

I - Installation et Documentation

II - Fonctions clé de Wireshark

- 1.1 - Manipulation des fichiers de capture**
- 1.2 - Format cap et pcapng**
- 1.3 - Les commentaires dans les fichiers et les paquets**
- 1.4 - Le temps dans Wireshark (référence, timeshift, affichage)**
- 1.5 - Les résolutions de noms**
- 1.6 - Fonction Decode As**
- 1.7 - Fonction File Properties**
- 1.8 - Fonction hiérarchie des protocoles**
- 1.9 - Fonction Conversations**
- 1.10 - Fonction Endpoints**
- 1.11 - IO/Graph**
- 1.12 - Fonction follow Stream**

III - Méthodes de capture du trafic

- 2.1 - Comparaison des différentes méthodes**
- 2.2 - Gestion et sélection des interfaces de capture**
- 2.3 - Lancement et arrêt des captures**
- 2.4 - Création d'un Ring Buffer**
- 2.5 - Exportation de paquets**
- 2.6 - Capture en ligne de commande**
- 2.7 - Mode promiscuous ou mode monitor**

IV - Les filtres

- 3.1 - Filtres de capture**

3.1.1 - Implémentation de filtres de capture (protocole, IP, MAC, port ou plage de ports)

3.1.2 - Recommandation sur l'usage des filtres de capture

3.2 - Filtres d'affichage

3.2.1 - Comparaison des filtres de capture et d'affichage

3.2.2 - Les méthodes pour créer un filtre d'affichage

a - manuelle

b - drag and drop

c - clic droit

3.2.3 - Utilisation de filtres membership (exemple tcp.port in {80,443})

3.2.4 - Les opérateurs logiques (AND, OR)

3.2.5 - Création de boutons pour accès rapide

3.2.6 - Identification de cas où le filtre d'affichage montre des résultats incomplets ou excessifs

3.2.7 - Analyse du comportement de l'opérateur ! (Not) selon son emplacement

3.2.8 - Application des filtres aux statistiques

3.2.9 - Création de filtres à partir de champs générés

V - Personnalisation de l'interface graphique selon les besoins

4.1 - Identifier les principaux composants de l'interface graphique (liste de paquets, détail de paquet, vue des octets, boutons, ...)

4.2 - Modifier la disposition des panneaux

4.3 - Utiliser et gérer des profils (création, modification, copie, ...)

4.4 - Utiliser et gérer les colonnes

4.5 - Techniques et règles de colorisation des paquets

4.6 - Utilisation de la carte colorée pour localiser les paquets

4.7 - Les préférences de protocoles

4.8 - Le marquage de paquets

VI - Identifier et analyser les protocoles courants disséqués par Wireshark

5.1 - ETHERNET

- 5.1.1 - Identifier les champs d'une trame Ethernet**
- 5.1.2 - Taille minimale et maximale des trames**
- 5.1.3 - Pourquoi le champ CRC n'est pas présent dans les trames dans Wireshark**
- 5.1.4 - Identifier les types Ethernet (ARP, IPv4, IPv6)**
- 5.1.5 - Distinguer les adresses Unicast, Multicast, Broadcast**
- 5.1.6 - Modification de l'en-tête des trames en présence de VLAN**

5.2 - ARP

- 5.2.1 - Rôle et fonctionnement du protocole ARP**
- 5.2.2 - identifier les types de paquets ARP**
- 5.2.3 - Créer des filtres pour les différents types de trafic ARP**
- 5.2.4 - Différences entre un broadcast ARP et un unicast ARP**

5.3 - IPv4

- 5.3.1 - Fonctions courantes du protocole IP**
- 5.3.2 - En-têtes du protocole IP (TTL, fragmenatation, Packet length, Protocol ID, IP ID)**
- 5.3.3 - Plages d'adresses IP publiques, privées, multicast et APIPA**
- 5.3.4 - Fonctionnement du NAT et impact sur les captures et leur analyse**
- 5.3.5 - Le champ TTL dans les paquets IP**
- 5.3.6 - Prévision de la distance en sauts depuis l'équipement de capture**
- 5.3.7 - Stratégies d'identification IP et utilisation en diagnostic**

5.4 - ICMPv4

- 5.4.1 - Identification et rôles des différents types de messages ICMP**
- 5.4.2 - Identification du paquet déclencheur d'un message ICMP (erreur ou réponse)**

5.5 - IPv6

- 5.5.1 - Les différents types d'adresses IPv6 (Link Global, Gloabal Unicast, Multicast)**

5.6 - ICMPv6

- 5.6.1 - Identifier et expliquer les composants du protocole de découverte des voisins et des routeurs**
- 5.6.2 - Identifier et expliquer les annonces et les sollicitations de voisins**

5.7 - UDP

5.7.1 - Identifier un trafic UDP

5.7.2 - Identifier les protocoles de niveau supérieur utilisant UDP

5.7.3 - Description de l'UDP Stream ID et des timestamps de conversation

5.7.4 - Pourquoi UDP est utilisé dans le trafic UDP en multicast ou en broadcast

5.8 - DHCPv4

5.8.1 - Les 4 phases DHCPv4 (DORA)

5.8.2 - Les différents buts d'un message de type DHCP Request

5.8.3 - Options et paramètres DHCP (router, dns, subnetmask, custom options)

5.8.4 - Relation entre adresses APIPA et DHCP

5.9 - DNS

5.9.1 - Identifier les requêtes et réponses DNS

5.9.2 - Utiliser les informations DNS pour identifier les trafics

5.9.3 - Les différents types d'enregistrements DNS

5.10 - TCP

5.10.1 - Composants d'un 3-way handshake

5.10.2 - Les méthodes pour rompre une session TCP

5.10.3 - Mesurer l'iRTT

5.10.4 - Description et calcul du MSS (Maximum Segment Size

5.10.5 - Utilisation des drapeaux (flags) dans l'établissement et la rupture d'une session TCP

5.10.6 - Utilisation et calcul des numéros de séquence et d'acquittement

5.10.7 - Les options TCP et leurs rôles (EOL, NOP,MSS,SACK,DSACK, Window scaling)

5.10.8 - les DUP ACK

5.10.9 - Identifier les plages de segments manquants en se basant sur les DUP ACK avec SACK ou DSACK

5.10.10 - Décrire les différentes lignes d'un graphe TCP Stream

5.10.11 - Décrire le rôle du réassemblage de segments dans Wireshark

5.10.12 - Description du TCP Stream ID et des timestamps de conversation

VII - Utilisation de Wireshark pour diagnostiquer des problèmes

courants

- 6.1 - Détermination d'une topologie par l'analyse de paquets**
- 6.2 - Analyser les numéros de séquence et d'acquittement en TCP**
- 6.3 - Distinguer lenteur applicatives et lenteurs liées au réseau**
- 6.4 - Identifier l'impact d'une valeur élevée de RTT dans le protocoles en requête/réponse (HTTP, SMB,SQL)**
- 6.5 - Identifier les problèmes liés à des tailles de fenêtre basse ou nulle**
- 6.6 - Identifier dans une capture des signes de problèmes potentiels grâce à ARP, DHCP ou ICMP**