Découverte de mots de passe

Les empreintes

- Forme de stockage d'un mot de passe
  - Le mot de passe n'est généralement pas stocké en clair
  - Application mathématique non réversible : Fonction de hachage
    - Le mot de passe sert d'antécédent
    - Un graine sert de diversifiant
    - Résultat de longueur constante prédéfinie
- La comparaison s'effectue toujours sur l'empreinte du mot de passe
- Le terme anglais : « `hash` »

Les empreintes

- Types d'empreintes
  - Pas d'empreinte ! Mot de passe en clair (telnet, pop3…)
  - Base64 (HTTP basic) (Encodage, pas un chiffrement !)
  - Cisco level 7 (vigenère)
  - MD5 (cisco)
  - Sha-2 (unix)
  - Hash LM/NT (windows)
  - Nombreux autres (sha1, wpa, mysql, vbulletin…)

Attaques sur les mots de passe

- Objectif :
  - récupérer un mot de passe à partir de son empreinte
- Outils :
  - Hashcat
  - John The Ripper
  - Aircrack-NG
  - ophcrack(rainbow tables)
  - Cain & Abel
  - ...

Attaques sur les mots de passe

- Différents types d'attaque
  - Dictionnaire (wordlist)
    - Tester tous les mots présents dans des dictionnaires thématiques
      - Ex: monde de Harry Potter, Planètes du système solaire, Acteurs…
  - Combinatoire
    - Les mots d'un dictionnaire sont ajoutés à tous les mots d'un autre dictionnaire
  - Dictionnaire avec des règles (Rules-based)
    - Application de règles sur des mots
      - Ex : remplacement des caractères « e » par le caractère « 3 »
  - Toggle-Case
    - Toutes les caractères d'un mot passent de lowercase à uppercase.
    - Toutes les combinaisons possibles sont réalisées

Attaques sur les mots de passe

- Différents types d'attaque
  - Hybride
    - Ajout de caractères à un mot
    - Ex : `pass, pass000, pass001, pass002, pass003…`
  - Masque de caractères
    - un jeu de caractère est défini pour chaque emplacement des caractères dans le mot.
    - Ex : ?l?d?l?u
    - alpha lower, chiffre, alpha lower, alpha upper
  - BruteForce
    - Tester toutes les combinaisons possibles de n caractères avec un charset xxx

Attaques sur les mots de passe

- Différents types d'attaque
  - Hybride
    - Ajout de caractères à un mot
    - Ex : `pass, pass000, pass001, pass002, pass003…`
  - Masque de caractères
    - un jeu de caractère est défini pour chaque emplacement des caractères dans le mot.
    - Ex : ?l?d?l?u
    - alpha lower, chiffre, alpha lower, alpha upper
  - BruteForce
    - Tester toutes les combinaisons possibles de n caractères avec un charset xxx

Attaques sur les mots de passe

- Plusieurs facteurs déterminants
  - nature de l'algorithme de chiffrement
    - LM (7 caractères, très rapide à casser)
    - bcrypt (ultra-lent !!!)
  - Temps
  - Puissance de calcul
    - CPU
    - CPU /GPU ?

Attaques sur les mots de passe

- 8x Nvidia GTX 1080 Hashcat Benchmarks
  - MD5 : 200.3 GH/s
  - NTLM 334.0 GH/s
  - bcrypt, Blowfish(OpenBSD) : 105.7 kH/s
  - OSX v10.8+ : 98618 H/s
  - 7-Zip : 60750 H/s
  - VeraCrypt PBKDF2-HMAC-Whirlpool + XTS 512 bit : 595 H/s (Truecrypt)

Attaques sur les mots de passe

- La connaissance de l'environnement d'où est extrait le hash a beaucoup d'importance :
  - Informations relatives de l'entreprise
    - Ex : nom du produit phare, nom du service informatique, nom du bâtiment…
  - Niveau de sensibilisation des administrateurs
  - Environnement culturel
  - Centres d'intérêt / Thématique
    - Ex : Systèmes planétaires…
  - Méthodes de travail des administrateurs
    - Ex : racine du mot de passe identique, seuls les deux derniers caractères changent
  - L'application elle-même !
    - Ex : Ashley Madison leaks

