Dumpster diving du 21ème siècle

The garbage is leaking juice

$ ./prez.sh --help

- Intro
- Analyses
  - Recherches sur cegep-ste-foy.qc.ca
  - Quelques chiffres
- Utilisations (Malicieuses)
  - Vol d’identités
  - Cassage de hash + Demo
- Responsabilités
  - *Sysadmin* / Dev
  - Utilisateurs

$ w | grep mdube

- Père de famille
- Analyste en sécurité chez GoSecure
  - Penetration Testing
- Co-administrateur du Hackfest de 2011 à 2015
  - Organiser War Games / CTFs
- Training: Ninjutsu
- Drink Scotch/Bourbon
- Intérêt: Système sécure par défaut


ONE DOES NOT SIMPLY
START A PROJECT WITHOUT CONSIDERING ETHICS
imgflip.com

POC Septembre 2016

- Participation du public!
  - Public: 0 email reçu
  - Friends: 3 email reçu
  - Équipe du HF: Après 3 appels à la participation, 7/18

- Constat:

Data Breach > Data Leak > **Password Leak**

- Data Breach
  - ISO/IEC 27040: compromise of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to protected data transmitted, stored or otherwise processed.
- Data Leak
  - Fuite de: Données clients, fiscales. Secrets d’entreprise.
- Password Leak
  - Fuite d’identité de clients. Généralement une association usager-mot_de_passe.

Analyses

Qu’est-ce qui se retrouve dans les poubelles des Internets?

Comment stocker un mot de passe?

Type de stockage	Description
Texte clair	
MD5	128 bits, vulnérable aux collisions, rapide à générer Utilisation: Désuet.
SHA*	160 bits, rapide à générer Utilisation: Assurer l'intégrité. Signature numériques.
bcrypt scrypt	184 bits, très lent, configurable **Utilisation: Stockage de mot de passes**

$ ls -l *.txt

source	hash	ct
MySpace	SHA1 unsalted	359 339 047
Adobe 155M	3des (key not found yet)	147 913 099
VK	cleartext	92 286 282
Linkedin	SHA1 unsalted	73 791 996
Mate 1	cleartext	27 403 818
000webhost	cleartext	15 268 730
Twitter	cleartext	12 723 215
Ashley Madison	bcrypt salted ($2a$12$)	588 528

$ man leaks

- https://haveibeenpwned.com
  - Site éthique. Permet de chercher si votre courriel est affecté.
  - ~1.4 milliard d'entrées
- https://leakedsource.com **- Maintenant fermé**
  - Analyses de plusieurs leaks
  - Permet d'afficher les données brutes (ex. Les mots de passes)
  - ~2.2 milliard d'entrées
- https://leakforums.net
  - Communauté de partage et discussions
- http://weknowyouremail.com https://www.thecthulhu.com http://dumps.bhafsec.com/infosec/dumps/ and others
  - Rendent disponible le téléchargement de leaks

nostalgeek@gmail.com pwned?

Oh no — pwned!

Pwned on 2 breached sites and found no pastes (subscribe to search sensitive breaches)

Notify me when I get pwned Donate

Breaches you were pwned in

A "breach" is an incident where a site's data has been illegally accessed by hackers and then released publicly. Review the types of data that were compromised (email addresses, passwords, credit cards etc.) and take appropriate action, such as changing passwords.

Dropbox: In mid-2012, Dropbox suffered a data breach which exposed the stored credentials of tens of millions of their customers. In August 2016, they forced password resets for customers they believed may be at risk. A large volume of data totalling over 68 million records was subsequently traded online and included email addresses and salted hashes of passwords (half of them SHA1, half of them bcrypt).

Compromised data: Email addresses, Passwords

LinkedIn: In May 2016, LinkedIn had 164 million email addresses and passwords exposed. Originally hacked in 2012, the data remained out of sight until being offered for sale on a dark market site 4 years later. The passwords in the breach were stored as SHA1 hashes without salt, the vast majority of which were quickly cracked in the days following the release of the data.

