RAPPORT TP 3 ET TP4

TP 3

# 1.Analyse de Trames avec Wireshark

## 1.1.Préambule

Adresse IP de la machine : 10.0.2.15  
Masque du réseau : 255.255.255.0  
Adresse IP de la passerelle : 10.0.2.2  
Adresse du serveur : 1.0.2.3

## 1.2.Prise en main de Wireshark

Graphical user interface, text, application, email

Description automatically generated

## 1.3. Ping

### Quelle adresse Ethernet est destinée la requête ARP (trame 1) émise par la machine cliente ? Il s'agit en fait de l'adresse de diffusion (broadcast). Elle ne correspond à aucune machine particulière ! A votre avis pourquoi doit on procéder ainsi ?

Broadcast (ff:ff:ff:ff:ff:ff) demande et récupère l'information de l’adresse source et de destination grâce au protocole ARP.

### Quel est le protocole de transport utilisé pour les échanges DNS (trames 3-4) ?

C’est le protocole UDP qui est utilisé.

### Observez en détail la réponse DNS (section Answers) et découvrez ainsi l'adresse IP de la machine www.google.com retourné par le serveur DNS

Graphical user interface, text

Description automatically generated  
L’adresse IP de la machine Google est 172.217.19.132.

### La requête ARP WHO HAS (trame 5) cherche à trouver l'adresse Ethernet de la machine 10.0.2.2. Pourquoi cette machine et non pas la machine cible www.google.com ?

La machine 10.0.2.2 sert de passerelle (je n’en suis pas certain car je n’ai pas trouvé d’informations précises).

### Vérifiez l'adresse Ethernet destination utilisée pour envoyer la trame 7.

C’est l’adresse 172.217.19.132.

### Observez la première requête / réponse ICMP (trames 7-8) et observez la valeur du champs type dans l'en-tête ICMP…

Pour la requête :

Text

Description automatically generated with medium confidence

Pour la réponse :

Graphical user interface, text, application

Description automatically generated with medium confidence

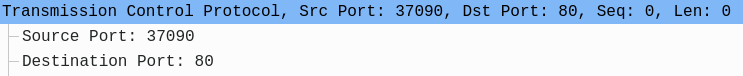
## 1.4.Une page web : je suis perdu !

### Que se passe-t-il quand je consulte une page web (par exemple, http://www.perdu.com) sur Internet avec mon navigateur préféré ?

Text

Description automatically generated with medium confidence

### Considérons la première trame TCP qui ouvre la connexion (trame 7). Trouvez dans l'en-tête TCP le port source et le port de destination. Ce dernier est standard pour tous les serveur web (80). A quoi correspond le flag SYN dans cette en-tête ?



Le port source est 37090 et le port de destination est 80.  
Le flag SYN (Synchronisation) permet la connexion entre le port source et le port destination.

### Identifiez dans la conversation TCP les trames correspondant à la requête HTTP et à la réponse HTTP…

La trame 10 correspond à la requête HTTP :

Graphical user interface, application, Word

Description automatically generated

Et comme indiqué sur cette trame, la trame 12 est la réponse à celle-ci :

Graphical user interface, application, Word

Description automatically generated

### Dans l'en-tête de la requête HTTP, on observe sur la première ligne qu'il s'agit de la requête GET / HTTP/1.1. Identifiez le rôle des champs suivants : User-Agent, Host, Connection.

User-Agent permet aux serveurs d’identifier le système, l’application, la version etc de la machine ayant envoyé la requête.  
Host correspond à l’URL et le port du serveur demandé (ici le port est sous-entendu).  
Connection : Définit si la connexion avec le serveur reste ouverte ou fermée après l’interaction avec ce même serveur.

Graphical user interface

Description automatically generated with low confidence

### Observez maintenant les différents champs dans la réponse HTTP et en déduire le logiciel serveur, la longueur et le type de contenu dans cette réponse.

Le logiciel serveur est Apache, la longueur est de 204 bits et le type de contenu est du HTML.

Text

Description automatically generated

### Immédiatement après l'en-tête HTTP, vous pouvez identifier le code HTML de la page web : <html>...</html>



### Trames 7-16 : Pour lire plus facilement la conversation TCP, vous pouvez faire un "clic droit" sur un des paquets TCP et sélectionner Suivre (Follow) → flux TCP (TCP Stream) dans le menu déroulant. Notez qu'il est possible de reconstruire précisément le fil de la conversation grâce aux numéros de séquence (en octets) qui se trouve dans l'en-tête TCP.

Graphical user interface, text, application

Description automatically generated

TP4

# Manipulation de paquets avec Scapy

## Demarrage d’un réseau virtuel

### Lancez tcpdump -i eth0 sur la passerelle immortal afin d'espionner le trafic échangé entre les autres machines. Lancez netstat -tupl pour voir quels services (et donc quels ports) sont ouverts sur opeth (ou syl).

Text

Description automatically generated

A picture containing text

Description automatically generated

## Prise en main de Scapy

### Lancez scapy3 sur la machine grave en tant que root (ou sudoer)

Text

Description automatically generated

### Il est également possible d'écrire des programmes Scapy sous forme d'un script Python, qu'il faut enregistrer avec un éditeur de texte, comme nano ou emacs

A screenshot of a computer

Description automatically generated with medium confidence

Text

Description automatically generated

## Ping

### Regardez dans le fichier ping.py un exemple d'utilisation de Scapy qui envoie un ping (ICMP) puis récupère la réponse. Essayez-le en recopiant le programme ligne par ligne, ou en faisant un copier/coller.

Text

Description automatically generated

## ARP

### Rappelez le fonctionnement du protocole ARP. Notez que le protocole ARP ne dispose que de deux opérations : la requête (Who Has) et la réponse. On peut alors utiliser ce protocole pour effectuer un ping dans le réseau local Ethernet. Il s'agit d'envoyer une requête ARP. Si la machine répond, c'est bien qu'elle est en vie !

Le protocole ARP fait le lien entre une adresse IP et une adresse physique. Il va d’abord interroger tous les périphériques et si la machine recherchée est bien présente elle enverra une réponse directe à l’émetteur.

### Commencez par construire une trame Ethernet avec Ether() vers l’adresse de broadcast FF:FF:FF:FF:FF:FF et encapsulez le datagramme ARP() à destination de l'adresse IP visée. Pour envoyer et recevoir une trame Ethernet, il faut utiliser la fonction srp1() (à la place de la fonction sr1() réservé aux paquets IP). On peut aussi utiliser dans cette fonction l'option timeout=1 pour limiter le temps d'attente à 1 seconde, dans le cas où il n'y a pas de réponse.

Graphical user interface

Description automatically generated with low confidence

## Services UDP : Daytime et Echo

### Suivez l'exemple du fichier daytime.py qui envoie un paquet UDP sur le port daytime (13) puis récupère et affiche la date envoyée en réponse. Essayez pas à pas.

Text

Description automatically generated  
Text

Description automatically generated

### Vous avez pu remarquer que le service udp echo est ouvert (port 7). Testez ce service en envoyant le message 'hello'. Quelle est la réponse ?

Avec le port udp echo :

Text

Description automatically generated

La réponse est visible sur la dernière ligne : b’hello’.