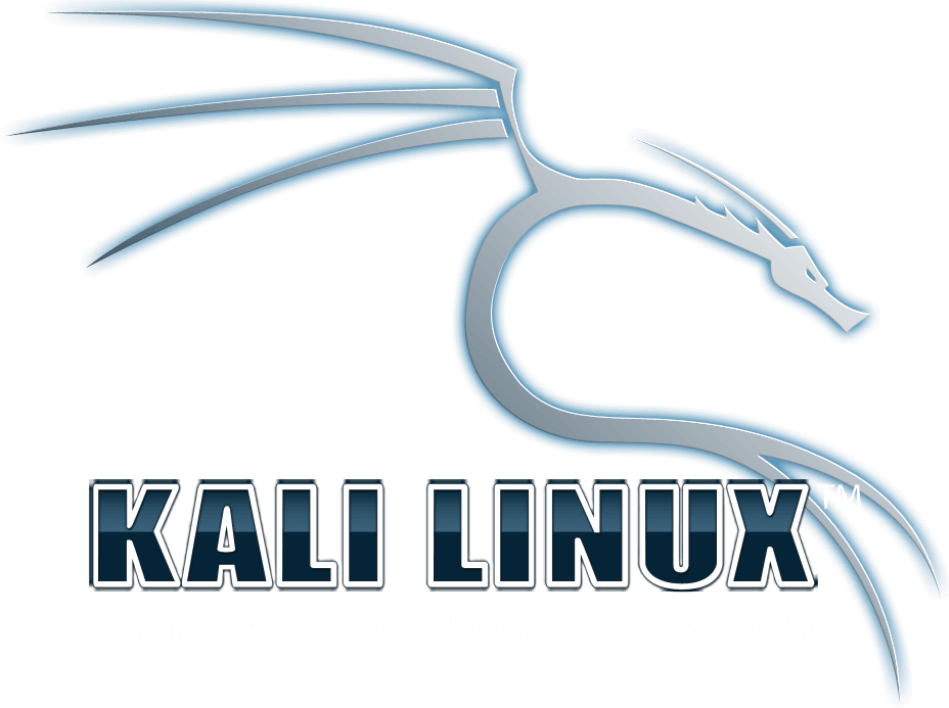
1TI/IR/RT/DA/IA : Réseaux Informatiques : Séance : Analyse réseau – Kali et Wireshark



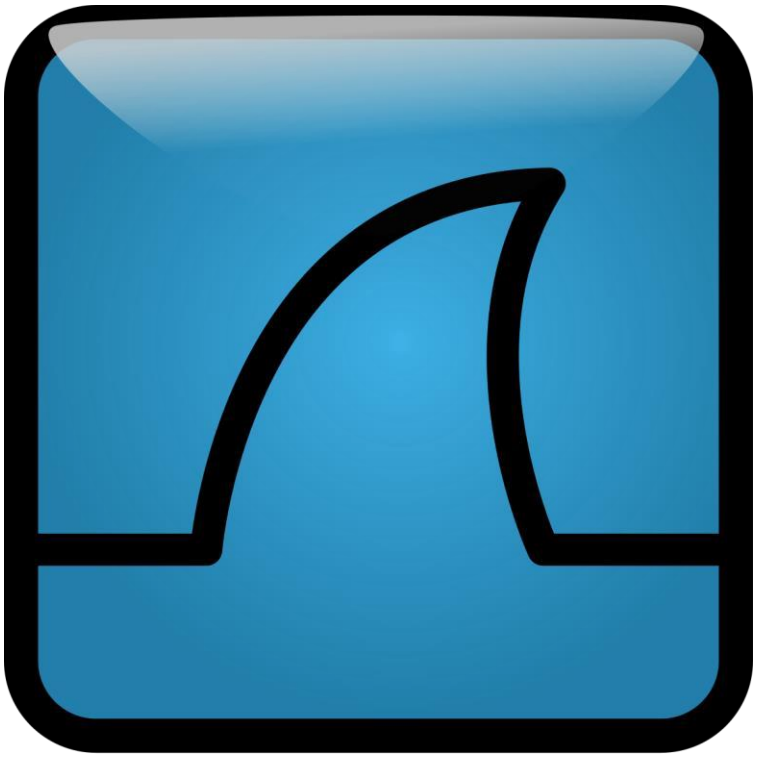


Table des matières

1. Rappels

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

N'oubliez pas de prendre notes !

