# Force Brute - Le problème du temps

*Dernière mise à jour*
*2016-01-20T00:00 - Assiste - Pierre Pinard*
*20.01.2016 - 00h00 - Paris - (Assiste - Pierre Pinard) - Mise à jour*
*01.05.2015 - 00h00 - Paris - (Assiste - Pierre Pinard) - Ressource - wfuzz*

***L'attaque en "Force brute" est l'une des méthodes utilisées en cryptanalyse pour tenter de casser un cryptage. Le principe en lui-même de l'attaque en "Force brute" ne vise pas exclusivement les "Mots de passe" mais c'est dans ce domaine que ce type d'attaques est essentiellement utilisé. L'attaque en "Force brute" vise un mot de passe à la fois.***

## Qu'est-ce qu'une attaque en " Force brute " ?

Il y a deux usages de la "Force brute" :

1. Un cybercriminel s'est procuré un "identifiant" et le "hashcode" du "mot de passe" associé à cet "identifiant" (ou des listes d'"identifiants" et les "hashcodes" des "mots de passe" associés. On ne se souci pas du moyen mis en oeuvre pour les obtenir (piratage d'un serveur, écoute par sniffer...). La question n'est pas là.

   L'attaque en "force brute" commence lorsque l'on dispose du couple "identifiant" et "chiffre clé" dont on ne peut rien faire. Il faut remonter du "chiffre clé" au "mot de passe" d'origine. Il faut casser le "chiffre clé" qui, normalement ne permet pas de remonter à la chaîne de caractères qui a servi à le générer.

   Puisque le cryptage du "mot de passe" est à sens unique (univoque), il n'y a pas de formule pour décrypter le "hashcode". La seule méthode possible est donc de recommencer : crypter toutes les combinaisons possibles de caractères autorisés, avec le même algorithme (MD5, SHA-1...), jusqu'à obtenir un "hashcode" identique à celui détenu. Il faut donc également savoir quel est l'algorithme qui a été utilisé. On peut le deviner par la longueur du "hashcode" (16 caractères, c'est du MD5, 20 caractères c'est du SHA-1 etc. ...).

   En utilisant du matériel spécialisé (réseau BotNet ou ordinateur à base de matériel spécialement développé pour les attaques en "Force brute" etc. ...), et après un certain temps de calcul, on fini par trouver le "mot de passe" à l'origine du "hashcode". On peut alors usurper l'identité du titulaire en utilisant son couple "identifiant" / "mot de passe".

   Le temps de calcul est totalement dépendant de :

   - Le puissance du matériel utilisé pour le calcul
   - La longueur des mots de passe (le nombre N maximum de caractères)
   - Le jeu de caractères utilisés.

### Les types de jeux de caractères

***Rappel - Les types de jeux de caractères***

Pour simplifier, en chiffrement, dont le chiffrement des mots de passe, les jeux de caractères utilisés sont classés en 4 types :

- Type 1 : Les 26 lettres de l'alphabet, toutes en majuscules ou toutes en minuscules (insensible à la case). Ce jeu de caractères est très restrictif et un

mot de passe court (8 à 12 caractères) est cassable en quelques minutes.
ABCDEFGHIJKLMNOPQRSTUVWXYZ
Ou
abcdefghijklmnopqrstuvwxyz

- Type 2 : Le type 1 augmenté des 10 chiffres soit 36 caractères. Très restrictif et cassable très rapidement.
  ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789
  Ou
  abcdefghijklmnopqrstuvwxyz0123456789

- Type 3 : Le type 2 augmenté de l'usage libre et différencié des majuscules/minuscules soit 62 caractères. Restrictif et cassable assez rapidement.
  ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz01234567

- Type 4 : Le type 3 augmenté d'un nombre plus ou moins restreint de caractères spéciaux et de caractères accentués (90 à > 100 caractères). C'est le seul type recommandé. Dans les évaluations de temps de calcul en attaque par "Force brute" ou de volume mémoire en attaques par "dictionnaire exhaustif", nous retiendrons un type 4 à 100 caractères.
  Exemples de jeux de caractères :
  ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz01234567
  §%µ
  Ou
  ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz01234567
  è_çà)=#{[|^@]}^¨$£¤ù%*µ,?;.:/!§

Le nombre de combinaisons possibles qu'il va falloir calculer est égal à :
Longueur maximum du mot de passe = M caractères.
Longeur du mot de passe = P caractères
Nombre de caractères dans le jeu de caractères = N
Indice i varie de 1 à P
Nombre de combinaisons possibles = $(P_{i=1} \times N) + (P_{i=2} \times N) + (P_{i=3} \times N) + (P_{i=4} \times N)$ etc. ... jusqu'à ce que i=P

En moyenne, il faut calculer la moitié des combinaisons possibles, ce qui peut prendre **plusieurs vies** si le "mot de passe" d'origine est long.

