ▶ ../run/john hash.txt
- ▶ 4) Du temps...

Exemples John

▶ Un RAR

- ▶ Rar2john fichier.rar>hash.txt
- ▶ John hash.txt

▶ Un PDF

- ▶ Pdf2john fichier.rar>hash.txt
- ▶ ...

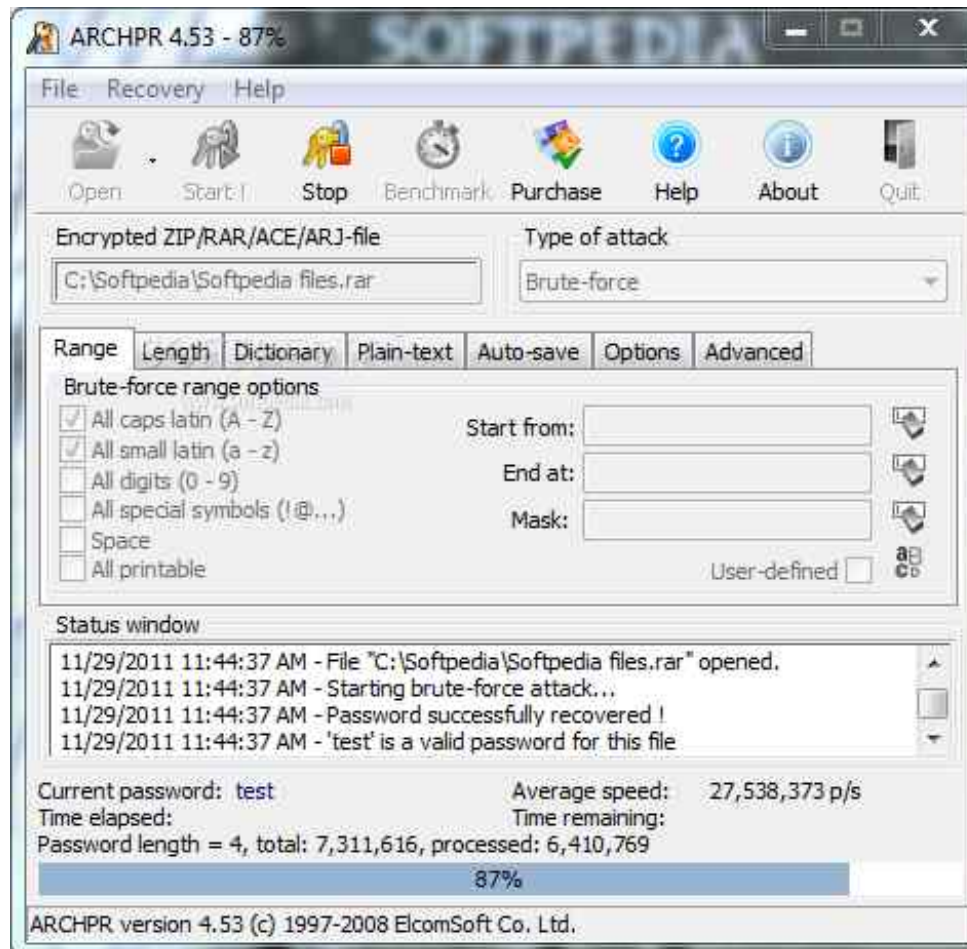
▶ Windows

- ▶ Récupérer le fichier System et le SAM (windows\system32\config)
- ▶ Dump des hash avec utilitaire Linux ex. bkhive, samdump2
 - ▶ bkhive system /root/hive.txt
 - ▶ samdump2 SAM /root/hive.txt > /root/hash.txt
 - ▶ samdump2 system SAM > /root/hashes/hash.txt
- ▶ john /root/hash.txt -format=nt2 -users=Administrateur

Beaucoup de solutions intégrées facilitent ces opérations

- ▶ **Windows (<8?)**
 - ▶ OphCrack
- ▶ **PDF, RAR, Docx,**
 - ▶ Elcomsoft
 - ▶ Passware
- ▶ **Backup iPhone, BB, etc.**
 - ▶ Elcomsoft, ...
- ▶ **Souvent un bon compromis temps/argent**
 - ▶ Ergonomie
 - ▶ Éviter les pb de version de python, perl, les paramétrages, etc.

