Glossaire – Projet Wireshark

Notions de base

- Trame (Frame) : Unité de données au niveau de la couche 2 (liaison de données) du modèle OSI. Elle contient les adresses MAC source et destination.

- Paquet (Packet) : Unité de données au niveau de la couche 3 (réseau). Il contient notamment l'adresse IP source et destination.

- PDU (Protocol Data Unit) : Unité de données spécifique à chaque couche OSI. Exemple : trame pour la couche 2, paquet pour la couche 3, segment pour la couche 4.

Modèle OSI (Open Systems Interconnection)

- Couche 1 – Physique : Transmission électrique ou optique des bits (non visible dans Wireshark).

- Couche 2 – Liaison de données : Gère les adresses MAC. Protocoles : Ethernet, ARP.

- Couche 3 – Réseau : Gère les adresses IP. Protocoles : IPv4, IPv6, ICMP.

- Couche 4 – Transport : Assure la communication de bout en bout. Protocoles : TCP, UDP.

- Couche 5 – Session : Établit, gère et termine les sessions (ex : SSL/TLS).

- Couche 6 – Présentation : Encodage/décodage des données (ex : chiffrement, compression).

- Couche 7 – Application : Interface avec l'utilisateur (ex : HTTP, FTP, DNS).

Protocoles et services

- ARP : Traduit une adresse IP en adresse MAC.

- TCP : Protocole de transport fiable avec établissement de connexion (SYN, ACK, FIN...).

- UDP : Protocole de transport non fiable mais rapide.

- DNS : Résout les noms de domaine en adresses IP.

- mDNS : Version locale de DNS utilisée dans les réseaux sans serveur DNS central.

- DHCP : Attribue automatiquement des adresses IP.

- SSL/TLS : Protocoles de sécurisation des communications (HTTPS, FTPS).

- FTP : Transfert de fichiers (en clair sans chiffrement).

- SMB : Partage de fichiers et d'imprimantes sous Windows.

- HTTPS : Version sécurisée de HTTP via TLS.

- ICMP : Utilisé pour les messages d'erreur (ex : ping).

Outils et formats

- Wireshark : Analyseur de paquets réseau en interface graphique.

- tshark : Version en ligne de commande de Wireshark.

- pcap / pcapng : Formats de fichiers utilisés pour stocker les captures réseau.

- Hexadécimal : Représentation des données binaires lisible pour l'analyse bas-niveau.

- Filtre d'affichage : Permet de filtrer les paquets visibles dans Wireshark (tcp, udp.port == 53, etc.).

- Filtre de capture : Limite les paquets enregistrés lors de la capture (port 80, host 8.8.8.8, etc.).

Expressions utiles

- Capturer le trafic réseau : Surveiller les paquets qui circulent sur une interface.

- Désencapsulation : Lire les couches imbriquées d'un paquet pour comprendre sa structure.

- Suivre un flux TCP : Reconstituer la communication entre deux hôtes.

- Interface réseau : Carte utilisée pour se connecter à un réseau (eth0, wlan0, etc.).

- Adresse MAC : Identifiant unique d'une interface réseau.

- Adresse IP : Adresse logique utilisée pour identifier une machine sur le réseau.

- Connexion en 3 temps : Mécanisme d'établissement de connexion TCP (SYN, SYN-ACK, ACK).

- Décodage base64 / MD5 / ASCII : Outils utiles pour analyser les données brutes dans les paquets.