TP1 d'observations

INTRODUCTION

</br>

L'objectif de ce TP est d'observer les différents éléments du réseau et d'en construire une représentation. L'outil utilisé est *netkit* qui permet de construire une architecture réseau à partir de machines virtuelles.

1. Lancement du lab

Récupérer sous Celene l'archive *labobs.tgz*. Une fois décompressé, se placer dans le dossier labobs et lancer la commande : *lstart*. Un ensemble de 16 machines virtuelles s'exécutent mais seuls deux terminaux pour alice et bob ont été lancés. Toutes les commandes seront exécutées sur une de ces deux machines. En revanche il sera possible de capturer des trames pour les observations sur différents réseaux de l'architecture construite dans ce lab. Pour cela le script *ecoute* est disponible et prend en paramètre le nom du réseau que l'on veut observer. Ce script permet de lancer *wireshark* un analyseur de paquets afin de capturer les trames échangées entre les machines virtuelles du lab. Il doit être lancé à partir du terminal de la machine hôte.

PARTIE 1 : géographie du réseau

</br> La première partie a pour objectif d'obtenir la géographie du réseau en utilisant des commandes simples localement ou de questions/réponses à un hôte distant.

2. Premières observations

Sur alice et bob exécuter la commande : *ifconfig*

Quelles sont les différentes adresses d'alice et bob ? alice :41.13.0.50 bob : 80.8.0.50

Sur bob exécuter la commande *ping 41.13.0.50* puis la commande *ping alice.blue.net*

Le nom du domaine auquel appartient bob est *red.net*. Quelles sont les deux commandes à exécuter sur alice permettant d'avoir une réponse de bob (*ping*).

Sur alice - ping 80.8.0.50 - ping bob.red.net

Sur alice exécuter à nouveau la commande *ping 80.8.0.50* mais en plaçant une sonde sur le réseau local d'alice.

1. **Sur la machine hôte exécuter la commande *./ecoute lana***
2. **A partir d'alice exécuter *ping 80.8.0.50***
3. **Observer les différents paquets échangés**
4. **Retrouver dans les trames ICMP les adresses manipulées**

41.13.0.50 80.8.0.50

3. Observations du cheminement avec routage

Exécuter la commande *route -n* *sur alice. Quel est le rôle de 41.13.0.1 ?*

c'est la passerelle pour communiquer avec bob

Exécuter la commande traceroute -n 80.8.0.50* *sur alice et traceroute -n 41.13.0.50* *sur bob. Quels sont les chemins suivis par les messages à partir d'alice et à partir de bob ?

alice : 41.13.0.1.1.2.3.4 10.0.0.2 2.3.4.110 bob :80.8.0.1.2.3.4.5 10.0.0.1.1.2.3.54 41.13.0.50

En utilisant les commandes vues précédemment, représenter schématiquement l'ensemble des machines sur la route entre alice et bob et les liens entre elles. Cette représentation sera à compléter dans la suite avec toutes les nouvelles machines observées.

PARTIE 2 : HTTP et SMTP

</br> La seconde partie a pour objectif d'observer et utiliser des protocoles haut niveau.

4. Observations du protocole http

*Sur alice exécuter la commande **lynx `http://www.lexique.com`**. Une page web doit s'afficher.*
Quelle est l'adresse du serveur web `www.lexique.com` *?*

adresse de `www.lexique.com` : 9.9.9.9

*La commande **nmap** permet de scanner les ports ouverts sur une machine. Exécuter sur le terminal d'alice la commande **nmap `www.lexique.com`** pour définir le port associé à **http**.*

http : 80/tcp

*A partir de bob exécuter à nouveau la commande **lynx `http://www.lexique.com`** mais en plaçant une sonde sur le réseau local de bob.*

1. *Sur la machine hôte exécuter la commande **./ecoute lanb***
2. *A partir de bob accéder à la page web `www.lexique.com`*
3. *Observer les différents paquets échangés (utiliser la fonction **suivre HTTP stream** à partir d'un clic droit sur la première trame http)*

Quels sont les différents protocoles présents : tcp http arp dns Quels sont les différentes étapes pour charger la page web : faire un schéma ...

