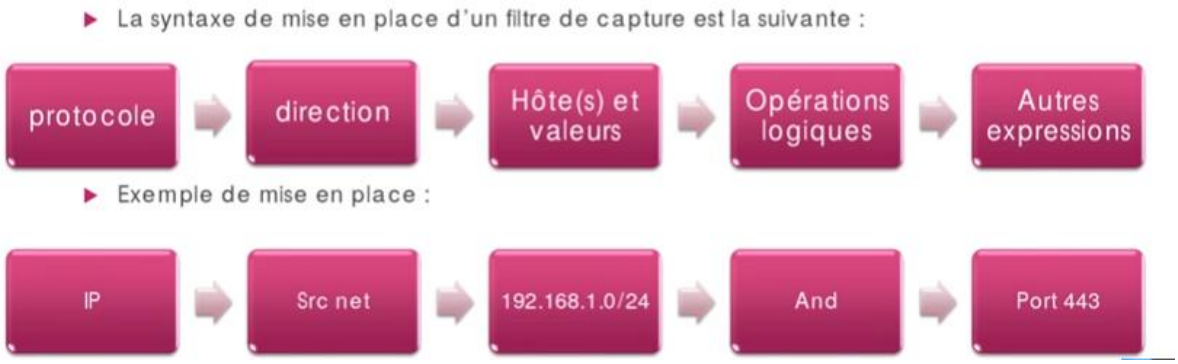
LE RENIFLEUR : WIRESHARK (Ecoutez votre réseau)

Wireshark est un analyseur de protocole réseau multiplateforme open source. Il vous permet d'examiner les données d'un réseau en direct ou d'un fichier de capture sur le disque.

Vous pouvez parcourir de manière interactive les données de capture, en fouillant dans juste le niveau de détail de paquet dont vous avez besoin. Wireshark possède plusieurs fonctionnalités puissantes, notamment un langage de filtre d'affichage riche et la possibilité d'afficher le flux reconstruit d'une session TCP. Il prend également en charge des centaines de protocoles et de types de médias.

1. Installer WireShark pour ceux tous qui n'ont pas Kali-Linux
2. Sélectionnez une interface réseau et connectez-vous (celle qui est active). Qu'observez-vous ?
3. **Méthodes de filtrage**



Une syntaxe correctement mise en place affiche une barre verte

Essayez les syntaxes suivantes :

a. Filtrer les trames de votre réseau passant par le port 443
   Votre IP_Src net_Votre réseau_and_port 443
b. Filtrer toutes les trames hors mis les trames tcp et udp lors de l'analyse
   Not tcp not udp
c. Filtrer les trames de votre réseau en excluant les trames passant par le port 8080
   Votre IP_Src net_Votre réseau_and_not port 8080
d. Filtrer toutes les communications de vos protocoles tcp, arp, udp

4. **Capture de mots de passe**

a. Relancer une nouvelle capture avec votre interface réseau
b. Initier une nouvelle connexion avec votre routeur et identifiez-vous (saisir vos credentiels => identifiant et mot de passe)
c. Arretez la capture du trafic dans Wireshark et filtrer votre trafic http pour n'avoir que les connexions http
d. Vous souhaitez retrouver toutes les connexions entre votre adresse ip et celle du serveur

Syntaxe : http and (ip.src==votre adresse) and (ip.dst==adresse de votre routeur)

En cliquant sur une trame vous avez la possibilité de veriifier les adresses source et destination au niveau de la couche Internet
Rendez-vous dans la couche application / http / Cliquer sur *Autorisation* et retrouver vos crédentiels !