TP WIRESHARK N°2

Ex 1

Le but de ce TP est d'envoyer une trame udp d'une machine virtuelle à une autre et à l'aide de Wireshark sniffer cette trame.

1. Dans votre filtre de capture Wireshark veuillez appliquer tout ce qui est filtre **udp**

2. Depuis l'une des machines virtuelles envoyer un message : *Bonjour ceci est un message privé envoyé dans un paquet udp*
   echo -en 'Bonjour ceci est un message privé envoyé dans un paquet udp' | netcat -u adresse ip 6060

3. Appliquer maintenant un filtre d'affichage afin de filtrer toutes les trames udp passant par le port 6060. (Le port 6060 a été choisi au hasard pour faciliter la recherche de la trame)
   Ip.addr==adresse ip and udp port==6060

4. Sélectionner la trame et aller dans la zone d'encapsulation. Vous remarquerez que chaque en-tête correspond à un niveau d'encapsulation (une couche précise du modèle OSI)

   a. Déroulez les en-têtes et visualisez les différents champs qui les composent. Quelle est la taille totale de la trame ?
   b. Quelle est la taille du paquet IPV4 ?
   c. Quelles sont les adresses source et destination utilisées dans cet échange ? Quels sont les ports source et destination ayant envoyé et reçu respectivement le message ?
   d. Retrouvez le message envoyé.
   e. Faire un clic droit sur la trame => suivre => flux udp. Que constatez-vous ?

Ex 2

Le but de ce TP est de récupérer un nom d'utilisateur et mot passe via une ***page de test de connexion***

1. Se rendre sur votre navigateur et chercher une page test de connexion quelconque
2. Saisir un login et mot de passe
3. Se rendre dans le filtre de capture Wireshark, arrêter la capture puis appliquer le filtre http
4. Rechercher les crédentiels de votre page test de connexion

Quelle correspondance avec le cours sur Nmap ?