Labo 3 : Protocoles – partie 2 (90 min)

1 Objectifs

Le but de ce labo est d'étudier divers protocoles (TCP et http) avec l'excellent outil gratuit d'analyse Wireshark

2 Configuration du poste de travail

Objectif Ouvrir une session utilisateur Username=**ursula** password=**user**

Remarques Votre PC (Vista Enterprise), désigné par Dx (D1-D16), est situé dans l'intranet

Action *Start – Run…* - **`\\10.1.1.1\FilesTD\Labo409\Labo3`**
S'authentifier sur le serveur Username=**rpi** password=**rpi**
Conserver cette fenêtre de partage

3 Protocoles TCP et http 40'

Objectif Etudier l'acquisition **http** produite avec un navigateur sur le site **www.td.unige.ch**

Action Ouvrir cette acquisition présente dans la fenêtre de partage

Question 3a Quelle est la valeur de l'adresse IP du poste client ?

Question 3b Quelle est la valeur de l'adresse IP du site web ?

Question 3c Quelle est la valeur utilisée par le *port source* du poste client ?

Question 3d Quelle est la valeur utilisée par le *port destination* de votre PC ?

Question 3e Situer les 3 paquets TCP responsables de l'établissement

Question 3f Quelle est la valeur aléatoire générée par le navigateur pour le champ *Sequence Number* ?

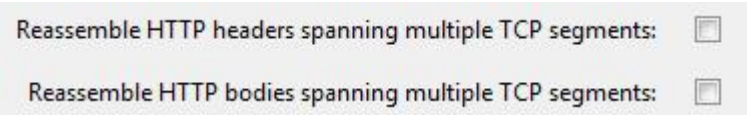
Question 3g Quelle est la valeur aléatoire générée par le serveur pour le champ *Sequence Number* ?

Question 3h A l'issue de cette phase d'établissement, combien d'octets le navigateur est-il autorisé à émettre ?

Question 3i A l'issue de cette phase d'établissement, combien d'octets le serveur est-il autorisé à émettre ?

Question 3j Situer la première requête http du client
Que signifie-t-elle ?

Remarque La trame 9 surprend car nous devrions logiquement avoir une réponse http 200 OK
Wireshark possède un mode par défaut **particulier** de décodage du protocole http qu'il convient de désactiver → Edit – Preferences – Ouvrir Protocoles – Sélectionner http
Désactiver



Question 3k Analyser les principaux éléments (taille, type, temps) de la réponse (trame 9)

Question 3l Identifier les paquets contenant cette page html de 3523 octets

Question 3m A quoi sert le paquet 21 ?

Question 3n A quoi servent les paquets 22, 23 et 24 ?

4	**Wireshark en mode statistique**	**10'**

Objectif Identifier les flux d'une acquisition pour le caractériser
L'outil Wireshark dispose de la fonction Statistics que vous allez découvrir avec l'acquisition **http** que vous venez d'étudier

Action Ouvrir cette acquisition puis sélectionner Statistics – Summary

Question 4a Quelle est la taille (en trame) de cette acquisition ?

Question 4b Quelle est la durée de cette acquisition ?

Objectif Quels sont les protocoles utilisés ?

Action Sélectionner Statistics – Protocol Hierarchy

Question 4c Quel est le pourcentage des paquets DNS ?

Objectif Quels sont les nœuds les plus bavards (paquets émis) ?

Action Sélectionner Statistics – Endpoints

Question 4d Combien de paquets ont été émis par le client ?

Objectif Quelles sont les échanges client – serveur ?

Action Sélectionner Statistics – Conversation

Question 4e Identifier chaque session (échanges TCP et UDP)

5	**Wireshark en mode statistique**	**20'**

Objectif Identifier les flux d'une acquisition **Traf_EIG** faite sur le réseau de l'EIG

Action Ouvrir cette acquisition puis sélectionner Statistics – Summary

Question 5a Quelle est la taille (en trame) de cette acquisition ?

Question 5b Quelle est la durée de cette acquisition ?

Objectif Quels sont les protocoles utilisés ?

Action Sélectionner Statistics – Protocol Hierarchy

Question 5c Quel est le pourcentage des paquets compatibles IP ?

Question 5d Quel est le protocole applicatif compatible TCP le plus utilisé ?

Objectif Quels sont les nœuds les plus bavards (paquets émis) ?

Action Sélectionner Statistics – Endpoints

Question 5e Quel est le nœud le plus bavard pour l'onglet Ethernet ?

Question 5f Quel est le nœud le plus bavard pour l'onglet IPv4 ?

Question 5g Les résultats 5e et 5f semblent incohérents (129.194.184.80 n'est pas un routeur). Expliquez-les

Objectif Quels sont les nœuds qui communiquent avec le serveur 129.194.184.80 ?

Action Configurer un filtre d'affichage **`ip.addr == 129.194.184.80`** , activer avec Apply
Marquer tous les paquets avec Edit – Mark All Packets
Sauver avec File – Save As – Marked packets (vos initiales pour le nom de fichier)
Ouvrir cette acquisition puis sélectionner Statistics – Conversation

Question 5h Quel est le nombre de partenaires au niveau IPv4 ?

Question 5i Quel est le partenaire compatible IP le plus bavard ?

Question 5j Quel est le partenaire compatible UDP ?

6	**Travail personnel**	**20'**

Objectif Etudier les protocoles mis en œuvre dans un contexte applicatif particulier
Choisir une application web, messagerie, telnet

Méthodologie Configurer correctement le filtre d'acquisition Wireshark
Identifier les champs intéressants : *username*, *password*, …
Utiliser la commande *Find (Hex value / String)*