Compromised data: Email addresses, Passwords

$ grep $pwned | wc -l leaks.txt

Domaine	Occurrence	Unique	Dupliqué
bell.net	57 160	42 590	14 570
cgi.com	8 883	7 283	1 600
ulaval.ca	2 082	2 009	73
hydro.qc.ca	3 009	2 292	717
carleton.ca	1 849	1 300	549
cegep-ste-foy.qc.ca	**227**	**175**	**52**
sce.carleton.ca	218	170	48

$ less vk.txt

- Count: 100M
- Hash Format: Cleartext
- Breach Date: 2012, Disclosure Date: 2016-06
- Scope: Russian Facebook
- Incident Handling: Bad
  - They denied that the site had been breached.

- Biggest cleartext password leak released.
- Make sure all your tools support UTF-8 if you want to play with it.

$ less mate1.txt

- Count: 28M
- Hash Format: Cleartext
- Breach+Disclosure Date: 2016-02 (February)
- Scope: Dating Site
- Incident Handling: Bad
  - They did not acknowledge the incident.

- Bonus
  - First and Last Name
  - Date of birth
- Lulz
  - The “Forgot password” feature was sending the passwords in cleartext

$ less 000webhost.txt

- Count: 15M
- Hash Format: Cleartext
- Breach+Disclosure Date: 2015-03 (March)
- Scope: Hosting Company
- Incident Handling: Excellent
  - Apologized.
  - Investigated and fixed the issue the same day.
  - Promoted user awareness.
  - https://www.000webhost.com/000webhost-database-hacked-data-leaked

$ grep -f friends.txt 000webhost.txt

```
   source   |         email                | username      |  pwd
------------+------------------------------+---------------+-------------
 000webhost | pl.maltais@hotmail.com       | Pier-Luc      | family13
 000webhost | marcandremeloche@gmail.com | Richard Smith | 1&h2isi92H!@H
```

$ less twitter.txt

- Count: 12M (~33M including duplicates)
- Hash Format: Cleartext
- Breach+Disclosure Date: 2016-06 (June)
- Scope: Social Network
- Vulnerability exploited: None
  - They were not breached. A botnet sniffed the data on user's computers and pushed it on the CnC.
- Incident Handling: Good
  - They acknowledge that the data was valid.
  - However, they asked people to "scrutinize the merits of any credential claim."
- Bonus
  - Password history / Login attempt?

$ less myspace.txt

- Count: 360M
- Hash Format: Unsalted SHA1 (first 10 char, lowercase)
- Breach Date: 2008, Disclosure Date: 2016-05
- Scope: Social Media for everyone
- Incident Handling: OK
  - They have invalidated the affected accounts.
  - No apologies and kindly “race to the bottom”.
    - We run automated tools… We’re starting criminal pursue.
  - https://myspace.com/pages/blog

$ less linkedin.txt

- Count: 164M (Initially ~64M in 2012)
- Hash Format: Unsalted SHA1
- Breach Date: 2012, Disclosure Date: 2016-05
- Scope: All businesses.
- Incident Handling: Bad
  - Took 5 days to force a password reset
  - “We have demanded that parties cease making stolen password data available and will evaluate potential legal action if they fail to comply.” (o rly?)
  - https://blog.linkedin.com/2016/05/18/protecting-our-members

$ grep -f friends.txt linkedin.txt

```
 source  |          email          | username |                 enc_pwd
---------+-------------------------+----------+----------------------------------
Linkedin | fgagnon@sce.carleton.ca |          | 49315af4bf79861070125c5e00a5506b73ed0fa6
```

```
┌─[mdube@sarouman] - [~] - [2017-03-21 11:53:40]
└─[0] <> grep Linkedin leaks_cegep-ste-foy.qc.ca | wc -l
124
```

$ less adobe.txt

- Count: 155M
- Hash Format: Encrypted (Key not disclosed, yet.)
- Breach+Disclosure Date: 2013-10 (October)
- Scope: Product users, Clients
- Incident Handling: ?

