

**B3 TP5 Compte Rendu**  
**Données Hachées**

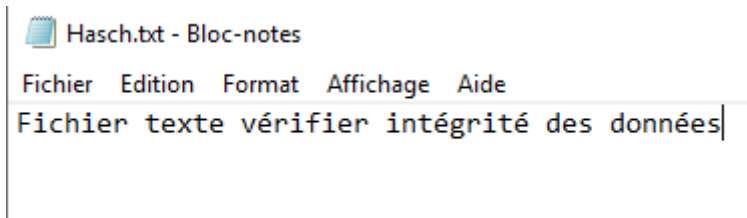
**Sommaire :**

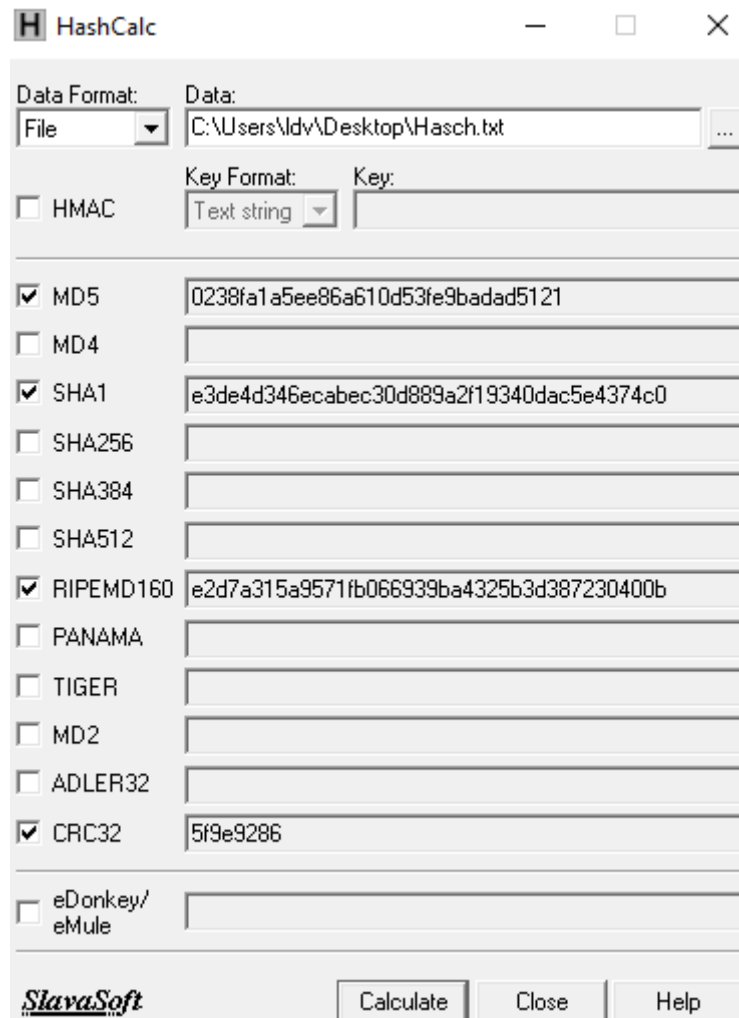
**Hasch**


**Tableaux :**

**Solutions**

# Hasch

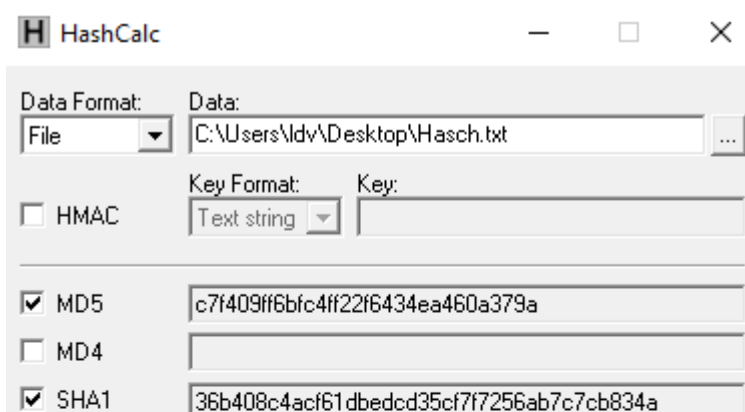




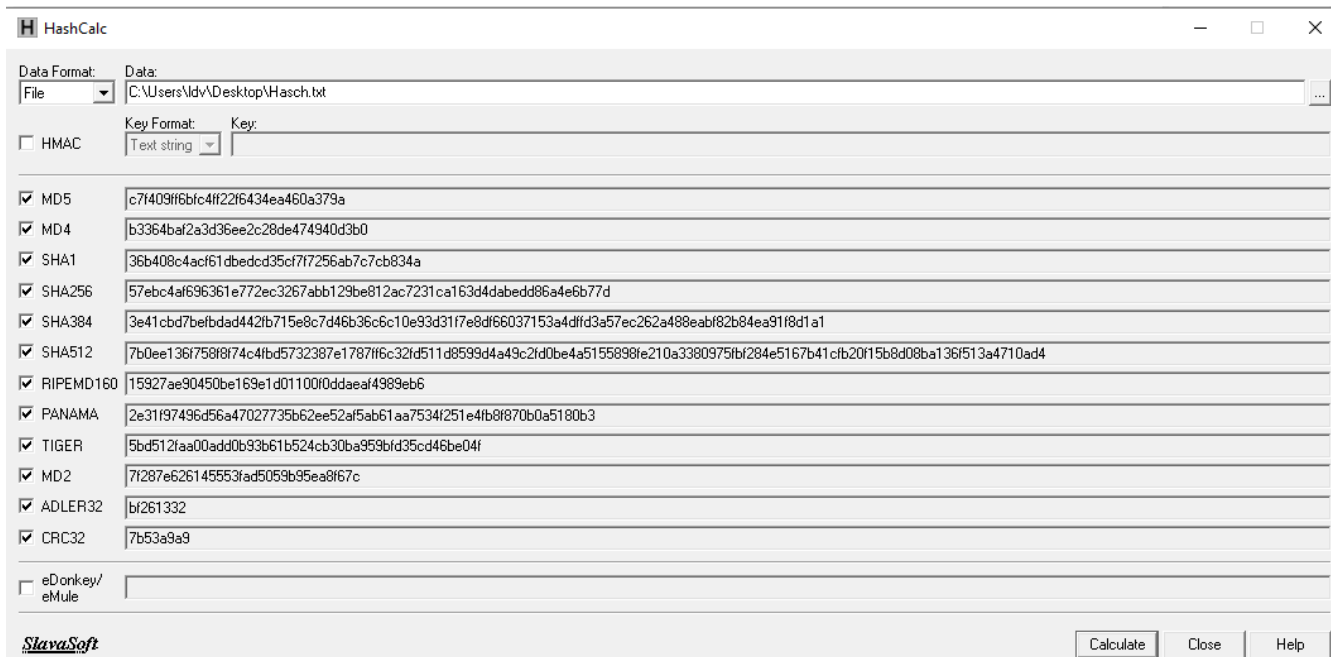
 Hasch.txt - Bloc-notes

Fichier Edition Format Affichage Aide

Fichier texte vérifier intégrité des données .







## Tableaux :

Date de l'incident	Entreprise touchée	Nombre de victimes Données volées Caractéristiques	Méthodes utilisées Mesure(s) de protection prise(s)	Source de référence
2024	Microsoft Exchange	28 000 serveurs	faille zero-day	<a href="https://www.sfrbusiness.fr/room/securite/cybersecurite-5-plus-grandes-cyberattaques.html/">https://www.sfrbusiness.fr/room/securite/cybersecurite-5-plus-grandes-cyberattaques.html/</a>
Septembre 2025	Cloudfare	?	DDOS 11,5 Térabits par seconde et plus de 5 milliards de paquets par seconde, sur seulement 35 secondes.	<a href="https://www.sfrbusiness.fr/room/securite/cybersecurite-5-plus-grandes-cyberattaques.html/">https://www.sfrbusiness.fr/room/securite/cybersecurite-5-plus-grandes-cyberattaques.html/</a>
Septembre 2023	Darkbeam	3,8 Milliards de données sur Cloud	Mauvaises configuration	<a href="https://www.sfrbusiness.fr/room/securite/cybersecurite-5-plus-grandes-cyberattaques.html/">https://www.sfrbusiness.fr/room/securite/cybersecurite-5-plus-grandes-cyberattaques.html/</a>
Janvier 2024	Hôpitaux	Toutes les données	Ransomwares	<a href="https://www.sfrbusiness.fr/room/securite/cybersecurite-5-plus-grandes-cyberattaques.html/">https://www.sfrbusiness.fr/room/securite/cybersecurite-5-plus-grandes-cyberattaques.html/</a>
