

Séance 10 – Analyse réseau – Kali et Wireshark:

1 Rappel

Dès votre entrée en classe, n'oubliez pas de supprimer les VM (y compris les fichiers!) de votre disque dur et de commencer à l'importation des VM's nécessaires. N'oubliez pas de prendre note !

2 Préparation

Téléchargez une VM préinstallée Kali Linux

<https://www.offensive-security.com/kali-linux-vmware-virtualbox-image-download/>

Choisissez la version normale pour **VirtualBox** (root/toor)

3 Table des matières

1	Rappel	1
2	Préparation	1
3	Table des matières	1
4	Objectifs	2
5	Kali Linux	2
1	Présentation	2
2	Utilisation	2
6	Wireshark	4
1	Présentation	4
2	Démarrage	4
7	ARP	5
1	La cache ARP	5
2	Capturez des paquets ARP et ICMP dans Wireshark	5
8	Analyse DHCP	6
1	Rappel théorique.....	6
2	Analyse avec Wireshark	6
9	Analyse DNS.....	7
10	Session TCP.....	8
1	Rappel théorique.....	8
2	Mise en évidence de l'établissement et de la clôture d'une session TCP à l'aide de Wireshark :	8
11	Analyse d'une session http.....	9
12	Analyse d'une session https	9
13	Mise en évidence des détails de la négociation TCP et suivi de flux TCP:.....	10

4 Objectifs

- Utiliser Wireshark
- Découvrir ARP
- Analyse de dialogues DHCP
- Analyse de dialogues DNS
- Ouverture de session TCP.
- Analyse de session http et https

5 Kali Linux

1 Présentation

Du site <https://docs.kali.org/introduction/what-is-kali-linux>:

Kali Linux is a Debian-based Linux distribution aimed at advanced Penetration Testing and Security Auditing. Kali contains several hundred tools which are geared towards various information security tasks, such as Penetration Testing, Security research, Computer Forensics and Reverse Engineering. Kali Linux is developed, funded and maintained by **Offensive Security**, a leading information security training company.

Kali Linux was released on the 13th March, 2013 as a complete, top-to-bottom rebuild of **BackTrack Linux**, adhering completely to **Debian** development standards.

2 Utilisation

1. Téléchargez l'image OVA comme mentionné dans le paragraphe *préparation*.
2. Importez-là dans Virtual-Box en réinitialisant la MAC.
3. Vérifiez que le réseau est bien en **Accès par pont**.
4. Démarrez la VM.

Login : **root**

Mot de passe : **toor**

5. Vous pouvez changer le clavier en cliquant sur *Show Applications*



Accédez aux settings



Region & Language

Ajoutez le clavier *French (Belgian)* dans les **Input Sources**.

Retirez le clavier par défaut.

6. Installez les outils **resolvconf** qui vous permettront de prendre en compte la définition de vos serveur DNS dans votre configuration réseau dans le fichier **interfaces**. Configurez le service resolvconf afin qu'il soit démarré au boot sur serveur :

```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# apt-get install resolvconf  
Reading package lists... Done  
Building dependency tree  
Reading state information... Done  
The following NEW packages will be installed:  
  resolvconf  
0 upgraded, 1 newly installed, 0 to remove and 1145 not upgraded.  
Need to get 74.2 kB of archives.  
After this operation, 196 kB of additional disk space will be used.  
Get:1 http://ftp.belnet.be/pub/kali/kali-rolling/main amd64 resolvconf all 1.79 [74.2 kB]  
Fetched 74.2 kB in 0s (153 kB/s)
```

```

root@kali:~# systemctl enable resolvconf
Synchronizing state of resolvconf.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable resolvconf
Created symlink /etc/systemd/system/sysinit.target.wants/resolvconf.service → /lib/systemd/system/resolvconf.service.
root@kali:~# systemctl start resolvconf
root@kali:~# systemctl status resolvconf
● resolvconf.service - Nameserver information manager
   Loaded: loaded (/lib/systemd/system/resolvconf.service; enabled; vendor preset: disabled)
   Active: active (exited) since Sun 2019-11-24 03:40:12 EST; 5s ago
     Docs: man:resolvconf(8)
  Process: 2522 ExecStartPre=/bin/mkdir -p /run/resolvconf/interface (code=exited, status=0/SUCCESS)
  Process: 2523 ExecStartPre=/bin/touch /run/resolvconf/postponed-update (code=exited, status=0/SUCCESS)
  Process: 2524 ExecStart=/sbin/resolvconf --enable-updates (code=exited, status=0/SUCCESS)
 Main PID: 2524 (code=exited, status=0/SUCCESS)

Nov 24 03:40:12 kali systemd[1]: Starting Nameserver information manager...
Nov 24 03:40:12 kali systemd[1]: Started Nameserver information manager.
root@kali:~#