- Bonus
  - Password Hints!

$ less dropbox.txt

- Count: 69M
- Hash Format: Salted bcrypt (2^8 iter) or Salted SHA1
- Breach Date: mid-2012, Disclosure Date: 2016-08
- Scope: File sharing on the cloud
- Incident Handling: Bad
  - Did not acknowledge the breach
  - Took 2 weeks to write a blog post
  - However, Dropbox has prompted users who may have been affected by the hack to reset their passwords.
    - But the prompt was selective
  - https://www.dropbox.com/help/9257

$ less ashley_madison.txt

- Count: 30M
- Hash Format: Salted bcrypt (2^12 iter)
- Breach+Disclosure Date: 2015-07 (july)
- Scope: Dating site encouraging affairs
- Incident Handling:

- Bonus
  - Looking for an affair?

Utilisations

Que faire avec ces données?

Activités du *black market* liées à des *leaks* ou hacks

- DDoS
- CC batches
- Botnets
- Trolling
- Malware variés (cryptomining, RATs, ransomware, …)
- Hits
- Drogues
- Phishing/spam
- Services de *rating* (falsifier des votes/reviews/réputations)
- Shipping/*muling*/livraison
- Fausses identités
- Briser des captchas

Utilisations?

- Connexion sur des sites
  - Manuellement (via un navigateur)
  - Massivement (via des outils)
- Bâtir des dictionnaires
  - Online Cracking: medusa, hydra, metasploit, etc.
- Cracker les hash
  - Offline Cracking: John or Hashcat
- Recommencer

Connexion sur des sites (Manuellement)

- Trop souvent, les *credentials* aux sites suivants sont trop similaires
  - Facebook
  - Twitter
  - LinkedIn
  - Google/OAuth
  - OWA du travail
  - YouTube
  - PornHub?

Connexion sur des sites (Massivement)

- https://github.com/philwantsfish/shard
  - A command line tool to detect shared passwords
  - Facebook, LinkedIn, Reddit, Twitter, Instagram, GitHub, BitBucket, Kijiji, DigitalOcean, Vimeo, Laposte, DailyMotion

Connexion sur des sites

- Utilisation de **shard** sur cegep-ste-foy.qc.ca
  - Texte clairs et Hash “unsalted”

- Nombre de comptes fonctionnels
  - Linkedin: **31**
  - Twitter: 4
  - Kijiji: 3

  - Incluant personnel pédagogique, gestionnaires, professeurs

```
{16-09-20 16:31}sarouman:~/Downloads mdube% proxychains java -jar shard-1.5.jar -u vive_ced_chaput@hotmail.com -p bingo1

[proxychains] config file found: /etc/proxychains.conf
[proxychains] preloading /usr/lib/libproxychains4.so
[proxychains] DLL init: proxychains-ng 4.11
16:31:48.871 [+] Selected single-user single-password mode
16:31:48.873 [+] Running 12 modules
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  www.facebook.co
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  www.linkedin.co
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  www.linkedin.co
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  www.reddit.com:
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  www.reddit.com:
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  www.reddit.com:
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  twitter.com:443
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  www.instagram.c
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  github.com:443
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  github.com:443
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  bitbucket.org:4
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  www.kijiji.ca:4
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  cloud.digitaloc
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  cloud.digitaloc
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  vimeo.com:443
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  vimeo.com:443
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  www.laposte.net
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  compte.laposte.
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  www.dailymotion
16:34:25.199 [+] vive_ced_chaput@hotmail.com:bingo1 - Kijiji
```

Dictionnaires

- *Rockyou.txt* a longtemps été la liste de référence
  - 32M non-uniques
  - *PLAINTEXT*
- Il y eu plusieurs *leaks* fort intéressants
  - Gawker
  - Stratfor
  - eHarmony
  - Evernote
  - …
- Survint le *leak* LinkedIn qui est maintenant la référence

