R303 Services Réseaux Avancés -TD1 : DNS "côté client"

Jean-Marc Pouchoulon

Septembre 2022

La copie d'écran suivante est le résultat d'une commande dig effectuée sur le serveur 195.83.225.1 , serveur autoritaire du domaine DNS ac-montpellier.fr.

```
root@68b7ec718820:/# dig  @195.83.225.1 www.ac-montpellier.fr

; <<>> DiG 9.8.4-rpz2+rl005.12-P1 <<>> @195.83.225.1 www.ac-montpellier.fr
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 62731
;; flags: qr aa rd; QUERY: 1, ANSWER: 2, AUTHORITY: 2, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; QUESTION SECTION:
;www.ac-montpellier.fr.         IN      A

;; ANSWER SECTION:
www.ac-montpellier.fr.  1800    IN      A       195.83.225.87
www.ac-montpellier.fr.  1800    IN      A       195.83.225.248

;; AUTHORITY SECTION:
ac-montpellier.fr.      86400   IN      NS      dns-slv-mntpllr.ac-lille.fr.
ac-montpellier.fr.      86400   IN      NS      renater.ac-montpellier.fr.

;; ADDITIONAL SECTION:
renater.ac-montpellier.fr. 86400 IN     A       195.83.225.1

;; Query time: 63 msec
;; SERVER: 195.83.225.1#53(195.83.225.1)
;; WHEN: Tue Jul 29 19:20:29 2014
;; MSG SIZE  rcvd: 148
```

Tandis que la copie d'écran suivante est le résultat d'une commande dig effectuée sur un des serveurs de Google. 8.8.8.8

```
root@68b7ec718820:/# dig  @8.8.8.8 www.ac-montpellier.fr

; <<>> DiG 9.8.4-rpz2+rl005.12-P1 <<>> @8.8.8.8 www.ac-montpellier.fr
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 54882
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;www.ac-montpellier.fr.         IN      A

;; ANSWER SECTION:
www.ac-montpellier.fr.  1019    IN      A       195.83.225.248
www.ac-montpellier.fr.  1019    IN      A       195.83.225.87

;; Query time: 47 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Tue Jul 29 19:20:45 2014
;; MSG SIZE  rcvd: 71
```

1 Analyse des deux réponses

1. La requête lancée par dig a-t-elle-abouti ?
2. A quoi correspond l'ID ?
3. Où retrouve-t-on les éléments suivants QUERY : 1, ANSWER : 2, AUTHORITY : 2, ADDITIONAL : 1 dans la réponse ?
4. Depuis quel port le serveur a-t-il répondu ?
5. Quel est le temps mis pour recevoir la réponse ?
6. Pourquoi a-t-on deux réponses à la requête faite ? Qu'en déduisez-vous sur le type d'architecture sous-jacent ?
7. Quelles différences constatez entre les deux réponses de dig ?
8. Qu'en déduisez vous ?

2 DNS et Linux

1. Quels sont les principaux fichiers relatifs à la "résolution de nom" sous Linux ?
2. Quel est le type de DNS d'une machine Linux ?
3. Peut-il servir de cache ?
4. Peut-il participer à la sécurité des transaction DNS ?
5. Peut-il être chaîné avec un autre DNS ?
6. Quel est le daemon systemd responsable de la résolution de nom . Quel est l'autre daemon impliqué ?
7. Utilisez resolvctl pour résoudre un F.Q.D.N, une adresse IP, trouvez le MX de umontpellier.fr, tous les enregistrements du domaine iutbeziers.fr ?
8. Comment obtenir la liste des DNS par interface réseau sur votre machine ?
9. Comment avoir les statistiques de cache sur votre resolver ?
10. Firefox peux-il utiliser DnsOverHTTPS. Si oui comment le configurer ? Comment vérifiez que vous êtes protégé ?
11. Pourquoi DoH peut il être problématique pour l'administrateur réseau ?

3 DNS et sécurité

1. Un attaquant afin de rediriger les flux d'un utilisateur vers un serveur contrôlé par ses soins, pourrait tenter de le faire au travers d'un enregistrement DNS forgé. L'idée est simple : on cherche à faire correspondre le nom du serveur demandé par l'utilisateur à une adresse IP appartenant à l'attaquant (en général l'attaquant reproduit un site web qui ressemble au vrai site web sauf que les identifiants bancaires sont récupérés par l'attaquant ...) Le Query ID ou encore appelé TXID (Transaction XID) est un identifiant unique lié à une requête DNS. Il est codé sur 16 bits. Si une réponse à une requête ne contient pas le TXID , elle sera ignorée. Ce TXID est donc une sécurité importante. Combien de TXID différent peut-on avoir ?
2. Analysez l'article de Stéphane Bortzmeyer article http ://www.bortzmeyer.org/comment-fonctionne-la-faille-kaminsky.html) afin de voir comment il a outrepassé la sécurité du TXID.
3. Pourquoi n'est-il pas bon d'avoir un DNS récursif ouvert à tout Internet ?
4. Si un serveur racine change d'adresse IP quel peut en être l'impact ?

4 DNS et PERFORMANCES

1. Avantages/inconvénients pour un DNS d'utiliser UDP ou TCP ?
2. L'utilisation de TCP est-il une solution à la faille de Kaminsky ?
3. Le graphique suivant montre depuis le navigateur Chrome le temps de résolution DNS en ms. Quel est le temps moyen de résolution depuis chrome ? Sachant qu'au delà d'une seconde d'attente un internaute songe à quitter un site web que pensez vous du temps pris par le DNS ? Quelles sont les stratégies possibles dans un navigateur afin d'améliorer les performances du DNS ?