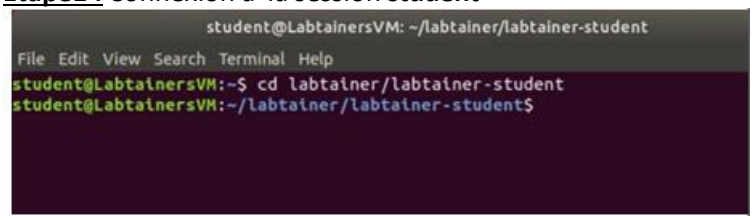
EZES DE SANGHA ANTONY DAN

BTS SIO G2

CYBER-SECURITE
ARP poisoning et Man In The Middle

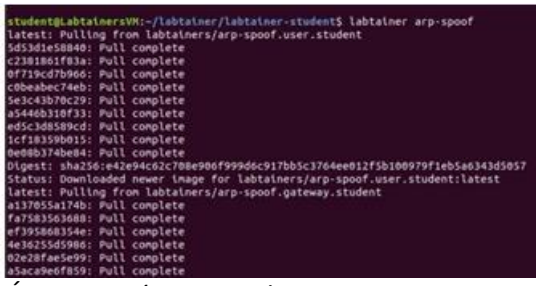
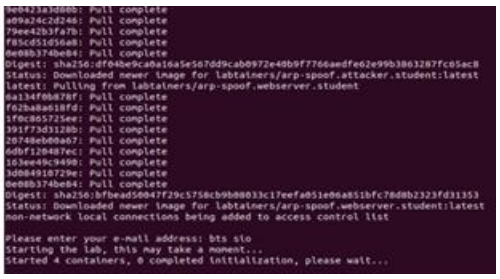
Etape1 : Connexion à la session **student**



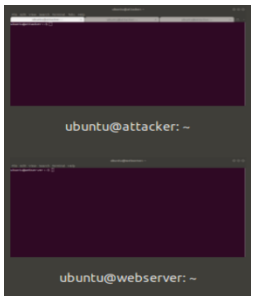
Étape 2 : Démarrer Labtainer

1. Ouvrir le terminal :
   - Accédez à votre terminal ou ligne de commande.

2. Exécuter la commande :
   - Tapez la commande suivante dans le terminal :

Labtainer arp-spoof
```
   - Appuyez sur `Entrée`.







Étape 2 : Démarrer Labtainer

1. Ouvrir le terminal :
   - Accédez à votre terminal ou ligne de commande.

2. Exécuter la commande :
   - Tapez la commande suivante dans le terminal :
     Labtainer arp-spoof
```
   - Appuyez sur `Entrée`.

3. Lancer les systèmes conteneurs :
   - Quatre systèmes conteneurs seront lancés automatiquement.
   - Ces conteneurs sont préconfigurés et reliés entre eux par un réseau virtuel

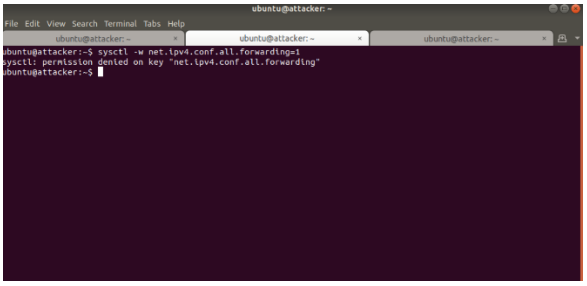


Préparation de l’attaquant

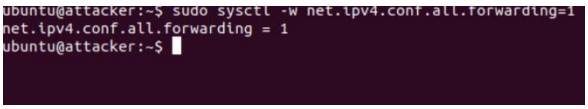
Nous avons tenté d'exécuter la commande `sysctl -w net.ipv4.conf.all.forwarding=1`, mais le système a renvoyé un message d'erreur indiquant :

"Permission refusée sur la clé 'net.ipv4.conf.all.forwarding'".

En d'autres termes, nous avons essayé de modifier une configuration IPv4 sans disposer des autorisations nécessaires. Pour pouvoir exécuter cette commande avec les privilèges de superutilisateur, il est recommandé d'utiliser `sudo` avant la commande.



*Apres avoir entrer la commande voici ce que ça nous donne



Étape 3 : Surveiller le trafic avec Wireshark

1. **Accéder au conteneur "Attacker" :**
   - Assurez-vous que nous êtes connecté au conteneur nommé "Attacker".