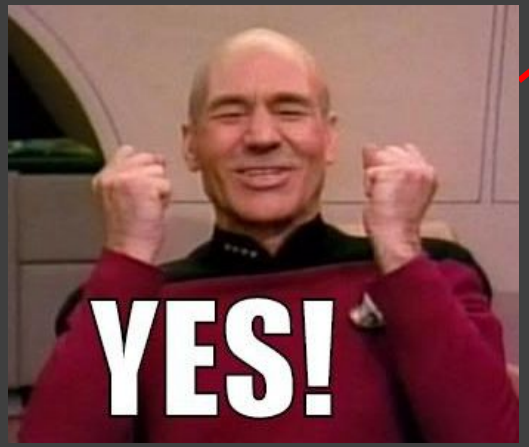
Dictionnaires

- Couvre bien plus des contextes variés
- Résume bien le style de mots de passes actuel
- Nouveaux patterns, nouvelles statistiques
- LinkedIn = 6x le data de rockyou
- Bien plus de monde utilise LinkedIn
- Plus récent
- Reset de 6.4M de comptes....
- ...sauf que 178M de comptes ont été *leaked*
- Causant ainsi plein d'utilisateurs à ne pas changer d'habitudes alors qu'ils auraient dû

Dictionnaires publiques

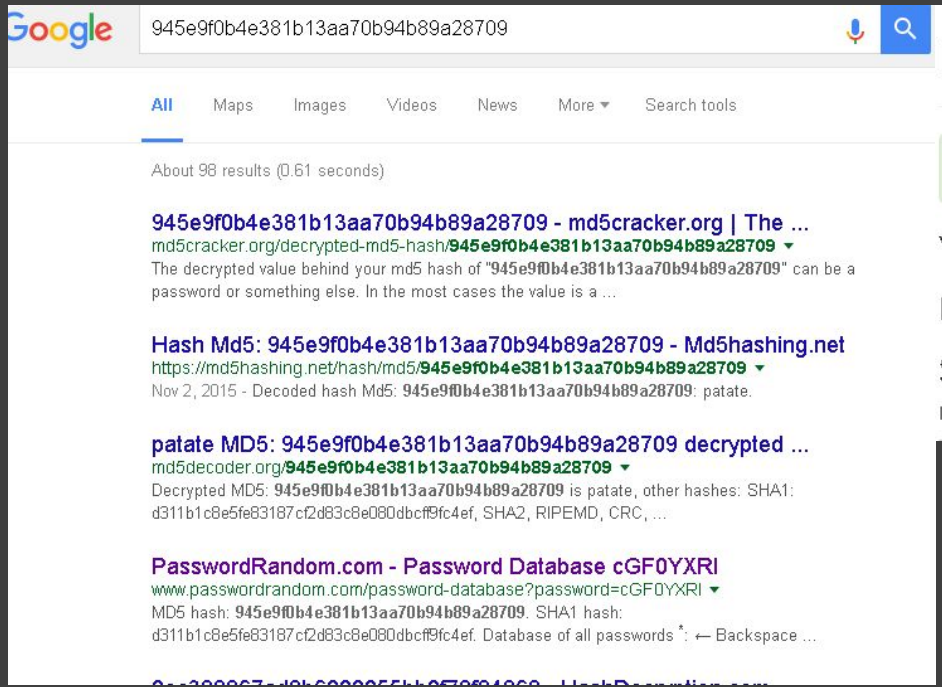
- https://hashes.org/public.php
  - Contient des wordlists associées à des leaks
  - 160M Linkedin = 96.87% cracked

