Labo 2 : Protocoles – partie 1 (90 min)

1 Objectifs

Le but de ce labo est d'étudier divers protocoles (ethernet, ARP, IP, ICMP, UDP et DNS) 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\Labo2`**
S'authentifier sur le serveur Username=**rpi** password=**rpi**
Conserver cette fenêtre de partage

3 Commandes arp et ping 15'

Action Ouvrir l'interface de command Command Prompt situé sur le bureau
La commande **ping** permet de vérifier si une machine distante est accessible

Exemple : **ping 10.1.1.1** teste si le serveur de fichiers est accessible.

Quelques adresses utiles :

10.1.0.1	Firewall (côté *intranet*)
10.1.1.1	Serveur de fichiers
10.1.1.10	Serveur DNS
10.1.4.1	E1
10.1.4.2	E2
...	...
10.1.4.x	Ex

Utilisation

```
C:\WINDOWS>ping

Usage: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
            [-r count] [-s count] [[-j host-list] | [-k host-list]]
            [-w timeout] destination-list

Options:
    -t             Ping the specifed host until interrupted.
    -a             Resolve addresses to hostnames.
    -n count       Number of echo requests to send.
    -l size        Send buffer size.
    -f             Set Don't Fragment flag in packet.
    -i TTL         Time To Live.
    -v TOS         Type Of Service.
    -r count       Record route for count hops.
    -s count       Timestamp for count hops.
    -j host-list   Loose source route along host-list.
    -k host-list   Strict source route along host-list.
    -w timeout     Timeout in milliseconds to wait for each reply.
```

```
C:\WINDOWS>arp

Displays and modifies the IP-to-Physical address translation tables used
by address resolution protocol (ARP).

ARP -s inet_addr eth_addr [if_addr]
ARP -d inet_addr [if_addr]
ARP -a [inet_addr] [-N if_addr]

-a               Displays current ARP entries by interrogating the
                 current protocol
                 data.

                 If inet_addr is specified, the IP and Physical
                 addresses for only the specified computer are
                 displayed.
                 If more than one network interface uses ARP, entries
                 for each ARP table are displayed.
-g               Same as -a.
inet_addr        Specifies an internet address.
-N if_addr       Displays the ARP entries for the network interface
                 specified by
                 if_addr.
-d               Deletes the host specified by inet_addr.
-s               Adds the host and associates the Internet address
inet_addr with
                 the Physical address eth_addr.
                 The Physical address is given as 6 hexadecimal bytes
                 separated by hyphens. The entry is permanent.
eth_addr         Specifies a physical address.
if_addr          If present, this specifies the Internet address of the
                 interface whose address translation table should be
                 modified.
                 If not present, the first applicable interface will be
                 used.
```

Question 3a Comment déterminez-vous l'adresse physique de votre station depuis un autre PC ?

Question 3b Comment déterminez-vous l'adresse physique de votre station depuis votre PC ?

Question 3c Qui a attribué cette adresse physique au PC ?

Question 3d Comment déterminez-vous le contenu du cache ARP ?

Question 3e A quoi sert le cache ARP ?

4	**Prise en main de Wireshark**	**30'**

Objectif Découvrir l'utilité d'un analyseur de protocole.
L'acquisition **labo2a.pcap** a été produite à partir de la commande **ping 10.1.1.1**

Action Démarrer Wireshark (raccourci bureau)
Identifier les principales commandes :

List interfaces
Show capture cptions
Start a new live capture
Stop the running capture
Restart the running capture
Open a capture file

Action Ouvrir l'acquisition **labo2a.pcap** située dans la fenêtre de partage

Objectif Comprendre les 3 vues affichées (Résumé – Analyse – Hexadécimal & ASCII)

Explication La vue du haut donne le résumé de chaque trame classé par ordre d'acquisition
La vue du milieu donne l'analyse détaillée des protocoles de la trame sélectionnée dans la vue précédente
La fenêtre du bas affiche les valeurs hexadécimales et ASCII de la trame sélectionnée

Question 4a Pour la trame 1, quelle est la valeur de l'adresse ethernet destination ? Pourquoi ?

