R201 TP 6 :

Audit des protocoles TCP et UDP via Wireshark

1. Environnement :

Machine Linux en interne

2. Etude des protocoles :

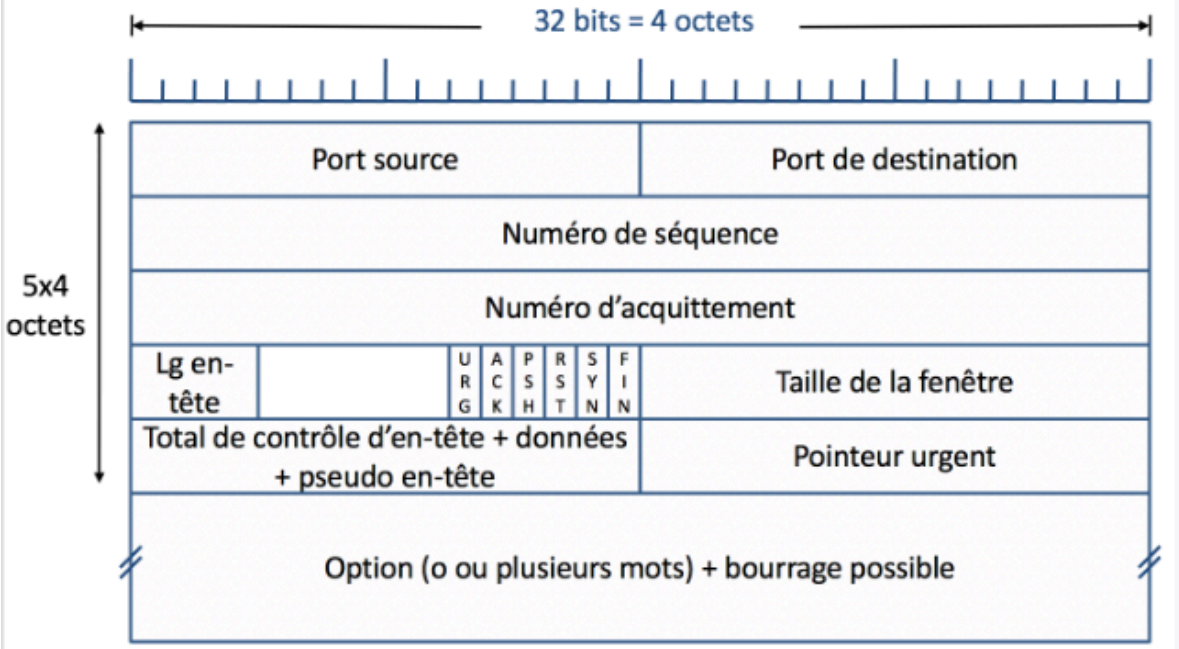
Le protocole **TCP est un protocole orienté connexion** :

il y a donc une phase d'établissement de la connexion `(le "bonjour en 3 fois" "3-way handshake")` qui précède les échanges d'informations entre la source et le destinataire, cette phase d'échanges terminée la connexion se termine par une phase de fermeture de la connexion `(4 segments : FIN, ACK (pour fermer la connexion dans un sens), FIN, ACK (pour fermer la connexion dans l'autre sens))`.

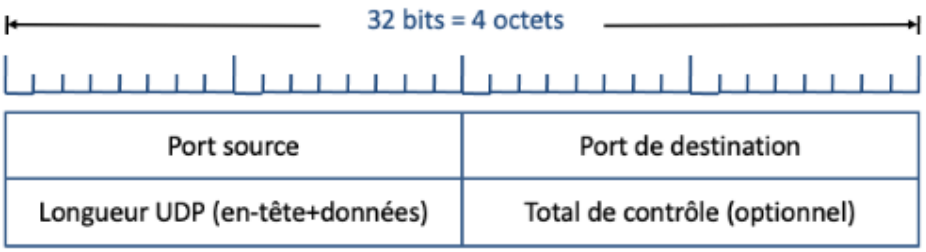
Le protocole **UDP est un protocole non orienté connexion** :

les informations à transmettre sont envoyées telles quelles, aucune phase d'établissement de la connexion, aucune fermeture.

Format en-tête segment TCP



Format en-tête datagramme UDP



Rappel :

- Comment TCP exerce-t-il la ré-émission de messages perdus et le ré-ordonnancement ?

  TCP utilise des numéros de séquence pour réordonner les paquets et des accusés de réception pour la réémission des paquets perdus.

