Séquence 4 - Bases des réseaux - suite
Gaetan.Richard@unicaen.fr (d'après Jean Saquet)

1 Avertissement

Cette feuille de T.P. pose un certain nombre de questions auxquelles il vous est demandé de répondre, et de rendre la feuille ainsi complétée. Inutile d'indiquer votre nom, le but n'étant pas de faire une interrogation écrite, mais d'évaluer globalement la compréhension des mécanismes réseaux.

2 Commandes lignes ou applications à utiliser

Déjà utilisées lors du précédent T.P. :
- Host (ou Dig) : permet d'interroger le serveur DNS
- Netdump et Wireshark : (taper `sudo netdump-tp`) pour capturer les trames et visualisez-les avec Wireshark.

Quelques commandes supplémentaires :
- Nmap : permet de visualiser les ports ouverts sur une machine. Exemple :
  `nmap mike.info.unicaen.fr`
- Telnet : permet d'ouvrir une connexion TCP avec un port d'une machine. Exemple :
  `telnet www.info.unicaen.fr 80`
  Attention, pour quitter la connexion, il peut être nécessaire de taper une combinaison de touches spéciale. Exemple :
  `Escape character is '^]'`

3 Trouver les serveurs DNS et mail, leurs adresses IPv4 et IPv6 s'il y a lieu

Utilisez la commande Host ou Dig pour répondre aux questions suivantes :
- Nom générique et adresses du serveur www du domaine info.unicaen.fr :
- Noms et adresses du ou des serveurs de noms du même domaine :
- Qu concluez-vous du résultat de cette dernière question ? :
- Le domaine info.unicaen.fr a-t-il un serveur de mail ?
- Pouvez-vous trouver tous les surnoms de www.unicaen.fr ? Indiquez-en au moins 3

Trouvez les noms et adresses des serveurs www, dns et mail du domaine renater.fr

— serveur www du domaine :

— serveurs de noms :

— serveur(s) de mail :

Recommencez l'obtention des adresses des serveurs www, de noms et de mail sur le domaine info.unicaen.fr, mais en posant la question au serveur d'adresse v4 8.8.8.8 (serveur dns public de google, cf : `http://code.google.com/intl/fr/speed/public-dns/docs/using.html`).

— résultats obtenus :

— explication :

4 Repérage des ports ouverts (sur des serveurs)

Utilisez la commande nmap pour lister les ports ouverts des machines (de info.unicaen.fr) dont vous avez trouvé les noms et adresses à la section précédente, ainsi que mike et le serveur de mail de unicaen.fr
Complétez le tableau ci-dessous (mettez une croix dans la case si le service est ouvert sur la machine, et pour chacun des services, indiquez le numéro de port correspondant dans la colonne "port" :

service	port	serveur www	serveur DNS	serveur mail de unicaen	mike.info.unicaen.fr
ssh					
http					
https					
smtp					
smtps					
pop3s					
imaps					
domain					

Vous pouvez également ajouter au tableau ci-dessus une colonne pour la machine averell.info.unicaen.fr.

Indiquez la signification des abréviations de certains de ces services (cherchez sur le web !) :

— ssh :
— smtp :
— https :
— domain :
— pop3s :
— imaps :

5 Tests de connexion à certains services

Cette section ne contient pas de lignes à compléter, mais les commandes testées pourront être utilisées dans la section suivante.

— Utilisez telnet pour essayer une connexion "manuelle" à un serveur. Exemples :
  — telnet averell.info.unicaen.fr 25
  — telnet www.info.unicaen.fr 80

  Si vous ne savez pas "parler" le protocole en question, déconnectez-vous (ctrl-[, puis "quit"). Vous pouvez au moins essayer un "`GET /`" en http.

6 Traces et analyse partielle de trames

Cette section nécessite l'utilisation de netdump pour capturer et wireshark pour visualiser les connexions faites par des commandes-lignes ou des utilisations de logiciels graphiques communicants. Indiquez comment tracer avec wireshark une connexion en filtrant pour ne pas avoir trop de trames capturées, par exemple, comment filtrer pour avoir ce qui concerne uniquement une requête à un serveur DNS ?
Réponse :

Pour chaque communication de la liste ci-dessous, indiquez si le protocole de niveau transport effectivement utilisé est TCP ou UDP, et si la communication utilise IPv4 ou IPv6.

— `host <nom-de-machine>`

— `host -l info.unicaen.fr`

— Si les deux communications ci-dessus utilisent ipv4 (resp. ipv6), peut-on forcer l'utilisation d'ipv6 (resp. ipv4) ? Si oui, comment ?

— envoi d'un mail (avec un logiciel tel que Thunderbird configuré avec vos paramètres)

— utilisation d'un navigateur pour accéder à un serveur web (interne, puis externe)

— telnet mike.info.unicaen.fr 13

Pour cette dernière commande, quel est le protocole d'application utilisé (cherchez sa RFC) ? Au niveau transport, peut on utiliser TCP, UDP ou les deux ?