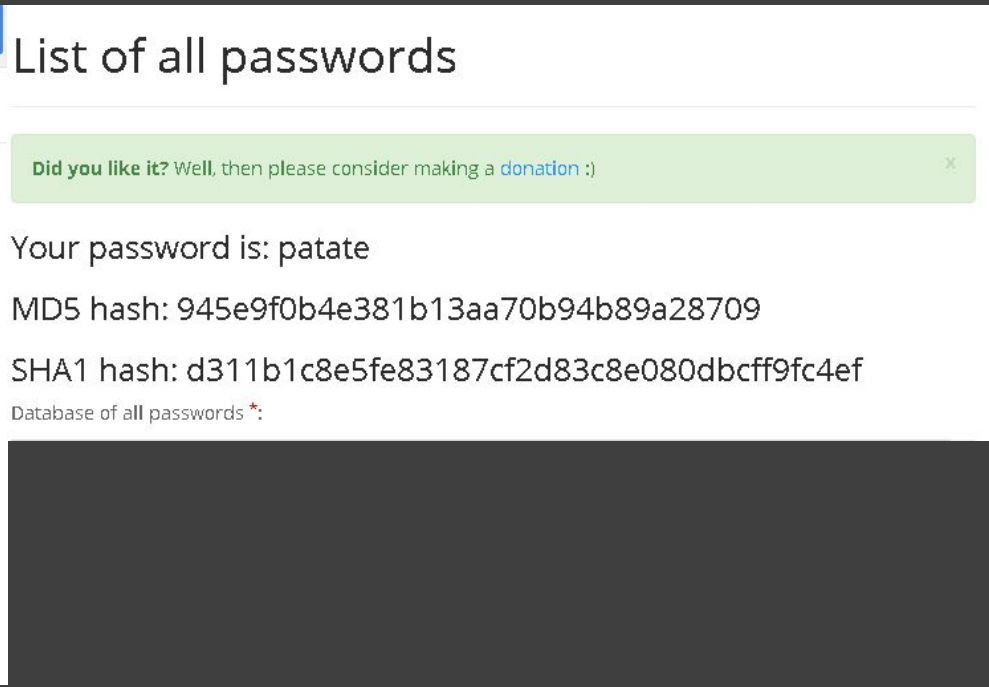
4920	L1nk3d1n (SHA1)	20.09.2016 - 19:33:41	61'829'262	59'892'114 (96.87%)



Cracker un hash? - LMGTFY

dakara@:/home/sys6x/.ssh# echo -n patate | md5sum
945e9f0b4e381b13aa70b94b89a28709 -





Cracker un hash?

- Bruteforce
- Attaques hybrides *wordlists*+mask
- *Wordlists*
- Combinaison de *wordlists*
- Permutations
- Règles de Markov
- Essentiellement sur des *hashtypes* rapides
  - MD5
  - SHA-1

Quelques chiffres sur le benchmarking

- Specs: 3x GeForce GTX 980
  - 6144 cuda cores
  - < 10k $

Technique	Hash Type	Speed
Pure wordlist	Unsalted SHA1	~3 700 000 000 H/s
Pure wordlist	Salted Bcrypt (2^12 iter = 4096)	~120 H/s
Wordlist + Rules	Unsalted SHA1	~31 000 000 000 H/s
Wordlist + Rules	Salted Bcrypt (2^12 iter = 4096)	~120 H/s
Pure bruteforce	Unsalted SHA1	~12 000 000 000 h/s
Pure bruteforce	Salted Bcrypt (2^12 iter = 4096)	~120 H/s

Demo

Don’t learn to hack, Hack to learn

Responsabilités

Que faire pour mitiger les impacts?

Responsabilités

- *Sysadmins* & Développeurs
  - Bon et mauvais façon de stocker les mots de passes
  - Bonnes et Mauvaises politiques de mots de passes

- Utilisateurs
  - Bon et mauvais mots de passes

[Sysadmin] Stockage: FAIL

- Cleartext - $password
  - Yeah! Encore utilisé en 2016!
- Encrypted - 3des($password, $key)
  - Pass is reversible...
- Unsalted SHA1 - sha1($password)
  - Easy to compute (very fast)
- Unsalted MD5 - md5($password)
  - Easy to compute (very fast)
  - Colision en boni !
- Salted MD5/SHA1/Others - md5($salt:$password)
  - Much Better. When properly done, requires other vulnerabilities to crack the dump
  - https://crackstation.net/hashing-security.htm

