Visualiser les échanges de courriels chiffrés avec Wireshark

Présentation

Un **analyseur de trame** est un outil **de base** de l'informaticien car il permet de comprendre ce qu'il se passe à un niveau très bas. Il permet aussi aussi de mettre en évidence de nombreux concepts théoriques du cours.

Wireshark (anciennement Ethereal) est un est un logiciel libre d'**analyse de protocole**, ou **packet sniffer**, utilisé dans le **dépannage** et l'**analyse du fonctionnement** des réseaux informatiques. Il est utilise pour **diagnostiquer** des dysfonctionnement dans un réseau informatique.

Un analyseur de protocoles (ou analyseur de réseaux ou de paquets) est un logiciel permettant **d'intercepter** et de consigner le trafic des données transférées sur un réseau de données. L'analyseur **capture** chaque **PDU** (protocol data unit - unité de données de protocole) des flux de données circulant sur le réseau.

Il permet de décoder et d'analyser leur contenu conformément aux spécifications **RFC** ou autres appropriées.

Wireshark est programmé pour reconnaître la structure de différents protocoles réseau.

Installation de Wireshark dans la VM Ubuntu

Avant d'installer un nouveau logiciel, mettrez à jour votre environnement Ubuntu.

- lancez un Terminal
- Mettez à jour votre environnement Ubuntu

```
$ sudo apt update
$ sudo apt upgrade
```

- installez Wireshark

```
$ sudo apt install wireshark
```

Durant l'installation il vous est demandé **d'autoriser** l'installation de **Dumcap**. Utilisez la touche **TAB** pour sélectionner le bouton **OK** et validez avec la touche entrée :

- **Autorisez** les utilisateurs non privilégiés à **utiliser Wireshark** :

Retour Accueil Bloc3

- Bloc3

From:
/ - **Les cours du BTS SIO**

Permanent link:
/doku.php/bloc3s1/wiresharkmessagerie?rev=1605210893

Last update: **2020/11/12 20:54**