2. L'attaque en "force brute" utilisée manuellement contre la procédure d'autentification (la page d'identification où on compose le couple "identifiant" / "mot de passe" du compte attaqué) en s'asseyant devant un écran / clavier (ou en simulant, par un robot travaillant automatiquement, la présence de quelqu'un composant un couple identifiant / mot de passe).

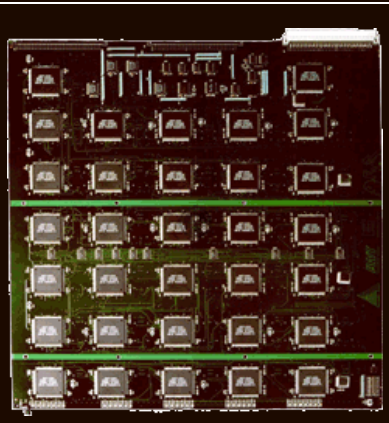
   Il faut posséder l'identifiant et essayer toutes les combinaisons possibles de caractères pour tomber finalement sur le bon "mot de passe".

   Cette forme d'usage de la "force brute" est possible contre un compte très peu sensible (compte sur un forum, sur un réseau social etc. ...) utilisant des mots de passe très courts. Elle est totalement illusoire et vouée à l'échec contre un compte sensible (banque, e-commerce, assurance, administration etc. ...). Ces comptes utilisent (théoriquement) plusieurs méthodes pour empêcher les attaques en "force brute" :

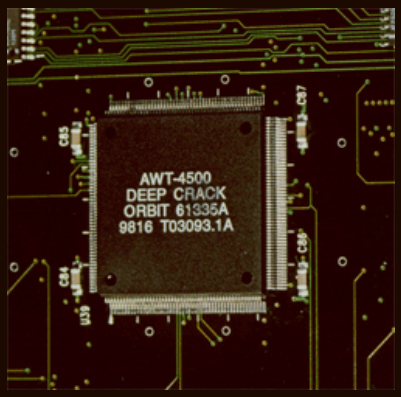
   - Détection automatique de plusieurs tentatives successives de "mots de passe" erronés.
   - Détection automatique de plusieurs tentatives successives de "mots de passe" erronés, les "mots de passe" tentés étant présentés de manière ordonnée. Cela oblige l'attaquant à tenter les "mots de passe" possibles dans un ordre aléatoire, ce qui introduit quelques dificultés, aussi bien pour une attaque "manuelle" que pour un logiciel d'un robot d'attaque.
   - Après un certain nombre de tentatives infructueuses (généralement 3 tentatives), le délais pour autoriser une nouvelle tentative s'allonge. En fonction de la longueur du "mot de passe", les combinaisons possibles sont tellement nombreuses que le temps moyen pour tomber sur le bon "mot de passe" risque d'être plus long que la fin probable de l'Univers ! Seuls les "mots de passe" très courts ont une toute petite chance d'être cassés par cette méthode. Et, comme les mots de passe très courts, très simples, ne protègent que des choses sans intérêt...
   - Une méthode de défense, lorsque l'autorité d'authentification à un doute (bon "mot de passe" mais précédé de nombreuses tentatives erronées), consiste à envoyer systématiquement un message du type "Erreur de mot de passe", y compris sur le bon "mot de passe". Si l'utilisateur est l'authentique détenteur du compte, il va insister avec son bon mot de passe que le système d'authentification laissera passer à la tentative suivante. Si l'utilisateur n'est pas le détenteur du compte, il va poursuivre son attaque en "force brute", ignorant le bon mot de passe qui vient de lui glisser entre les doigts.

- Un bon "captcha" ralenti encore une attaque en "force brute" faite manuellement et élimine définitivement une attaque robotisée.

