

A dark blue vertical bar runs down the left side of the page. A blue arrow points to the right from this bar, containing the date.

18/02/2021

# Compte Rendu Cybersécurité 2

Several thin, curved lines in shades of blue and grey originate from the bottom left and sweep upwards and to the right.

Julien Condomines  
SIO 1

## Table des matières

Connaissances .....	2
Que devient le MDP une fois entrée dans une base de données ? Quelles sont les techniques liées à cette manipulation ? .....	2
Quelles sont les différentes attaques qu'un MDP peut subir ? .....	2
Que pensez vous d'un clé de taille 64bits dont chacun peut prendre la valeur (0-1) ?	3
Essayer d'exprimer un rapport entre le nombre de caractères d'un mot de passe et le temps d'attaque pour le trouver ? .....	3
Quelles sont les logiciels que vous connaissez pour crackez un mot de passe ? .....	3
Connaissez vous un gestionnaire de mots de passe, quelle est son utilité ? .....	5
Quelles ont les conseils que vous prodigueriez pour créer un mdp ? .....	5
Peut-on améliorer la technique du mot de passe ? Si oui, comment ? .....	6
Conclusion .....	6
Annexe .....	7

## Connaissances

**Que devient le MDP une fois entrée dans une base de données ? Quelles sont les techniques liées à cette manipulation ?**

Lorsqu'un mot de passe est rentré dans une base de données, il est stocké. Cependant il ne va pas forcément être stocké de la même manière qu'il a été écrit à la base. En effet, selon comment son administrateur la configure, le mot de passe va peut-être être haché, c'est-à-dire transformé à l'aide d'un procédé particulier en une suite de caractères sans qu'il soit possible de le retransformer par la suite. Ce mot de passe haché va donc prendre la place du mot de passe rentré par l'utilisateur dans la base de données, cependant, l'utilisateur n'aura pas à rentrer le hach pour se connecter mais le mot de passe de base, qui fait office de référence pour le hach dans la base de données. Le problème des fonctions de hachage est qu'elles entraînent des collisions. Elles transforment une suite de caractères de longueur non déterminée (infinité de possibilités) en une suite fixe de caractères (nombre fini de possibilités).

Il y a différentes techniques de hachage utilisées actuellement, il y a tout d'abord le Md5, une fonction de hachage qui a déjà été cassé mais quand même beaucoup utilisé, il y a aussi d'autres fonctions de hachage comme sha256 ou Whirlpool mais moins connu. De plus, il existe d'autres manières de masquer un mot de passe lorsque l'on le stock. Il y a tout d'abord Salt qui consiste à rajouter des caractères au mot de passe déjà existant, ou bien l'on peut rajouter le login d'un compte au mot de passe haché afin d'être sûr qu'un hash ne correspond pas à deux mots de passe différents.

**Quelles sont les différentes attaques qu'un MDP peut subir ?**

Attaque par dictionnaire :

Une attaque qui profite du fait que les utilisateurs ont tendance à employer des mots communs et des mots de passe courts. Le pirate utilise une liste de mots communs, le dictionnaire, et les essaye, bien souvent avec des chiffres avant et/ou après les mots.

Force brute :

L'utilisation d'un programme pour générer des mots de passe potentiels ou même des ensembles de caractères aléatoires. Ces attaques commencent par les mots de passe faibles et couramment utilisés puis évoluent. Les programmes qui exécutent ces attaques essayent habituellement des variantes avec des majuscules et minuscules.

Interception de trafic :

Au cours de cette attaque, le cyber-escroc utilise un logiciel comme les renifleurs de paquet pour surveiller le trafic réseau et enregistrer les mots de passe lorsqu'ils sont transmis. Si cette information n'est pas chiffrée, la tâche est plus simple. Cependant, même les informations chiffrées peuvent être déchiffrées, selon le niveau de sécurité de la méthode de chiffrement utilisée.

