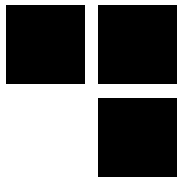
SYNACKTIV
DIGITAL SECURITY

Cassage avancé d'empreintes de mots de passe

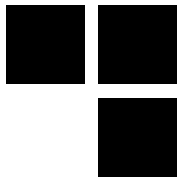
Le 13 novembre 2014
JSSI Rouen 2014
Par Julien Legras

Plan



1. Présentation de Synacktiv
2. Présentation du contexte
3. Stockage des mots de passe
4. Cassage des empreintes
5. Des bonnes pratiques

Plan



1 Présentation de Synacktiv

2 Présentation du contexte

3 Stockage des mots de passe

4 Cassage des empreintes

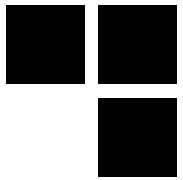
5 Des bonnes pratiques

Présentation de Synacktiv

Activités

- Tests d’intrusion externes, internes et *Red Team*
- Audits de sécurité
- Audits d’homologation ARJEL
- Analyse post-intrusion
- Hébergement sécurisé
- Assistance technique sur de grands projets
- Formations en sécurité informatique
- Recherche de vulnérabilités

Plan



1 Présentation de Synacktiv

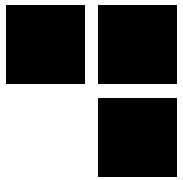
2 Présentation du contexte

3 Stockage des mots de passe

4 Cassage des empreintes

5 Des bonnes pratiques

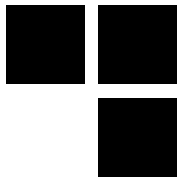
Présentation du contexte



- Besoin de mots de passe partout

↪ Complexité de gestion réduisant la *force* des mots de passe pour pouvoir les retenir

Présentation du contexte



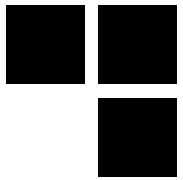
- Besoin de mots de passe partout

↪ Complexité de gestion réduisant la *force* des mots de passe pour pouvoir les retenir

- Politiques mises en place dans les entreprises

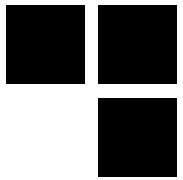
↪ Éviter les mots de passe triviaux

Présentation du contexte



- Besoin de mots de passe partout
  - ↪ Complexité de gestion réduisant la *force* des mots de passe pour pouvoir les retenir
- Politiques mises en place dans les entreprises
  - ↪ Éviter les mots de passe triviaux
- Pourquoi casser des empreintes de mots de passe ?
  - ↪ Avancer plus rapidement dans une intrusion

Plan



1 Présentation de Synacktiv

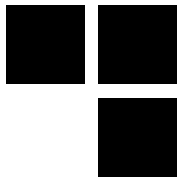
2 Présentation du contexte

3 Stockage des mots de passe
- Les empreintes
- Sur les systèmes
- Sur les sites web

4 Cassage des empreintes

5 Des bonnes pratiques

Stockage des mots de passe
Les empreintes



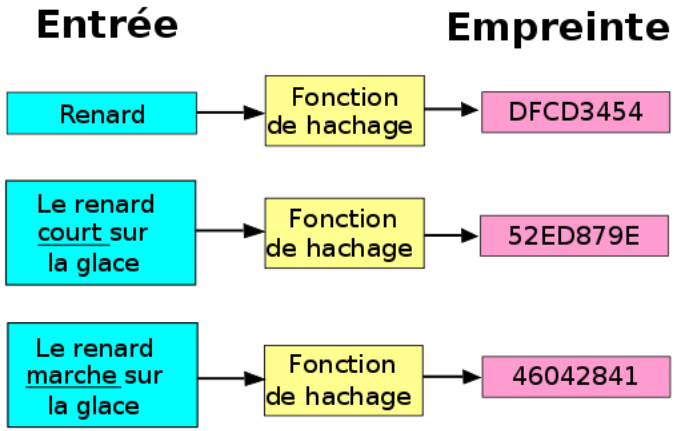
Définition

Résultat d’une fonction de hachage appliquée sur un message.

Stockage des mots de passe
Les empreintes

Définition

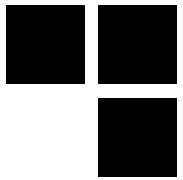
Résultat d'une fonction de hachage appliquée sur un message.



`http://fr.wikipedia.org/wiki/Fonction_de_hachage`

La fonction de hachage doit résister aux attaques sur la première pré-image, seconde pré-image et aux collisions.

