TP DNS

M2 CySec UGA
Aurélien Monnet-Paquet

Décrire et commenter le fichier de configuration /etc/resolv.conf de votre host :

```
# Dynamic resolv.conf(5) file for glibc resolver(3) generated by resolvconf(8)
# DO NOT EDIT THIS FILE BY HAND -- YOUR CHANGES WILL BE OVERWRITTEN
nameserver 127.0.1.1
search e.ujf-grenoble.fr
```

Quel est le (ou les) suffixe(s) ajouté(s) par défaut aux noms sur ces serveurs?

e.ujf-grenoble.fr

Quels sont les adresses des serveurs DNS de l'ufrima ?
ufrima.imag.fr has address 195.221.225.1

Quel est leur nom ?
boole.imag.fr is an alias for ufrima.imag.fr.

Interrogation DNS

root@knuth09:~ # host toto
toto.imag.fr has address 129.88.65.34
toto.imag.fr mail is handled by 10 mx1.imag.fr.
toto.imag.fr mail is handled by 10 mx2.imag.fr.

Pour toto, on remarque, que son adresse est 129.88.65.34
Et qu'il possède deux serveurs de mails, qui sont 10 mx1.imag.fr et 10 mx2.imag.fr

root@knuth09:~ # host ftp
Host ftp not found: 3(NXDOMAIN)

ftp n'a pas été trouvé.

root@knuth09:~ # host www
www.imag.fr is an alias for rillette.imag.fr.
rillette.imag.fr has address 129.88.34.211
rillette.imag.fr mail is handled by 10 mx2.imag.fr.
rillette.imag.fr mail is handled by 10 mx1.imag.fr.

Dans ce cas, on remarque que www n'est pas le serveur principal. Et qu'il est un alias de rillette.

root@knuth09:~ # host www.
Host www. not found: 3(NXDOMAIN)

www. n'a pas été trouvé.

root@knuth09:~ # host ufrima
ufrima.imag.fr has address 195.221.225.1

root@knuth09:~ # host www.google.com
www.google.com has address 216.58.211.68
www.google.com has IPv6 address 2a00:1450:4007:80b::2004

root@knuth09:~ # host www.google.fr
www.google.fr has address 216.58.211.67
www.google.fr has IPv6 address 2a00:1450:4007:80b::2003

root@knuth09:~ # host www.nic.fr
www.nic.fr is an alias for web01.nic.fr.
web01.nic.fr has address 192.134.5.5
web01.nic.fr has IPv6 address 2001:67c:2218:30::5

Pourquoi dans certains cas plusieurs adresses apparaissent dans les réponses ?

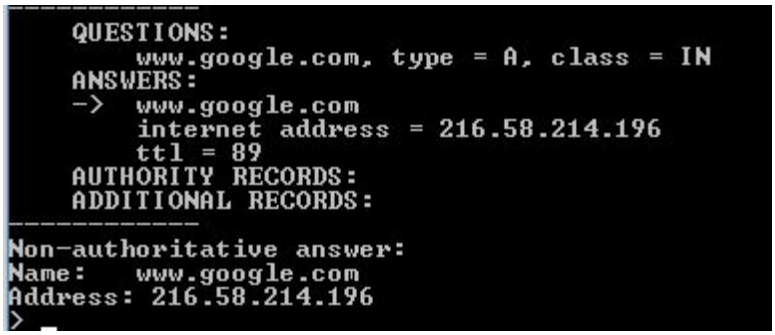
Dans certain cas, il y a plusieurs adresses dans une réponse car il peut y avoir plusieurs adresses pour un seul nom de domaine.

Serveurs de zone DNS

Dig NS . renvoi 13 noms
Dig NS fr. renvoi 5 noms
Dig NS imag.fr renvoi 2 noms

"non-authoritative answer" signifie que la réponse reçu ne provient pas du serveur officiel du domaine de la requête. On a eu a faire a un relai.

Les requêtes DNS



Combien existe-il de serveurs pour la zone google.com. ?
4

La liste des adresses des différentes machines www.google.com est-elle toujours donnée dans le même ordre par le serveur DNS ?
Non.

Quel intérêt ?
Load balancing.

Est ce que le DNS client possède un cache ?
Non.

Quel est le protocole de niveau transport utilisé par DNS ?
UDP si la taille est inferieur à 512 octets. Sinon (>512 octets) c'est TCP qui est utilisé. Par contre, l'échange des bases de données se fait toujours en TCP.

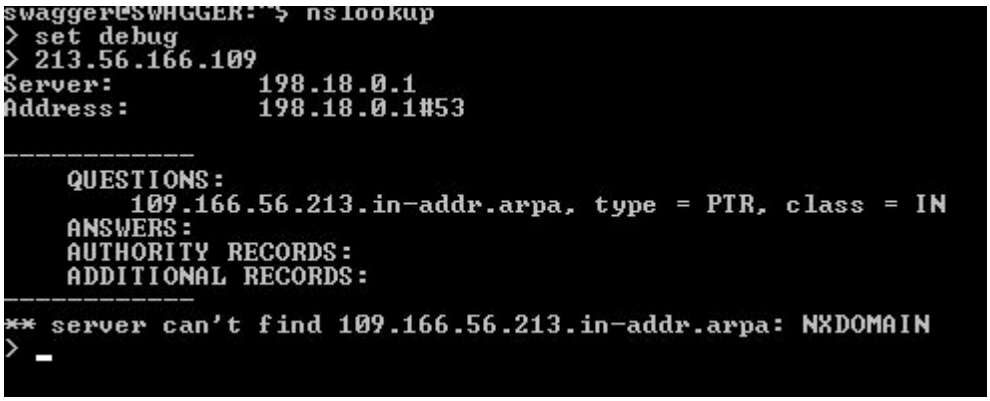
Quel est le port réservé au serveur DNS ?
53.

```
swagger@SWAGGER:~$ host -d -t mx cybersecurity.imag.fr
Trying "cybersecurity.imag.fr"
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 53685
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;cybersecurity.imag.fr.          IN      MX

;; ANSWER SECTION:
cybersecurity.imag.fr.  1800    IN      CNAME   sites-ljk.imag.fr.

Received 63 bytes from 198.18.0.1#53 in 62 ms
swagger@SWAGGER:~$
```

```
swagger@SWAGGER:~$ host -d -t cname cybersecurity.imag.fr
Trying "cybersecurity.imag.fr"
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 18821
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;cybersecurity.imag.fr.          IN      CNAME

;; ANSWER SECTION:
cybersecurity.imag.fr.  1656    IN      CNAME   sites-ljk.imag.fr.

Received 63 bytes from 198.18.0.1#53 in 30 ms
swagger@SWAGGER:~$ host -d -t www.google.com
host: invalid type: www.google.com

swagger@SWAGGER:~$ host -d -t www.google.fr
host: invalid type: www.google.fr

swagger@SWAGGER:~$
```

Conclusions ?

Les noms canoniques sont des alias a un nom de domaine.
Google.com et google.fr n'ont pas d'alias car ils ne fournissent qu'un seul service.



Type de requete : PTR 12 Pointeur vers un autre espace du domaine (résolution inverse)