```

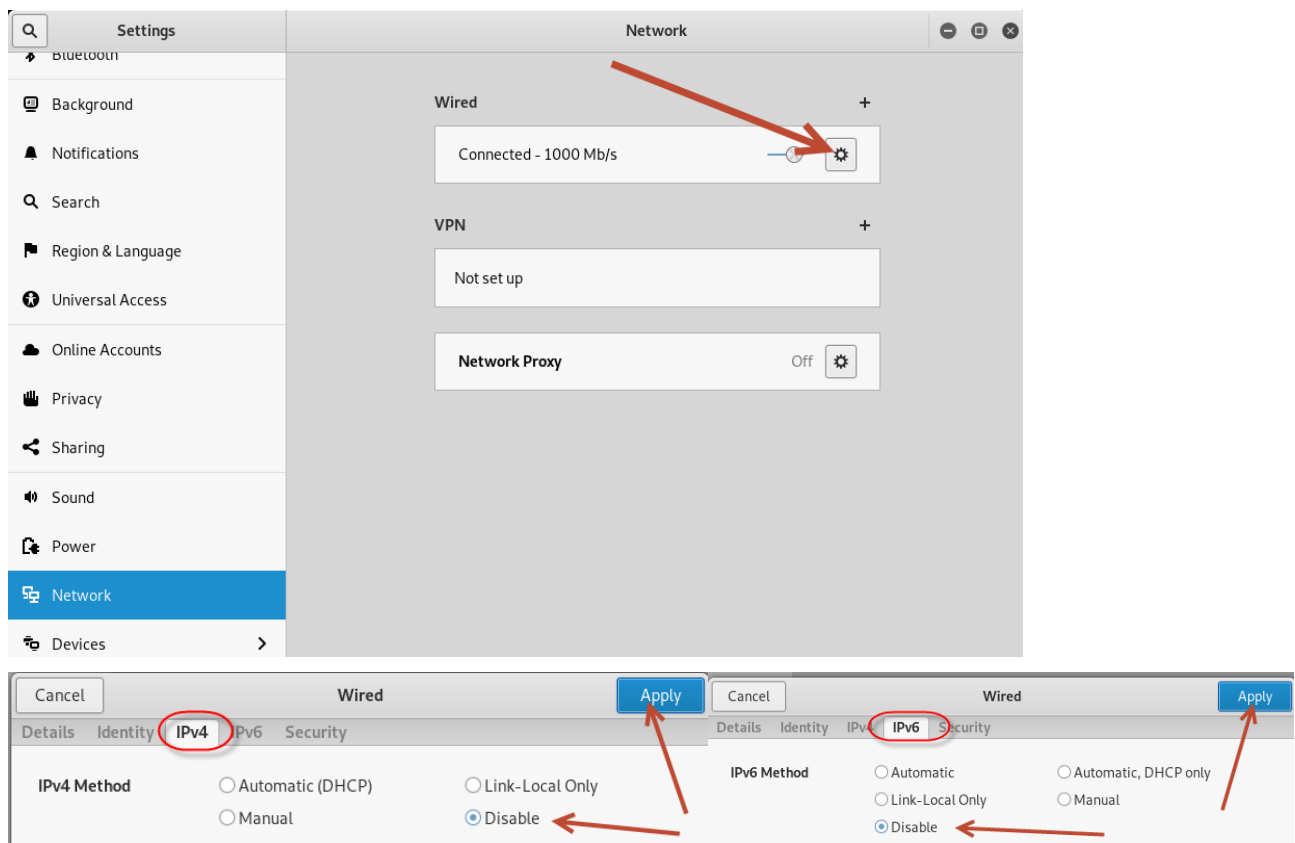
7. Découvrez le nom de votre interface afin de le configurer ultérieurement en client DHCP :

```

root@kali:~# ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
   link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
   inet 127.0.0.1/8 scope host lo
       valid lft forever preferred_lft forever
   inet6 ::1/128 scope host
       valid lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
   link/ether 08:00:27:7c:8e:8e brd ff:ff:ff:ff:ff:ff
   inet 192.168.1.12/24 brd 192.168.1.255 scope global dynamic eth0
       valid lft 3544sec preferred_lft 3544sec
   inet6 fd0c:f2cf:1448:0:fda3:f6ae:ce80:377d/64 scope global noprefixroute