Stockage des mots de passe
Sur les systèmes

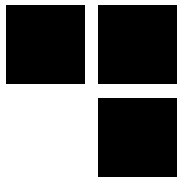


Windows

- Avant Windows NT : LM (LanMan), basé sur DES

↪ limité à 14 caractères, insensible à la casse

Stockage des mots de passe
Sur les systèmes



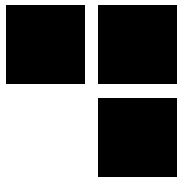
Windows

- Avant Windows NT : LM (LanMan), basé sur DES

↪ limité à 14 caractères, insensible à la casse

- À partir de Windows NT : NTLM, basé sur MD4

Stockage des mots de passe
Sur les systèmes



Windows

- Avant Windows NT : LM (LanMan), basé sur DES

↪ limité à 14 caractères, insensible à la casse

- À partir de Windows NT : NTLM, basé sur MD4

Unix/GNU Linux

- Utilisation de libcrypt : descrypt, bcrypt, md5crypt, sha256crypt, sha512crypt...

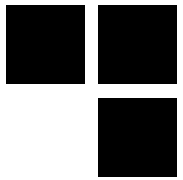
↪ Large choix d'algorithmes salés

Stockage des mots de passe
Sur les sites web

CMS

- Drupal 7 : 16 385 tours de SHA512 salé
- Wordpress : MD5 salé par défaut, Blowfish et DES supportés

Stockage des mots de passe
Sur les sites web



CMS

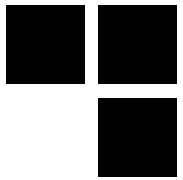
- Drupal 7 : 16 385 tours de SHA512 salé
- Wordpress : MD5 salé par défaut, Blowfish et DES supportés

Autres

- Parfois stockés en clair
- Simple MD5

↪ Faible sensibilisation du développement sécurisé

Plan



1 Présentation de Synacktiv

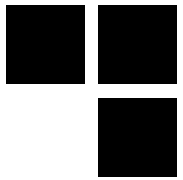
2 Présentation du contexte

3 Stockage des mots de passe

4 Cassage des empreintes
- Méthodes
- Principaux outils
- Le projet Kraqozorus

5 Des bonnes pratiques

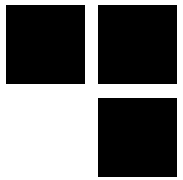
Cassage des empreintes
Méthodes



Incrémental

- Essayer tous les candidats possibles dans un espace donné

Cassage des empreintes
Méthodes



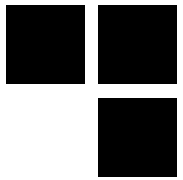
Incrémental

- Essayer tous les candidats possibles dans un espace donné

Attaque par dictionnaire

- Générer des candidats à partir d’un dictionnaire et de règles de dérivations

Cassage des empreintes
Méthodes



Rainbow tables

- Tables de correspondance pré-calculées pour une recherche inversée

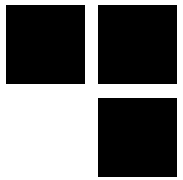
Cassage des empreintes
Méthodes

Rainbow tables

- Tables de correspondance pré-calculées pour une recherche inversée

↪ Utilisable principalement avec les empreintes non salées

Cassage des empreintes
Méthodes



Rainbow tables

- Tables de correspondance pré-calculées pour une recherche inversée

↪ Utilisable principalement avec les empreintes non salées

↪ Très volumineux :
  - ntlm_mixalpha-numeric#1-9 → 1009 GB
  - md5_mixalpha-numeric-all-space#1-8 → 1049 GB (`www.freerainbowtables.com`)

Cassage des empreintes
Principaux outils

John the Ripper

- Opensource et extensible
- Grande liste d'algorithmes supportés
- Pour CPU à l'origine, certains algorithmes portés sur GPU

Cassage des empreintes
Principaux outils

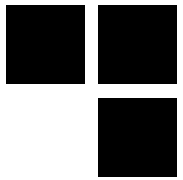
John the Ripper

- Opensource et extensible
- Grande liste d'algorithmes supportés
- Pour CPU à l'origine, certains algorithmes portés sur GPU

oclHashcat

- Algorithmes les plus communs supportés
- Conçu uniquement pour GPU

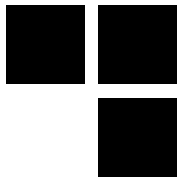
Cassage des empreintes
Le projet Kraqozorus



Présentation

- Infrastructure de cassage d’empreintes de mots de passe

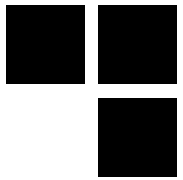
Cassage des empreintes
Le projet Kraqozorus



Présentation

- Infrastructure de cassage d’empreintes de mots de passe
- Recyclage automatique des mots de passe trouvés