2. Préparation

Téléchargez une VM préinstallée Kali Linux sur le site : https://www.kali.org/get-kali/#kali-virtual-machines
Choisissez la version 64 bits pour **VirtualBox.**
Le login et le mot de passe par défaut sont **kali/kali.**

3. Objectifs

- Utiliser Wireshark.
- Découvrir ARP.
- Analyse de dialogues DHCP.
- Analyse de dialogues DNS.
- Ouverture de session TCP.
- Analyse des sessions HTTP et HTTPS.

4. Kali Linux

Présentation

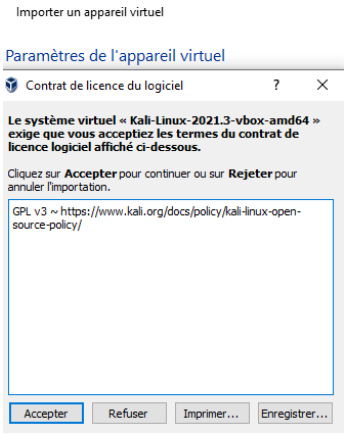
Selon le site officiel[1], Kali Linux est une distribution basée Debian visant à prester des tests de pénétration avancés et des audits de sécurité. Kali détient des centaines d'outils destinées à de multiples tâches de sécurité de l'information telles que les tests d'intrusion, la criminalistique informatique et l'ingénierie inverse. Kali Linux est une solution multiplateforme, accessible et disponible gratuitement pour les professionnels de la sécurité de l'informatique et les amateurs.

La distribution a été publiée le 13 mars 2013 en tant que reconstruction complète de BackTrack Linux respectant entièrement les normes de développement Debian.

[1] https://docs.kali.org/introduction/what-is-kali-linux

Utilisation

1. Téléchargez l'image OVA comme mentionné dans le paragraphe **<u>Préparation</u>**.
2. Importez-la dans VirtualBox en réinitialisant l'adresse MAC. Vous devez **accepter** les termes du contrat de licence logiciel[2].

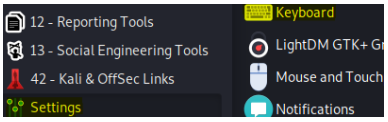


3. Vérifiez que le réseau est bien en **Accès par pont**.
4. Démarrez la VM avec le login et le mot de passe : **kali/kali**.

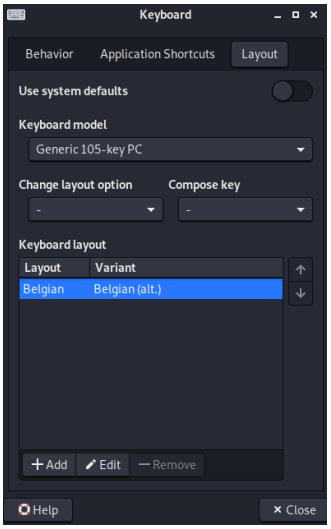
   Attention le clavier par défaut est en QWERTY !

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

Accédez aux Settings et accédez dans **Keyboard :**



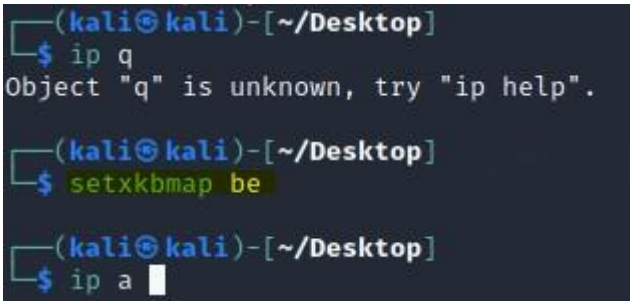
Ajoutez le clavier **Belgian(alt.)** dans **Keyboard Layout** après avoir désactivé le système par défaut. Retirez le clavier par défaut pour arriver à une configuration similaire :



[2] https://www.kali.org/docs/policy/kali-linux-open-source-policy/

Il y a une solution alternative temporaire pour changer le clavier via le terminal.

