|  |  |
| --- | --- |
|  |  |
| **Présentation** | Manipulations de base sur un réseau |
| **Mots-clés** | ARP, TCP, interfaces Ubuntu |
| **Auteur.e(s)** | ReseauCerta, , Naval Postgraduate School |
| **Période de réalisation** | Novembre 2023 |

# Table des matières

[Table des matières 1](#_Toc151496874)

[Contexte de travail 2](#_Toc151496875)

[I. Qu’est-ce qu’un labtainer ? 2](#_Toc151496876)

[II. Le serveur Proxy (serveur mandataire) et ses usages 2](#_Toc151496877)

[III. Les machines labtainer 2](#_Toc151496878)

[Le Labtainer Network Basics 3](#_Toc151496879)

[I. Contexte du labtainer 3](#_Toc151496880)

[II. L’environnement pour le labtainer « network-basics » 3](#_Toc151496881)

[III. L’environnement pour le labtainer « network-basics » 3](#_Toc151496882)

[IV. Compte rendu d’activité 3](#_Toc151496883)

[Les activités du Labtainer Network Basics 4](#_Toc151496884)

[I. Les interfaces des machines 4](#_Toc151496885)

[II. ARP 4](#_Toc151496886)

[III. TCP 5](#_Toc151496887)

[IV. Soumission 6](#_Toc151496888)

# Contexte de travail

## Qu’est-ce qu’un labtainer ?

1. Un labtainer est un environnement (machine virtuelle et TP) mis à disposition par **l'université américaine Naval Postgraduate School**.

Une machine virtuelle avec Ubuntu desktop est fournie ici : <https://nps.edu/web/c3o/virtual-machine-images>

Dans cette machine virtuelle, chaque TP est un "lab" qui télécharge d'autres machines (containers) Docker.

Attention : chaque fois qu’un lab est exécuté pour la première fois, le framework télécharge automatiquement tout ce qui est nécessaire à partir du Docker Hub.

Une connexion internet est nécessaire.

## Le serveur Proxy (serveur mandataire) et ses usages

Le principe du serveur Mandataire (ou Proxy) a été vu dans le labtainer précédent.

Si votre machine se trouve derrière le prox, il doit être configuré.

## Les machines labtainer

1. L’authentification sur la machine virtuelle **labtainer** se fait avec **student**, mot de passe **password123**. Comme la VM est en clavier qwerty, il faudra taper **pqsszord&é** ou **pqsszord123** si vous disposez d’un pavé numérique sur votre clavier.
2. **La dernière version de virtual box (7.0.10 à minima) est conseillée lors de la dernière release de labtainer (septembre 2023) pour ne pas avoir d'erreurs.**

# Le Labtainer Network Basics

## Contexte du labtainer

Cet TP explore les concepts de base du réseau dans un environnement Linux :

* Le fonctionnement du protocole du protocole ARP,
* l’utilisation du ping
* une brève introduction à TCP/IP.

L'utilitaire **tcpdump** est utilisé pour afficher le trafic réseau.

Cet TP fournit un environnement dans lequel il est possible d’observer le trafic généré par les opérations de base du réseau.

Ce laboratoire et ses connaissances sont nécessaires à d’autres exercices de mise en réseau Labtainer. (exemple le laboratoire sur l'usurpation d'identité ARP).

## L’environnement pour le labtainer « network-basics »

Cet atelier s'exécute dans le Framework Labtainer, disponible sur http://nps.edu/web/c3o/labtainers.

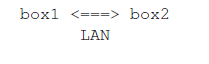
Ce site comprend des liens vers une machine virtuelle prédéfinie sur laquelle Labtainers est installé, mais Labtainers peut être exécuté sur n'importe quel Linux hôte qui prend en charge les conteneurs Docker.

Depuis votre répertoire labtainer-student, démarrez le laboratoire en utilisant :

**labtainer network-basics**

## L’environnement pour le labtainer « network-basics »

Ce laboratoire comprend deux ordinateurs en réseau : box1 et box2.



Les deux ordinateurs sont connectés via un réseau virtuel que vous pouvez traiter comme un seul câble Ethernet reliant les deux ordinateurs.

Lorsque le laboratoire démarre, vous verrez deux terminaux virtuels, un connecté à chaque ordinateur.

Ce laboratoire est conçu pour se concentrer sur Les adresses IP et les interfaces réseau.