### Attaque de l'intercepteur :

Au cours de cette attaque, le programme du pirate ne surveille pas seulement les informations qui sont transmises mais s'introduit lui-même activement au milieu de l'interaction, en empruntant généralement l'identité d'un site Web ou d'une application. Cela permet au programme d'enregistrer les identifiants de l'utilisateur ainsi que d'autres informations sensibles comme les numéros de compte et de sécurité sociale.

### Attaque de l'enregistreur de frappe :

Un cyber-escroc parvient à installer un logiciel comme le keylogger qui enregistre les touches saisies sur le clavier par l'utilisateur, lui permettant ainsi de connaître non seulement le nom d'utilisateur et le mot de passe d'un compte, mais également le site Web ou l'application exacte sur laquelle l'utilisateur s'est connecté avec les identifiants. Ce type d'attaque survient généralement après une autre attaque au cours de laquelle le logiciel malveillant enregistreur de frappe est installé sur son ordinateur.

### **Que pensez vous d'un clé de taille 64bits dont chacun peut prendre la valeur (0-1) ?**

Une clé de taille 64bits qui ne peut que prendre la valeur 0 et 1 n'est pas assez sûr, en effet, plus la clé à une taille élevée, plus elle peut comprendre de valeurs et de caractères, plus il sera compliqué de la cracker et donc d'obtenir les mots de passe.

### **Essayer d'exprimer un rapport entre le nombre de caractères d'un mot de passe et le temps d'attaque pour le trouver ?**

Plus le nombre de caractère d'un mot de passe est élevé, plus il faudra de temps pour le cracker car il faudra essayer un plus grand nombre de mots de passe.

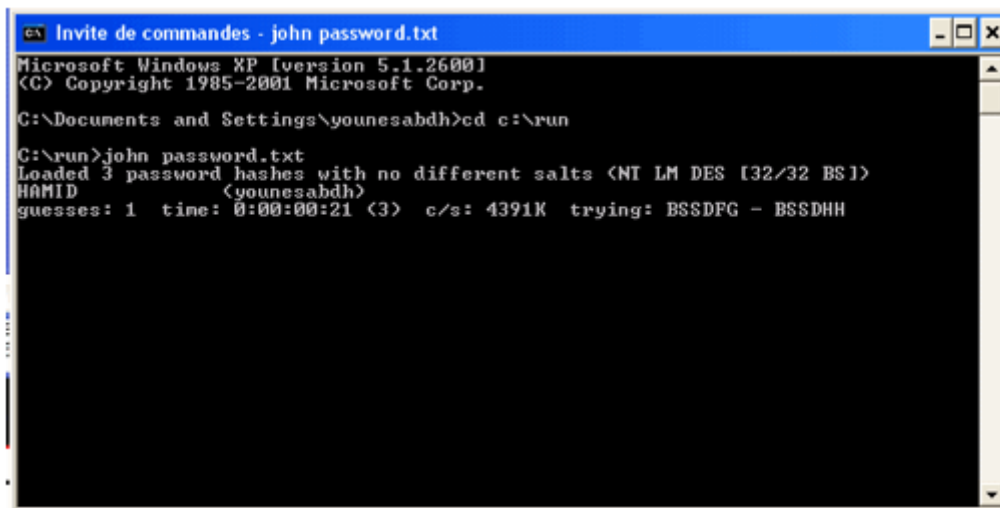
### **Quelles sont les logiciels que vous connaissez pour crackez un mot de passe ?**

On peut tout d'abord prendre pour exemple JhonTheRipper (Jhon), un logiciel libre très populaire qui fonctionne sur de nombreuses plateformes. Il y en a d'autres comme Aircrack, Cain & Abel, Ophcrack...

John dispose de trois modes d'actions, le mode simple, l'attaque par dictionnaire, et le mode incrémental. Par défaut, les trois modes sont exécutés dans cet ordre l'un après l'autre, bien qu'il soit possible de lancer John directement dans un des modes.

#### **Mode Simple :**

Dans ce mode John effectue quelques transformations sur le nom d'utilisateur, pour casser les mots de passes les plus faibles. Pour l'utilisateur toto, il essayerait "ToTo, toto123, ToTo123, etc...". Ce mode est le plus rapide à effectuer, un mot de passe qui serait cassé par cette méthode serait un mauvais mot de passe.