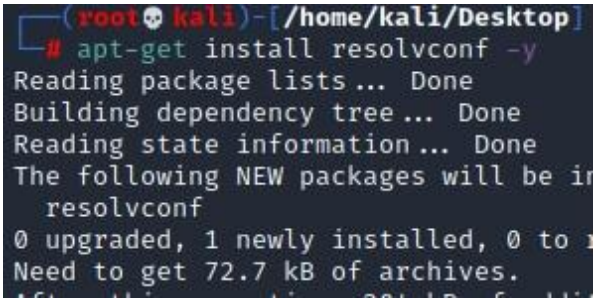
Vous pouvez utiliser la commande ***setxkmap be***.

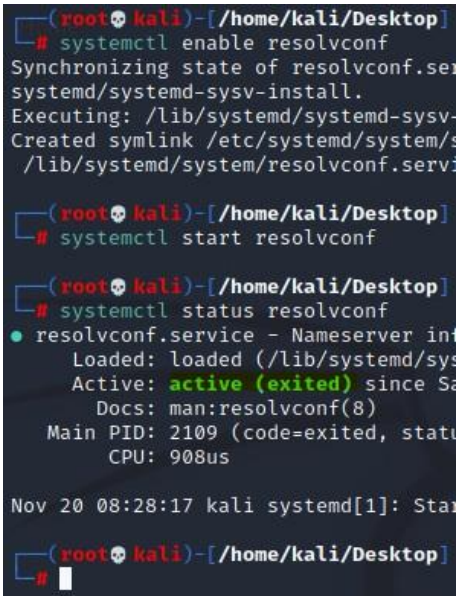


6. Mettez-vous en root avec la commande ***sudo su.***

Installez l'outil **resolvconf** qui vous permettra de prendre en compte la définition de vos serveurs DNS dans votre configuration réseau dans le fichier **/etc/network/interfaces**. Configurez le service resolvconf afin qu'il s'active au démarrage de la machine virtuelle.

N'oubliez pas de procéder à un **update,** afin de mettre les jours la version des paquets/outils, avant d'installer.

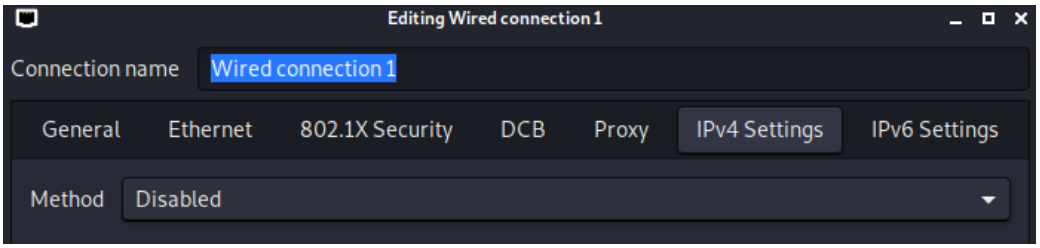




7. Découvrez le nom de votre interface qui vous offre une adresse IP dynamique.

```
┌──(root💀kali)-[/home/kali/Desktop]
└─# ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group def
ault 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 08:00:27:43:73:bc brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.47/24 brd 192.168.1.255 scope global dynamic noprefixroute
 eth0
```

8. Allez dans **Settings/Advanced Network Configuration** et désactivez les méthodes de configuration graphiques IPv4 et IPv6.



9. Configurez votre carte réseau en client DHCP via la ligne de commande et de façon persistante. Rebootez et vérifiez votre configuration réseau.