```

8. Désactivez la configuration du réseau graphique. Pour ce faire, allez dans : Settings / Network :



9. Configurez votre carte réseau en client DHCP via la ligne de commande et de façon persistance.

Rebootez et vérifiez votre configuration réseau.

6 Wireshark

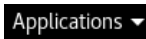
1 Présentation

Wireshark is the world's foremost and widely-used network protocol analyzer. It lets you see what's happening on your network at a microscopic level and is the de facto (and often de jure) standard across many commercial and non-profit enterprises, government agencies, and educational institutions. Wireshark development thrives thanks to the volunteer contributions of networking experts around the globe and is the continuation of a project started by Gerald Combs in 1998.

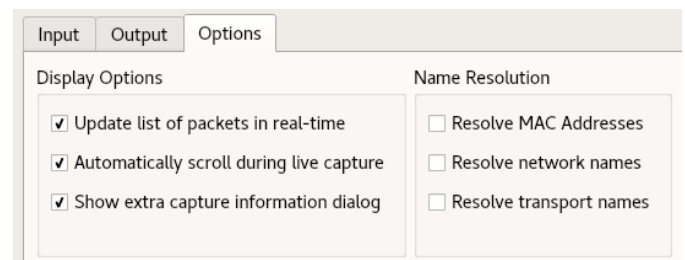
Du site <https://www.wireshark.org/> :

2 Démarrage

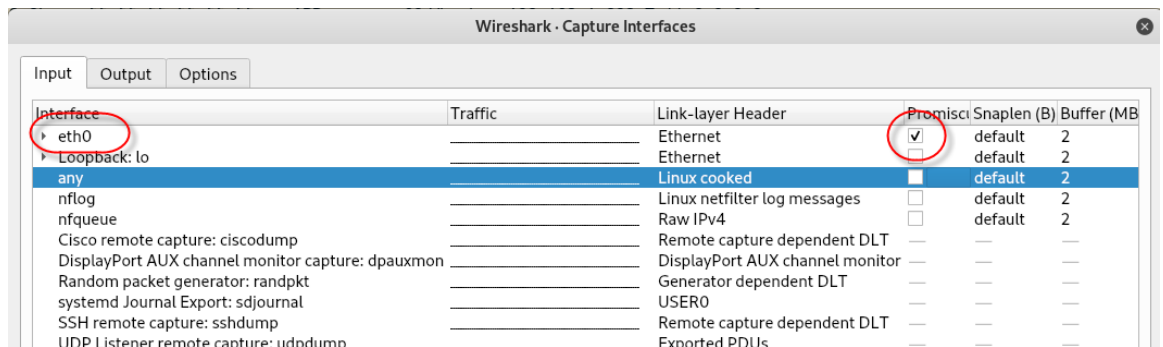
- a) Pour démarrer Wireshark, cliquez sur **Applications** → *Sniffing and Spoofing* → *Wireshark*. Ignorez l'erreur *Lua* si elle apparaît.



