WireShark

Sommaire

1 Installation

Pour installer wireshark il faut taper une ligne de commande :

```
root# apt-get install wireshark
```

Il faut ensuite se mettre dans le groupe propriétaire pour pouvoir utiliser ce logiciel

```
root# adduser <login> wireshark
```

Après avoir fait cela, on doit fermer et rouvrir la session pour que l'ajout de l'utilisateur au groupe propriétaire soit pris en compte.

2 Utilisation en ligne de commande

2.1 Création du dossier de stockage des captures.

Le chemin de destination sera le même pour les commandes qui suivent.

```
root# mkdir <destination>
```

On donne ensuite les droits au propriétaire et au groupe propriétaire

```
root# chown :wireshark  <destination>
```

```
root# chmod 2750  <destination>
```

2.2 Script de capture

.

Le script capture doit être (dé)placé dans /sbin/

2.3 Lancer une capture

Pour lancer le script de capture il faut entrer la commande suivante dans un terminal :

```
root# capture <interface_réseau>
```

Pour stopper la capture il faut faire un ctrl^C sur le terminal ou elle a était lancé.