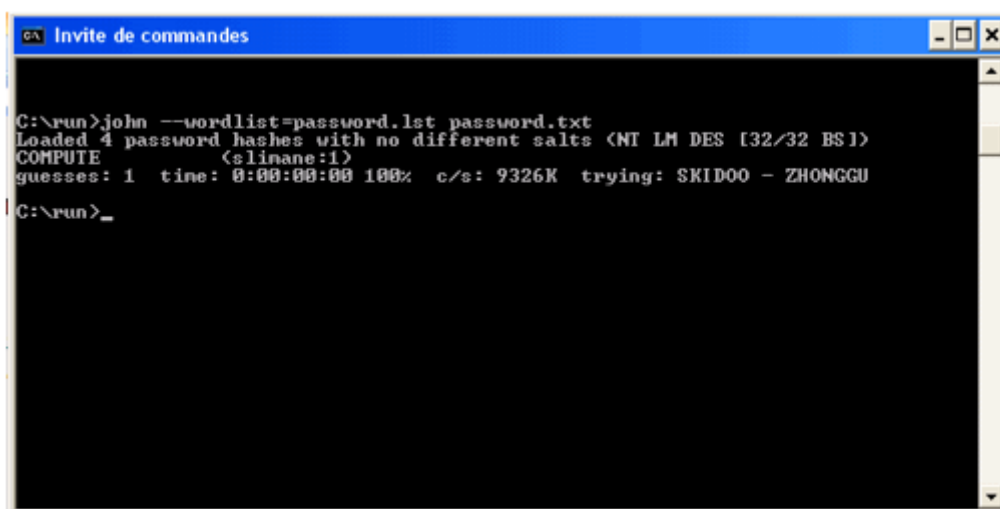
```
GA Invite de commandes - john password.txt
Microsoft Windows XP [version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\younesabdh>cd c:\run

C:\run>john password.txt
Loaded 3 password hashes with no different salts <NT LM DES [32/32 BS]>
HAMID          <younesabdh>
guesses: 1  time: 0:00:00:21 <3>  c/s: 4391K  trying: BSSDFG - BSSDHH
```

### Attaque par dictionnaire :

Dans ce mode, John essaye un à un tous les mots d'une liste de mots de passe potentiels, en leur appliquant les mêmes transformations que dans le mode précédent.



```
GA Invite de commandes

C:\run>john --wordlist=password.lst password.txt
Loaded 4 password hashes with no different salts <NT LM DES [32/32 BS]>
COMPUTE       <elinane:1>
guesses: 1  time: 0:00:00:00 100%  c/s: 9326K  trying: SKID00 - ZHONGGU

C:\run>_
```

On sait déjà que le dictionnaire de mots de passe travaille seulement sur les informations personnelles de la victime, mais la victime peut être plus maline et utilise un mot de passe hybride.

### Mode incrémental :

Dans ce mode, John va essayer toutes les combinaisons de caractères possibles, jusqu'à trouver le mot de passe. Tous les caractères étant testés, ce mode est techniquement infaillible, bien que la robustesse du mot de passe influe grandement sur le temps de calcul nécessaire à le trouver.

Afin d'augmenter la pertinence de l'algorithme, John implémente la recherche des caractères par fréquence d'utilisation, pour rechercher d'abord les caractères les plus utilisés statistiquement.

```

C:\Documents and Settings\younesabdh>cd c:\run
C:\run>john --incremental password.txt
Loaded 2 password hashes with no different salts (NT LM DES [32/32 BS])
guesses: 0 time: 0:00:00:20 c/s: 4377K trying: ASMPSHY - ASMPE?
guesses: 0 time: 0:00:00:25 c/s: 4554K trying: TH5NT98 - TH5NTY0
guesses: 0 time: 0:00:00:36 c/s: 4812K trying: MONOUDO - MONONY%
guesses: 0 time: 0:00:00:43 c/s: 4940K trying: FM08523 - FM0850F
guesses: 0 time: 0:00:00:45 c/s: 4958K trying: TAU20C - TAU239
guesses: 0 time: 0:00:00:48 c/s: 4980K trying: PPPTI03 - PPPTU4A
guesses: 0 time: 0:00:00:54 c/s: 5034K trying: PT79104 - PT79145
guesses: 0 time: 0:00:01:11 c/s: 5165K trying: 0JDAMH - 0JDAM?
guesses: 0 time: 0:00:03:23 c/s: 4865K trying: JBIPIGH - JBIPK2&
guesses: 0 time: 0:00:03:31 c/s: 4891K trying: 138729E - 138720R