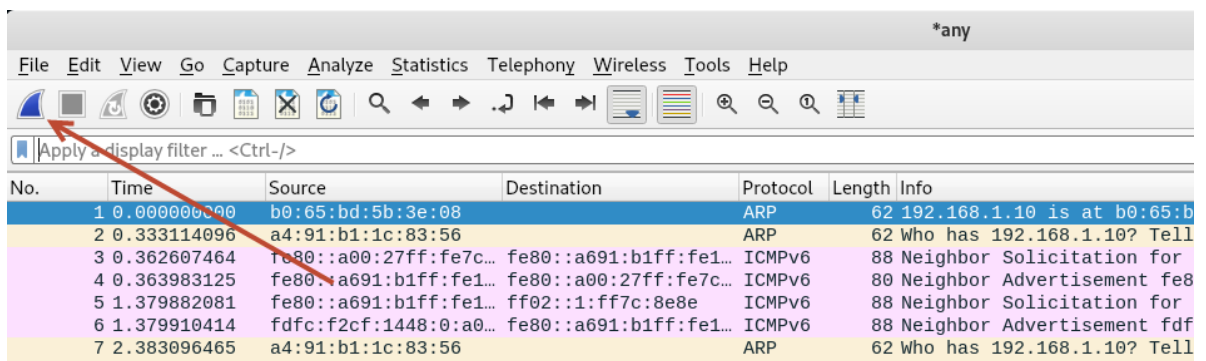
- b) Modifiez les options de capture pour désactiver la résolution des MAC Addresses : **Capture** → **Options** → **Options**

