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

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'identifcation 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 sollications de voisins

5.7 - UDP

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 lenteuts liées au réseau

6.4 - Identifier l'impact d'une valeur élevée de RTT dans le sprotocoles en réquête/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