PROTECTION DE FICHIERS PAR CHIFFREMENT

Pour sécuriser nos données, nous allons apprendre à utiliser un outil de chiffrage informatique. Le but de ce laboratoire est de savoir utiliser cet outil et d'en comprendre les principes.

Marche à suivre :

1) Télécharger le logiciel « TrueCrypt » sur le site suisse https://truecrypt.ch/downloads/
2) Installez-le en version portable (extraction simple des fichiers)
3) Lancez le logiciel et démarrez la création d'un nouveau conteneur de fichiers encrypté non caché, puis suivez-les instructions suivante lors de la création
4) Au moment de la création, aller dans l'onglet « Benchmark » et tester votre machine pour voir les performances de chiffrage avec les différents algorithmes
5) Trouvez une réponse à la question suivante : en comparant les différents résultats de benchmark pour les algorithmes de chiffrage, que peut-on conclure lorsqu'on combine des algorithmes successivement pour crypter des données?
6) Choisissez Serpent-AES pour le chiffrage puis SHA-512 comme algorithme de hachage
7) Saisissez la taille du conteneur, un seul MB suffira (1 MB)
8) Entrez un mot de passe en respectant les règles de sécurité suivantes :
    a. Le mot de passe doit contenir au moins plusieurs mots d'au moins 20 lettres
    b. Le mot de passe doit contenir des caractères spéciaux et des lettres : remplacez donc les « e » par des « 3 », les « i » par des « | », les « o » par des « 0 », les « a » par des « @ » et les « s » par « $ »
    c. Par exemple le mot de passe « geeks_are_strong_and_nice » donnera « g33k$_@r3_$tr0ng_@nd_nIce »
9) Une fois le fichier conteneur chiffré créé, montez-le dans le logiciel « TrueCrypt » comme un volume de donnée puis déposez un fichier texte dedans contenant un texte de votre choix
10) Démontez ensuite le volume puis fermez le logiciel « TrueCrypt »
11) Essayez par la suite d'ouvrir le fichier chiffré sans utiliser le logiciel « TrueCrypt », que pouvez-vous remarquer ? Arrivez-vous à lire votre fichier texte ?

Vous savez maintenant comment fonctionne un logiciel de chiffrage et comment sécurisé des données dans un conteneur. En informatique, les ressources et applications sont souvent placées dans des conteneurs afin de les protéger.