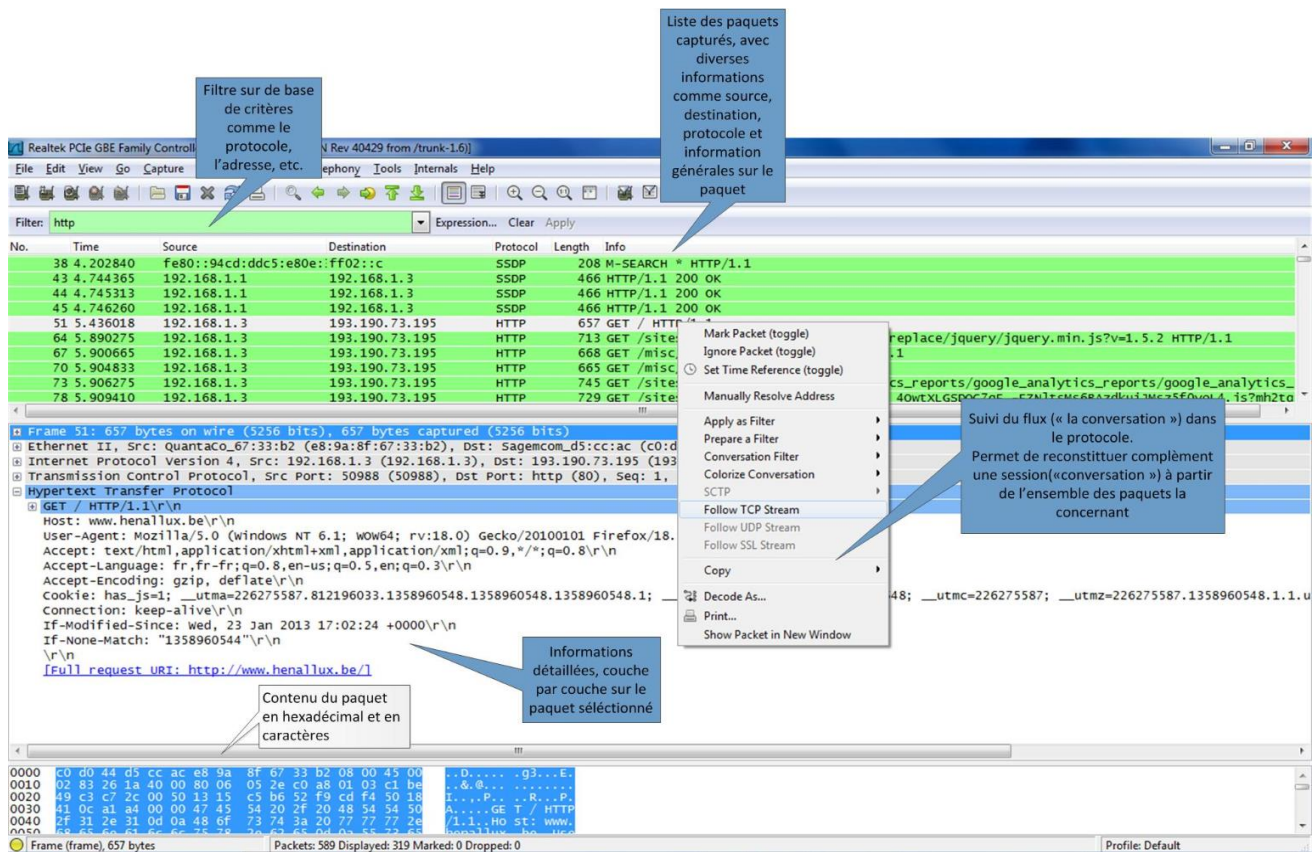


- c) Vous pouvez alors choisir l'interface sur laquelle vous allez écouter :



- d) Et ensuite démarrer votre écoute sur le réseau afin de voir les différents paquets capturés.





7 ARP

1 La cache ARP

- a) Pour afficher la table ARP, tapez simplement la commande `ip neigh show`.

```
root@kali:~# ip neigh show
10.101.210.1 dev eth0 lladdr 00:1a:2f:40:24:c8 REACHABLE
```

- b) Demandez l'adresse IP de la VM de la Kali votre voisin.
 c) Exécutez un ping vers la VM de votre voisin.
 d) Affichez à nouveau la cache ARP, vous devez y trouver la correspondance entre l'IP de votre voisin et sa MAC.

2 Capturez des paquets ARP et ICMP dans Wireshark

- a) Démarrez Wireshark et capturez les paquets de votre interface connectée par pont (sans doute eth0).
 b) Appliquez un filtre permettant de n'afficher que les message ARP.
 Inscrivez **arp** dans le champ *Apply a display filter* : `arp`
 Vous voyez déjà quelques messages, recherchez à quoi ils correspondent.
 c) Effacez la table ARP → `ip neigh flush all`.
 d) Vérifiez que l'IP de votre voisin n'a plus de MAC associée → `ip neigh show`.
 e) Éditez le filtre pour ne capturer que les messages arp ou ICMP (ping).
 → `arp or icmp`
 f) Redémarrez la capture Wireshark sans sauvegarder la précédente →



- g) Relancer un ping vers votre voisin, stoppez la trace et analysez le Wireshark.
- h) Vous pouvez constater le dialogue suivant :
- Un paquet ARP est envoyé en broadcast pour demander qui à l'adresse <IP_voisin>.
 - Votre voisin répond sur votre MAC en spécifiant sa MAC
 - Les ping peuvent alors débuter grâce aux liens entre IP et MAC

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	08:00:27:37:80:5a	ff:ff:ff:ff:ff:ff	ARP	42	Who has 192.168.100.105? Tell 192.168.100.106
2	0.000536357	40:b8:9a:6e:df:89	08:00:27:37:80:5a	ARP	60	192.168.100.105 is at 40:b8:9a:6e:df:89
3	0.000561390	192.168.100.106	192.168.100.105	ICMP	98	Echo (ping) request id=0x0f09, seq=1/256, ttl=64 (reply in 4)
4	0.000974398	192.168.100.105	192.168.100.106	ICMP	98	Echo (ping) reply id=0x0f09, seq=1/256, ttl=128 (request in 3)

- i) Vérifiez à nouveau la table des MAC pour s'assurer que l'information sur votre voisin est à nouveau présente.
- j) Jetez un œil aux informations sur chaque couche présentée par Wireshark en cliquant comme mentionné ci-dessous :

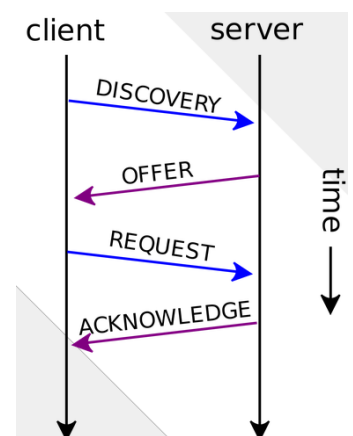
▶ Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
 ▶ Ethernet II, Src: 08:00:27:37:80:5a, Dst: ff:ff:ff:ff:ff:ff
 ▶ Address Resolution Protocol (request)