### Matériel, cartes et processeurs spécialisés pour des attaques en " Force brute "



*Deep Crack - Cartes multi-processeurs spécialisées pour des attaques en Force Brute*




*Deep Crack - Processeurs spécialisées pour des attaques en Force Brute*

## Casser les mots de passe en Force Brute ou par dictionnaire exhaustif

### Evaluation du temps nécessaire en fonction du nombre de combinaisons possibles
### Evaluation de la mémoire nécessaire en fonction du nombre de combinaisons possibles

En rouge, les attaques " jouables - possibles " (donc signalant des mots de passe faibles en longueur et en jeu de caractères)

### Type 1 : Jeu de 26 caractères (tout majuscules ou tout minuscules)

| Mots de passe de : | | | | | | | |
|---|---|---|---|---|---|---|---|
| | 8 caractères | 9 caractères | 10 caractères | 11 caractères | 12 caractères | 13 caractères | 14 caractères |
| Rang 1 | 26 | 26 | 26 | 26 | 26 | 26 | 26 |
| Rang 2 | 676 | 676 | 676 | 676 | 676 | 676 | 676 |
| Rang 3 | 17 576 | 17 576 | 17 576 | 17 576 | 17 576 | 17 576 | 17 576 |
| Rang 4 | 456 976 | 456 976 | 456 976 | 456 976 | 456 976 | 456 976 | 456 976 |
| Rang 5 | 11 881 376 | 11 881 376 | 11 881 376 | 11 881 376 | 11 881 376 | 11 881 376 | 11 881 376 |
| Rang 6 | 308 915 776 | 308 915 776 | 308 915 776 | 308 915 776 | 308 915 776 | 308 915 776 | 308 915 776 |
| Rang 7 | 8 031 810 176 | 8 031 810 176 | 8 031 810 176 | 8 031 810 176 | 8 031 810 176 | 8 031 810 176 | 8 031 810 176 |
| Rang 8 | 208 827 064 576 | 208 827 064 576 | 208 827 064 576 | 208 827 064 576 | 208 827 064 576 | 208 827 064 576 | 208 827 064 576 |
| Rang 9 | | 5 429 503 678 976 | 5 429 503 678 976 | 5 429 503 678 976 | 5 429 503 678 976 | 5 429 503 678 976 | 5 429 503 678 976 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Rang 10 | | | 141 167 095 653 376 | 141 167 095 653 376 | 141 167 095 653 376 | 141 167 095 653 376 | 141 167 095 653 376 |
| Rang 11 | | | | 3 670 344 486 987 780 | 3 670 344 486 987 780 | 3 670 344 486 987 780 | 3 670 344 486 987 780 |
| Rang 12 | | | | | 95 428 956 661 682 200 | 95 428 956 661 682 200 | 95 428 956 661 682 200 |
| Rang 13 | | | | | | 2 481 152 873 203 740 000 | 2 481 152 873 203 740 000 |
| Rang 14 | | | | | | | 64 509 974 703 297 200 000 |

**Type 1 - Combinaisons possibles (mots de passe possibles)**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | 217 180 147 158 | 5 646 683 826 134 | 146 813 779 479 510 | 3 817 158 266 467 290 | 99 246 114 928 149 500 | 2 580 398 988 131 890 000 | 67 090 373 691 429 000 000 |

**Type 1 - Temps de calcul nécessaire pour construire un dictionnaire intégral (en jours) - En rouge ce qui est " jouable ". Basé sur le matériel construit par nsa.unaligned.org en 2007.**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| En 2007 | 0 | 0,03 | 0,66 | 17 | 447 | 11 628 | 302 319 |
| En 2009 | 0 | 0 | 0 | 1 | 20 | 517 | 13 463 |

**Type 1 - Mémoire de stockage nécessaire, en teraoctets, pour un tel dictionnaire contenant "Mot de passe", Hash MD5, Hash SHA-1 (Recherches par dichotomie, Recherche par B-Tree)**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | 9 556 | 254 101 | 6 753 434 | 179 406 439 | 4 763 813 517 | 126 439 550 418 | 3 354 518 684 571 |
| | 19 112 | 508 202 | 13 506 868 | 358 812 877 | 9 527 627 033 | 252 879 100 837 | 6 709 037 369 143 |