Cassage des empreintes
Le projet Kraqozorus



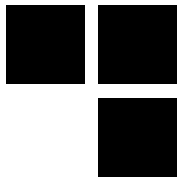
Présentation

- Infrastructure de cassage d'empreintes de mots de passe
- Recyclage automatique des mots de passe trouvés

Exemple : Asynacktiv*2014fr

↪ Double dérivation du mot de passe synacktiv*2014 :

Cassage des empreintes
Le projet Kraqozorus



Présentation

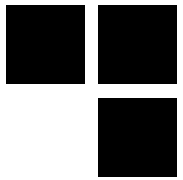
- Infrastructure de cassage d'empreintes de mots de passe
- Recyclage automatique des mots de passe trouvés

Exemple : Asynacktiv*2014fr

↪ Double dérivation du mot de passe synacktiv*2014 :

1. synacktiv

Cassage des empreintes
Le projet Kraqozorus



Présentation

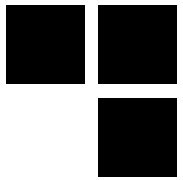
- Infrastructure de cassage d'empreintes de mots de passe
- Recyclage automatique des mots de passe trouvés

Exemple : Asynacktiv*2014fr

↪ Double dérivation du mot de passe synacktiv*2014 :

1. synacktiv
2. synacktiv*2014

Cassage des empreintes
Le projet Kraqozorus



Présentation

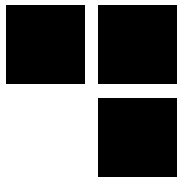
- Infrastructure de cassage d'empreintes de mots de passe
- Recyclage automatique des mots de passe trouvés

Exemple : Asynacktiv*2014fr

↪ Double dérivation du mot de passe synacktiv*2014 :

1. synacktiv
2. synacktiv*2014
3. Asynacktiv*2014

Cassage des empreintes
Le projet Kraqozorus



Présentation

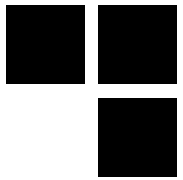
- Infrastructure de cassage d'empreintes de mots de passe
- Recyclage automatique des mots de passe trouvés

Exemple : Asynacktiv*2014fr

↪ Double dérivation du mot de passe synacktiv*2014 :

1. synacktiv
2. synacktiv*2014
3. Asynacktiv*2014
4. Asynacktiv*2014fr

Plan



1 Présentation de Synacktiv

2 Présentation du contexte

3 Stockage des mots de passe

4 Cassage des empreintes

5 Des bonnes pratiques
- Utilisateurs
- Développeurs
- Administrateurs

Des bonnes pratiques
Utilisateurs

Résister aux attaques incrémentales

- Avoir un mot de passe long d’au moins 15 caractères

Des bonnes pratiques
Utilisateurs

Résister aux attaques incrémentales

- Avoir un mot de passe long d'au moins 15 caractères

Résister aux attaques par dictionnaires

- Ne pas se baser sur un seul mot

↪ Mélanger des mots de différentes langues

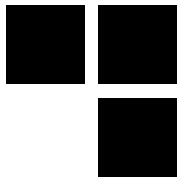
↪ Se baser sur une phrase simple à retenir

Des bonnes pratiques
Utilisateurs

Un seul mot de passe fort à retenir ?

- Utiliser un gestionnaire de mots de passe tel que Keepass
  - ↪ Génération de mots de passe aléatoires
  - ↪ Chiffrement des mots de passe

Des bonnes pratiques
Développeurs

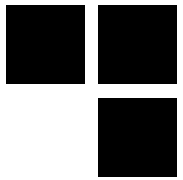


- Utiliser des méthodes existantes, testées et éprouvées

  `https://www.owasp.org/index.php/Password_Storage_Cheat_Sheet`

↪ Utiliser le *key stretching* (PBKDF2)

Des bonnes pratiques
Développeurs



- Utiliser des méthodes existantes, testées et éprouvées

  `https://www.owasp.org/index.php/Password_Storage_Cheat_Sheet`

↪ Utiliser le *key stretching* (PBKDF2)

- Attention aussi aux fonctionnalités de réinitialisation de mots de passe

  `https://www.owasp.org/index.php/Forgot_Password_Cheat_Sheet`

Des bonnes pratiques
Administrateurs

Windows (Active Directory)

- Désactiver l'algorithme faible LM
- Limiter l'historique des mots de passe
- Ne pas forcer les changements trop fréquents de mots de passe

Des bonnes pratiques
Administrateurs

Windows (Active Directory)

- Désactiver l'algorithme faible LM
- Limiter l'historique des mots de passe
- Ne pas forcer les changements trop fréquents de mots de passe

Unix/GNU Linux

- Privilégier sha512crypt : très lent à casser (5 000 tours par défaut).

AVEZ-VOUS
DES QUESTIONS ?

MERCI DE VOTRE ATTENTION,

SYNACKTIV
DIGITAL SECURITY