Tutoriel : Utilisation de Wireshark

Wireshark est un outil puissant et populaire pour capturer et analyser le trafic réseau. Il est essentiel pour les administrateurs réseau, les ingénieurs en sécurité et toute personne cherchant à diagnostiquer ou comprendre le fonctionnement d'un réseau.

Installation de Wireshark

Sous Windows

1. Accédez au site officiel de Wireshark : https://www.wireshark.org.
2. Téléchargez la version compatible avec votre système (64-bit ou 32-bit).
3. Lancez le fichier d'installation et suivez les étapes.
4. Cochez l'installation de **Npcap** lorsqu'elle est proposée (indispensable pour capturer les paquets).
5. Une fois l'installation terminée, ouvrez Wireshark.

Sous Linux

1. Ouvrez un terminal.

Installez Wireshark avec la commande suivante :
sudo apt update && sudo apt install wireshark

2.
3. Lors de l'installation, acceptez l'ajout des utilisateurs non-root pour capturer les paquets.

Ajoutez votre utilisateur au groupe Wireshark :
sudo usermod -aG wireshark $USER

4.
5. Déconnectez-vous puis reconnectez-vous pour que les modifications prennent effet.

Sous macOS

1. Installez **Homebrew** si ce n'est pas déjà fait : https://brew.sh.
2. Installez Wireshark avec la commande :
   brew install --cask wireshark

Tutoriel Wireshark

Démarrer avec Wireshark

1. **Lancez Wireshark** : Une fois ouvert, vous verrez une liste d'interfaces réseau disponibles sur votre machine.
2. **Choisissez une interface** : Sélectionnez celle que vous voulez surveiller (Wi-Fi, Ethernet, etc.).
    - Si vous n'êtes pas sûr, regardez l'activité sur chaque interface pour identifier celle qui reçoit le plus de trafic.
3. Cliquez sur **Start Capturing Packets** (▸) pour démarrer la capture en temps réel.

Comprendre le Mode Promiscuous

- Par défaut, une carte réseau ne traite que les paquets qui lui sont adressés.
- Le **mode promiscuous** permet à la carte réseau de capturer **tous les paquets** transitant sur le réseau, même ceux destinés à d'autres appareils.
- Ce mode est activé par défaut dans Wireshark. Pour vérifier :
    1. Allez dans **Capture > Options**.
    2. Assurez-vous que "Enable promiscuous mode" est coché.

Remarque : Le mode promiscuous est particulièrement utile sur des réseaux en mode hub ou lorsqu'un port de monitoring est configuré sur un switch.

Capturer et Analyser les Paquets

Étapes pour Capturer des Paquets

1. **Démarrer la capture** : Cliquez sur ▸ pour commencer.
2. **Laisser tourner** : Attendez quelques minutes pour accumuler suffisamment de données.
3. **Arrêter la capture** : Cliquez sur ■ pour terminer.

Analyse des Paquets

1. **Explorer les résultats** : Les paquets capturés s'affichent dans une liste.
2. **Sélectionner un paquet** : Cliquez sur un paquet pour afficher ses détails dans les panneaux inférieurs.
    - **Panneau supérieur** : Liste des paquets capturés.
    - **Panneau du milieu** : Informations détaillées sur le paquet (couches réseau).
    - **Panneau inférieur** : Données brutes du paquet (hexadécimal et texte).

Tutoriel Wireshark

Utilisation des Filtres d'Affichage

- Les filtres d'affichage permettent de **concentrer l'analyse sur des paquets spécifiques**.
- Voici quelques exemples de filtres courants :
    - **http** : Affiche uniquement les paquets HTTP.
    - **ip.addr == 192.168.1.1** : Montre les paquets impliquant une adresse IP spécifique.
    - **tcp.port == 443** : Affiche le trafic HTTPS.

Pour appliquer un filtre :

1. Tapez le filtre dans la barre en haut de l'écran.
2. Appuyez sur **Entrée**.

Ajouter des Règles de Coloration (Coloring Rules)

Les règles de coloration vous permettent de **mettre en évidence visuellement certains types de trafic** :

1. Allez dans **View > Coloring Rules**.
2. Cliquez sur le bouton "+" pour ajouter une nouvelle règle.
3. Définissez un filtre et choisissez une couleur.

Exemple : Pour colorer les paquets HTTP en vert :
http

    ○
4. Cliquez sur **OK** pour enregistrer.
5. Les paquets correspondant à ce filtre apparaîtront désormais avec la couleur définie.

Astuce : Les règles de coloration facilitent la reconnaissance rapide des types de trafic importants dans une capture dense.

Analyse du Trafic Entre Deux Switches

1. **Configurer le monitoring sur le switch** :
    - Connectez un ordinateur avec Wireshark à un port configuré en mode SPAN (port miroir).

Sur un switch Cisco, utilisez ces commandes :
configure terminal

monitor session 1 source interface [interface_source]

monitor session 1 destination interface [interface_monitoring]

exit

    -
2. **Lancer la capture dans Wireshark** :
    - Sélectionnez l'interface réseau connectée au port de monitoring.
    - Cliquez sur ▸ pour démarrer.
3. **Appliquer des filtres pour analyser des protocoles spécifiques** :

Exemple : Affichez uniquement le trafic STP (Spanning Tree Protocol) :
stp

    -

Exemple : Filtrez les paquets VLAN :
vlan

    -
4. **Analyser les résultats** : Recherchez des anomalies ou des paquets inattendus entre les switches.

Sauvegarder et Exporter

1. Pour sauvegarder une capture complète :
    - Allez dans **File > Save As**.
    - Donnez un nom au fichier (format `.pcap` ou `.pcapng`).
2. Pour exporter des paquets spécifiques :
    - Appliquez un filtre.
    - Sauvegardez uniquement les paquets filtrés.

Bonnes Pratiques pour les Débutants

1. **Pratiquez sur un réseau local** : Évitez de capturer du trafic sur des réseaux publics sans autorisation.
2. **Commencez avec des filtres simples** : Limitez la capture aux ports ou adresses pertinentes.
3. **Sauvegardez vos sessions** : En cas d'erreur, vous pourrez toujours revenir aux captures précédentes.

Conclusion

Wireshark est un outil incontournable pour comprendre et analyser le trafic réseau. Avec ses fonctionnalités comme le mode promiscuous, les filtres d'affichage et les règles de coloration, même un débutant peut rapidement identifier et résoudre des problèmes réseau. Prenez le temps de vous familiariser avec ces concepts et explorez les nombreuses possibilités offertes par cet outil !