**Type 2 : Jeu de 36 caractères (tout majuscules ou tout minuscules + 10 chiffres)**
**(cas de certains algorithmes de chiffrement qui ne tiennent pas comptes des majuscules/minuscules (insensibles à la case) et mettent le mot de passe à plat - par exemple l'algorithme de chiffrement LanManager Hash sous Windows, qui commence par transformer les minuscules en majuscules)**

| Mots de passe de : | | | | | | | |
|---|---|---|---|---|---|---|---|
| | 8 caractères | 9 caractères | 10 caractères | 11 caractères | 12 caractères | 13 caractères | 14 caractères |
| Rang 1 | 36 | 36 | 36 | 36 | 36 | 36 | 36 |
| Rang 2 | 1 296 | 1 296 | 1 296 | 1 296 | 1 296 | 1 296 | 1 296 |
| Rang 3 | 46 656 | 46 656 | 46 656 | 46 656 | 46 656 | 46 656 | 46 656 |
| Rang 4 | 1 679 616 | 1 679 616 | 1 679 616 | 1 679 616 | 1 679 616 | 1 679 616 | 1 679 616 |
| Rang 5 | 60 466 176 | 60 466 176 | 60 466 176 | 60 466 176 | 60 466 176 | 60 466 176 | 60 466 176 |
| Rang 6 | 2 176 782 336 | 2 176 782 336 | 2 176 782 336 | 2 176 782 336 | 2 176 782 336 | 2 176 782 336 | 2 176 782 336 |
| Rang 7 | 78 364 164 096 | 78 364 164 096 | 78 364 164 096 | 78 364 164 096 | 78 364 164 096 | 78 364 164 096 | 78 364 164 096 |
| Rang 8 | 2 821 109 907 456 | 2 821 109 907 456 | 2 821 109 907 456 | 2 821 109 907 456 | 2 821 109 907 456 | 2 821 109 907 456 | 2 821 109 907 456 |
| Rang 9 | | 101 559 956 668 416 | 101 559 956 668 416 | 101 559 956 668 416 | 101 559 956 668 416 | 101 559 956 668 416 | 101 559 956 668 416 |
| Rang 10 | | | 3 656 158 440 062 980 | 3 656 158 440 062 980 | 3 656 158 440 062 980 | 3 656 158 440 062 980 | 3 656 158 440 062 980 |
| Rang 11 | | | | 131 621 703 842 267 000 | 131 621 703 842 267 000 | 131 621 703 842 267 000 | 131 621 703 842 267 000 |
| Rang 12 | | | | | 4 738 381 338 321 620 000 | 4 738 381 338 321 620 000 | 4 738 381 338 321 620 000 |
| Rang 13 | | | | | | 170 581 728 179 578 000 000 | 170 581 728 179 578 000 000 |
| Rang 14 | | | | | | | 6 140 942 214 464 820 000 000 |

## Type 2 - Combinaisons possibles (mots de passe possibles)

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | 2 901 713 047 668 | 104 461 669 716 084 | 3 760 620 109 779 060 | 135 382 323 952 046 000 | 4 873 763 662 273 660 000 | 175 455 491 841 852 000 000 | 6 316 397 706 306 670 000 000 |

## Type 2 - Temps de calcul nécessaire pour construire un dictionnaire intégral (en jours) - En rouge ce qui est " jouable ". basé sur le matériel construit par nsa.unaligned.org en 2007.

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| En 2007 | 0,01 | 0,47 | 17 | 610 | 21 962 | 790 627 | 28 462 569 |
| En 2009 | 0 | 0 | 1 | 27 | 976 | 35 139 | 1 265 003 |

## Type 2 - Mémoire de stockage nécessaire, en teraoctets, pour un tel dictionnaire contenant "Mot de passe", Hash MD5, Hash SHA-1 (Recherches par dichotomie, Recherche par B-Tree)

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | 127 675 | 4 700 775 | 172 988 525 | 6 362 969 226 | 233 940 655 789 | 8 597 319 100 251 | 315 819 885 315 333 |
| | 255 351 | 9 401 550 | 345 977 050 | 12 725 938 451 | 467 881 311 578 | 17 194 638 200 502 | 631 639 770 630 667 |

