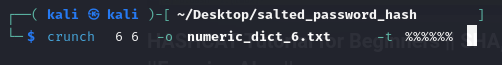
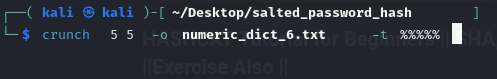
D’abord nous avons chercher des infos sur les mots de pass salés et comment ils fonctionnent.

-En analysant la longueur du hash qui est de 40 caractères, nous déduisons qu’il s’agit d’un hash obtenu par l’algorithme sha1.

-Ensuite nous cherchons les solutions disponibles pour retrouver les mots de passe a savoir l’utilisation de l’outil HASHCAT de kali linux. Cet outil est open source et nous offre une multitude d’option pour retrouver un mot de passe à partir du hash.

En suivant les informations disponibles sur la page du TP, nous nous sommes intéressés au mot de passe uniquement numérique qui date d’avant Mai 2019. Ainsi nous avons généré trois dictionnaires de respectivement 5, 6 et 7 chiffres pour appliquer une attaque par force brute.

Commande :



A partir de la, nous avons essayé de trouver la bonne commande pour appliquer une attaque sachant que la longueur du salt est de 5 caractère numérique.

La commande suivante nous a permis de trouver un mot de passe correspondant parmis les 6 disponibles :

hashcat -m 100 -a 6 -o output.txt password numeric\_dict\_5.txt ?d?d?d?d?d

ou l’option :

-m 100 : option pour choisir le mode d’attaque , ici 100 correspond a l’attaque sha1

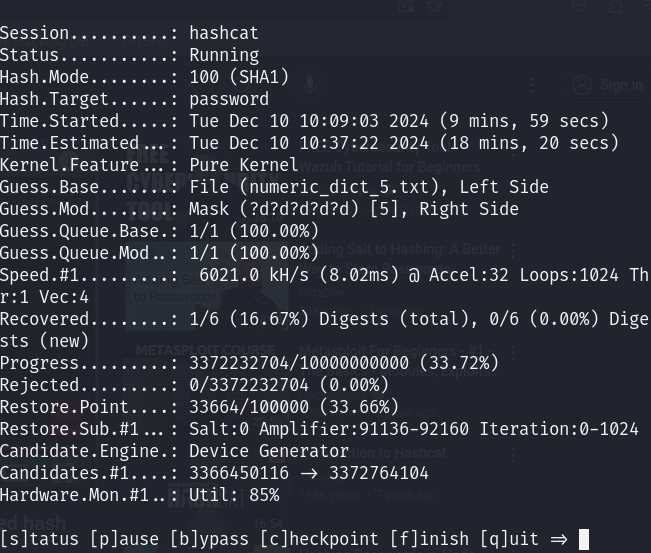
-a 6 : qui correspond à une **attaque hybride "wordlist + mask"**

**-o output.txt qui est notre fichier de sortie qui va contenir les cracks potentiellement trouvés**

**Numeric\_dict\_5.txt : ce fichier designe notre dictionnaire de 5 caractères numériques**

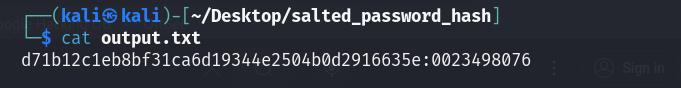
**?d ?d ?d ?d ?d : on ajuste 5 caractères aléatoires pour le salt.**

Le résultat de la commande est le suivant :



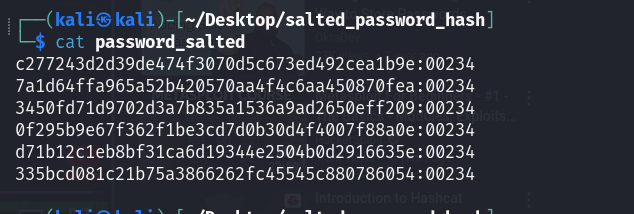
Dans la partie recovered, nous avons trouvé un mot de pass récupéré.

Ainsi le contenu du fichier output.txt nous donne :



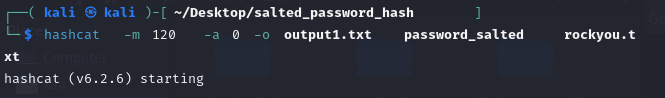
Nous avons donc un premier mot de pass trouvé pour le username « Tomtom ».

* Pour la suite nous avons, sachant que le sujet mentionne que le salt est invariant et que la forme de la fonction de hachage est CommonHash($salt,$pass) donc dans notre cas sha1($salt,$pass), nous avons posé l’hypothèse que le salt est les 5 premiers chiffres de notre mot de pass trouvé donc 00234.
* Ayant trouvé le salt, nous avons donc concaténer le hash au salt comme le montre l’image qui suit :



Ensuite nous avons utilisé ce fichier dans une commande de hashcat pour trouver les autres mots de pass grace au dictionnaire rockyou.txt

-La commande finale nous permet de trouver les autres mots de passe



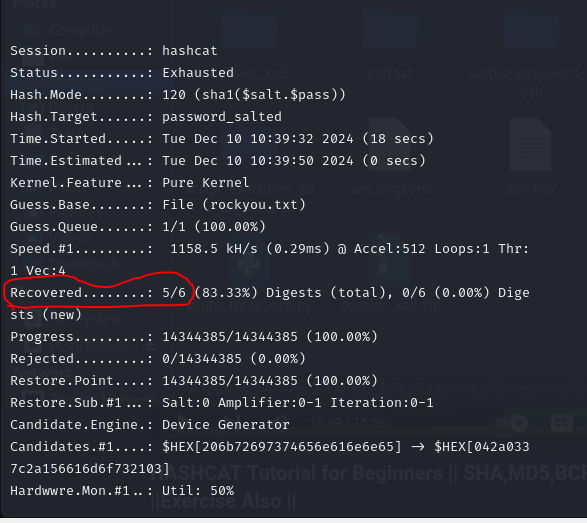
Dans cette commande l’option :

-m 120 permet de choisir le mode sha1($salt,$pass) qui est notre format

-a 0 permet de définir le mode d’attaque en dictionnaire simple

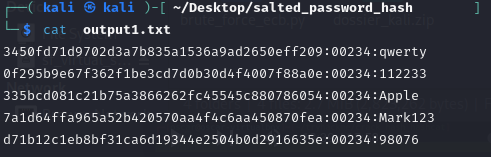
-le fichier rockyou.txt est un dictionnaire de mot de passe utilisé pour méner cette attaque.

En exécutant cette commande on trouve l’image suivant en sortie :



En rouge nous pouvons voir qu’il nous a rétrouvé 5 mots de pass sur 6. Il s’agit des autres mots de pass hormis celui trouvé prémièrement,

Le contenu du fichier output1.txt est :



Ce qui correspond au mot de pass pour chacun des hash.

En fin de compte le fichier faisant la correspondance entre les mots de pass et les username est :