Question 4b Pour la trame 2, quelle est la valeur recherchée ?

Question 4c Quel est l'interval de temps entre ces 2 trames ?

Question 4d Quel est l'empilement pour les trames 1 et 2 ?

Question 4e Quelle est l'utilité de la trame 3 ?

Question 4f Pour cette trame 3, quelles sont les valeurs des principaux champs de la couche IP ?

Question 4g Pour cette trame 3, combien de bytes utiles transportent la couche ICMP ?

Question 4h Quel est l'empilement pour les trames 3 et 4 ?

Question 4i Quel est l'interval de temps entre ces 2 trames ?
Choisir le mode approprié d'affichage → View – Time Display Format – ???

Question 4j Quelles sont les valeurs du champ Type ?

5 Protocoles Ethernet, ARP, IP, UDP, DNS 20'

Objectif Etudier l'acquisition **labo2b** produite avec la commande **ping www.unige.ch**

Action Ouvrir cette acquisition

Objectif Activer un **filtre d'affichage** afin de ne conserver que les flux dns

Action

puis **Apply**

Remarque La couleur verte signifie que la syntaxe est correcte

Question 5a A quoi sert le paquet 3 ?

Question 5b Pour ce paquet 3, quelle est la valeur utilisée par le *port source* ?
Pourquoi ?

Question 5c Pour ce paquet 3, quelle est la valeur utilisée par le *port destination* ?
Pourquoi ?

Question 5d A quoi sert le paquet 4 ?

Question 5e Quelle est la durée de vie de la correspondance précédente ?

Question 5f Quel est l'empilement des paquets DNS utilisés ?

Question 5g Quelle l'adresse IP du poste qui génère la trame 1

Question 5h Quelle l'adresse IP du poste qui génère la trame 2

Question 5i Quelle l'adresse IP du poste qui génère la trame 5

Question 5j Quelle l'adresse IP du poste qui génère la trame 6

Question 5k Préciser la configuration TCP/IP du poste qui génère la trame 1

6 Wireshark en mode acquisition avec filtrage d'adresse 20'

Objectif Analyser le trafic entre votre PC (client) et un partenaire (serveur)
Un filtre est donc nécessaire pour que l'analyseur n'acquière que ce flux client – serveur et pas celui de tous les ordinateurs du réseau *(promiscuous mode)*
Configurer le **filtre d'acquisition** pour qu'il ne prenne en compte que les flux entrant et sortant de votre PC.

Théorie Tous les analyseurs possèdent **2 types de filtres**
Vous avez utilisé au **§5 un filtre d'affichage** afin de n'afficher que les paquets de type DNS
Vous allez cette fois configurer **un filtre d'acquisition**

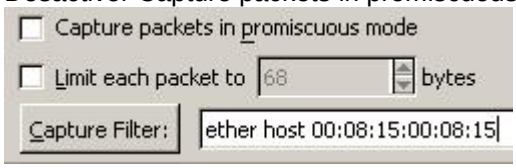
Action Sélectionner *Show the capture options…*

Syntaxe

host 192.168.0.1	pour configurer un filtre (adr IP source ou destination)
src host 192.168.0.1	pour configurer un filtre (adr IP source)
dst host 192.168.0.1	pour configurer un filtre (adr IP destination)
ether host 00:08:15:00:08:15	pour configurer un filtre (adr Ethernet source ou destination)
ether src 00:08:15:00:08:15	pour configurer un filtre (adr Ethernet source)
ether dst 00:08:15:00:08:15	pour configurer un filtre (adr Ethernet destination)
port 80	pour configurer un filtre (port source ou destination)
port 80 and host 192.168.0.1	
tcp port http	

Remarque Le bouton Capture filter affiche quelques exemples et donne accès à la documentation (bouton Help)

Action Désactiver Capture packets in promiscuous mode et activer divers filtres (ethernet, IP)



Remarque Ne pas oublier de vider tous les caches

Action **Start** pour démarrer l'acquisition Wireshark
Produire du trafic avec la commande **ping www.luth.se**
Stop pour terminer l'acquisition

Question Observez-vous tous les paquets ARP, DNS, ICMP attendus ?