## Compte rendu d’activité

**Pendant et à la fin du labtainer, vous devez rédiger un compte rendu d’activité qui comprend :**

* **La mise en place de la machine dans Virtual box,**
* **L’installation de la machine,**
* **Les paramétrages pour le Proxy,**
* **Les configurations effectuées avant sa réalisation,**
* **Les commandes utilisées et leur rôle**
* **L’analyse du résultat du labtainer.**

**Des copies d’écran peuvent être bienvenues.**

# Les activités du Labtainer Network Basics

## Les interfaces des machines

**Utilisez cette commande : adresse IP sur les deux ordinateurs pour vous familiariser avec les interfaces réseau.**

**ip addr**

**Quel est le résultat obtenu ?**

**Nous nous concentrons sur la 2ème entrée dans chaque affichage de la commande ip addr, c'est-à-dire les entrées eth0.**

#### ****L’adresse Physique****

**La valeur link/ether, (par exemple un résultat tel que 02:42:ac:00:00:03) est l'adresse MAC, de l’interface réseau, qui apparaît dans les en-têtes des paquets Ethernet.**

**Souvent, les adresses MAC sont liées au matériel physique, par exemple une interface Ethernet. Mais dans ce laboratoire, le réseau est virtuel, tout comme les adresses MAC sont virtuelles.**

#### ****L’adresse logique****

**L'autre adresse intéressante est étiquetée inet, (par exemple 172.0.0.3/24).**

**C'est l'adresse IPv4 qui apparaît dans les en-têtes des paquets IP.**

**Dans cet exemple, le /24 nous indique que le sous-réseau associé à cette interface est 172.0.0 et l'adresse de l'ordinateur sur ce sous-réseau est le numéro 3.**

**La valeur qui suit la barre oblique vous indique comment de nombreux bits de l'adresse IP de 32 bits sont alloués pour nommer le sous-réseau.**

**Les bits restants sont utilisés pour nommer le périphérique sur le sous-réseau.**

**Les adresses IP décrites ci-dessus permettent aux ordinateurs de se reconnaître ente eux et ainsi de communiquer.**

**Cependant, au niveau de la couche la plus basse, c'est-à-dire la couche liaison qui communique directement avec le support physique ou virtuel, les adresses MAC sont utilisées pour communiquer.**

**Il doit donc exister un moyen de traduire les adresses IP en adresses MAC.**

## ARP

#### ****Tester le protocole ARP****

**Le protocole ARP (Address Resolution Protocol) est utilisé pour mapper les adresses IP aux adresses MAC. Sur la box2, taper la commande**

**Arp -a**

**Quel est le résultat obtenu ?**

Cette commande permet d’afficher le mappage actuel. Notez que rien ne s'affiche car la table ARP est vide.

Quand nos deux ordinateurs démarrent pour la première fois, ils ne connaissent pas les adresses MAC de chacun.

Sur box1, démarrez le programme tcpdump afin de pouvoir observer le trafic réseau :

**sudo tcpdump -vv -n -e -i eth0**

**Les options de Tcpdump sont les suivantes**

**-vv** – Fournit une sortie détaillée

**-n** – n'effectue pas de recherche DNS inversée (**nslookup**) et affichez uniquement les adresses IP.

**-e**  Affiche les adresses MAC Ethernet.

**-i eth0** Affiche le trafic sur l'interface eth0.

Vous remarquerez peut-être qu’une partie du trafic affiché n'est pas lié aux actions que vous effectuez (exemple, « sollicitation de routeur »). paquets ou paquets de flux. Ignorez-les.

Sur la BOX2, utilisez la commande ping pour envoyer un ping à box1

**ping 172.0.0.2 -c 2**

Observez le trafic dans tcpdump. Vous devriez voir la requête ARP de la Box2 demandant l'adresse MAC de celui qui gère le trafic vers l’adresse IP box1.

Notez que l'adresse MAC de destination dans la requête ARP est **ff:ff:ff:ff:ff:ff.**

Il s’agit d’un message diffusé et vu par chaque interface Ethernet du réseau local.

Et la réponse ARP de box1 apparaît. Une fois que les deux cases associent les adresses IP aux adresses MAC, elles peuvent échanger des paquets de couche réseau.

Dans ce cas, vous verrez les paquets ICMP. Le premier paquet est un est **ICMP echo reply** envoyé par la box1.