## Type 3 : Jeu de 62 caractères (majuscules + minuscules + 10 chiffres)

| Mots de passe de : | | | | | | | |
|---|---|---|---|---|---|---|---|
| | 8 caractères | 9 caractères | 10 caractères | 11 caractères | 12 caractères | 13 caractères | 14 caractères |
| Rang 1 | 62 | 62 | 62 | 62 | 62 | 62 | 62 |
| Rang 2 | 3 844 | 3 844 | 3 844 | 3 844 | 3 844 | 3 844 | 3 844 |
| Rang 3 | 238 328 | 238 328 | 238 328 | 238 328 | 238 328 | 238 328 | 238 328 |
| Rang 4 | 14 776 336 | 14 776 336 | 14 776 336 | 14 776 336 | 14 776 336 | 14 776 336 | 14 776 336 |
| Rang 5 | 916 132 832 | 916 132 832 | 916 132 832 | 916 132 832 | 916 132 832 | 916 132 832 | 916 132 832 |
| Rang 6 | 56 800 235 584 | 56 800 235 584 | 56 800 235 584 | 56 800 235 584 | 56 800 235 584 | 56 800 235 584 | 56 800 235 584 |
| Rang 7 | 3 521 614 606 208 | 3 521 614 606 208 | 3 521 614 606 208 | 3 521 614 606 208 | 3 521 614 606 208 | 3 521 614 606 208 | 3 521 614 606 208 |
| Rang 8 | 218 340 105 584 896 | 218 340 105 584 896 | 218 340 105 584 896 | 218 340 105 584 896 | 218 340 105 584 896 | 218 340 105 584 896 | 218 340 105 584 896 |
| Rang 9 | | 13 537 086 546 263 600 | 13 537 086 546 263 600 | 13 537 086 546 263 600 | 13 537 086 546 263 600 | 13 537 086 546 263 600 | 13 537 086 546 263 600 |
| Rang 10 | | | 839 299 365 868 340 000 | 839 299 365 868 340 000 | 839 299 365 868 340 000 | 839 299 365 868 340 000 | 839 299 365 868 340 000 |
| Rang 11 | | | | 52 036 560 683 837 100 000 | 52 036 560 683 837 100 000 | 52 036 560 683 837 100 000 | 52 036 560 683 837 100 000 |
| Rang 12 | | | | | 3 226 266 762 397 900 000 000 | 3 226 266 762 397 900 000 000 | 3 226 266 762 397 900 000 000 |
| Rang 13 | | | | | | 200 028 539 268 670 000 000 000 | 200 028 539 268 670 000 000 000 |
| Rang 14 | | | | | | | 12 401 769 434 657 500 000 000 000 |

## Type 3 - Combinaisons possibles (mots de passe possibles)

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | 221 919 451 578 090 | 13 759 005 997 841 600 | 853 058 371 866 182 000 | 52 889 619 055 703 300 000 | 3 279 156 381 453 600 000 000 | 203 307 695 650 123 000 000 000 | 12 605 077 130 307 700 000 000 000 |

## Type 3 - Temps de calcul nécessaire pour construire un dictionnaire intégral (en jours) - En rouge ce qui est " jouable ".

**basé sur le matériel construit par nsa.unaligned.org en 2007.**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| En 2007 | 1 | 62 | 3844 | 238328 | 14 776 336 | 916 132 832 | 56 800 235 584 |
| En 2009 | 0 | 3 | 171 | 10 592 | 656 726 | 40 717 015 | 2 524 454 915 |

**Type 3 - Mémoire de stockage nécessaire, en teraoctets, pour un tel dictionnaire contenant "Mot de passe", Hash MD5, Hash SHA-1 (Recherches par dichotomie, Recherche par B-Tree)**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | 9 764 456 | 619 155 270 | 39 240 685 106 | 2 485 812 095 618 | 157 399 506 309 773 | 9 962 077 086 856 050 | 630 253 856 515 383 000 |
| | 19 528 912 | 1 238 310 540 | 78 481 370 212 | 4 971 624 191 236 | 314 799 012 619 546 | 19 924 154 173 712 100 | 1 260 507 713 030 770 000 |