- Comment TCP exerce-t-il le contrôle de flux ?

  TCP utilise des fenêtres de réception pour contrôler le flux de données entre l'émetteur et le récepteur.

- Comment TCP exerce-t-il le contrôle de congestion ?

  TCP utilise un algorithme de contrôle de congestion, tel que TCP Reno, qui ajuste la fenêtre de congestion pour éviter la congestion du réseau.

- Comment TCP exerce-t-il le multiplexage des applications ?

  TCP utilise des ports pour multiplexer les applications.

- Parmi les services précédents, quels sont ceux offerts par UDP ?

  UDP offre des services de multiplexage des applications, mais ne fournit pas de mécanismes de ré-émission, de réordonnancement, de contrôle de flux ou de contrôle de congestion.

3. Etude du trafic TCP :

Trafic normal

TCP est encapsulé dans SSH, FTP ou HTTP. Pour générer un trafic TCP vous pouvez donc utiliser ses services. Mais on peut également utiliser l'outil netcat permettant d'ouvrir des connexions réseau TCP ou UDP ce que vous allez d'abord utiliser ici.

Netcat permet d'ouvrir simplement un serveur grâce à la commande **nc -l hote num_port** : un serveur sur l'hôte "hôte" à l'écoute sur le port "num_port". On peut aussi ne pas préciser l'hôte et l'ouverture se fera sur la boucle locale (interface lo).

Un client peut alors se connecter grâce à la commande **nc hote num_port**.

- Lancez Wireshark sur l'interface boucle locale (lo) avec un filtre de capture TCP

- Lancez dans un terminal un serveur sur la boucle locale à l'écoute sur le port 8000

  nc -l 8000

- Lancez dans un autre terminal un client

  nc localhost 8000

- Envoyer des messages
- Finissez la discussion par **ctrl+D**.
- Coupez la capture Wireshark et filtrez cette discussion.

On lance une RT-Box et une machine linux en interne

Linux :

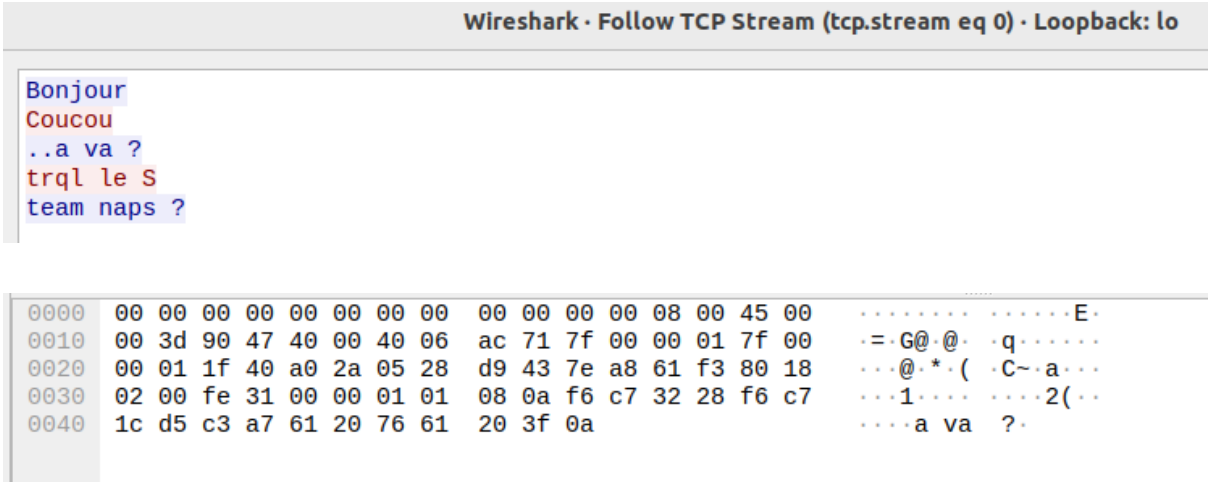
apt update

apt install wireshark

On lance Wireshark sur notre terminal Linux. (loopback.io)

On lance une capture Wireshark avec un filtre TCP (tcp)

Clique droit > Suivre :

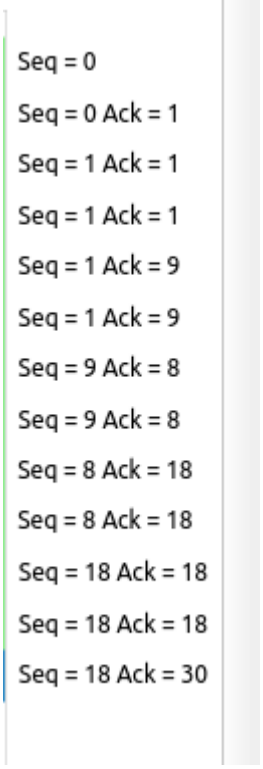


Statics des flux :

