Projet Sécurité: CTF

GROUPE	BACKDOOR	**SCENARIO 21/10**
PHASE 1	DEVELOPPEMENT CTF	***USB***
NIVEAU	MOYEN	

Operation Data Leak

Une entreprise est en train de mener une enquête interne sur une possible fuite de données. Ils soupçonnent que quelqu'un a utilisé une clé USB pour extraire des informations confidentielles de leur réseau. Il faut donc trouver des preuves de la fuite de données.

Temps estimé: 50 mins

Etapes

1/Stéganographie:

Sur la clé USB, on trouve un fichier “image.jpg”. Il semble être une image ordinaire, mais il contient des informations cachées. Grace à un ensemble d’outils, il faut découvrir tout contenu caché dans cette image. C’est ainsi qu’on retrouve le premier flag.

2/Rétro-ingénierie:

On trouve également un fichier exécutable. Ce programme semble être lié à la fuite de données. On l’analyse l'analyser pour comprendre comment il fonctionne et s'il contient des indices sur la source de la fuite. C’est le deuxième flag.

3/Analyse de fichiers:

En fouillant plus en profondeur, on découvre un fichier texte "Password.txt" sur la clé USB. Cependant, il est protégé par un mot de passe. On doit trouver le mot de passe pour accéder à son contenu, qui pourrait révéler des informations cruciales sur la fuite de données, et ainsi le troisième flag.

4/Fichier caché:

Alors qu'on explore la clé USB, on remarque que l'espace libre disponible sur la clé est plus petit que la taille totale de tous les fichiers visibles. Cela suggère qu'il y a peut-être un fichier caché sur la clé. Il suffit alors de trouver ce fichier caché et d'extraire son contenu pour obtenir le quatrième flag.