**Type 4 : Jeu de 100 caractères (majuscules + minuscules + 10 chiffres + 38 caractères spéciaux et accentués)**

| Mots de passe de : | | | | | | | |
|---|---|---|---|---|---|---|---|
| | 8 caractères | 9 caractères | 10 caractères | 11 caractères | 12 caractères | 13 caractères | 14 caractères |
| Rang 1 | 100 | 100 | 100 | 100 | 100 | 100 | 100 |
| Rang 2 | 10 000 | 10 000 | 10 000 | 10 000 | 10 000 | 10 000 | 10 000 |
| Rang 3 | 1 000 000 | 1 000 000 | 1 000 000 | 1 000 000 | 1 000 000 | 1 000 000 | 1 000 000 |
| Rang 4 | 100 000 000 | 100 000 000 | 100 000 000 | 100 000 000 | 100 000 000 | 100 000 000 | 100 000 000 |
| Rang 5 | 10 000 000 000 | 10 000 000 000 | 10 000 000 000 | 10 000 000 000 | 10 000 000 000 | 10 000 000 000 | 10 000 000 000 |
| Rang 6 | 1 000 000 000 000 | 1 000 000 000 000 | 1 000 000 000 000 | 1 000 000 000 000 | 1 000 000 000 000 | 1 000 000 000 000 | 1 000 000 000 000 |
| Rang 7 | 100 000 000 000 000 | 100 000 000 000 000 | 100 000 000 000 000 | 100 000 000 000 000 | 100 000 000 000 000 | 100 000 000 000 000 | 100 000 000 000 000 |
| Rang 8 | 10 000 000 000 000 000 | 10 000 000 000 000 000 | 10 000 000 000 000 000 | 10 000 000 000 000 000 | 10 000 000 000 000 000 | 10 000 000 000 000 000 | 10 000 000 000 000 000 |
| Rang 9 | | 1 000 000 000 000 000 000 | 1 000 000 000 000 000 000 | 1 000 000 000 000 000 000 | 1 000 000 000 000 000 000 | 1 000 000 000 000 000 000 | 1 000 000 000 000 000 000 |
| Rang 10 | | | 100 000 000 000 000 000 000 | 100 000 000 000 000 000 000 | 100 000 000 000 000 000 000 | 100 000 000 000 000 000 000 | 100 000 000 000 000 000 000 |
| Rang 11 | | | | 10 000 000 000 000 000 000 000 | 10 000 000 000 000 000 000 000 | 10 000 000 000 000 000 000 000 | 10 000 000 000 000 000 000 000 |
| Rang 12 | | | | | 1 000 000 000 000 000 000 000 000 | 1 000 000 000 000 000 000 000 000 | 1 000 000 000 000 000 000 000 000 |
| Rang 13 | | | | | | 100 000 000 000 000 000 000 000 000 | 100 000 000 000 000 000 000 000 000 |
| Rang 14 | | | | | | | 10 000 000 000 000 000 000 000 000 |

**Type 4 - Combinaisons possibles (mots de passe possibles)**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | 10 101 010 101 010 100 | 1 010 101 010 101 010 000 | 101 010 101 010 101 000 000 | 10 101 010 101 010 100 000 000 | 1 010 101 010 101 010 000 000 000 | 101 010 101 010 101 000 000 000 | 10 101 010 101 010 100 000 000 000 |

**Type 4 - Temps de calcul nécessaire pour construire un dictionnaire intégral (en jours) - En rouge ce qui est " jouable ".**
**basé sur le matériel construit par nsa.unaligned.org en 2007.**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| En 2007 | 46 | 4552 | 455 166 | 45 516 560 | 4 551 656 031 | 455 165 603 068 | 45 516 560 306 818 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| En 2009 | 2 | 202 | 20 230 | 2 022 958 | 202 295 824 | 20 229 582 359 | 2 022 958 235 859 |

**Type 4 - Mémoire de stockage nécessaire, en teraoctets, pour un tel dictionnaire contenant "Mot de passe", Hash MD5, Hash SHA-1 (Recherches par dichotomie, Recherche par B-Tree)**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | 444 444 444 | 45 454 545 455 | 4 646 464 646 465 | 474 747 474 747 475 | 48 484 848 484 848 500 | 4 949 494 949 494 950 000 | 505 050 505 050 505 000 000 |
| | 888 888 889 | 90 909 090 909 | 9 292 929 292 929 | 949 494 949 494 949 | 96 969 696 969 697 000 | 9 898 989 898 989 900 000 | 1 010 101 010 101 010 000 000 |

## Sécurité informatique - Comment je me fais avoir - Comment ne pas me faire avoir

- Comment je me fais avoir - Comment mon ordinateur se fait infecter.
- Méthodes classiques de déploiement des attaques et malveillances
- Je respecte les 10 commandements
- Je prépare mon PC, le premier jour (Kit de sécurité)
- Je maintiens mon PC totalement à jour
- J'accélère Windows
- J'accélère Internet
- Je vérifie tous mes plugins d'un seul clic (à faire tous les jours) - Article explicatif

- Face à une contamination : Procédure gratuite de décontamination anti-malwares, anti-crapwares, anti-adwares.
- Face à une contamination, j'ai la Safe Attitude