Ensuite on coche la case en bas à gauche : limiter au filtre d'affichage

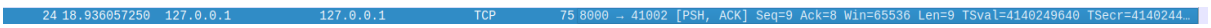
et au milieu on met : TCP flows

- Vérifiez que les numéros de séquence et d'acquittement correspondent bien à ce que vous avez vu en cours et TD.



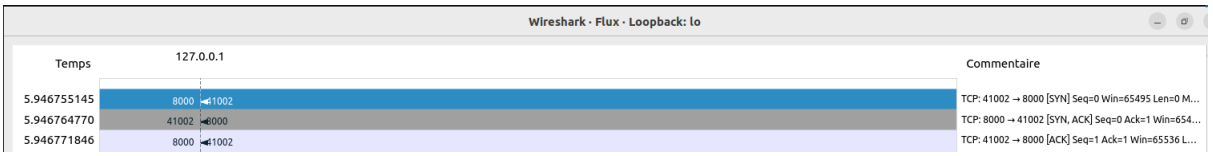
  Ils correspondent bien à ce vus en td.

- Le champ taille de fenêtre (Win) est codé sur 2 octets, sa valeur maximale est donc de 65535 octets. Pourtant vous pouvez apercevoir des valeurs plus grandes pour ce champ dans cet échange.



Recherchez dans l'analyse Wireshark d'une de ces trames, une raison grâce à laquelle c'est possible.

- Identifiez les segments TCP liés à la phase d'établissement de la connexion TCP ("3-way handshake") et vérifiez - par rapport au cours - les fanions/drapeaux/flags TCP apparaissant ainsi que les numéros de séquence et d'acquittement.



- Identifiez les segments TCP liés à la fermeture de la connexion TCP et vérifiez - par rapport au cours - les fanions/drapeaux/flags TCP apparaissant.

Connexion multiple

Ouvrez maintenant plusieurs connexions SSH sur une même machine. Les connexions se mélangent-elles ? Pourquoi ?

On se met sur le serveur et on tappe le commande ssh administrateur@adress_ip_de_la_rt_box(172.31.25.XX)

ssh administateur@localhost

Si ça marche pas faire la commande :

sudo apt install openssh-server

sudo -s

ssh administateur@localhost

```
administrateur@rt-mv:~$ ssh administrateur@localhost
administrateur@localhost's password:
Welcome to Ubuntu 22.04.1 LTS (GNU/Linux 5.19.0-35-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

267 mises à jour peuvent être appliquées immédiatement.
267 de ces mises à jour sont des mises à jour de sécurité.
Pour afficher ces mises à jour supplémentaires, exécuter : apt list --upgradable

Last login: Mon Mar 25 11:18:42 2024 from 127.0.0.1
```

Consultez un même site depuis plusieurs onglets d'un même navigateur web. Les connexions se mélangent-elles ? Pourquoi ?

Lorsque vous consultez un même site depuis plusieurs onglets d'un même navigateur web, les connexions TCP peuvent se mélangent.

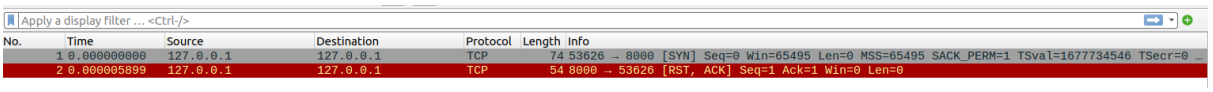
Cela est dû au fait que les connexions TCP sont gérées par le système d'exploitation (OS) de l'ordinateur et non par le navigateur web. Lorsque vous ouvrez plusieurs onglets d'un même site web dans un navigateur, chaque onglet ouvre une nouvelle session de navigation, mais les connexions TCP sont gérées par le système d'exploitation.

Ouverture vers un port non utilisé :

- Capturez les trames TCP issues d'une demande de connexion vers un port non utilisé.

Le port 43774 surligné est le port du serveur, tandis que les autres ports correspondent aux clients.

- Expliquez ce qu'il se passe.



On a que deux trames

Connexion coupée

- Capturez les trames TCP issues d'une connexion coupée.

