Les commandes liées au réseau sous UNIX
Les applications de base

Objectif

L'objectif de ce TP est d'illustrer l'utilisation de protocoles et commandes de bases liés au réseau sur les machines Unix et certaines applications (telnet, FTP, SMTP et POP3)

Attention : Durant cette séance de TP, votre mot de passe ainsi que les données que vous allez faire transiter sur le réseau risquent d'être compromis. Il est CONSEILLE de changer temporairement de mot de passe.

1 La configuration du réseau sous Unix

En utilisant les commandes `/sbin/ifconfig` et `/bin/netstat`étudiées la semaine dernière ? Déterminer :

- Quelle est l'adresse IP de votre machine ?
- Quelle est l'adresse MAC de votre machine ? Par qui sont fixées ces adresses ?
- Quelle est l'adresse du réseau ?
- Quelle est l'adresse de broadcast du réseau ?
- Quel est le masque du réseau ?
- Quelle est la classe du réseau ?
- A quoi correspond le champ MTU ?
- A quoi sert l'interface lo, quelle est son adresse IP ?
- Quelles sont les connexions utilisant les protocoles internet actives sur votre machine ?

Faire tourner netstat en mode continu et exécuter la commande `telnet arcadia`

- Que se passe-t-il ?

2 ARP et adresses IP

Lire la page de manuel concernant la commande :

`/sbin/arp`

- Afficher le contenu de la table ARP
- Même question mais en affichant les adresses IP au lieu des noms de machines
- Exécuter la commande : `ping mail.univ-tln.fr`
- Quelles sont les adresses MAC et IP de cette machine ?
- Exécuter la commande : `ping 193.49.96.2`
- Que constatez vous ? Pourquoi ?
- Quel est le rôle de la commande `host` ?
- Que donnent les commande `host mail` et `host mail etud1` ? Pourquoi ?

3 Analyse du protocole ARP

Nous allons utiliser un programme d'écoute de trames capable de décoder les protocoles que nous avons étudiés : ethereal (`http://www.ethereal.com/`)

Une introduction à ethereal est présentée ici : `http://www.ethereal.com/docs/user-guide/chap03.html`

Lancer le programme ethereal, et commencer la capture des trames du protocole utilisé par ping en partance ou à destination de votre machine. Pour cela ethereal propose des filtres **appliqués lors de la capture**, ne seront gardés que les paquets pour lesquels le filtre est vrai.

Les filtres se décomposent en 3 parties :

- le **protocole** qui peut être ether, fddi, ip, arp, rarp, decnet, lat, sca, moprc, mopdl, tcp ou udp,
- la **direction** qui peut être src ou dst,
- un **champ** qui peut être host, net ou port suivi d'une valeur.

Les opérateurs and, or et not peuvent être utilisés pour combiner des filtres.
Attention il existe aussi des filtres d'affichage (appliqués après la capture).
Analyser une séquence de résolution d'adresse avec ARP en suivant la méthode suivante :

- Utiliser : ether proto
  arp comme filtre pour ethereal
- Afficher la table ARP
- Faire un ping sur une machine qui n'est pas dans la table
- Arrêter la capture et analyser les deux trames échangées
- Que s'est-il passé ? A qui est destinée la première trame ? D'où vient la seconde ?
- Quelle est la longueur utile des données transportées dans la trame Ethernet lors d'une requête ARP ?

4 Analyse de la commande ping

Lire le man de la commande `/bin/ping`.

- Quel est le protocole utilisé par cette commande ?

Exécuter la commande `ping sis.univ-tln.fr` et arrêter la capture au bout de 10 trames `maximum`.

Pour les trames 1 à 4, analyser le contenu : de la trame ethernet, de la trame IP, de la trame ICMP.

Est-ce que les trames des autres machines apparaissent dans votre analyseur ? Pourquoi ?

Exécuter la commande `ping 10.1.78.254`

- Que se passe-t-il ?
- Quel message est retourné par ping quand vous essayez d'atteindre une machine qui n'existe pas sur le réseau local ?
- Quelles trames circulent sur le réseau ?
- Que fait la commande `ping -s 3200 -c 1 maitinfo14` ?
- Que s'est-il passé au niveau des trames Ethernet ?

DEMANDER AVANT DE LANCER LA COMMANDE SUIVANTE

- Comment effectuer un ping en broadcast sur le réseau local ?
- Que se passe-t-il dans la table arp ?

5 Analyse de la commande traceroute

Lire le man de la commande traceroute, Capturer les trames ICMP et UDP en partance ou à destination de votre machine et lancer la commande `traceroute microsoft.com`. Arrêter la capture dès la fin de la commande

Déduire de l'analyse des trames le fonctionnement de cette commande (cf. paramètre Time To Live (TTL) de ping).

6 Les problèmes de sécurité

Après avoir configuré "correctement" ethereal, depuis votre machine faire un telnet puis un ftp sur la machine `arcadia` en utilisant le compte de login `‘‘ test ’’` dont le password est `‘‘ secret ’’`.

- Comment se déroule la connexion ? Que constatez-vous ?
- Essayer de saisir des commandes ?
- Que constatez-vous ?
- Que fait la commande ssh ?

Effectuer une connexion ssh sur votre machine en écoutant les trames avec ethereal.

- Que remarquez vous ?

7 Première approche des applications

Pour illustrer les différentes applications (ftp, telnet, pop3 et smtp) et leur mode de fonctionnement vous aller simuler le fonctionnement d'un client en vous connectant sur le port de l'application en utilisant un client telnet. Chacun de ces protocoles utilise un langage à base de commandes. Ces commandes sont définies dans les documents suivants :

- FTP (`http://www.ietf.org/rfc/rfc959.txt`)
- pop3 (`http://www.ietf.org/rfc/rfc1939.txt`)
- smtp (`http://www.ietf.org/rfc/rfc0821.txt`)

Après avoir parcouru ces documents :

7.1 Analyse des protocoles

En utilisant le logiciel ethereal et en vous appuyant sur les RFC, vérifier comment fonctionnent les applications standard :

- Faites ftp sur la machine `ftp.univ-tln.fr` (comparer cette machine avec (`mail.univ-tln.fr`)), déplacement dans les repertoires et téléchargement d'un fichier.
- Utilisez mozilla pour envoyer un courrier électronique, quel est le protocole utilisé, comment se passe l'échange ? Envoyer un mail avec une pièce jointe et contenant des caractères accentués.
- Utilisez mozilla lire vos courriers électroniques, quel est le protocole utilisé, comment se passe l'échange ?

7.2 Simulation d'une application avec telnet

en utilisant la commande `telnet` et en vous connectant sur un port spécfifique :

- Connectez-vous sur le serveur pop3 où se trouvent vos mails (`etud.univ-tln.fr`)
  - affichez la liste de vos messages
  - affichez l'en-tête du premier message, à quoi correspondent ces informations.
  - consultez le contenu du dernier message.
  - consultez le contenu et l'en-tête du dernier message ayant une pièce jointe.
- Envoyez vous un mail "à la main"
- Faire de même avec le serveur Web `www.univ-tln.fr`, quel protocole est utilisé ?

8 Sécurité du courrier électronique

Reportez-vous à cette page `http://www.thawte.com/email/` pour mettre en place les éléments nécessaire de sécurité pour le courrier électronique.