[Sysadmin] Stockage: Success

- Critères
  - Super lent
    - Ne pas utiliser les algo conçus pour être performants (MD* et SHA*)
    - Configurer des itérations afin de compenser l'évolution de la vitesse des machines
  - Hash relativement long
    - Rendre les collisions le plus rare possible
  - Utiliser un ou plusieurs SALT(S)
    - Salt unique à l'application - Nécessiterait d'autres vulnérabilités pour cracker un dump
    - Salt unique à l'usager - Rend inutilisable les compromis espace-temps (rainbow tables)
- Le meilleur type de hash connu: bcrypt
  - Holy Shit, Dropbox and Ashley Madison did it right !

[Sysadmin] Stockage: Success

Bcrypt: Thanks stackoverflow.com

Stored in the database, a `bcrypt` "hash" might look something like this:

```
$2a$10$vI8aWBnW3fID.ZQ4/zo1G.q1lRps.9cGLcZEiGDMVr5yUP1KUOYTa
```

This is actually three fields, delimited by "$":

- `2a` identifies the `bcrypt` algorithm version that was used.
- `10` is the cost factor; 2^{10} iterations of the key derivation function are used (which is not enough, by the way. I'd recommend a cost of 12 or more.)
- `vI8aWBnW3fID.ZQ4/zo1G.q1lRps.9cGLcZEiGDMVr5yUP1KUOYTa` is the salt and the cipher text, concatenated and encoded in a modified Base-64. The first 22 characters decode to a 16-byte value for the salt. The remaining characters are cipher text to be compared for authentication.

[Sysadmin] Mauvaises politiques

[Sysadmin] Mauvaises politiques

You must keep your new password for a **minimum of 24 hours** before attempting to change it again.
The password will expire 60 days after being created and can be changed before, on, or after the expiration date.

PASSWORD CRITERIA				
Password **Must**	Password **Must Not**			
Be **EXACTLY 8 characters** in length	Match any of your previous 10 passwords used			
Contain at least 1 Uppercase and 1 Lowercase letter	Contain your Logon ID or more than 2 consecutive characters from your first or last name			
Contain at least 1 Number	Contain consecutive repeating characters (e.g., 'aa', '$$', '22')			
Contain at least 1 of the following 3 special characters - @#$. (No other special characters are allowed.)	Be too similar to your previous password – specifically, *must not contain 3 or more consecutive characters that match the same relative character positions with your previous password.*			
	Begin with any of these reserved words (list subject to change by DISA)			
	APPL	ASDF	BASIC	CADAM
	DEMO	FOCUS	GAME	IBM
	LOG	NET	NEW	PASS
	ROS	SIGN	SYS	TEST
	VALID	VTAM	XXX	1234
	Begin with Month abbreviations – JAN, FEB, MAR, APR, MAY, JUN, JUL, AUG, SEP, OCT, NOV, DEC			

Trouble getting your new password to PASS? Click HERE to view a brief training video that can help
(accessible from the ATRRS home page, Support => User Training => ATRRS-101 Online, ATRRS-101 Modules).

[Sysadmin] Mauvaises politiques

- Trop de conditions
- Restreindre l'entropie (caractères spéciaux, pas d'espace, …)
  - Aucune bonne raison pour empêcher des caractères
- Tl;dr
- Longueur minimum trop élevée ou maximum trop bas
- Trop de restrictions et vous aidez les attaquants
  - Élimine des possibilités et sauve du temps aux attaquants

[Sysadmin] Mauvaises politiques

- Encourager l’usager à:
  - Éviter les *passwords* prévisibles
  - Écrire leurs mots de passe sur des *post-it*
  - Appeler le support pour changer des MDP oubliés
  - Ignorer la politique ou tentent de contourner
- Cause des *lockouts* et de la perte de productivité
- Max 8-10 caractères

[Sysadmin] Bonnes politiques

- Faire comprendre les avantages en éduquant
  - Inclut de la formation et des ateliers
- Tout pour compliquer la tâche de l'attaquant
- Politiques décrites clairement
- Présentement le marché recommende 8 caractères et plus.
  - Personnellement: 15 et plus.
- Passphrase > password

[Utilisateurs] Mythes

- Les grosses compagnies ont assez d'argent pour bien sécuriser.
- Les calculateurs de force de mots de passe sont efficaces.