- k) Demandez à votre voisin l'adresse IP de sa machine hôte (windows) et répétez les étapes c) à i) avec celle-ci. La différence est que le firewall bloque les ping.
- l) Vous pouvez constater que même avec un firewall ICMP echo reply couche 3 (pas de *reply* au *ping*), la MAC est découverte. Selon vous, pourquoi ?
- m) Recommencez l'opération en faisant un ping vers 8.8.8.8.
- Pouvez-vous voir la MAC associée à 8.8.8.8 dans la cache ARP ?
 - Pouvez-vous voir la MAC associée à 8.8.8.8 dans Wireshark ?
 - Si oui ou non, selon vous, pourquoi ?

8 Analyse DHCP

1 Rappel théorique

Une requête DHCP complète comporte plusieurs étapes, comme indiqué sur le schéma ci-contre (voir cours théorique).



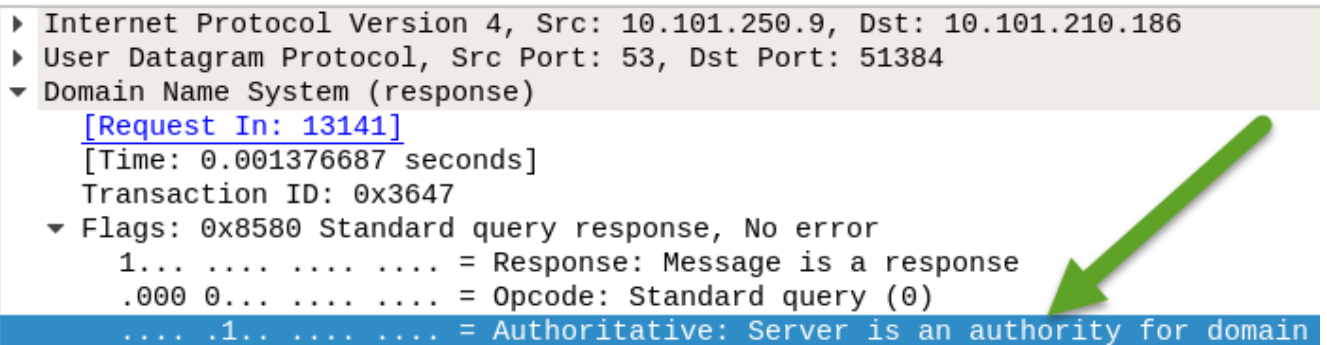
2 Analyse avec Wireshark

- a) Dans un premier temps, informez le serveur DHCP que vous libérez votre adresse → `dhclient -r -v eth0` (-v permet d'afficher les logs).
- b) Démarrez Wireshark et capturez l'interface eth0.
- c) Appliquez le filtre `udp.srcport == 68 or udp.srcport == 67` (attention à bien l'appliquer avec un <ENTER>). Selon vous pourquoi utiliser ce filtre pour mettre en évidence les échanges liés au protocole DHCP ?
- d) Faites une demande au serveur DHCP pour obtenir un nouveau bail → `dhclient -v eth0`.
- e) Analysez la capture Wireshark. Est-elle semblable à la théorie ?

- f) Demandez à nouveau au serveur DHCP de libérer votre adresse et capturez le message dans Wireshark. Quel est-il, à quoi correspond l'adresse IP source et destination ?