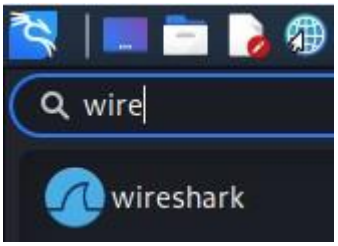
5. Wireshark

Présentation

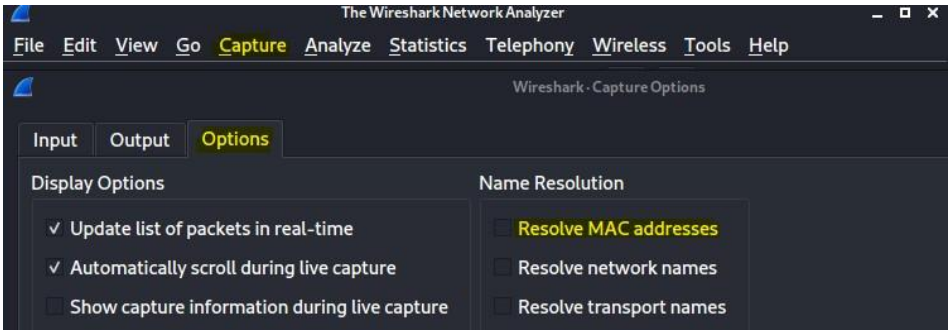
Selon le site https://www.wireshark.org/, Wireshark est l'analyseur de protocoles réseaux le plus utilisé au monde. Il permet de voir ce qui se passe sur votre réseau et il constitue la norme de facto dans de nombreuses entreprises commerciales, ASBL, agences gouvernementales et dans des établissements d'enseignement. Le développement du logiciel est supporté grâce à des contributions volontaires d'experts en réseaux. Il est la continuation d'un projet lancé par Gerald Combs en 1998.