Attaques sur les mots de passe

- Un peu d'aide…
  - https://hashcat.net/wiki/doku.php?id=example_hashes
  - http://pentestmonkey.net/cheat-sheet/john-the-ripper-hash-formats
  - http://tools.kali.org/password-attacks/hash-identifier

Attaques sur les mots de passe

- Connaître l'origine du hash !
  - Longueurs de hashes de longueur 32 caractères :
    - NT
    - MD5
    - md5(md5(md5($pass)))
    - md5(md5($salt).$pass)
    - md5($salt.md5($pass))
    - md5($pass.md5($salt))
    - md5($username.0.$pass)
    - md5(strtoupper(md5($pass)))
    - …

Quelle algorithme choisir ???

HashIdentifier

HASH: 098f6bcd4621d373cade4e832627b4f6

Least Possible Hashs:

[+] RAdmin v2.x
[+] NTLM
[+] MD4
[+] MD2
[+] MD5(HMAC)
[+] MD4(HMAC)
[+] MD2(HMAC)
[+] MD5(HMAC(Wordpress))
[+] Haval-128
[+] Haval-128(HMAC)
[+] RipeMD-128
[+] RipeMD-128(HMAC)
[+] SNEFRU-128
[+] SNEFRU-128(HMAC)
[+] Tiger-128
[+] Tiger-128(HMAC)
[+] md5($pass.$salt)
[+] md5($salt.$pass)
[+] md5($salt.$pass.$salt)
[+] md5($salt.$pass.$username)
[+] md5($salt.md5($pass))
[+] md5($salt.md5($pass))
[+] md5($salt.md5($pass.$salt))
[+] md5($salt.md5($pass.$salt))
[+] md5($salt.md5($salt.$pass))
[+] md5($salt.md5(md5($pass).$salt))
[+] md5($username.0.$pass)
[+] md5($username.LF.$pass)
[+] md5($username.md5($pass).$salt)
[+] md5(md5($pass))
[+] md5(md5($pass).$salt)
[+] md5(md5($pass).md5($salt))
[+] md5(md5($salt).$pass)
[+] md5(md5($salt).md5($pass))
[+] md5(md5($username.$pass).$salt)
[+] md5(md5(md5($pass)))
[+] md5(md5(md5(md5($pass))))
[+] md5(md5(md5(md5(md5($pass)))))
[+] md5(sha1($pass))
[+] md5(sha1(md5($pass)))
[+] md5(sha1(md5(sha1($pass))))
[+] md5(strtoupper(md5($pass)))

Attaques sur les mots de passe

A NE PAS FAIRE !

- Rechercher le hash sur Internet
  - Le hash sera potentiellement ajouté à une liste de hashes à casser par un robot. Quid si le nom de l'entreprise se trouve dedans ?

- Laisser les fichiers « .pot » trainer sur des serveurs…
  (fichier qui contient les hashes et mots de passe cassés)

Astuces sous Windows

- Algorithme LM

https://technet.microsoft.com/en-us/library/hh994558(v=ws.10).aspx
https://technet.microsoft.com/en-us/library/hh994565(v=ws.11).aspx

  - The password is padded with NULL bytes to exactly 14 characters. If the password is longer than 14 characters, it is replaced with 14 NULL bytes for the remaining operations.
  - The password is converted to all uppercase.
  - only ASCII characters !
  - The password is split into two 7-byte (56-bit) keys.
  - Each key is used to encrypt a fixed string.
  - The two results from step 4 are concatenated and stored as the LM hash.

Astuces sous Windows

- Algorithme NT https://technet.microsoft.com/en-us/library/hh994565(v=ws.11).aspx
  - The NT hash of the password is calculated by using an unsalted MD4 hash algorithm. MD4 is a cryptographic one-way function that produces a mathematical representation of a password. This hashing function is designed to always produce the same result from the same password input, and to minimize collisions where two different passwords can produce the same result.

