Projet SécuRT

Introduction

Ce rapport décrit le processus de création d'un défi CTF forensique de niveau débutant. Le défi consiste à analyser une image pour trouver un flag caché dans ses métadonnées. Ce type d'exercice est idéal pour initier les participants aux bases de l'analyse forensique et à l'utilisation d'outils comme ExifTool.

Objectif du Défi

- **Nom du défi** : Analyse d'image suspecte.
- **Objectif** : Trouver un flag au format `FLAG{example_flag}` caché dans une image JPEG.
- **Public cible** : Débutants en cybersécurité et en analyse forensique.
- **Durée estimée** : 5 à 10 minutes.

Description du Scénario

Un fichier image (`image.jpg`) a été récupéré dans le cadre d'une enquête. Les enquêteurs pensent qu'il contient un message secret caché dans ses métadonnées. Vous devez analyser l'image pour retrouver ce message.

Insertion du flag dans les métadonnées

Outil utilisé : **ExifTool**.

exiftool -Comment="FLAG{this_is_a_simple_flag}" queda.jpg

Détail de l'opération :

- Le flag `FLAG{this_is_a_simple_flag}` a été inséré dans le champ **Comment** des métadonnées de l'image.

Vérification : La commande suivante a été exécutée pour s'assurer que le flag a bien été ajouté :

exiftool queda.jpg

Résultat :

Comment : FLAG{this_is_a_simple_flag}

Instructions Fournies aux Participants

Fichier fourni :

- `queda.jpg` : L'image suspecte contenant le flag.

Consignes :

1. Analysez l'image pour trouver le flag caché dans ses métadonnées.
2. Utilisez des outils tels que **ExifTool** ou tout autre analyseur de métadonnées.

3. Trouvez le flag au format `FLAG{example_flag}`.

Outils recommandés :

⑩ **ExifTool** (disponible sur Linux, macOS et Windows).
Commande pour analyser les métadonnées :

exiftool

Je pense également ajouter un douzième exercice qui demande aux participants de trouver un message situé dans un document. Cependant, ce document est caché dans une image JPEG.