**ctrl-c** permet de sortir du t**cpdump** sur box1. Utilisez la commande **arp -a** sur les deux box pour afficher le contenu actuel de la table ARP.

Ces entrées ARP permettent aux deux BOX de s'adresser sans répéter la demande/réponse ARP.

**Quel est le résultat obtenu ?**

#### ****Faire confiance aux réponses ARP****

L'utilisation d'ARP pour mapper des adresses IP sur des adresses MAC nécessite un certain niveau de confiance.

Lorsqu'une BOX demande : “to which MAC address should I send packets for this IP address?”

( à quelle adresse MAC dois-je envoyer des paquets pour cette adresse IP ?, C’est faire confiance au fait que la bonne BOX va répondre.

#### ****Communiquer au-delà du sous-réseau****

Vous avez observé comment ARP permet aux ordinateurs d'un sous-réseau commun de communiquer en utilisant des adresses IP. mappés aux adresses MAC.

Mais qu’en est-il des ordinateurs qui ne partagent pas de sous-réseau ?

Ce type de communication nécessite l'utilisation de paquets « fowarding and routing », au travers, par exemple, d’une passerelle.

## TCP

Dans cette section, nous examinerons brièvement certains paquets IP au sein d'une session TCP, en particulier la méthode du “**three way handshake**” (Le principe de la synchronisation des échange au niveau du protocole TCP se nomme « handshake » ou la poignée de main en trois temps de TCP)

Redémarrez le **tcpdump** sur box1, cette fois sans l’option **-e**:

**sudo tcpdump -vv -n -i eth0**

Ensuite, sur box2, lancez une session ssh vers box1. Nous ne finaliserons pas réellement la connexion, nous souhaitons simplement regarder en début de séance :

**Ssh 172.0.0.2**

Il en résulte des paquets IP qui incluent **proto TCP,** ce qui nous indique que le protocole TCP est utilisé.

#### Premier échange TCP

Les informations d'adresse dans le premier paquet, montrent ceci :

**172.0.0.3.34104 > 172.0.0.2.22**

Ce qui indique que le paquet est envoyé depuis BOX2.

Le numéro à la fin de l'adresse BOX 2 ***(*34014)** représente un numéro de port TCP éphémère qui sera utilisé pour la session.

Le numéro à la fin de l'adresse de l'adresse BOX1 est **22**, représente le numéro de port utilisé par le protocole **ssh**.

Les valeurs Flags entre parenthèses sur le premier paquet sont **[S],** ce qui indique qu'il s'agit d'un paquet **SYN**, c'est-à-dire la première étape des trois échanges de paquets ‘handshake » de prise de contact qui initie une session TCP.

#### Second échange TCP

Le 2ème paquet va de la BOX1 à la BOX2. Notez les numéros de port.

Les drapeaux sur le deuxième paquet sont **[S.],** qui indique un paquet **SYN-ACK**, c'est-à-dire le 2ème paquet de la poignée de main (Handshake).

#### Troisième échange TCP

Le troisième paquet complète le poignée de main avec un **ACK** envoyé de box2 à box1.

A noter les champ des « Indicateurs » est simplement un point, qui ne reflète aucun indicateur.

**seq 1, ack 1,** dans ce troisième paquet reflète l’accusé de réception et que le numéro de séquence de la session TCP commence à 1.

Cela termine le « handshake ».. Les paquets suivants font partie d'une session connectée (fiable) dans laquelle le protocole TCP garantit que les paquets ne sont pas perdus et sont disposés dans le bon ordre pour être livrés aux applications : ici un client SSH et un serveur SSH.

La notion de paquets perdus est peu probable dans le cas des deux BOX présentées ici.

Ce qui n’est pas le cas des échanges sur la toile mondiale qu’est internet.

## Soumission

Une fois l'atelier terminé, retournez dans le terminal de votre système Linux utilisé pour démarrer l'atelier et saisissez :

**stoplab**

Lorsque vous arrêtez l'atelier, le système affiche un chemin d'accès aux résultats de l'atelier compressés sur votre système Linux.

Mettre une copie du contenu de ce fichier dans votre compte rendu d’activité

Ce laboratoire a été développé pour le cadre Labtainer par la Naval Postgraduate School, Center for Cybersécurité et cyberopérations dans le cadre du prix n° 1438893 de la National Science Foundation. l’œuvre est dans le domaine public mais ne peut être reproduite.