Password	Microsoft	The Password Meter
jjjjjjjjjjjjjjjjjjjj	Best	Very Weak
Jessica1234567	Strong	Very Strong
Qwertyabc123	Strong	Strong

- La complexité bat la longueur.
- Le plus long le mot de passe, le mieux c'est

[Utilisateurs] Bonnes politiques

- Utiliser un gestionnaire de mots de passe comme KeePass
- Utiliser des termes peu connus, très spécifiques

- Éviter de réutiliser les mots de passes
- Éviter d’incrémenter

[Utilisateurs] Bonnes pratiques

- Utiliser d'autres langues
  - Qui penserait que votre mot de passe est *dievushka (девушка)*?
- Faites des fautes ou permutations intentionnelles
  - alibaabet04Vauleur
- Ne pas inclure de données personnelles
  - patate701004
- Mixer des *charsets* et inclure des caractères uniques
  - jamÉlançeザンギエフ
- Filtrer les passwords de rockyou.txt et 500worstpwds.txt
  - Et leurs traductions peut-être….

Les pires mots de passe en 2015

RANK	PASSWORD	CHANGE FROM 2014
1	123456	Unchanged
2	password	Unchanged
3	12345678	1 ↗
4	qwerty	1 ↗
5	12345	2 ↘
6	123456789	Unchanged
7	football	3 ↗
8	1234	1 ↘
9	1234567	2 ↗
10	baseball	2 ↘
11	welcome	NEW
12	1234567890	NEW
13	abc123	1 ↗
14	111111	1 ↗

Mots de passes de cegep-ste-foy.qc.ca

```
Top 10 passwords
koala111 = 4 (4.17%)
666666 = 3 (3.13%)
sport9 = 2 (2.08%)
perles = 2 (2.08%)
somata = 2 (2.08%)
truite = 2 (2.08%)
pitchou = 2 (2.08%)
napoleon = 2 (2.08%)
165082182419725 = 2 (2.08%)
patataouf = 2 (2.08%)
```