2. **Lancer Wireshark pour surveiller le trafic :**
   - Dans le terminal du conteneur "Attacker", tapez la commande suivante :
     wireshark -ki eth0
     ```
   - Appuyez sur `Entrée`.

Explications supplémentaires :

- Wireshark :
  - Wireshark est un analyseur de paquets réseau utilisé pour capturer et inspecter les données circulant sur un réseau en temps réel.
     ```

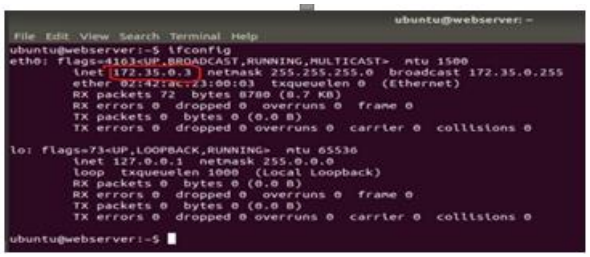
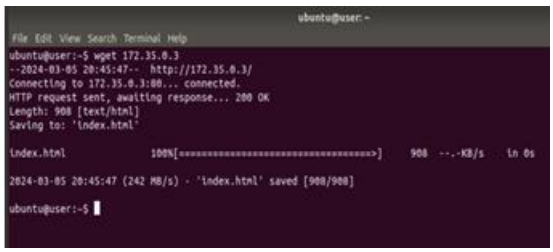
- **Option `-k` :
  - Cette option lance automatiquement la capture de paquets dès le démarrage de Wireshark.
[2]
- **Option `-i eth0` :
  - Cette option spécifie l'interface réseau `eth0` pour la capture des paquets. `eth0` est généralement l'interface réseau principale dans de nombreux conteneurs.

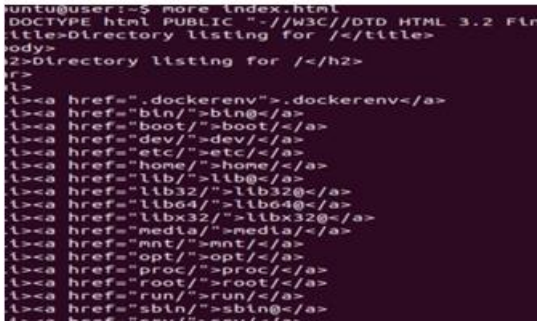
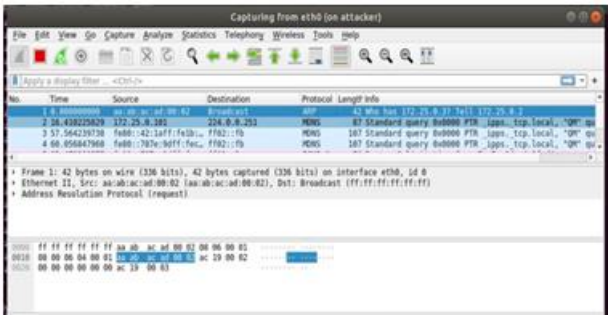
Ces étapes nous permettrons de surveiller et d'analyser le trafic réseau transitant via le conteneur "Attacker" en utilisant Wireshark.

Étape 4 : Solliciter le serveur Web

1. Déterminer l'adresse du Webserver :
  - Depuis le conteneur "Attacker" ou un autre conteneur où nous pouvons analyser le réseau, identifions l'adresse IP du Webserver. Nous pouvons utiliser Wireshark pour inspecter le trafic réseau ou utiliser une commande réseau comme `ifconfig` ou `ip a`.

2. Accéder au conteneur "User" :
  - Assurons-nous que nous sommes connectés au conteneur nommé "User".

3. Effectuer une requête HTTP vers le serveur Web :
  - Dans le terminal du conteneur "User", utilisons la commande suivante pour envoyer une requête HTTP au serveur Web :
    wget <adresse-du-webserver>
    ```
  - Remplaçons `<adresse-du-webserver>` par l'adresse IP que nous avons déterminée pour le serveur Web.

Explications supplémentaires :

- `wget` :
  - `wget` est un utilitaire en ligne de commande pour télécharger des fichiers depuis le web via HTTP, HTTPS et FTP.