```

Comme le montre cette figure, il est recommandé de laisser l'attaque incrémental en dernier, car elle prend beaucoup de temps pour trouver un mot de passe.

## Connaissez vous un gestionnaire de mots de passe, quelle est son utilité ?

Un gestionnaire de mots de passe est un type de logiciel ou de service en ligne qui permet à un utilisateur de gérer ses mots de passe, soit en centralisant l'ensemble de ses identifiants et mots de passe dans une base de données (portefeuille), soit en les calculant à la demande. Il y en a de nombreux comme notamment Keepass, un logiciel gratuit et libre de droits recommandé par l'Etat, Kaspersky ou encore le gestionnaire de mots de passe de Google.

## Quelles sont les conseils que vous prodigueriez pour créer un mdp ?

La robustesse d'un mot de passe dépend en général d'abord de sa complexité, mais également de divers autres paramètres, Il faudrait donc choisir des mots de passe d'au moins 12 caractères de types différents (majuscules, minuscules, chiffres, caractères spéciaux).

## Peut-on améliorer la technique du mot de passe ? Si oui, comment ?

Pour améliorer la technique du mot de passe, on peut mettre en place une double authentification, comme le font les banques ou google lors de la connexion. En plus du mot de passe, l'utilisateur reçoit un mail ou bien un sms sur son téléphone avec un code généré aléatoirement que l'utilisateur doit rentrer s'il veut se connecter.

## Conclusion

Durant ce travail pratique, nous avons pu découvrir ce qui se passe autour des mots de passe. Comment ceux-ci doivent être créés de manière à être solides et dur à cracker, les sites où l'on peut tester son mot de passe afin de voir le temps qu'il faudrait pour le cracker, les différents types d'attaque ainsi que les logiciels qui peuvent être utilisés, les logiciels disponibles pour gérer nos mots de passe ou encore comment améliorer la sécurité lors de la connexion à un compte.

## Annexe

```
static void Main(string[] args)
{

    int b = 0;
    int c = 0;
    Console.WriteLine("Ecrire le nombre de caractères souhaité : ");
    string nbrCarac1 = Console.ReadLine();
    int nbrCarac = Convert.ToInt32(nbrCarac1);
    Console.WriteLine("//");
    while (c <= nbrCarac)
    {

        if (b < nbrCarac)
        {
            Random aleEntier = new Random();
            int randomEntier = aleEntier.Next(10);
            Console.WriteLine(randomEntier);
            Console.WriteLine("//");
            b++;
        }

        if (b < nbrCarac)
        {
            Random aleMin = new Random();
            char randomLettreMin = (char)aleMin.Next('a', 'z');
            Console.WriteLine(randomLettreMin);
            Console.WriteLine("//");
            b++;
        }
    }
}
```



```
    }

    if (b < nbrCarac)
    {
        Random aleMaj = new Random();
        char randomLettreMaj = (char)aleMaj.Next('A', 'Z');
        Console.WriteLine(randomLettreMaj);
        Console.WriteLine("/");
        b++;
    }

    if (b < nbrCarac)
    {
        string[] tabRandom = new string[] { "!", "#", "$", "%", "&", "(", ")", "*", "+", ",", "-",
        ".", "/", ":", ";", "<", "=", ">", "?", "@", "o", "+" };
        Random randomCaracSpecial = new Random();
        int randomCaracSpe = randomCaracSpecial.Next(23);
        Console.WriteLine(tabRandom[randomCaracSpe]);
        Console.WriteLine("/");
        b = b + 1;
    }
    c = b;
    c++;
}
}
```