## Sécurité informatique - Contre-mesures

1. **Contre-mesures préventives de base :**

   - Contre l'ingénierie sociale qui arrive à vous convaincre d'ouvrir un fichier ou d'ouvrir une pièce jointe d'un e-mail ou installer une fausse mise à jour, vue dans une publicité, d'une technologie, ou de visiter un site manifestement malveillant, etc. ..., il n'existe et n'existera jamais aucune contre-mesure. C'est dans votre tête que cela se passe. Si vous n'avez pas compris que **le Web n'est pas du tout une zone de confiance et n'est qu'une zone de requins cherchant à vous bouffer**, rien ni personne ne pourra rien pour vous. Votre premier antivirus est celui que vous avez entre les oreilles. On réfléchi d'abord, on clique, éventuellement, après.
   - Ne vous reposez jamais sur le fait d'avoir installé des outils de sécurité. N'abaisser jamais votre niveau de vigilance. Prudence est mère de sureté.
   - Nécessité impérative d'être toujours à jour de tous les correctifs connus aux failles de sécurité afin d'empêcher les cybercriminels de les exploiter, avec :
     - Windows Update (mécanisme Microsoft gratuit de mise à jour de Windows et des produits Microsoft)
     - Secunia PSI (mécanisme gratuit de mise à jour d'un très grand nombre de produits autres que ceux de Microsoft).
   - Toujours installer EMET afin de rendre l'exploitation des failles de sécurité inconnues extrêmement compliquée. EMET est un utilitaire de Microsoft, gratuit, qui empêche l'exploitation des vulnérabilités logicielles grâce à des technologies de réduction des risques de sécurité. Ces technologies fonctionnent comme des protections spéciales et des obstacles que l'auteur de l'attaque doit mettre en échec pour exploiter les vulnérabilités logicielles. Ces technologies de réduction des risques de sécurité ne garantissent pas la non-exploitation des vulnérabilités. Toutefois, elles font en sorte que l'exploitation soit aussi difficile que possible.
   - Toujours installer la version gratuite (détection seule, sans correction) de Hitman Pro. Hitman Pro utilise, simultanément, et de manière déportée (cloud), les moteurs :
     - Dr Web
     - Emsisoft Anti-Malware
     - G Data (lui-même une combinaison d'Avast et BitDefender)
     - BitDefender
     - Ikarus Security Software
     - Kaspersky Lab
   - Toujours vérifier, 1 à 2 fois par jour, d'un seul clic, la Mise à jour de tous les plugins de tous les navigateurs.
   - Toujours bloquer la totalité des mécanismes publicitaires.
   - Afin d'éviter, en amont, l'infection de votre système par des programmes malveillants, dont certains Cryptowares et Ransomwares, téléchargez et installez les outils temps réel suivants :

Kaspersky Internet Security avec la fonction de protection contre les programmes de blocage de l'écran activée.
- Malwarebytes Anti-Malware (version complète, commerciale)

- Toujours disposer de Malwarebytes Anti-Malware.

2. **Contre-mesures curatives de base :**

- Décontamination anti-adwares, anti-malwares, anti-crapwares, anti-rogues, anti-fakes, anti-scarewares, etc. ....

  Le but est, essentiellement, d'éliminer les malveillances ou cybercriminalités de type :

  - « Malwares » Logiciels malveillants - Processus malicieux - Détection et arrêt puis éradication
  - « Services » Détection et arrêt des Services malicieux puis éradication
  - « Processus cachés » Détection et arrêt des processus cachés
  - « Spywares » Logiciels d'espionnage - Détection et arrêt puis éradication
  - « Hijacker » Détournement des réglages et du comportement des mécanismes (page de démarrage du navigateur, etc. ...)
  - « Adware » Mécanismes publicitaires responsables de l'une des formes de bombardement publicitaire
  - « Plugins » et extensions (ou modules additionnels) dans les navigateurs
  - « Extensions » (ou modules additionnels ou add-on, add-in, addin, addon) dans les navigateurs
  - « PUP » (**P**otentialy **U**nwanted **P**rogram - « *Logiciels potentiellement indésirables* »)
  - « PUM » (**P**otentialy **U**nwanted **M**odification - « *Modifications non sollicitées de certains réglages* » dont dans le registre)
  - « DLL » Détection, déchargement puis éradication des DLLs malicieuses (appartenant à des malveillances)
  - « Nettoyage des raccourcis »
  - « Proxy » - Détection et suppression de proxy malicieux
  - « Hosts » - Analyse du DNS local
  - « Rootkit » - Les " Rootkit " disposent de tous les moyens pour se rendre totalement furtifs et indétectables
  - « Trojans » - Chevaux de Troie - innombrables malveillances classées, par simplification, sous le terme de Trojans
  - « Crapwares » Logiciels crapuleux
  - « Scarewares » Logiciels vous faisant peur pour vous inciter à les acheter
  - « Barres d'outils (Toolbars) »

