Bloc 3 - Cybersécurité - TP Cyber

HACHAGE ET SALAGE : INTÉGRITÉ ET PROTECTION DES MOTS DE PASSE

Terminal Debian et Firefox.

Nom : ..... **Date :** .....

1. Intégrité d'une ordonnance et empreintes

1. En observant les chaînes produites par `sha256sum` et `sha512sum`, que pouvez-vous déduire sur la taille du résultat par rapport à la taille du texte d'origine (14 caractères) ?

2. Après avoir remplacé `1g` par `2g`, comparez la nouvelle empreinte SHA-256 avec la précédente. Que concluez-vous sur l'impact d'une modification, même mineure, et sur la garantie d'intégrité ?

3. `sha256sum` et `openssl dgst -sha256` donnent la même empreinte. Que cela prouve-t-il sur la conception de SHA-256 ?

2. Mots de passe et tables précalculées

4. Trois empreintes MD5 ont été soumises à CrackStation : `5f4dcc3b5aa765d61d8327deb882cf99`, `098f6bcd4621d373cade4e832627b4f6` et `8b1a9953c4611296a827abf8c47804d7`. Quels mots de passe le service affiche-t-il ?

5. Le hachage est conçu pour être irréversible. Comment CrackStation peut-il retrouver ces mots de passe ? Expliquez avec la notion de table précalculée (rainbow table).

3. Sel et facteur de coût

6. Le mot de passe `password`, associé au sel `x8Z!9`, donne la chaîne `passwordx8Z!9`. Que renvoie CrackStation pour son empreinte MD5 ? Pourquoi le sel rend-il la table géante du pirate inefficace ?

7. À 10 milliards d'empreintes MD5 par seconde, combien de temps faut-il pour tester 100 milliards de candidats ? Détaillez le calcul.

8. Avec un facteur de coût de 0,1 seconde par empreinte, combien de temps faut-il pour tester les 100 milliards de candidats ? Ce délai est-il acceptable pour un patient qui se connecte ? Justifiez.

4. De l'intégrité à la preuve électronique

9. Pourquoi une empreinte SHA-256 seule ne suffit-elle pas à prouver l'origine et la date d'une ordonnance ? Citez au moins deux mécanismes complémentaires et ce qu'ils apportent.

5. Bilan Référentiel BTS SIO & Carnet de bord

Bilan du TP adossé au Référentiel Officiel BTS SIO

Compétences & Savoirs mobilisés :

- **C-3.2.1** : Protéger l'identité numérique d'une organisation.
- **C-3.2.2** : Déployer les moyens appropriés de preuve électronique.
- **S-3.2.1** : Chiffrement, authentification et preuve : principes et techniques
- **S-3.2.0** : Protection et archivage des données : principes et techniques
- **S-3.1.2** : Principes de la sécurité : disponibilité, intégrité, confidentialité, preuve

Preuves à insérer dans votre carnet de bord :

- Capture terminal : empreintes SHA-256 avant/après modification et échec de sha256sum -c.
- Capture CrackStation : mots de passe retrouvés, puis empreinte salée non reconnue.
- Note de synthèse : différence entre intégrité, authenticité, date et preuve.