Gmail Proof

Auteur	Catégorie	Niveau
Cécile	Forensic	Intro

Énoncé :

Intro

La boite email de cette personne a été saisie dans le cadre d'une enquête car un de ses contacts ferait de la vente illicite. Nous y cherchons une preuve, peux tu nous aider ?

Pièce Jointe

Un fichier emails.mbox

Préparation du challenge

Objectif

Faire découvrir le forensic et son utilité. Découvrir quelques commandes Linux utiles pour ceux qui ne connaissent pas.

Flag

NHM2I{Qu3Del4PubSur73mail!}

Démarche

Création et alimentation d'une boite gmail avec des adresses emails créées pour l'occasion. Extraction de celle ci au format .mbox qui est le format du fichier de données Gmail.

Résolution :

Solution débutant :

On dézippe le fichier :

```
tar -xJf emails.tar.xz
```

On essaye d'ouvrir le fichier. On tombe sur une multitude de textes. On essaye de filtrer avec le format du flag :

```
cat emails.mbox | grep NHM2I
```

On obtient le flag :