DNS : exercice N°1
resolver/dig/dns inverse/tcpdump

1. Configurer le resolver sur votre poste de travail

Créer le fichier /etc/resolv.conf qui contient les informations suivantes :

```
search ws.nsrc.org
nameserver 10.10.0.241
```

2. Interroger le DNS en utilisant 'dig'

2a. Pour chacune des commandes, trouver la section ANSWER et noter les résultats. Noter bien aussi le TTL. Repeter la commande. Avez-vous le meme TTL ?

Les réponses sont –elles d'un serveur autoritaire ?

LES COMMANDES

```
# dig www.afribone.net.ml. a

# dig zcp.bf. mx

# dig intif.francophonie.org. a

# dig <domaine de votre choix> a

# dig <domaine de votre choix> mx

# dig tiscali.co.uk. txt

# dig ripe.net. txt

# dig geek.tiscali.co.uk. a
```

2b. Maintenant envoyer des requêtes vers un autre serveur cache. Combien de temps chaque réponse prend – t-elle avant d'être reçu ?

```
# dig @ns1.technologia.net. news.bbc.co.uk. a

# dig @ns1.technologia.net. yahoo.com. a

# dig @<serveur de votre choix> <domaine de votre choix> a
```

3. Consultations du DNS inverse

Maintenant essayer quelques requêtes du DNS inverse.

Notes

1- Rappelez-vous d'inverser les quatre (4) parties de l'adresse IP,

2- Ajouter '**.in-addr.arpa.**', et faire la requête d'un Enregistrement de Ressources (ER) de type **PTR .**

a)
(Pour 212.74.112.66)
```
# dig 66.112.74.212.in-addr.arpa. ptr
```

b)Répéter la requête pour une autre adresse IP de votre choix

c)Maintenant essayer la forme courte de dig en utilisant le flag (le drapeau) '-x' pour la consultation inverse

```
# dig -x 212.74.112.66
```

```
# dig @<serveur de votre choix> -x < adresse ip de votre choix>
```

4. Utiliser tcpdump pour afficher le trafic DNS

Dans les fenêtres distinctes, taper les commandes suivantes :
(*Note : vous devez être root*)

```
# tcpdump -n -s 1500 -i eth0 udp port 53
```

Ceci affiche tous les paquets UDP sortants et entrants du port 53 (port DNS) de votre machine.

Maintenant aller dans une autre fenêtre et répéter quelques requêtes 'dig' sur des voisins.
Observer l'affichage de tcpdump,
Rechercher l'adresse IP source et de destination de chaque paquet.

Description des paramètres de la commande
```
# tcpdump -n -s 1500 -i eth0 udp port 53
```

-n
: Empêche tcpdump de faire des consultations DNS inverse sur des paquets qu'il reçoit et qui produisent des trafics DNS additionnels (confusions)

-s 1500
: tcpdump lis le paquet entier (autrement le tcpdump lit seulement les en-têtes)

-i eth0
: Sur quelle interface écouter (eth0)

udp port 53
: Un filtre qui correspond seulement aux paquets UDP sortants et entrants du port 53