Couches réseau, capture et DNS

Ce TD/TP a pour but la prise en main de l'outil Wireshark, la compréhension du modèle en couches et du protocole applicatif DNS. Vous devrez rendre sur Universitice un compte-rendu lié aux questions de TP ; il doit être au format PDF, soit à partir d'un code LaTeX, soit à partir d'un logiciel de traitement de texte type LibreOffice. Les réponses doivent être rédigées et quand c'est possible illustrées par des captures d'écran de votre travail (ligne de commande, Wireshark, etc.). Vous soumettrez aussi vos captures (dans la mesure du raisonnable concernant leur taile) ainsi que vos éventuels fichiers C.

Exercice 1 *Modèles et couches réseau*

1) Quelles sont les différentes couches du modèle OSI ?

2) Nommez les protocoles que vous connaissez et placez-les dans les différentes couches du modèle OSI.

3) A quoi sert le modèle TCP/IP et quelle est la différence avec le modèle OSI ?

Exercice 2 *Capture et filtrage*

1) (TP) Lancez Wireshark. Démarrez une capture en sélectionnant l'interface externe. Depuis un terminal, utilisez la commande `ping` sur un nom de domaine de votre choix, qui réponde. Arrêtez la capture. Quels protocoles ont été capturés ? A quelle couche de quel modèle correspondent-ils ?

2) (TP) Cliquez sur une trame DNS et identifiez (dans le cadre contenant les différentes couches) les différents protocoles en jeu. À quelle(s) couches appartiennent-elles ?

3) (TP) Trouvez les paquets correspondant au ping ; qu'avez-vous comme informations sur ces paquets ? De même que pour DNS, identifiez les différents protocoles utilisés.

4) (TP) Ces paquets contiennent des adresses IP, mais vous avez effectué un ping sur un nom de domaine. Identifiez les autres paquets qui font cette résolution de nom.

5) (TP) Filtrez sur les paquets de ping en cliquant droit sur "Internet Control Message Protocol" dans le détail du paquet, puis "Appliquer comme un filtre > Sélectionné". Observez la modification du contenu de la barre de filtre, et sur la liste des paquets eux-mêmes.

6) (TP) Sans toucher au filtre, relancez une capture et faites un ping vers l'adresse "172.16.3.1", puis arrêtez la capture. Que constatez-vous cette fois-ci ?

7) (TP) Relancez la capture, pinguez le nom de domaine précédemment sélectionné et ajoutez un filtre sur l'adresse IP destination en sélectionnant cette fois "Appliquer comme un filtre > ...and Selected". Observez encore la modification du contenu de la barre de filtre. Que manque-t-il ?

8) (TP) Directement dans la barre, remplacez le lexème `ip.dst` par `ip.addr`. Que cela change-t-il ?

Exercice 3 ***DNS***

1) A quoi sert le DNS ?

2) Comment se déroule une requête DNS pour résoudre le nom de domaine www.l3info.net ?

3) Qu'est-ce qu'une requête récursive ? et itérative ?
Choisissez un nom de domaine existant sur Internet. Il doit être suffisamment spécifique pour que vous soyez le seul à l'utiliser.

4) (TP) Affichez le contenu du fichier `/etc/resolv.conf`. A votre avis, à quoi sert le `nameserver` qui y figure ?

5) (TP) Utilisez la commande **dig** sur le nom de domaine que vous avez choisi. Quelles informations apparaissent ?

6) (TP) Recherchez d'autres sous-domaines pour le même nom de domaine (par exemple, pour `www.google.com`, il y a `mail.google.com`, `drive.google.com`, etc.). Analysez les différences entres les entrées : sont-elles du même type ? S'agit-il d'un nom canonique (alias) ? Quelle erreur apparaît lorsque le nom n'existe pas ?

7) (TP) Avec l'option `norecurse` et en recherchant successivement les serveurs de noms de chaque sous-domaine avec `dig @serveurDNS NS <domaine>`, faites vous-même itérativement toutes les requêtes DNS pour chaque composant du nom de domaine en commençant par la droite (le top-level domain ou TLD). Attention, une fois arrivé au dernier sous-domaine, vous devrez chercher directement un résultat (le type par défaut est `A` et non `NS`).

8) (TP) Quelle est la durée de vie de chaque enregistrement ? A quoi sert cette valeur ?

9) (TP) Remplacez les options de la dernière commande par l'option `+trace`. Quels sont les domaines traversés et les serveurs interrogés ? La requête est-elle récursive ? Faites le lien avec la question précédente.

10) (TP) Effectuez une requête **Mail eXchanger** en spécifiant `dig MX <nom>` sur votre domaine. A quoi sert ce type de requête ? Obtenez-vous une adresse IP ? Si non, obtenez-en une, puis vérifiez qu'un serveur SMTP écoute bien sur cette IP avec la commande `telnet A.B.C.D 25`.