- Adresse du Webserver :
  - Il s'agit de l'adresse IP du serveur Web hébergé dans l'un des conteneurs, que nous devons déterminer à l'étape précédente.

En suivant ces étapes, nous serons en mesure de solliciter le serveur Web depuis le conteneur "User" en effectuant une requête HTTP, ce qui nous permettra de tester la connectivité et l'interaction entre les conteneurs.







**Étape 5** : Vérifier le contenu du fichier et analyser le trafic
    ```

1. Vérifier le contenu du fichier `index.html` :
   - Depuis le conteneur "User", nous allons vérifier le contenu du fichier `index.html` récupéré par l'utilisateur. Utilisons la commande suivante :
     more index.html
     ```
   - Cette commande affichera le contenu du fichier `index.html` directement dans le terminal.

2. Vérifier le trafic capturé dans Wireshark :
   - Revenons au conteneur "Attacker" où Wireshark est en cours d'exécution.
   - Analysons le trafic capturé pour confirmer la requête HTTP que nous avons effectuée et pour examiner les réponses du serveur Web.
   - Nous pouvons rechercher les paquets HTTP dans Wireshark pour vérifier les détails de la communication entre le conteneur "User" et le serveur Web.

Explications supplémentaires :

- more index.html` :
  - La commande `more` permet de visualiser le contenu d'un fichier page par page dans le terminal.

- Wireshark :
  - Wireshark nous permet d'analyser le trafic réseau en temps réel. Nous devons rechercher les paquets HTTP pour vérifier les requêtes et réponses échangées entre les conteneurs.

En suivant ces étapes, nous pourrons vérifier le contenu du fichier `index.html` récupéré et analyser le trafic réseau capturé pour mieux comprendre l'interaction entre les conteneurs et la réponse du serveur Web.







**<u>Étape 6</u>** : Exécuter les commandes d'usurpation ARP

1. Ouvrir des sessions supplémentaires dans le conteneur "Attacker" :
   - Nous devons ouvrir deux nouvelles sessions de terminal dans le conteneur "Attacker". Cela peut être fait en utilisant un multiplexeur de terminal comme `tmux` ou en ouvrant simplement deux nouvelles fenêtres de terminal.

2. Exécuter la première commande ARP spoofing :
   - Dans la seconde session du conteneur "Attacker", exécuter la commande suivante :

     sudo arpspoof -t "172.25.0.2" "172.25.0.3"
     ```
   - Cette commande trompe la machine à l'adresse IP `172.25.0.2` en lui faisant croire que l'attaquant est `172.25.0.3`.

3. Exécuter la seconde commande ARP spoofing :

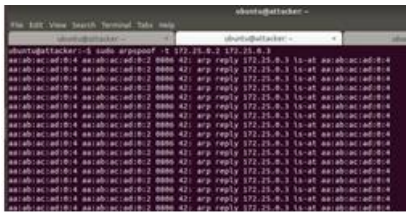
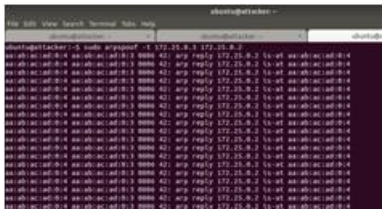
- Dans la troisième session du conteneur "Attacker", exécuter la commande suivante :
  ```bash
  sudo arpspoof -t "172.25.0.3" "172.25.0.2"
  ```
- Cette commande trompe la machine à l'adresse IP `172.25.0.3` en lui faisant croire que l'attaquant est `172.25.0.2`.

Explications supplémentaires :

- `sudo arpspoof` :
  - `arpspoof` est un outil utilisé pour l'usurpation ARP, permettant de rediriger le trafic réseau en trompant les machines cibles au sujet de l'adresse MAC associée à une adresse IP donnée.

- Option `-t` :
  - Cette option spécifie la cible de l'usurpation ARP. La première adresse IP est celle de la machine cible, et la seconde adresse IP est celle que nous voulons usurper.

En suivant ces étapes, nous serons en mesure de configurer l'usurpation ARP entre les deux machines spécifiées, ce qui nous permettra de rediriger et d'inspecter leur trafic réseau.

