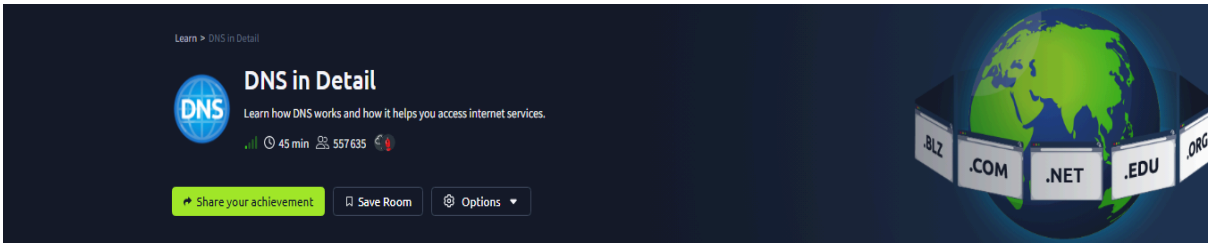


DNS in Detail | 29 Septembre, 2025

Auteur : **GhostHunt3rx**
Email : anonymousinconnu10@gmail.com

Tâche 1 : Qu'est-ce que le DNS ?

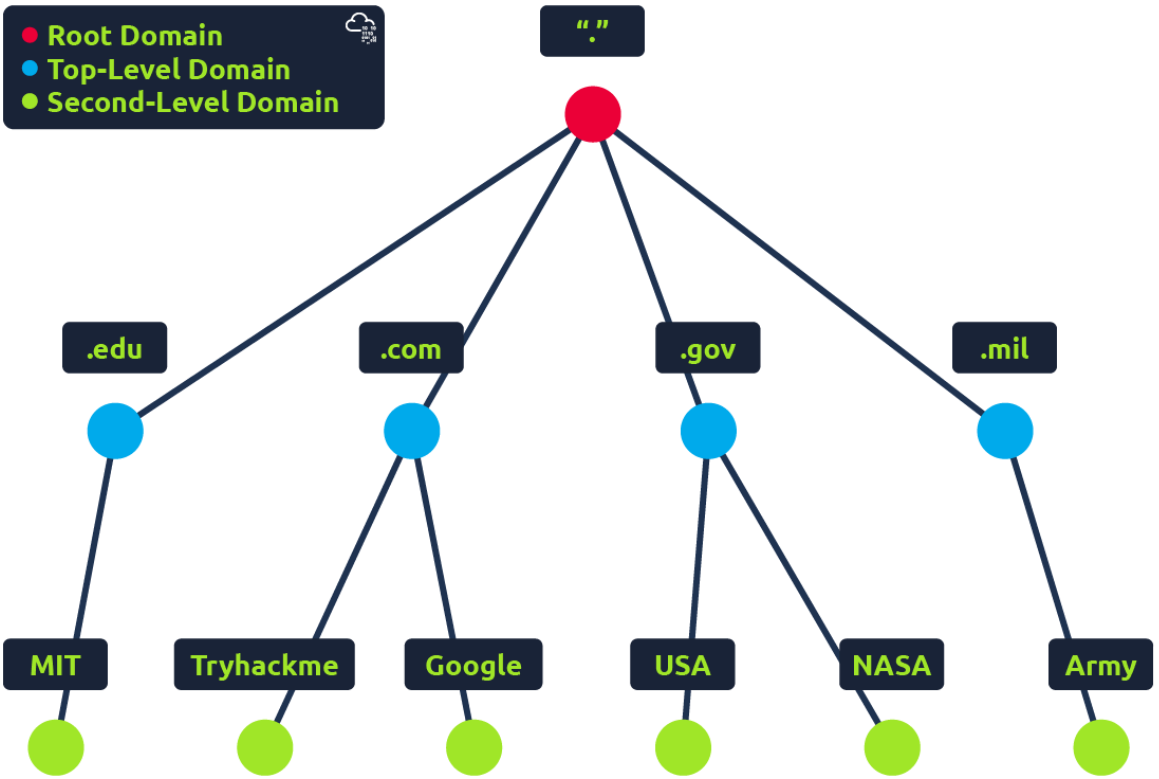
Qu'est-ce que le DNS ?

Le **DNS** (**D**omain **N**ame **S**ystem) nous permet de communiquer facilement avec des appareils sur Internet sans avoir à mémoriser des numéros complexes. Tout comme chaque maison dispose d'une adresse unique pour y envoyer du courrier, chaque ordinateur connecté à Internet dispose d'une adresse unique pour communiquer, appelée adresse IP. Une adresse IP se présente sous la forme suivante : ***104.26.10.229***, soit **4** séries de chiffres compris entre **0** et **255**, séparés par un point.