Démarrage

1. Pour démarrer Wireshark, recherchez le logiciel dans les Applications. Ignorez l'erreur LUA si elle apparait.

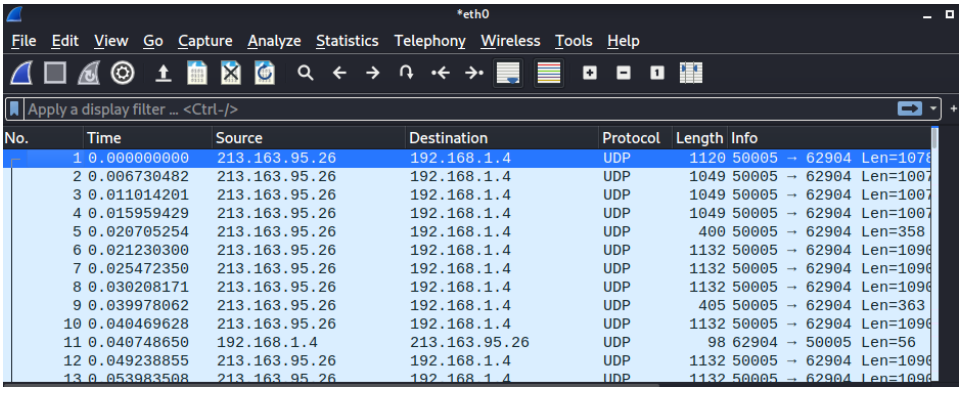


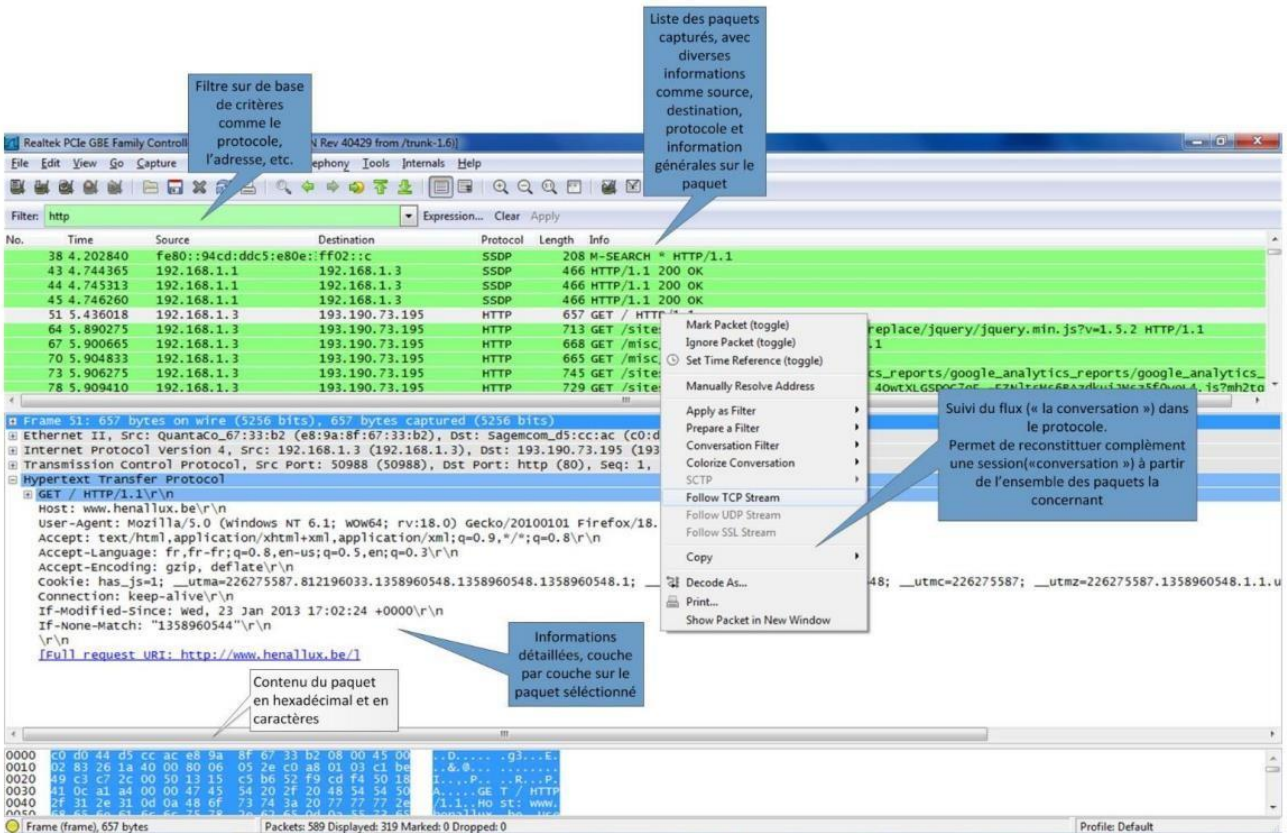
2. Modifiez les options de capture pour désactiver la résolution des adresses MAC :
   Capture → Options → Options



3. Vous pouvez alors choisir l'interface sur laquelle vous allez écouter. Prenez la **eth0** puisque c'est l'interface réseau qui « relie » la VM au reste du réseau.

4. Démarrez l'écoute sur le réseau afin de voir les différents paquets capturés.





6. ARP

Cache ARP

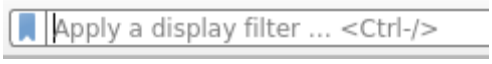
1. Pour afficher la table ARP, tapez la commande ***ip neigh show***

2. Demandez l'adresse IP de la VM de votre voisin et exécutez un ping vers lui.
3. Affichez de nouveau la table ARP, vous devez y trouver la correspondance entre l'IP de votre voisin et son adresse MAC.

Capture de paquets ARP et ICMP dans Wireshark

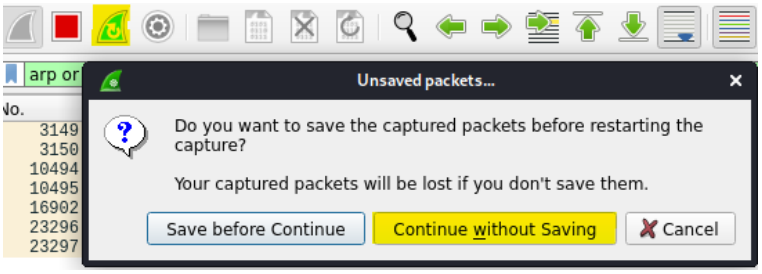
1. Démarrez Wireshark et capturez les paquets de votre interface connectée par pont (sans doute eth0).

2. Appliquez un filtre permettant de n'afficher que les messages ARP. Inscrivez ***arp*** dans le champ *Apply a display filter* :

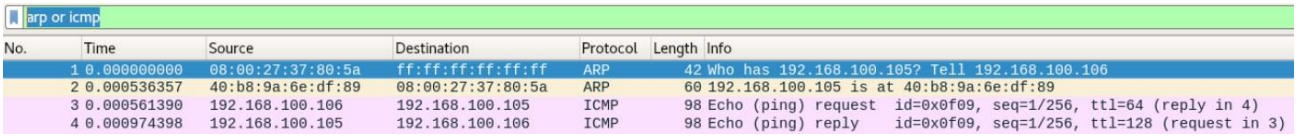


Vous voyez déjà quelques messages. Recherchez à quoi ils correspondent.