?	Arup	25 Millions \$	Cyberattaques E-mail	<a href="https://www.sfrbusiness.fr/room/securite/cybersecurite-5-plus-grandes-cyberattaques.html/">https://www.sfrbusiness.fr/room/securite/cybersecurite-5-plus-grandes-cyberattaques.html/</a>

## Solutions

### **Avec une protection Anti-DDOS au coeur du réseau**

C'est-à-dire de protéger les accès internet, en cas d'attaque volumétrique (nombreuses) le trafic sera interrompu pour préserver l'accès légitime et maintenir l'activité des serveurs.

### **Avec une protection Anti-DDOS sur site**

Dispositif adapté pour détecter et bloquer les attaques rapidement, compléter avec un pare-feu (WAF) des protections anti-bot.

### **Redirection cloud et Nettoyage du flux**

Selon l'exposition, une redirection peut-être activer comportant des capacités de scrubbing (lavage) afin de filtrer le flux des demandes indésirables

### **Supervision et réponse 24h/24 7j/7 par un SOC**

Équipe d'experts spécialisés dans la surveillance, sécurité, déclenchements automatisés des contre mesures, visant l'amélioration des politiques de défenses.

## **Visibilité et pilotage via SelfCare**

A l'aide d'un indicateurs/reporting et d'un contrôle de mécanismes de défenses il serait possible d'ajuster les protections

## **Test et Préparations**

Des tests et des préparations à des cas de figures poussant à montrer les faiblesses de la sécurité peuvent être faits pour comprendre quels points améliorer et où se trouvent les points les plus sensibles.



