M3102-- TP 1

Préambule

Premièrement il faut configurer votre machine.

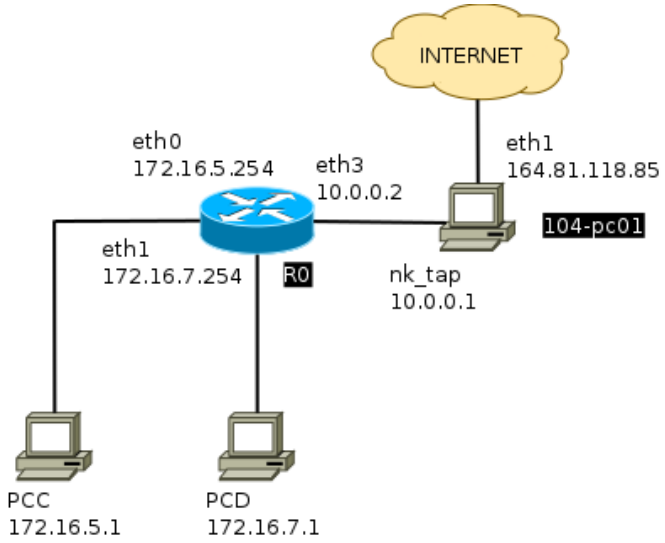
Après d'avoir bien configuré votre machine, assurez-vous de la bonne configuration de votre VM en utilisant la commande ifconfig. Vérifiez le routage en faisant un ping vers l'adresse 8.8.8.8. Finalement, faites un ping vers www.google.fr.

Si une de ces vérifications ne marche pas, alors faites les modifications nécessaires pour assurer un bon fonctionnement de la VM. Passez ensuite au prochain exercice.

Exercice I : Création et configuration d'un lab Netkit

L'installation de Netkit, ainsi que sa configuration, ont déjà été effectuées sur la VM que vous utilisez. Pour utiliser Netkit sur une autre machine vous pouvez faire l'installation tous seuls en aillant sur : https://netkit-ng.github.io/

On travaillera sur le réseau vu en CM, mais en commençant par la version limitée ci-dessous :



1. Commencez par récupérer le lab netkit correspondant au réseau ci-dessus sur la machine enseignant 164.81.118.124 (ou 144.81.118.61 en 105) en utilisant le navigateur de votre VM. Décompressez l'archive (en tant qu'utilisateur ***iut***) à l'aide de la commande suivante :

```
$ tar -xf M3102_lab_TP1.tar
```

Placez vous alors dans le dossier ***M3102_lab_TP1*** ainsi créé, et lancez le lab à l'aide de la commande `lstart` (toujours en tant qu'utilisateur ***iut***).

2. Assurez-vous maintenant que le lab a correctement démarré en vérifiant :
   - les interfaces et les adresses IP présentes sur **R0**:

     commande : _____

     résultat : _____

   - les interfaces présentes sur les deux autres machines :

     commande : _____

     résultat sur PCC : _____

     résultat sur PCD : _____

   - la nouvelle interface créée sur la machine physique :

     commande : _____

     résultat : _____

3. Vérifiez que la configuration IP de **R0** (coté Internet) est correcte en contactant successivement (et en corrigeant l'éventuel problème à chaque étape) :
   - le réseau local :

     commande : _____

     résultat : _____

   - une machine hors du réseau local :

     commande : _____

     résultat : _____

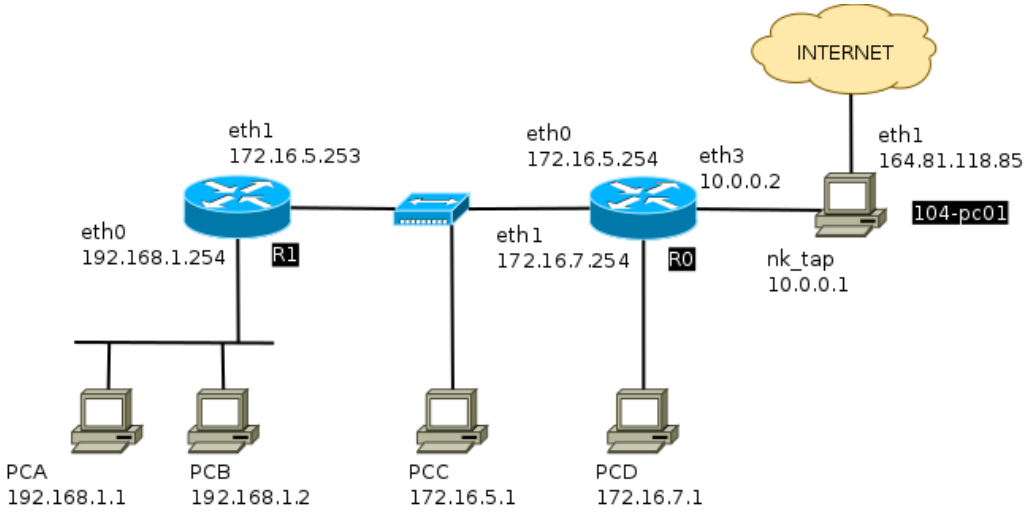
   - une machine distante via son nom :

     commande : _____

     résultat : _____

Exercice II : Lab étendu et le routage

Dans cet exercice nous allons étendre le lab de l'exercice précédent. Le but serait d'avoir un réseau qui correspond à celui de la figure ci-dessous.