3. Effacez la table ARP : ***ip neigh flush all***
4. Vérifiez que l'IP de votre voisin n'a plus de MAC associée : ***ip neigh show***
5. Éditez le filtre pour ne capturer que les messages arp ou ICMP (ping) : arp or icmp
6. Redémarrez la capture Wireshark sans sauvegarder la précédente.



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



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

11. Demandez à votre voisin l'adresse IP de sa machine hôte (windows) et répétez les étapes 3 à 9 incluse. La différence est que le firewall bloque les pings.

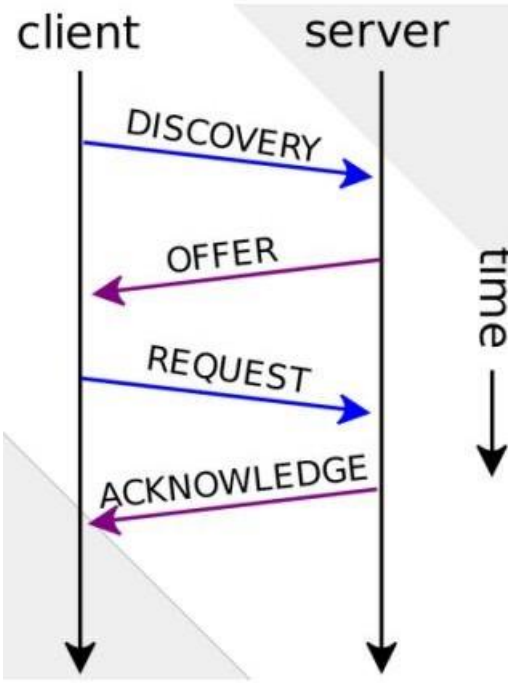
12. Vous pouvez constater que même avec un firewall ICMP echo reply couche 3 (pas de reply au ping), la MAC est découverte. Selon vous, pourquoi ?

13. 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 ?

7. Analyse DHCP

Rappel théorique

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



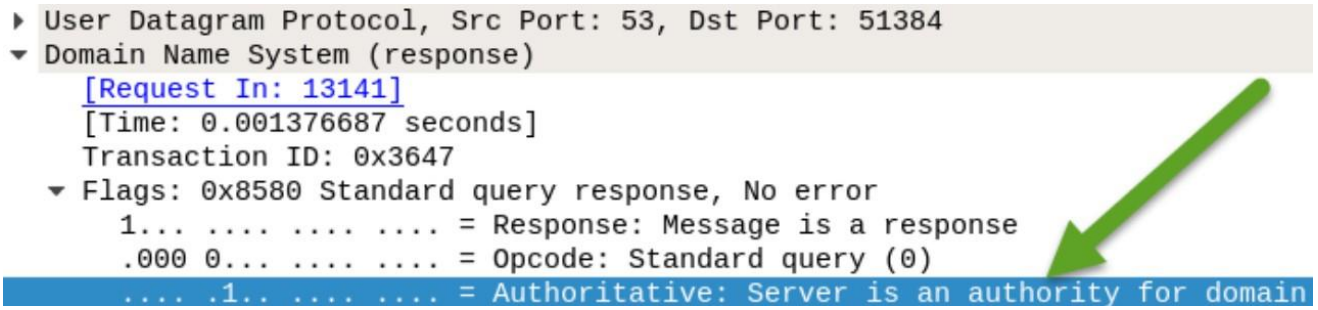
Analyse avec Wireshark

1. Dans un premier temps, informez le serveur DHCP que vous libérez votre adresse ***:***

   dhclient -r -v eth0 (-v permet d'afficher les logs).
2. Démarrez Wireshark et capturez l'interface eth0.
3. 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 ?
4. Faites une demande au serveur DHCP pour obtenir un nouveau un bail : ***dhclient-v eth0***
5. Analysez la capture Wireshark. Est-elle semblable à la théorie ?
6. Demandez à nouveau au serveur DHCP de libérer votre adresse et capturez le message dans Wireshark.
   Qu'en est-il, à quoi correspond l'adresse IP source et l'adresse IP de destination ?