La commande nc pour netcat est un outil très utile pour tester des protocoles client-serveur. Il permet d'ouvrir des connexions réseau (sockets) et de réaliser des échanges en ligne de commande.
Par exemple pour tester le protocole http dans le terminal de bob, lancer la même sonde que précédemment et reprendre les commandes :

1. *nc -v www.perdu.com 80*
2. *GET / HTTP/1.0*
3. *Host: www.perdu.com*
4. *Une ligne vide*
5. *Valider par la touche Entrée*

5. Observations du protocole smtp

Faire cette partie uniquement s'il vous reste beaucoup de temps !
*A l'aide du logiciel **pine**, vérifier qu'alice et bob peuvent bien échanger des courriers électroniques. Leurs adresses respectives sont alice@jmail.com et bob@cold.net et leur mot de passe à tous les deux est guest.*
*Dans la configuration de **pine**, identifiez les paramètres de connexion aux différents serveurs impliqués.*

alice : bob :

*Pour observer les échanges, lancer une sonde sur le réseau d'alice **./ecoute lana**. Avec **pine** d'alice rédiger un mail à destination de bob. Reproduire cet envoi avec **nc** après avoir cherché quel est le port ouvert pour le protocole smtp sur la machine smtp.jmail.com*

nmap smtp.jmail.com "port"

*Compléter l'observation en lancant une sonde sur le réseau rezo **./ecoute rezo** et sur le réseau de bob **./ecoute lanb** . Quel est le chemin suivi par le mail jusqu'à bob ? Quel est le protocole utilisé pour la réception ?*

le chemin : imap :

PARTIE 3 : DNS

</br> La troisieme partie a pour objectif d'observer le fonctionnement du protocole DNS pour faire le lien entre adresses IP et noms de domaines.

6. Observations du protocole DNS

*La commande **dig** (DNS lookup utility) permet de tester la résolution de nom. Exécuter **dig www.perdu.com** sur bob et sur alice.*

Quel est le serveur qui peut faire la résolution de nom ? -> (sur bob : 2.3.4.110) (sur alice : 1.2.3.54) Quels sont les échanges réalisés ?

*Sur alice et bob le fichier **/etc/resolv.conf** contient les informations sur le serveur DNS accessible pour la résolution de nom. Vérifier qu'on retrouve les informations précédentes (cat /etc/resolv.conf).*

*Lancer deux sondes respectivement sur le réseau **lana** et **rezo** puis exécuter la commande **lynx http://www.lexique.com** sur alice. Observer les trames DNS dans les deux captures.*

nameserver 172.17.0.1

*Il est possible également d'utiliser la commande **dig -t MX jmail.com** pour trouver des informations sur un serveur smtp d'un domaine. Vérifier que les informations obtenues sont celles contenues dans les fichiers de configuration des clients mail.*

PARTIE 4 : Configuration

Quelques notions de configuration.

7. Ajout d'une machine sur le réseau d'alice

*A partir de la machine hôte ajouter une machine au réseau **lana** avec la commande **vstart --eth0=lana anne** et la configurer*

1. *ifconfig eth0 41.13.0.110/24*
2. *route add default gw 41.13.0.1*
3. *compléter le fichier /etc/resolv.conf*

Vérifier que les commandes suivantes fonctionnent

1. *lynx http://www.perdu.com*
2. *ping bob.red.net*

PARTIE 5 : ARP

Dans cette partie il s'agit d'observer comment s'effectue le transfert des messages d'une machine à l'autre. Quelles sont les adresses manipulées et les différentes étapes réalisées ?

8. Observations du rôle de ARP

*Sur alice exécuter la commande **ping -c 2 41.13.0.110** (ou **ping -c 2 41.13.0.1** si la partie 4 n'a pas été faite) après avoir lancé une sonde sur le réseau **lana**.*

1. *Quelles sont les deux premières trames capturées ?*
2. *Quelles sont les adresses manipulées par ces deux premières trames ?*
3. *Et en particulier à qui est envoyée la première trame ?*
4. *Quel est le rôle d'ARP ?*

*Renouveler la commande **ping** sur alice. Quelles sont les nouvelles trames capturées ?*

*Exécuter la commande **arp -n** sur alice.*

contenu de la table :

Observer les trames icmp capturées et en particulier les adresses MAC/IP.

request : reply :

9. Dernière commande

*Pour arrêter le lab exécuter la commande **lcrash***