1. Modifiez maintenant la structure de votre lab de manière à ce qu'il corresponde au réseau ci-dessus. Vous placerez le fichier ***interfaces*** adéquat dans le dossier de **PCB**, de manière à pouvoir l'utiliser pour configurer la machine.

2. Créez alors un fichier ***.startup*** pour les machines **PCA** et **PCB**. Celui de **PCA** contiendra la configuration IP complète, tandis que celui de **PCB** chargera le fichier ***interfaces*** mis en place à la question précédente.

   Démarrez alors les machines supplémentaires à l'aide de la commande `lstart`.

3. Mettez maintenant en place sur **R0** la route lui permettant de joindre le réseau contenant **PCA** et **PCB**. Vérifiez que le routage est activé sur **R1**, puis vérifiez la connectivité entre **R0** et **PCA**/**PCB**.

   Quelle est la commande à utiliser pour assurer le routage ?

   Et pour vérifier la connexion ?

4. A ce point les machines PCC et PCD devrait pouvoir joindre la machine physique, mais pas inversement. Vérifiez ceci. Quel est le message d'erreur obtenu ?

5. Mettez maintenant en place la route permettant à la machine physique de répondre à **PCC** et **PCD**. Vérifiez que ces deux machines ont maintenant accès à Internet.

   Commande utilisée :

6. Faites en sorte que **PCA** et **PCB** aient également accès à Internet.

   Commande utilisée :

Exercice III : Etude de services

Dans cette dernière partie, vous allez utiliser `tcpdump` et le réseau créé sous Netkit pour étudier certains services.

1. Lancez une capture, cette fois sur la machine **PCB** et sur la machine **R0** (interface en 172.16.5.254), en précisant que vous souhaitez observer le trafic de type ICMP :

   ```
   $ tcpdump -i eth0 -e icmp
   ```

2. Lancez alors un ping sur la machine **PCA** à destination de **PCC**. Quelle différence observez-vous entre le message *ICMP request* capturé par **PCB** et celui capturé par **R0** ? Pourquoi ?

3. Créez un nouvel utilisateur nommé iut sur la machine **PCB** et attribuez-lui le mot de passe iut :

   ```
   # adduser iut
   ```

4. Créez alors un fichier de votre choix dans le home directory de ce nouvel utilisateur. Toujours sur la machine **PCB**, démarrez alors le service ***proftpd*** et vérifiez qu'il est bien à l'écoute.

   - Commande pour le démarrage : _____
   - Commande pour la vérification : _____
   - Résultat obtenu :

5. Lancez une capture de trames sur la machine **PCB** (coté 192.168.1.2) avec les options suivantes qui permettent de sauver les trames capturées dans le fichier *ftp.pcap* :

```
tcpdump -i eth0 -s 0 -w /hostlab/ftp.pcap
```

6. Connectez-vous alors depuis la machine **PCA** sur le serveur FTP en utilisant le compte iut *:*

   ```
   $ ftp 192.168.1.2
   ```

   Une fois authentifié.e, récupérez le fichier créé à la question précédente (commande `get`), puis déconnectez-vous (commande `bye`). Arrêtez alors la capture avec `Ctrl`+C.

7. Utilisez alors Wireshark pour retrouver la trame contenant le fichier transféré. Le fichier de la capture se trouve dans le dossier *M3102_lab_TP1*.

   De quelle trame s'agit-il ?

   Que contient la partie données ?

8. Modifiez maintenant le fichier de configuration de ***proftpd*** (il est situé dans ***/etc***), afin que l'écoute se fasse sur le port 22 et non plus sur le port 21. Redémarrez le serveur et vérifiez que le port d'écoute a bien changé.

   Emplacement du fichier de configuration : _____

   Modification du fichier :

9. Refaites maintenant la manipulation de la question 7 et examinez les nouvelles trames capturées à l'aide de Wireshark.

   Protocole applicatif indiqué par Wireshark : _____

   Protocole réellement contenu dans les trames : _____

   Le contenu du fichier est-il toujours visible ? _____

   Concluez sur le fonctionnement de Wireshark et sur la validité des résultats qu'il donne.

10. Arrêtez alors le service ftp sur **PCB** et remplacez-le par le service **ssh**. Répétez encore une fois la manipulation de la question 7 mais en utilisant cette fois **sftp**. Changez également le nom du fichier utilisé pour stocker les trames capturées.

    ```
    $ sftp iut@192.168.1.2
    ```

    Pouvez-vous toujours accéder au contenu du fichier transféré ? _____

11. Étudiez plus en détail la capture. Quelles trames présentes dans cette nouvelle capture montre qu'il s'agit bien cette fois d'un dialogue sécurisé ?