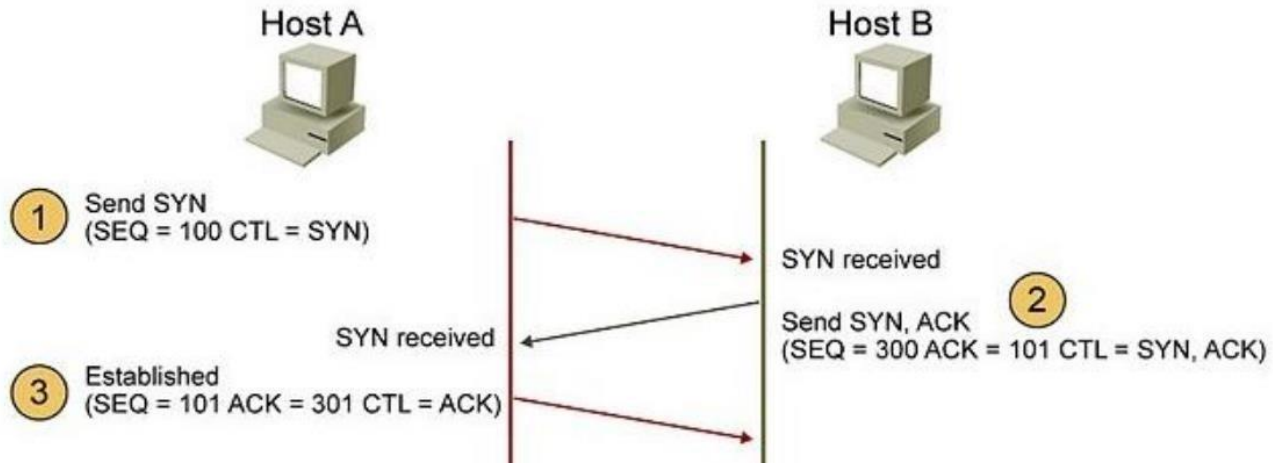
8. Analyse DNS

1. Démarrez une capture Wireshark. Appliquez le filtre **dns**.
2. En ligne de commande, exécutez un nslookup de toto.com.
3. Comparez le serveur DNS mentionné dans votre nslookup et celui spécifié dans les captures Wireshark.
4. Quel est le port de destination de la requête DNS ? Quel est le port source de la réponse DNS ?
5. Est-ce en TCP ou UDP ?
6. Regardez aux champs **Queries et Answers** de la requête et de la réponse. Sont-ils présents dans les deux cas ?
7. Tentez un nslookup vers www.cacahuète.com. Qu'observez-vous dans le nslookup et dans le Wireshark ?
8. 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.



9. Session TCP

Rappel théorique



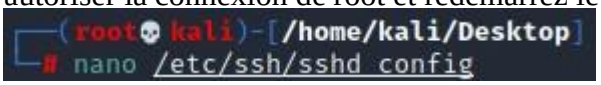
Lors de de l'établissement d'une session TCP, les étapes suivantes sont effectuées.

- 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.

Mise en évidence de l'établissement et de la clôture d'une session TCP via Wireshark

1. Demandez à votre voisin de configurer le service SSH afin que vous puissiez vous connecter avec l'utilisateur **kali**. Il suffira juste de démarrer le service SSH via la commande :

> **Curiosité** : Si vous voulez accéder en SSH avec un utilisateur root. Il faudra démarrer le service mais aussi configurer le fichier **/etc/ssh/sshd_config.** Il suffira de décommenter et de modifier la ligne *PermitRootLogin*.
>
> Cette ligne est par défaut configurée ***prohibit-password.*** Donc root ne peut pas utiliser le service SSH par défaut.
>
> Changez-la en ***yes*** pour autoriser la connexion de root et redémarrez le service SSH.



