Laboratoire 2: Le protocole DNS

L'objectif de ce deuxième laboratoire est d'analyser quelques caractéristiques du fonctionnement du protocole DNS (Domain Name Server). Nous allons nous servir des outils suivants:

- Les utilitaires réseaux disponibles sur Windows: `ipconfig` et `nslookup`
- Un navigateur web
- Le logiciel Wireshark

1. Manipulation de `ipconfig`

`ipconfig` est un outil indispensable pour déboguer des problèmes de réseaux. ipconfig peut être utilisé pour afficher l'information TCP/IP incluant l'adresse IP de votre poste de travail, les adresses des serveurs DNS, le type de carte réseau, etc... Par exemple, si vous tapez la commande

```
ipconfig /all,
```

vous obtiendrez la fenêtre CMD ci-dessous.

`ipconfig` est aussi utilisé pour gérer l'information DNS stockée dans votre poste de travail. Nous avons vu en classe que les enregistrements DNS les plus récents sont stockés dans le cache. Pour consulter les enregistrements dans le cache, tapez la commande:

```
>ipconfig /displaydns
```

Vous pouvez constater que chaque enregistrement a une durée de vie (*TTL-Time-To-Live*).
Pour effacer le contenu du cache, tapez la commande:

```
>ipconfig /flushdns
```

2. Utilisation de DNS avant une requête HTTP

Dans cette partie du laboratoire, nous allons analyser des messages DNS qui précèdent une requête HTTP.

Effectuez les étapes suivantes :

- Utilisez d'abord `ipconfig` pour vider le cache DNS de votre machine.
- Ouvrez votre navigateur (vous pouvez avoir besoin de vider le cache du navigateur).
- Démarrez Wireshark et tapez "dns" dans la partie filtre. Le filtre permettra d'afficher uniquement les messages DNS.
- Commencez la capture avec Wireshark.
- En utilisant votre navigateur, visitez le site: http://www.ietf.org
- Arrêtez la capture.

Répondez aux questions suivantes :

a. Localisez les paquets DNS requête et réponse. Quel est le protocole de la couche transport utilisé, TCP ou UDP?
b. À Quelle adresse IP la requête DNS est envoyée? Utilisez la commande ipconfig pour déterminer l'adresse IP du serveur DNS local. Est-ce que les deux adresses IP sont les mêmes?
c. Examinez la requête DNS. Quel est le "type" de cette requête? Est-ce que cette requête contient des réponses?
d. Examinez la réponse DNS. Combien de réponses sont fournies? Quel est le contenu de chaque réponse?
e. Cette page web contient des images. Avant de télécharger chaque image, est ce que votre poste de travail a envoyé d'autres requêtes DNS?

3. Utilisation de DNS avec `nslookup`

`nslookup` permet à partir du poste de travail d'envoyer une requête DNS à n'importe quel serveur DNS (serveur DNS racine, serveur DNS TLD-Top_level_Domain ou un serveur DNS intermédiaire). Pour réaliser cette tâche `nslookup` envoie une requête au serveur DNS spécifié, reçoit la réponse de ce serveur DNS et affiche le résultat de la recherche.

Effectuez les étapes suivantes :

- Ouvrez une fenêtre d'invite commande DOS
- Commencez la capture avec Wireshark
- Tapez la commande `nslookup www.lemonde.fr.` (Important: le dernier point doit faire partie de votre commande afin d'éviter que votre client DNS n'ajoute des suffixes au nom de domaine.)
- Arrêtez la capture

Répondez aux questions suivantes:

f. Quelle est le port de destination de la requête DNS? Quelle est le port source de la réponse DNS?
g. À quelle adresse IP la requête DNS est-elle envoyée? Est-ce l'adresse IP de votre serveur DNS local?
h. Examinez une des requêtes DNS résultat de la commande `nslookup`. Quel est le "type" de la requête? Est-ce que la requête contient des réponses?
i. Examinez la réponse DNS de la requête de la question h. Combien y-a-t-il de réponses? Que contient chaque réponse? Inscrivez les trois ou quatre premières lignes de la réponse.

4. Requête DNS inversée (reverse DNS lookup)

Cette section permettra d'analyser un nouveau type de requête DNS, à savoir les requêtes inversées.

Effectuez les étapes suivantes :

- Lancez une nouvelle capture avec Wireshark

- Tapez la commande `nslookup 8.8.4.4`
- Arrêtez la capture

Répondez aux questions suivantes:

j. Examinez la requête DNS résultat de la commande `nslookup`. Quel est le "type" de la requête? Quel est le nom de domaine contenu dans la question formulée par la requête?

k. Examinez la réponse DNS de la requête de la question j. Combien y-a-t-il de réponses? Que contient chaque réponse? À quoi correspond la valeur contenue dans la réponse?

l. 8.8.4.4 correspond à l'adresse IP du serveur DNS de google. Donnez la commande qui permet d'utiliser ce serveur pour faire la résolution DNS à la place de votre serveur DNS local par défaut.

m. Lancez la commande de la question g. et analyser le comportement de votre client DNS. (Vous pouvez utiliser Wireshark pour avoir une idée plus claire sur ce qui se passe.)

5. Requête DNS itérative

Dans cette dernière section, nous allons découvrir la différence entre les requêtes DNS itératives et celle récursives.

Effectuez les étapes suivantes:

- Lancez une nouvelle capture avec Wireshark
- Tapez la commande `nslookup`
- Tapez la commande `set norecursive`
- Tapez `www.umoncton.ca`
- Arrêtez la capture

Répondez aux questions suivantes:

n. Avant d'analyser les paquets capturés par Wireshark, donnez une première explication de la dernière réponse obtenue par `nslookup.` En d'autres termes, pourquoi on n'arrive pas à obtenir l'adresse IP de www.umoncton.ca?

o. Dans Wireshark, examinez la requête DNS résultat de la commande `nslookup`. Quel est le "type" de la requête?

p. Examinez la réponse DNS de la requête de la question p. Combien y-a-t-il de réponses? À quoi sert le contenu des "Authority RRs"?

q. Quel est l'effet de la commande `set norecursive` sur le comportement du client DNS?

r. Utilisez le contenu des "Authority RRs" pour lancez une commande nslookup qui permet d'obtenir l'adresse IP de www.umoncton.ca