Nicolas. Lilou (12/10/2025) **BTS SIO1**

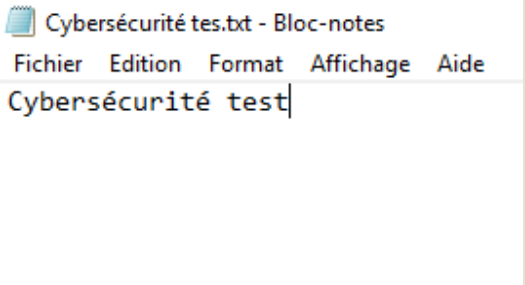
B03 TP05 - Cybersécurité

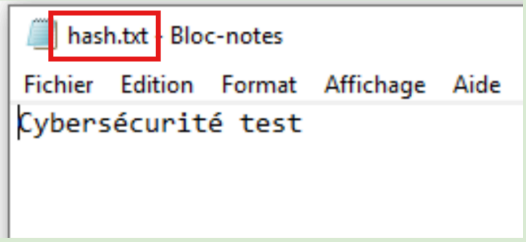
La problématique : *Nous allons devoir utiliser un programme de condensation pour vérifier l'intégrité des données et s'informer sur des cas de fuite de données*

La cybersécurité : données hachées

Étape 1 : Créer un fichier texte

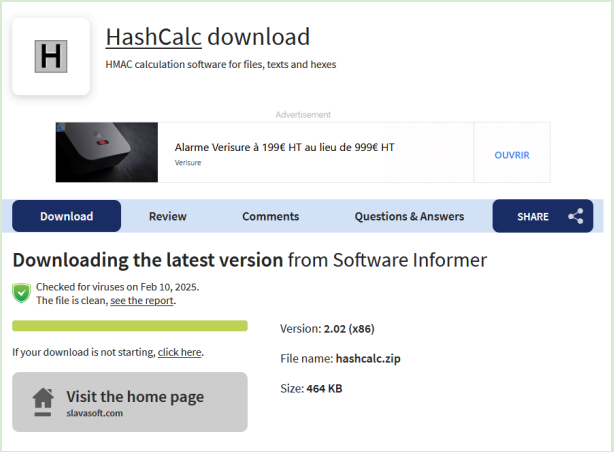
Nous devons créer un fichier texte que nous nommerons hash.txt dans l'application bloc note

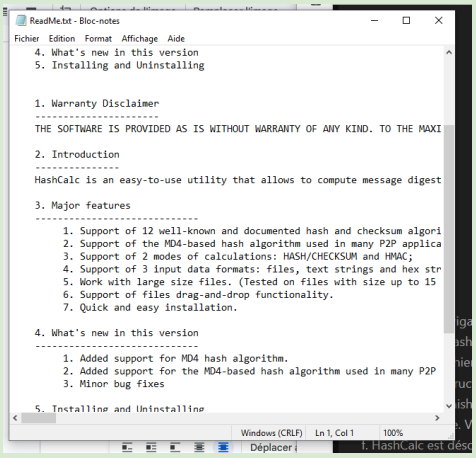




Étape 2 : Installer HashCalc

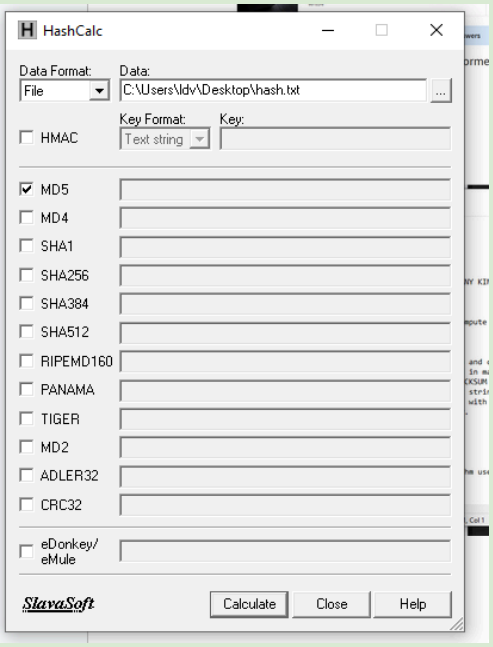
Nous devrons ensuite installer HashCalc et suivre les instructions



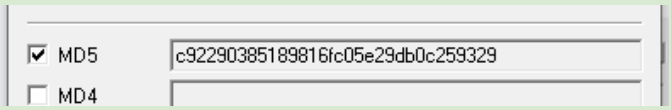


Étape 3 : Calculer un algorithme pour le fichier Hash.txt

Nous devons ensuite configurer les éléments de manière à ce que dans “data format” nous retrouvons “file”.
Nous devons sélectionner le fichier dans nous avons besoin (“hash.txt”) et décocher tout les algorithmes sauf MD5.