## Derrière le rideau

## Références

## Ressources

wfuzz - un outil et des dictionnaires d'attaqus en force brute (recherche de hiérarchies de répertoires et découverte de répertoires, etc. ...)

## Requêtes similaires

*Historique des mises à jour de cette page*
*10.01.2013 - 00h00 - Paris - (Assiste - Pierre Pinard) - Mise à jour*
*01.04.2012 - 00h00 - Paris - (Assiste - Pierre Pinard) - Mise à jour*
*25.09.2012 - 00h00 - Paris - (Assiste - Pierre Pinard) - Mise à jour de notre article antérieur (versions 1997-2007)*

Commentez cet article...

Assiste.Forums
Sécurité informatique et protection de la vie privée sur Internet

Recherche... Rechercher
Recherche avancée

Index du forum ‹ Assiste ‹ Encyclopédie

FAQ Membres M'enregistrer Connexion

# Attaque de mots de passe en force brute

**Modérateur:** Modérateurs et Modératrices

RÉPONDRE Dans ce sujet... Rechercher

1 message • Page 1 sur 1

## Attaque de mots de passe en force brute

de **pierre** » 16 07 2012

Attaque de mots de passe en force brute - Le problème du temps que cela prend :

L'attaque en "Force brute" est l'une des méthodes utilisées en cryptanalyse pour tenter de casser un cryptage. Le principe en lui-même ne vise pas exclusivement les "Mots de passe" mais c'est dans ce domaine que ce type d'attaques est essentiellement utilisé. L'attaque en "Force brute" vise un mot de passe à la fois.

Du matériel spécialisé a même été construit pour conduire des attaques en Force Brute.

Le jeu consiste à tenter toutes les combinaisons possibles de chiffres / lettres / caractères spéciaux... jusqu'à trouver le bon.

Cela prend du temps... beaucoup de temps...

## Force Brute - Casser les mots de passe : Attaque en Force brute et le problème du temps

**pierre**

Messages: 18838
Inscription: 20 05 2002
Localisation: Ici et maintenant

MP

_____
**Pierre (aka Terdef)**
**Appel à donation - Le site a besoin de votre aide**

**Préventif :**
**Comment je me fais avoir ? Comment mon ordinateur se fait infecter ?**
**Protéger le navigateur, la navigation et la vie privée**
**Bloquer la publicité et la surveillance sur le Web**
**Choisir un antivirus** ou choisir **Kaspersky PURE**
**Installer Malwarebytes Anti-Malware (MBAM) - Version Premium**
**Accélérer la vitesse et les performances de Windows**
**Accélérer la vitesse d'Internet**
**Mise à jour de tous les plugins, pour tous les navigateurs, d'un seul clic.**

**Curatif :**
**Décontamination anti-malwares**
**Forums de décontamination recommandés**

**Il ne sera répondu à aucune demande de dépannage posée en MP (Messagerie Privée). Les demandes doivent être publiques et les réponses doivent profiter au public.**

RÉPONDRE

1 message • Page 1 sur 1

Retourner vers Encyclopédie

Aller à: Encyclopédie Aller

**QUI EST EN LIGNE**

Utilisateurs parcourant ce forum: Aucun utilisateur enregistré et 96 invités

Index du forum

L'équipe du forum • Supprimer les cookies du forum • Heures au format UTC [ Heure d'été ]



Autres sites du Réseau...

Assiste (Sécurité informatique et Protection de la Vie privée sur l'Internet

## Note d'information : Droits d'auteur attachés à cette page



### Responsabilité

Le principe d'absence de responsabilité du site d'origine, au regard des contenus des sites cibles pointés, est rappelé par l'arrêt du 19 septembre 2001 de la Cour d'Appel de Paris. Les propos que je tiens ici reflètent mon opinion et sont des suggestions - le visiteur n'est pas obligé de les suivre.



*Fiche rédigée en écoutant*

**Faire un lien vers cette page**