9 Analyse DNS

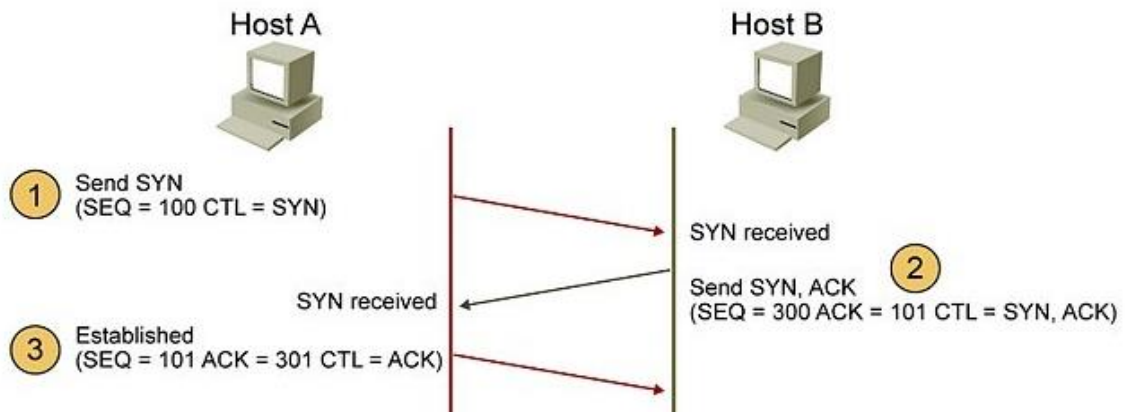
- a) Démarrez une capture Wireshark. Appliquez le filtre **dns**.
- b) En ligne de commande exécuter un nslookup :
`nslookup toto.com`
- c) Comparez le serveur DNS mentionné dans votre *nslookup* et celui spécifié dans les captures Wireshark.
- d) Quel est le port de destination de la requête DNS ? Quel est le port source de la réponse DNS ?
- e) Est-ce en TCP ou UDP ?
- f) Regardez aux champs *Queries* et *Answers* de la requête et de la réponse. Sont-ils présents dans les deux cas ?
- g) Tentez un nslookup vers www.cacahuète.com. Qu'observez-vous dans le *nslookup* et dans le Wireshark ?
- h) Vérifiez la réponse DNS entre un nslookup vers **toto.com** et vers **portail.henallux.be**. Un Flag est modifiable par le serveur DNS pour qu'il puisse spécifier s'il est **autoritatif** pour le nom de domaine ou non.



```
▶ Internet Protocol Version 4, Src: 10.101.250.9, Dst: 10.101.210.186
▶ User Datagram Protocol, Src Port: 53, Dst Port: 51384
▼ Domain Name System (response)
  [Request In: 13141]
  [Time: 0.001376687 seconds]
  Transaction ID: 0x3647
  ▼ Flags: 0x8580 Standard query response, No error
    1... .. = Response: Message is a response
    .000 0... .. = Opcode: Standard query (0)
    .... .1.. .. = Authoritative: Server is an authority for domain
```

10 Session TCP

1 Rappel théorique



Lors de de l'établissement d'une session TCP, les étapes suivantes sont effectuées.

Host A envoie un paquet TCP **SYN**chronize à Host B (SEQ=X)

Host B reçoit **SYN** de A

Host B envoie un **SYN**chronize-**ACK**nowledgement à A (SEQ=Y, ACK=X+1)

Host A reçoit **SYN-ACK** de B

Host A envoie un **ACK**nowledge à B (SEQ=X+1, ACK=Y+1)

Host B reçoit le **ACK**

La session TCP est établie

2 Mise en évidence de l'établissement et de la clôture d'une session TCP à l'aide de Wireshark :

- a) Demandez à votre voisin de configurer le service SSH afin que vous puissiez vous connecter avec l'utilisateur root, et ensuite de démarrer ce service.

```
root@kali:~# nano /etc/ssh/sshd_config
```

Décommentez et modifiez la ligne PermitRootLogin

```
# Authentication:
#LoginGraceTime 2m
PermitRootLogin yes
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10
```

```
root@kali:~# systemctl start ssh
```

- b) Démarrez une capture Wireshark. Appliquez le filtre `ip.addr eq <IP_voisin>`.
- c) Établissez une session `ssh` vers votre voisin → `ssh <IP_voisin>`.
- d) Vérifiez la théorie dans la capture.
- e) Demandez à votre voisin de stopper le service `ssh` :
- ```
root@kali:~# systemctl stop ssh
```
- f) Recommencez la capture et analysez celle-ci.