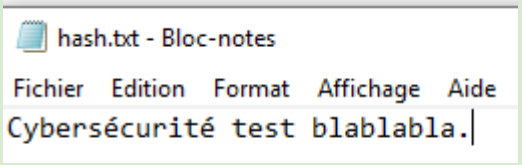


Après avoir appuyer sur “Calculate” nous obtenons la valeur suivante



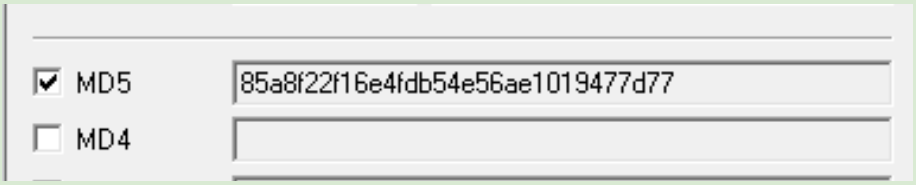
Étape 4 : Modifier le fichier Hash.txt

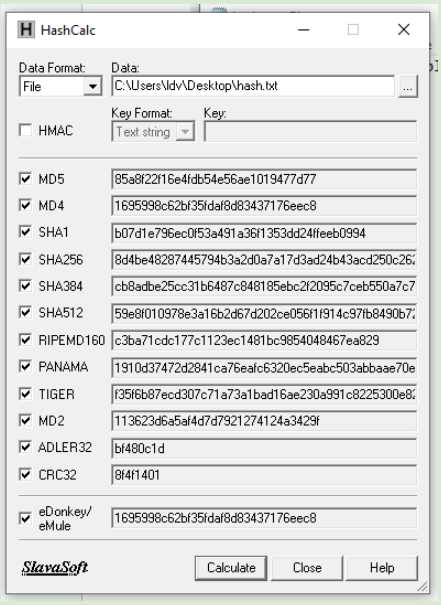
Il nous est ensuite de modifier le texte et d’enregistrer ces modifications



Étape 5 : Calculer un nouvel algorithme pour le fichier hash.txt

Nous appuyons de nouveau sur calculate et nous obtenons une nouvelle valeur.
Nous cochons ensuite tous les algorithmes et affichons des valeurs de longueur différente.





Les différents types d'algorithmes de hachage produisent des sorties de longueurs différentes car ils sont conçus ainsi pour répondre à divers besoins de sécurité et d'efficacité

Plus le hash est long et plus la sécurité est augmentée et vice-versa.

La cybersécurité : données volées

Recherche sur les failles

Date de l'incident	Entreprise touchée	Nombre de victimes / Données volées	Méthodes utilisées	Mesure(s) de protection prise(s)	Source de référence
2017	Equifax	147 millions de personnes (noms, SSN, dates de naissance)	Exploitation d'une faille dans Apache Struts (vulnérabilité web)	Renforcement des patchs de sécurité, surveillance accrue, notification aux victimes	https://www.cnet.com/news/equifax-data-breach-what-you-need-to-know/

2013	Target	40 millions de cartes de crédit/débit volées	Malware sur les systèmes de paiement	Amélioration des systèmes de détection d'intrusions, migration vers la technologie EMV	https://www.csoonline.com/article/2130877/target-breach-the-5-security-mistakes-that-led-to-the-attack.html
2020	Twitter	Comptes de personnalités pris en otage, données sensibles exposées	Attaque de phishing ciblée, compromission d'employés	Renforcement des contrôles d'accès, formation du personnel, 2FA renforcé	https://www.bbc.com/news/technology-53480469
2018	Facebook	29 millions de comptes touchés, données personnelles volées			Condamnation de Facebook par la CNIL au titre d'une collecte illégale des données des internautes

Remarques générales

Parmis mes les mesures il y a :

- **Patch management rigoureux** (appliqué les mises à jour et correctifs de sécurité dès qu'ils sont disponibles pour éviter l'exploitation de vulnérabilités connues).
- **Sensibilisation et formation** (formation des employés aux risques de phishing, et bonnes pratiques de cybersécurité).
- **Mise en place de systèmes de détection et de prévention d'intrusion** (IPS)
- **Authentification forte** (utiliser une authentification renforce la sécurité)
- **Sauvegardes régulières**

Conclusion: Ce TP m’a appris qu' utiliser un programme de condensation permet de vérifier que les données ne sont pas modifiées et d’éviter les fuites d’informations. C’est un outil important pour assurer la sécurité des données.