Laboratoire 3

1 Durée prévue : 4h00

2 Objectifs

- L'étudiant sera capable d'expliquer l'adressage matériel (MAC ou Ethernet) permettant la communication limitée sur le réseau local Ethernet
- L'étudiant sera à même d'expliquer l'adressage logiques (IPv4 ou IPv6) permettant l'identification des hôtes clients et serveurs sur le réseau Internet.
- L'étudiant pourra repérer les requêtes et les réponses du Domain Name System (DNS) permettant de résoudre les noms FQDN (Fully Qualified Domain Name) en adresse IP.
- L'étudiant devra détailler les étapes de l'établissement de sessions TCP (three way handshake).
- L'étudiant sera à même de comprendre la notion de numéro de séquence utilisée pour l'acquittement des données transmises entre client et serveur.
- L'étudiant saura schématiser les niveaux de protocoles mis en œuvre lors d'une simple requête de page Web.

3 Prérequis

- VM Kali Linux
- Une connexion à Internet à partir de la VM Kali Linux

4 Introduction

Un site WEB est un ensemble de données structurées et organisées, comprenant plusieurs types de médias : texte, image, son, vidéo, etc.

La consultation de ces informations s'effectue par un logiciel, un navigateur WEB. Les données sont en réalité transmises au navigateur, à sa demande, par un serveur WEB. Un site WEB met donc en œuvre une relation client/serveur. Les protocoles principalement utilisés pour échanger des informations entre client et serveur, sont http, HyperText Transfert Protocol et HTTPS, HyperText Transfert Protocol Secure. Secure, signifie sécurité, bien que ce ne soit pas une garantie absolue de sécurité. Les langages les plus utilisés pour la description des contenus du WEB sont le HTML et le XHTML.

Lorsque nous souhaitons consulter un site web, nous commençons par entrer l'adresse du site dans notre navigateur WEB, c'est-à-dire son URL (Uniform Resource Locator).