## 11 Analyse d'une session http

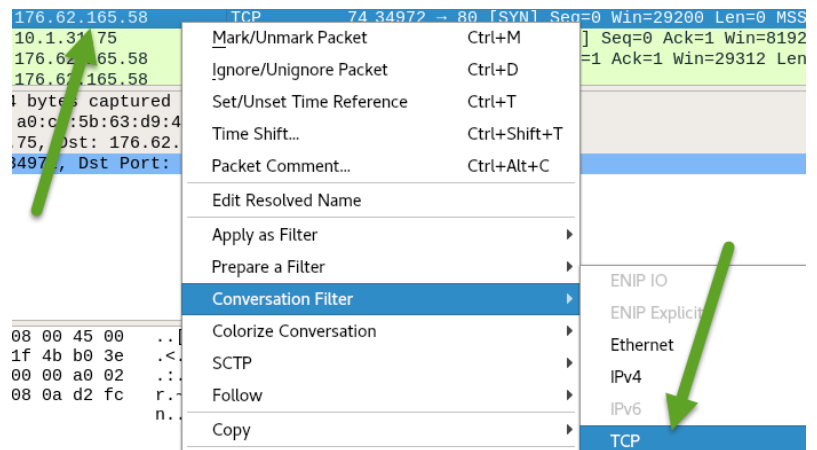
- a) Ouvrez une fenêtre dans FireFox de kali.
- b) A l'aide de nslookup, trouvez l'IP du site [www.this-page-intentionally-left-blank.org](http://www.this-page-intentionally-left-blank.org).
- c) Démarrez une capture Wireshark. Appliquez le filtre `(ip.addr eq <Votre_IP> or ip.addr eq <IP_du_site>) and (tcp or dns)`.
- d) Surfez sur le site [www.this-page-intentionally-left-blank.org](http://www.this-page-intentionally-left-blank.org) et analysez la capture.
- e) Redémarrez Wireshark avec comme filtre `http`.
- f) Surfez sur la page <http://chickenonaraft.com/>.
- g) Remarquez dans la capture Wireshark toutes les informations s'y trouvant :
  - css de la page
  - chanson
  - image
  - texte
  - ...

## 12 Analyse d'une session https

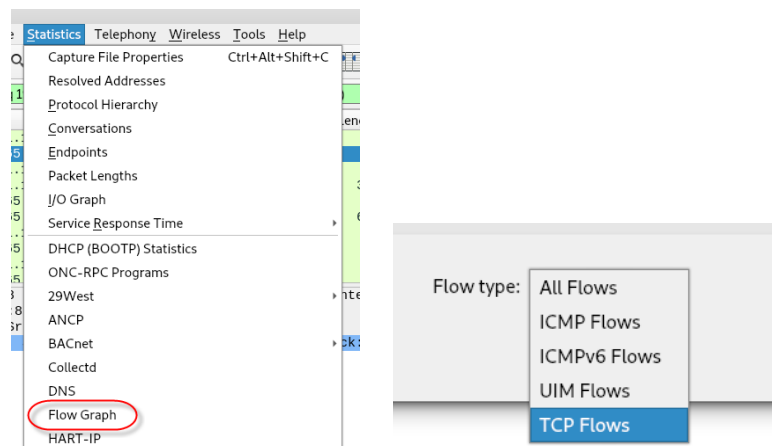
- a) Ouvrez une fenêtre dans FireFox de kali.
- b) Démarrez une capture Wireshark. Appliquez le filtre `tcp.port eq 443`.
- c) Surfez sur le site <https://portail.henallux.be/> et analysez la capture.
- d) Refaites de même sur le port 80 → que pouvez-vous en conclure ?

## 13 Mise en évidence des détails de la négociation TCP et suivi de flux TCP:

- Ouvrez une fenêtre dans FireFox de kali.
- Démarrez une capture Wireshark. Appliquez le filtre `tcp.port eq 80`.
- Cherchez l'IP du site `www.henallux.be` à l'aide de `nslookup`.
- Surfez sur le site `www.henallux.be`. Faites un click droit sur le premier paquet mentionnant l'IP du site WEB → *Conversation filter* → *TCP*.  
Vous ne voyez plus que les paquets liés au flux TCP.



- Ensuite allez dans *Statistics* → *Flow Graph* et choisissez de ne montrer que les paquets filtrés qui sont en TCP.



- Vous pouvez maintenant voir tout le flux TCP de votre session.  
Au début, l'ouverture de la session avec le triple handshake ainsi que la clôture de la session à la fin du flux.

