Alerte à la poste!!

On suspecte des connexions depuis différentes dsi de laposte vers des ip reconnues malveillantes.

Dans le fichier **connexion.log**, on a enregistré les ip qui ont été accédées depuis des ordinateurs de la poste entre 2015 et 2019. Sur chaque ligne on lit l'ip qui a été accédée, le login de la personne et la date/heure de connexion.

A vous de jouer pour retrouver le/les hackers (blackhat) infiltrés.

1. Parcourez le fichier pour trouver la liste de tous les utilisateurs qui se sont connectés, enregistrez cette liste dans un fichier **utilisateurs.txt**.

Indice : cherchez la fonction split()

1. On soupçonne qu'une personne se connecte en dehors des heures d'ouverture des bureaux (8h-19h), peut-être depuis un poste distant. Utilisez un script pour retrouver l'identifiant de cette personne ainsi que l'ip à la laquelle elle se connectait

2. Le service de sécurité informatique a fournit un fichier contenant les ips dangereuses : **warning.txt**. Lisez ce fichier pour construire une liste contenant toutes les ip dangereuses.

A l'aide de cette liste, relevez dans le fichier connexion.log tous les utilisateurs qui se sont connectés sur une de ces ip, on produira un fichier **suspect.txt** avec une ligne par utilisateur et le nombre de fois qu'il s'est connecté à une ip interdite

In [1]:
```
#TBD
```

In [ ]:
```

```