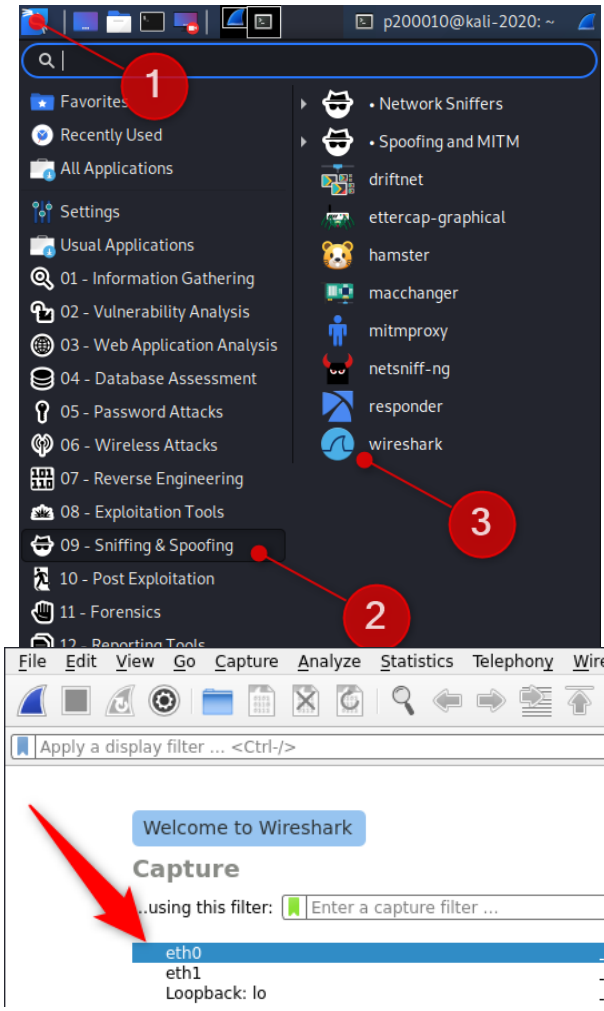
5 Exercice1 - Phase préparatoire

1. Démarrez votre VM Kali Linux et connectez vous avec votre compte créé lors du laboratoire Systèmes d'exploitations.

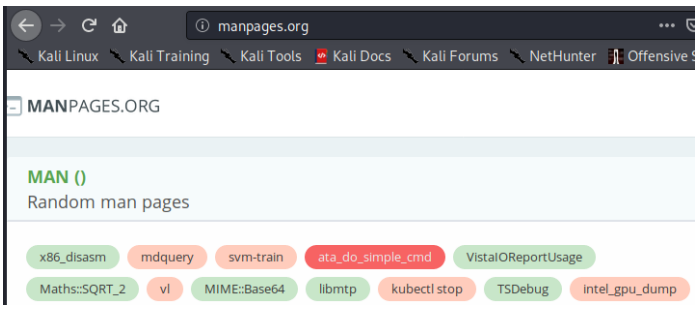
2. Identifiez l'adresse IP et l'interface utilisée sur votre système. En ligne de commande : **`sudo ifconfig`** ou **`sudo ip addr`**
   Normalement, l'interface utilisée pour atteindre internet doit être dans le réseau 192.168.254.0/24

3. Exécutez le logiciel Wireshark sur la VM Kali Linux du laboratoire réseau (09 – Sniffing & Spoofing → wireshark)

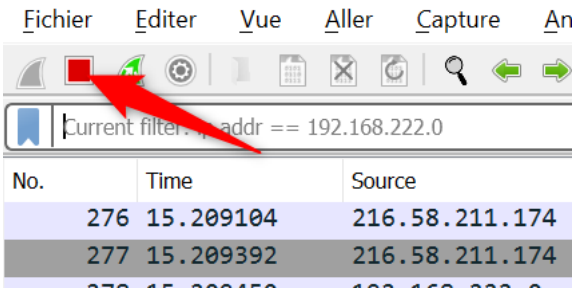
4. Entamez une capture du trafic réseau en double cliquant sur l'interface d'accès vers Internet.
   Dans mon cas, je double-clic sur l'interface eth0.
   Ceci démarre automatiquement la capture des trames sur l'interface sélectionnées.



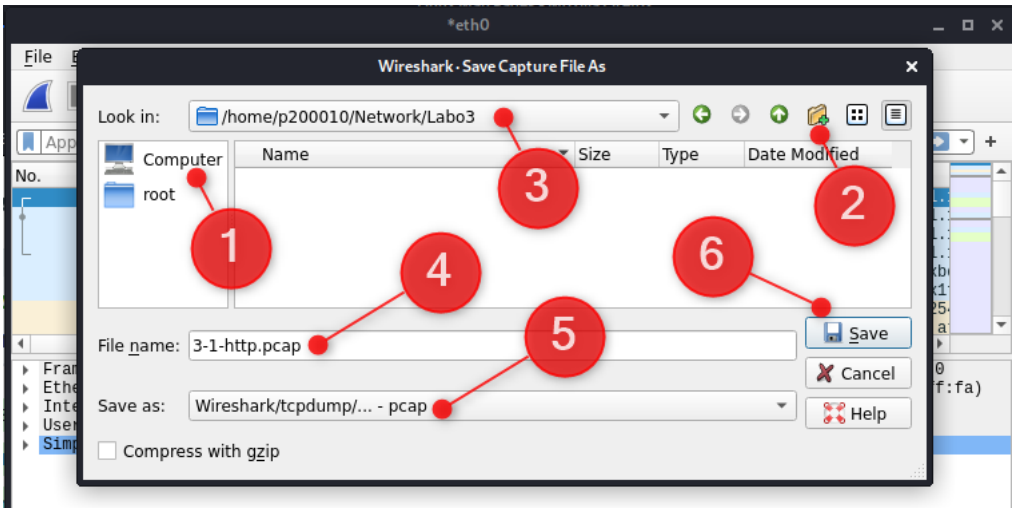
5. Ouvrez votre navigateur WEB préféré et visiter l'URL http://manpages.org directement en tapant celle-ci dans la barre d'adresse.