C'est quand même plus sympa



Exemple OphCrack

ophcrack LiveCD



Ophcrack Graphic mode
Ophcrack Graphic UESA mode
Ophcrack Text mode

More about ophcrack to...

Use Ophcrack the best way
Try to autoconfigure your
card and use the maximum
allowed resolution

Default resolution to 4...

The screenshot shows the OphCrack application interface. At the top, there is a menu bar with icons for Load, Delete, Save, Tables, Stop, Help, Exit, and About. Below the menu bar, there are three tabs: Progress, Statistics, and Preferences. The main window displays a table of users and hashes, and a progress bar for directory searches.

User	LM Hash	NT Hash	LM Pwd 1	LM Pwd 2	NT Pwd
!Supervisor...		31D6CFE0...			empty
toto		1EF82030F...			
Administrator	8d483a84a...	33cc539403...	GUESSME	001	Guessvie001
Philippe	b906f7976d...	b91e46819...	MAISON2	empty	maison2
Guest	3a5d42642...	f1f23d5f2a0...	ZF2Y11P	5PKMWP4	z12Y1p5PKMwP4
	eaef446f97...	ac051662cd...	TR3	empty	tr3
	ce304571fc...	db129418a...	#%	empty	#%
		da7e06bcb...			o*
	a13aa0f3a...	f01d6062ef...			
	3e64533dfr...	595f3de7eh...			

Table	Directory	Status	Progress
XP free fast	/mnt/ext3/ta...	36% in RAM	[Progress bar]
table0		36% in RAM	[Progress bar]
table1		36% in RAM	[Progress bar]
table2		36% in RAM	[Progress bar]
table3		36% in RAM	[Progress bar]
Vista free	/mnt/ext3/ta...	22% in RAM	[Progress bar]
table1		43% in RAM	[Progress bar]
table3		43% in RAM	[Progress bar]
XP	/mnt/ext3/ta...	10% in RAM	[Progress bar]

Preload: done Brute force: done Pwd found: 9/29 Time elapsed: 0h 2m 38s

Présentation François Delost

- ▶ **les méthodes de force brutes et leurs optimisations**
 - ▶ rainbow tables,
 - ▶ les freins
 - ▶ dérivations de mots de passe,
 - ▶ autres,

- ▶ **les dictionnaires**
 - ▶ open source, du commerce,
 - ▶ custom - social engineering,
 - ▶ custom - extraction mémoire vive (dump ou hibernat)
 - ▶ autres

Présentation Antoine Laureau

- ▶ La puissance de calcul...les choix des processeurs (CPU, GPU, ...), les clusters de GPU:
 - ▶ 8 R9 290X: SHA256 : 11231.8 MH/s
 - ▶ 8 GTX TITAN X: 19345.2 MH/s
 - ▶ Intel 5960X: 76.31MH/s

- ▶ Les temps prévisibles
 - ▶ <http://calc.opensecurityresearch.com>

Les mots de passe qu'on aime bien

- ▶ Le backup iTunes chiffré contient le wallet en clair, les mails
 - ▶ Outil adhoc elcomSoft
- ▶ Mac
 - ▶ La session Mac donne accès au Wallet et aux mots de passe des systèmes distants
- ▶ Windows
 - ▶ La session PC donne accès aux mots de passe des navigateurs, etc.
- ▶ Téléphones mobiles
 - ▶ --> voir présentation Sami Kodja

Les bonnes surprises

- ▶ **Le post-it**
 - ▶ Au moins pour orienter le dictionnaire
- ▶ **Il y avait un keylogger sur la machine**
 - ▶ Les fichiers du KL sont en clairs,
 - ▶ Le KL a un master password (trouver le mot de passe session pour relancer l'environnement)
- ▶ **La question : Code pénal - Article 434-15-2**
 - ▶ 3 ans – 45000€- en cas de non divulgation...