Astuces sous Windows

- Ces hashes LM sont stockés (pour une machine qui ne se trouve pas dans un domaine) dans la base SAM (Security Account Manager).
- L'extraction du contenu de la base SAM est généralement présenté de la façon suivante : `Compte:ID:hash LM:hashNT`

```
Administrateur:500:fd4073eb1f08fc7d17306d272a9441bb:721f1cfe4d817952b4e37e06611af75d:::
goliath:1003:df12ceaf40b8d522aad3b435b51404ee:cc6b47433d1af17145c5555b61305232:::
HelpAssistant:1000:1cb98ff4d96db0a01afc7a85585c9f67:0210e639280ecbc8d4a1648bcc96ef20:::
Invité:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
prenom.nom:1004:a0fc2965c7a4a770a6f6affcc5d745cf:6bae22d3ca265843803a38b175f10caa:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:af9b2ab062975971cd4fd9e8f00c0925:::
titi:1007:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
toto:1006:bac14d04669ee1d1aad3b435b51404ee:fbbf55d0ef0e34d39593f55c5f2ca5f2:::
user:1005:22124ea690b83bfbaad3b435b51404ee:57d583aa46d571502aad4bb7aea09c70:::
```

Astuces sous Windows

- Le cassage du mot de passe LM étant plus rapide que le cassage du NT, il convient de s'attaquer en premier au hash LM ;
- Le mot de passe trouvé aura subi les modifications liées au traitement des hashes LM (uppercase et limitation 14 caractères) ;
- Les mots de passe trouvés vont grandement aider pour la recherche du vrai mot de passe !

```
Administrateur:500:fd4073eb1f08fc7d17306d272a9441bb:721f1cfe4d817952b4e37e06611af75d:::
goliath:1003:df12ceaf40b8d522aad3b435b51404ee:cc6b47433d1af17145c5555b61305232:::
HelpAssistant:1000:1cb98ff4d96db0a01afc7a85585c9f67:0210e639280ecbc8d4a1648bcc96ef20:::
Invité:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
prenom.nom:1004:a0fc2965c7a4a770a6f6affcc5d745cf:6bae22d3ca265843803a38b175f10caa:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:af9b2ab062975971cd4fd9e8f00c0925:::
titi:1007:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
toto:1006:bac14d04669ee1d1aad3b435b51404ee:fbbf55d0ef0e34d39593f55c5f2ca5f2:::
user:1005:22124ea690b83bfbaad3b435b51404ee:57d583aa46d571502aad4bb7aea09c70:::
```

Toutefois, cela ne fonctionne plus à tous les coups car cela dépend de la politique de sécurité en place…

Astuces sous Windows

```
Administrateur:500:fd4073eb1f08fc7d17306d272a9441bb:721f1cfe4d817952b4e37e06611af75d:::
goliath:1003:df12ceaf40b8d522aad3b435b51404ee:cc6b47433d1af17145c5555b61305232:::
HelpAssistant:1000:1cb98ff4d96db0a01afc7a85585c9f67:0210e639280ecbc8d4a1648bcc96ef20:::
Invité:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
prenom.nom:1004:a0fc2965c7a4a770a6f6affcc5d745cf:6bae22d3ca265843803a38b175f10caa:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:af9b2ab062975971cd4fd9e8f00c0925:::
titi:1007:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
toto:1006:bac14d04669ee1d1aad3b435b51404ee:fbbf55d0ef0e34d39593f55c5f2ca5f2:::
user:1005:22124ea690b83bfbaad3b435b51404ee:57d583aa46d571502aad4bb7aea09c70:::
```

aad3b435b51404eeaad3b435b51404ee : valeur d’un mot de passe vide LM

titi et Invité ont le même hash NT : ils ont le même mot de passe !

Or Invité ne dispose pas de mot de passe par défaut, donc titi n’a pas de mot de passe !

Questions ?