6. Dès que la page du site manpages.org s'affiche, stoppez la capture du trafic réseau dans Wireshark.



7. Créez un dossier **Network/Labo3** dans votre home directory et sauvegardez-y votre capture de trames sous le nom **3-1-http-manpages.pcap** via les étapes suivantes :
   0. Menu File>Save As… ;
   1. Naviguez jusqu'à votre home directory **/home/eXXXXXXX**;
   2. Via le boutton create new folder,
   3. Créez-y l'arborescence Network\Labo3 ;
   4. Nommez votre fichier **3-1-http**
   5. Sélectionnez le format pcap (pas ngpcap) ;
   6. Cliquez sur Save.



6 Exercice2 – Analyse des données capturées

Vous allez analyser de manière détaillée les différentes phases reprises dans la capture du trafic réseau lors de votre requête vers la page http://manpages.org

Rédigez un document de synthèse en numérotant vos réponses aux questions ci-après. Le document devra comporter une entête renseignant votre nom et prénom, votre groupe classe, ainsi que LABO3 et un pied de page avec le titre du cours « UE01 – Réseaux Informatiques – Labo », ainsi que le numéro de page.

6.1 Identifier les protocoles capturés

1. Quelle est la liste des protocoles indiqués dans la colonne Protocol de la fenêtre de liste des trames capturées ?

   Confirmer que la capture contient bien la séquences des protocoles DNS, TCP et HTTP.

6.2 Les filtres

2. Visitez la documentation des filtres de l'outils Wireshark https://www.wireshark.org/docs/dfref/ et trouvez la syntaxe pour filtrer les trames associées à vos requêtes DNS pour la résolution du nom manpages.org.
   Vous pouvez également vous aider de google pour obtenir la syntaxe du filtre à utiliser.
   Appliquez ce filtre et identifiez les éléments ci-dessous

6.3 Identifier les rôles à partir des adresses

Analysez la trame correspondant au premier message de requête DNS émis par le client Web.

3. Quelles sont les adresses physique (MAC) et IP du client (source) ?

4. Quel est le contenu du champ type de la trame Ethernet ?

5. Quelles sont les adresses physique (MAC) et IP du destinataire ?

6. À quelles machines correspondent ces adresses du destinataire ?

6.4 Repérer les informations de l'en-tête IP

Analysez l'en-tête IP du premier message de requête DNS émis par le client Web.

7. Quelle est la taille de l'en-tête ? Quelle est la longueur totale du paquet ?

8. Repérer le champ «type de protocole» dans l'en-tête. Quel est le type de protocole de la couche transport présent dans les données du paquet ?

6.5 Repérer les informations de l'en-tête UDP

Analysez l'en-tête UDP du premier message DNS émis par le client Web.

9. Quels sont les numéros de ports du client et du serveur ? Quelles sont les particularités de ces valeurs ? Quel est le protocole de couche application présent dans les données du message ?

10. Quelle est la valeur indiquée dans le champ longueur de l'en-tête UDP ? Est-ce qu'elle correspond à l'information donnée dans l'en-tête du paquet IP ?

6.6 Reconnaître la requête posée par le client DNS

Analysez le message de requête DNS émis par le client Web.

11. Quel est le champ qui indique si le message est une requête ou une réponse ?

12. Quelle est l'information présente dans le corps de la requête ? Identifier le type et la classe de la requête.

13. Quel est l'identificateur de transaction de la requête ?

6.7 Caractériser la réponse du serveur DNS

On considère maintenant la réponse à la requête précédente.

14. Quelles sont les adresses physique (MAC) et IP de la réponse DNS ?

    Vérifier que les adresses attendues sont présentes.

15. Quel est le nombre d'octets contenus dans les données du paquet IP ? Pourquoi la quantité de données est-elle plus importante que celle du paquet de requête ?

16. Quel est l'identificateur de transaction de la réponse ? Est-ce qu'il correspond à la requête ?

17. Combien de réponses sont disponibles dans le message de réponse ? Quelle est la signification des valeurs TTL (Time-to-live) ?