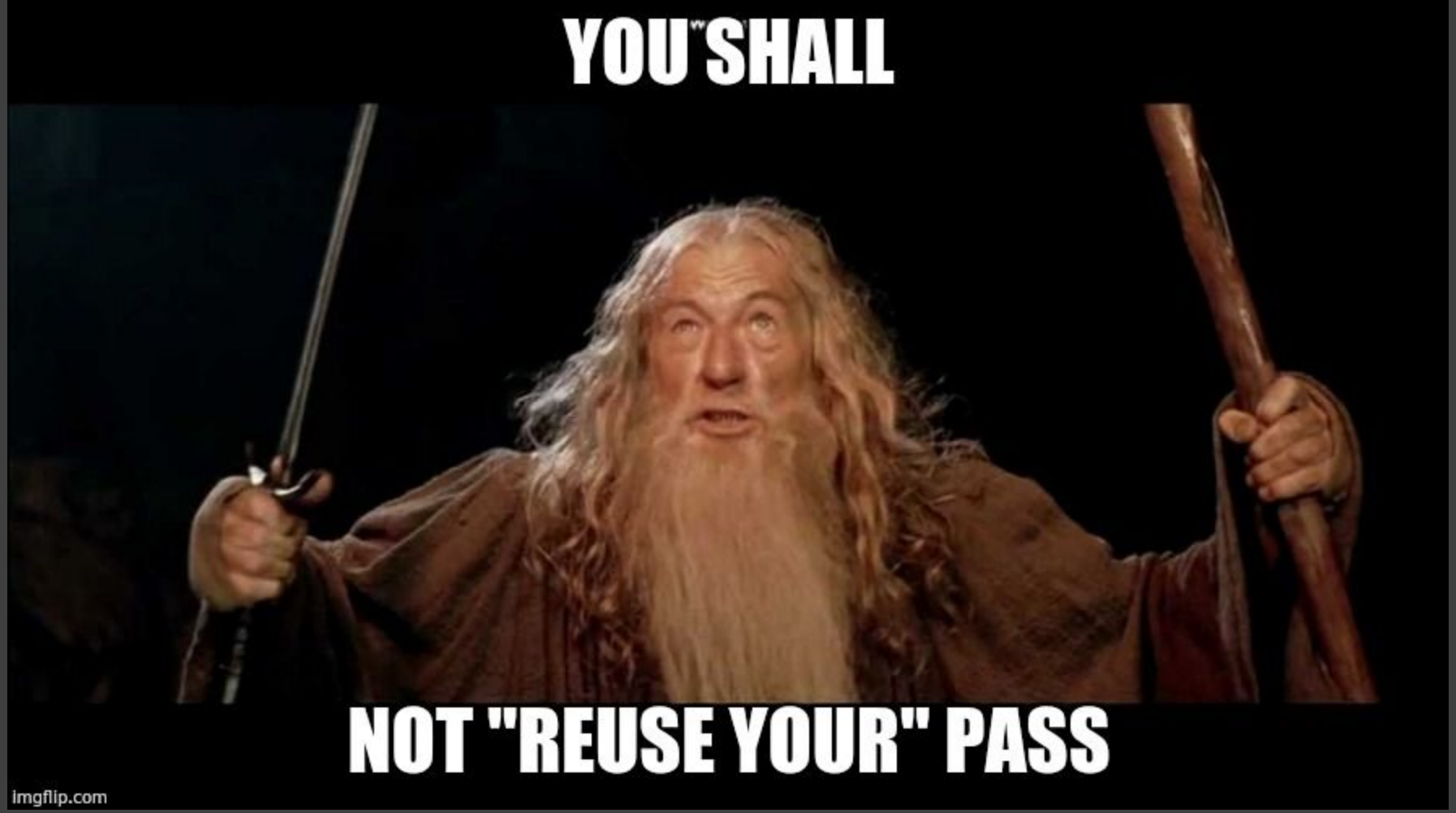
```
Top 10 base words
koala = 4 (4.17%)
ybo4ufp = 2 (2.08%)
perles = 2 (2.08%)
somata = 2 (2.08%)
truite = 2 (2.08%)
pitchou = 2 (2.08%)
napoleon = 2 (2.08%)
antonin = 2 (2.08%)
sport = 2 (2.08%)
patataouf = 2 (2.08%)
```

```
Password length (length ordered)
6 = 23 (23.96%)
7 = 19 (19.79%)
8 = 29 (30.21%)
9 = 9 (9.38%)
10 = 5 (5.21%)
11 = 4 (4.17%)
12 = 2 (2.08%)
13 = 2 (2.08%)
15 = 12 (12.5%)
```

```
Months (Abreviated)
jan = 1 (1.04%)
mar = 2 (2.08%)
jul = 1 (1.04%)

Days (Abreviated)
None found

Includes years
2010 = 2 (2.08%)
2011 = 1 (1.04%)

Years (Top 10)
2010 = 2 (2.08%)
2011 = 1 (1.04%)
```

Ressources intéressantes

- Forums hashcat
- Mailing-list openwall/johntheripper
- IRC
  - Irc.freenode.net
    - #hashcat
    - #openwall
- /r/passwords
- Cracking CTFs *writeups*
  - *CMIYC*
  - *PHDays Hashrunner*
  - *...plenty more*


YOU SHALL
NOT "REUSE YOUR" PASS
imgflip.com

Merci !