Étape 7 : Reconnecter au serveur Web depuis le conteneur "User"

1. Accéder au conteneur "User" :
   - Assurons-nous que nous sommes connectés au conteneur nommé "User".

2. Effectuer une requête HTTP vers le serveur Web :
   - Dans le terminal du conteneur "User", utilisons la commande suivante pour envoyer une nouvelle requête HTTP au serveur Web :
     ```bash
     wget <adresse-du-webserver>
     ```
Remplaçons `<adresse-du-webserver>` par l'adresse IP du serveur Web que nous avons déterminée précédemment.

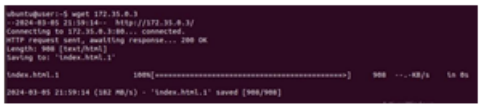
Explications supplémentaires :

- `wget` :
  - `wget` est un utilitaire en ligne de commande pour télécharger des fichiers depuis le web via HTTP, HTTPS et FTP.

- Adresse du Webserver :
  - Il s'agit de l'adresse IP du serveur Web hébergé dans l'un des conteneurs. Cette adresse devrait être la même que celle utilisée lors de l'étape précédente.

-En suivant ces étapes, nous serons en mesure de solliciter à nouveau le serveur Web depuis le conteneur "User" en effectuant une requête HTTP. Cela nous permettra de vérifier si les usurpations ARP mises en place à l'étape 6 affectent la communication entre le conteneur "User" et le serveur

Web.



Étape 8 : Observer le trafic TCP avec Wireshark

1. Accéder au conteneur "Attacker" :
   - Assurons-nous que nous sommes toujours connectés au conteneur "Attacker" où Wireshark est en cours d'exécution.

2. Filtrer le trafic TCP dans Wireshark :
   - Dans Wireshark, nous pouvons appliquer un filtre pour afficher uniquement le trafic TCP. Utilisons le filtre suivant :
   ```
   tcp
   ```
   - Nous pouvons taper ce filtre dans la barre de filtre en haut de la fenêtre Wireshark et appuyer sur `Entrée`.

3. Observer les échanges de paquets TCP :
   - Regardons les paquets capturés pour observer les échanges entre le client légitime (le conteneur "User") et le serveur Web. Nous devrions voir les requêtes HTTP initiées par `wget` ainsi que les réponses du serveur Web.

Explications supplémentaires :

- Filtre TCP dans Wireshark :
  - Le filtre `tcp` nous permet de restreindre la vue aux paquets utilisant le protocole TCP, ce qui facilite l'analyse des communications HTTP.

- Analyse des paquets :
  - En observant les paquets TCP, nous pouvons voir les requêtes et réponses HTTP, identifier les adresses IP source et destination, et vérifier le contenu des paquets échangés.

En suivant ces étapes, nous pourrons utiliser Wireshark pour analyser le trafic TCP capturé pendant les échanges de paquets entre le client légitime (conteneur "User") et le serveur Web. Cela nous permettra de vérifier l'impact des usurpations ARP sur la communication réseau.

Etape 9: Stopper le labtainer Avec la commande **stoplab arp-spoof**

QUESTIONS

Pourquoi l'attaquant n'attend-il pas simplement des requêtes ARP de ces 2 systèmes pour y répondre ?

L'attaquant ne se contente pas d'attendre les requêtes ARP des systèmes ; en envoyant de manière proactive des réponses ARP falsifiées, il peut détourner le trafic plus rapidement et de manière plus fiable à son avantage.

A l'inverse, quelle est la faiblesse du procédé d'envoi de réponses ARP non-sollicitées ?

La principale faiblesse de l'envoi de réponses ARP non sollicitées par l'attaquant est qu'il peut être plus facilement détecté et contrecarré par les systèmes cibles. Ceux-ci peuvent vérifier l'authenticité des réponses ARP reçues et utiliser des techniques d'ARP sécurisé pour identifier ce comportement suspect.

Pour quelle raison l'attaquant envoie une ARP "unsolicited" toutes les secondes, et non pas juste une seule fois ?

L'attaquant envoie de manière répétée des réponses ARP non sollicitées pour conserver durablement le contrôle du trafic réseau, en s'adaptant aux changements et en contrecarrant les mises à jour des tables ARP des systèmes cibles.

D'après vous, comment le switch peut-il s'apercevoir qu'il y a une supercherie ?

Le switch peut détecter la supercherie en analysant les incohérences dans les tables ARP, les comportements anormaux du trafic réseau, et en utilisant des techniques de détection d'attaques ARP implémentées.