18. Pour synthétiser cette partie, faite un croquis des piles de protocoles des couches accès réseau à application pour le client et le serveur DNS. Identifier les adresses, les numéros des protocoles présents dans les en-têtes et les unités de données (PDUs) bout en bout.

6.8 Caractériser l'établissement de la connexion TCP

A l'aide d'un filtres sur l'adresse IP du site visité, repérez la ligne qui correspond au premier segment TCP de l'établissement de connexion en trois étapes (three ways handshake) entre le client et le serveur HTTP.

19. Quels sont les hôtes identifiés par les adresses MAC et IP de cette ligne de capture ? Quelles sont les valeurs des champs type et protocole respectivement attendues pour cette trame et ce paquet ?

    Vérifiez que ces champs et adresses correspondent au rôle de chacun des deux hôtes en communication.

20. Quels sont les numéros de ports utilisés par le client et le serveur ? Quelle est la signification de ces deux valeurs ?

21. Quel est le numéro de séquence choisi par le client ? Quelle est la taille maximale de segment (Maximum Segment Size ou MSS) proposée par le client ?

22. Quelle est la signification de l'indicateur d'état SYN ?

Identifiez la ligne de capture qui correspond au second segment TCP dans l'établissement de la connexion en trois étapes (three ways handshake).

23. Quel est le numéro de séquence choisi par le serveur ? Quelle est la taille maximale de segment (Maximum Segment Size ou MSS) renvoyée par le serveur ?

24. Quelle est la signification des indicateurs d'état SYN et ACK ?

25. Pourquoi le numéro de séquence du client a-t-il été incrémenté à 1 ?

Identifiez la ligne de capture qui correspond au dernier segment TCP dans l'établissement de la connexion.

26. Quelle est la signification de l'indicateur d'état ACK ?

27. Que peut-on conclure sur l'état de la connexion entre le client et le serveur HTTP à partir des deux numéros de séquence ?

28. Pour synthétiser cette partie, réalisez un schéma en flèche de l'établissement d'une session TCP (three ways handshake).

6.9 Caractériser les éléments de la requête HTTP GET

Identifiez la ligne de capture qui correspond au message HTTP GET.

29. Quelles sont les valeurs des numéros de séquence et d'acquittement de l'en-tête TCP ?.

    Vérifiez que tout correspond aux valeurs attendues.

30. Quels sont les indicateurs d'état actifs de l'en-tête TCP ? Expliquer pourquoi.

31. Quelles sont les longueurs de l'en-tête et de la «charge» du message TCP ?

On considère maintenant le contenu du message HTTP GET.

32. Comparez le texte décodé dans la fenêtre d'affichage de la pile de protocoles avec le contenu de la fenêtre d'affichage brut.

    Comptez le nombre d'octets du message et vérifiez que ce nombre correspond au champ longueur de l'en-tête TCP.

33. Quel est le prochain numéro de séquence attendu dans le message suivant émis par le serveur HTTP ?

6.10 Caractériser les éléments de la réponse HTTP

34. Déterminez si le serveur répond avec un message HTTP ou un segment TCP ACK ?

35. Quel est le numéro de séquence émis par le serveur HTTP ? Est-ce qu'il correspond à la valeur attendue ?

On considère maintenant l'en-tête du message réponse HTTP.

36. Quelle est la longueur de la «charge» indiquée dans l'en-tête TCP ?

37. Quels sont les indicateurs d'état actifs de l'en-tête TCP ? Expliquer pourquoi.

38. Quel est le prochain numéro de séquence attendu dans le message suivant émis par le client?

On considère maintenant le corps du message réponse HTTP.

39. Quel est le code dans le message de réponse ?

40. Sélectionnez ce code avec la souris dans la fenêtre d'affichage de la pile de protocoles et comparer avec ce qui est affiché sur la page du navigateur Web.

6.11 Conclusions

41. Listez les trois grandes étapes analysées au niveau du trafic réseau lors d'une requête de page Web.