- Que se passe-t-il sur le réseau ? Mettre une capture de ces segments dans votre compte-rendu à partir de l'outil de visualisation d'échanges de Wireshark.

Pour fournir une capture de segments à partir de Wireshark ou tout autre outil de capture de paquets, je vous recommande de le faire sur votre propre système, car cela nécessite l'accès au réseau concerné. Une fois que vous avez capturé les segments TCP avec Wireshark, vous pouvez examiner les échanges entre les machines pour voir comment les connexions sont établies, les données sont envoyées et les ré-émissions sont gérées.

- Le timer de ré-émission utilisé dans ce cas par TCP, a-t-il une durée fixe ? Comment évolue-t-il ? Quel intérêt ?

Quant au timer de ré-émission utilisé par TCP, il n'a pas une durée fixe. Il évolue dynamiquement en fonction des conditions du réseau. Initialement, TCP utilise un timer relativement court pour détecter les pertes de segments et les ré-émettre rapidement. Si aucune réponse n'est reçue avant l'expiration du timer, le timer est augmenté de manière exponentielle dans le cadre de l'algorithme de retransmission exponentielle (exponential backoff). Cette augmentation progressive du timer permet à TCP de ré-essayer d'envoyer les segments après des délais de plus en plus longs, réduisant ainsi la charge sur le réseau en cas de congestion.

- Combien de temps TCP insiste-il avant d'arrêter de réémettre.

TCP continue de ré-émettre les segments perdus jusqu'à ce qu'il reçoive un accusé de réception valide ou qu'un nombre maximal de tentatives soit atteint. Ce nombre maximal de tentatives est généralement déterminé par une politique de ré-émission, qui peut être basée sur un nombre fixe ou une durée maximale.

- Si la deuxième machine se reconnecte, que se passe-t-il ?

Si la deuxième machine se reconnecte, le processus de connexion TCP habituel s'applique. Une nouvelle session TCP est établie entre les deux machines, avec un nouvel ensemble de numéros de séquence et d'autres paramètres de connexion. Les données sont ensuite échangées comme dans toute nouvelle connexion TCP. Si des données étaient en transit lors de la déconnexion initiale, elles ne sont pas ré-établies automatiquement. Il incombe aux applications de gérer la reprise de la communication là où elle s'était interrompue, si nécessaire.

4. Analyse de ports :

Avec Netcat

Il est possible de faire avec netcat et l'option -z

- Lancez dans un terminal un serveur sur la boucle locale à l'écoute sur le port 800
- **nc -l 800** Lancez Wireshark sur l'interface boucle locale (lo)
- Lancez dans un terminal le scan Netcat sur la plage réduite 800-802
- **nc -z localhost 800-802** Coupez la capture Wireshark et filtrez cette discussion.
- Filtre Wireshark pour aider **tcp.port == 800** Que fait netcat pour scanner un port ? Mettre une capture du scan du port 800 dans votre compte-rendu. Mettre aussi une capture du scan d'un

port non ouvert comme le 801 par exemple dans votre compte-rendu.

Avec Nmap

Un outil bien plus puissant et tout aussi connu pour faire de l'analyse de ports est Nmap. Vous allez pour finir ce TP capturer et analyser grâce à Wireshark différent type de scans via Nmap.

Les scans se font sur votre localhost - Attention : il n'est pas autorisé de scanner une machine qui n'est pas à vous -

- Pour chacun de ces scans, vous devez comme l'analyse du scan via netcat :
    1. Lancez un serveur dans un terminal (nc -l 800)
    2. Lancez Wireshark sur la boucle locale, le filtre d'affichage tcp.port == 800 va vous aider
    3. Lancez le scan puis analyser le résulat : quel(s) format(s) de segment TCP est/sont envoyé(s) pour chaque type de scan ? Mettre les captures de chaque scan du port 800 dans votre compte-rendu.

Les scan à analyser sont les suivants :

1. nmap -sS localhost
2. nmap -sT localhost
3. nmap -sA localhost
4. nmap -sF localhost
5. nmap -sM localhost
6. nmap -sN localhost
7. nmap -sW localhost
8. nmap -sX localhost

Pour finir, Nmap peut aussi faire des scans UDP avec la commande nmap -sU localhost.

- Lancez Wireshark. Lancez la commande nmap -sU localhost. Filtrez l'analyse d'un port, par exemple udp.port == 800. Conclure sur le fonctionnement de ce scan : quel type de trame

est envoyé ? Quel type de de trame est retourné ? Mettre une capture dans votre compte-rendu.