2. Démarrez une capture Wireshark. Appliquez le filtre **ip.addr eq** <IP_voisin>.
3. Établissez une session SSH vers votre voisin: ssh <IP_voisin>.
4. Vérifiez la théorie dans la capture.
5. Demandez à votre voisin de stopper le service ssh :

6. Recommencez la capture et analysez celle-ci.

10. Analyse d'une session HTTP

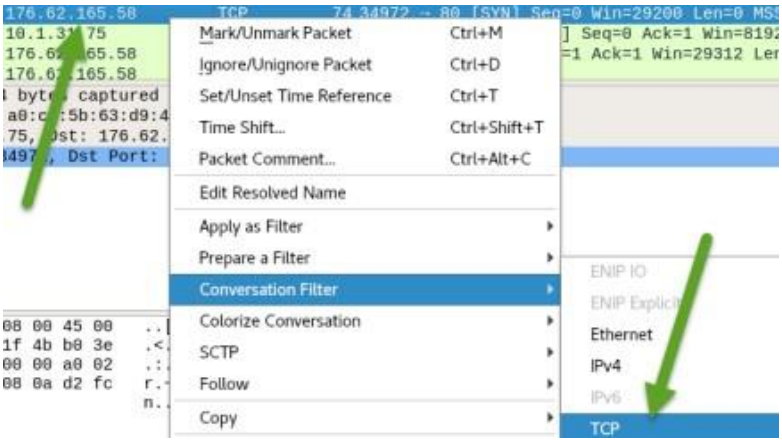
1. Ouvrez une fenêtre dans Firefox de la VM.
2. À l'aide de nslookup, trouvez l'IP du site https://this-page-intentionally-left-blank.org.
3. Démarrez une capture Wireshark en appliquant le filtre :
   (ip.addr eq <Votre_IP> or ip.addr eq <IP_du_site>) and (tcp or dns)
4. Surfez sur le site www.this-page-intentionally-left-blank.org et analysez la capture.
5. Redémarrez Wireshark avec comme filtre *http*.
6. Surfez sur la page http://chickenonaraft.com/.
7. Remarquez dans la capture Wireshark toutes les informations s'y trouvant :
   - CSS de la page ;
   - Chanson ;
   - Image ;
   - Texte ;
   - …

11. Analyse d'une session HTTPS

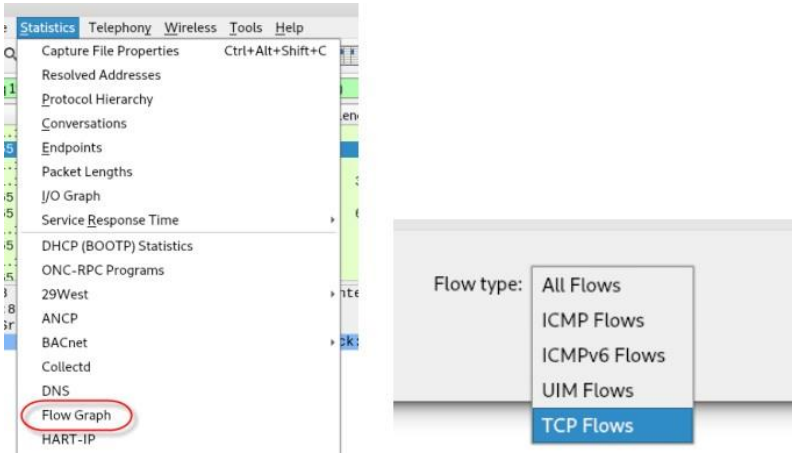
1. Ouvrez une fenêtre dans Firefox de kali.
2. Démarrez une capture Wireshark. Appliquez le filtre *tcp.port eq 443*.
3. Surfez sur le site https://portail.henallux.be et analysez la capture.
4. Appliquez le même filtre mais sur le port 80. Que pouvez-vous en conclure ?

12. Mise en évidence des détails de la négociation TCP et suivi de flux TCP

1. Ouvrez une fenêtre dans Firefox de kali.
2. Démarrez une capture Wireshark. Appliquez le filtre *tcp.port eq 80*.
3. Cherchez l'IP du site www.henallux.be à l'aide de **nslookup**.
4. Surfez sur le site www.henallux.be. Faites un clic 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.



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



6. 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.