Lorsque vous souhaitez visiter un site web, il n'est pas très pratique de mémoriser cette série de chiffres compliquée, et c'est là que le DNS peut vous aider. Ainsi, au lieu de mémoriser **104.26.10.229**, vous pouvez mémoriser **tryhackme.com**.

Tâche 2 : Hiérarchie des domaines

Hiérarchie des domaines



TLD (domaine de premier niveau)

Un **TLD** est la partie la plus à droite d'un nom de domaine. Ainsi, par exemple, le TLD de tryhackme.com est ***.com***. Il existe deux types de TLD :

- les **gTLD** (domaines génériques de premier niveau) et
- les **ccTLD** (domaines nationaux de premier niveau).

Historiquement, les gTLD avaient pour but d'indiquer à l'utilisateur la finalité du nom de domaine. Par exemple, *.com* désignait les sites à vocation commerciale, *.org* les organisations, *.edu* l'éducation et *.gov* les administrations publiques.

Les ccTLD étaient utilisés à des fins géographiques, par exemple .ca pour les sites basés au Canada, .co.uk pour les sites basés au Royaume-Uni, etc.
En raison de cette demande, on assiste à un afflux de nouveaux gTLD tels que .online, .club, .website, .biz et bien d'autres encore.
Pour obtenir la liste complète de plus de 2 000 TLD, cliquez ici (*https://data.iana.org/TLD/tlds-alpha-by-domain.txt*).

Domaine de deuxième niveau

Prenons l'exemple de tryhackme.com : la partie .com est le TLD, et tryhackme est le domaine de deuxième niveau. Lors de l'enregistrement d'un nom de domaine, le domaine de deuxième niveau est limité à 63 caractères + le TLD et ne peut utiliser que les lettres a-z, les chiffres 0-9 et les tirets (il ne peut pas commencer ou se terminer par un tiret, ni comporter plusieurs tirets consécutifs).

Sous-domaine

Un sous-domaine se trouve à gauche du domaine de deuxième niveau et est séparé par un point. Par exemple, dans le nom admin.tryhackme.com, la partie admin est le sous-domaine. Un nom de sous-domaine est soumis aux mêmes restrictions de création qu'un domaine de deuxième niveau, à savoir une limite de 63 caractères et l'utilisation exclusive des lettres a-z, des chiffres 0-9 et des tirets (il ne peut pas commencer ou se terminer par un tiret ni comporter plusieurs tirets consécutifs). Vous pouvez utiliser plusieurs sous-domaines séparés par des points pour créer des noms plus longs, tels que jupiter.servers.tryhackme.com. Mais la longueur doit être limitée à 253 caractères maximum. Il n'y a pas de limite au nombre de sous-domaines que vous pouvez créer pour votre nom de domaine.

Tâche 3 : Types d'enregistrements

Types d'enregistrements DNS

Le DNS n'est toutefois pas réservé aux sites Web, et il existe plusieurs types d'enregistrements DNS. Nous allons passer en revue certains des plus courants que vous êtes susceptible de rencontrer.

Enregistrement A

Ces enregistrements renvoient à des adresses IPv4, par exemple 104.26.10.229

Enregistrement AAAA

Ces enregistrements renvoient à des adresses IPv6, par exemple 2606:4700:20::681a:be5

Enregistrement CNAME

Ces enregistrements renvoient vers un autre nom de domaine, par exemple, la boutique en ligne TryHackMe a le nom de sous-domaine store.tryhackme.com qui renvoie un enregistrement CNAME shops.shopify.com. Une autre requête DNS serait alors envoyée à shops.shopify.com pour déterminer l'adresse IP.

Enregistrement MX

Ces enregistrements renvoient à l'adresse des serveurs qui gèrent les e-mails pour le domaine que vous interrogez. Par exemple, une réponse d'enregistrement MX pour tryhackme.com ressemblerait à alt1.aspmx.l.google.com. Ces enregistrements sont également accompagnés d'un indicateur de priorité. Celui-ci indique au client dans quel ordre essayer les serveurs, ce qui est parfait si le serveur principal tombe en panne et que les e-mails doivent être envoyés à un serveur de secours.

Enregistrement TXT

Les enregistrements TXT sont des champs de texte libre dans lesquels toutes les données textuelles peuvent être stockées. Les enregistrements TXT ont de multiples utilisations, mais l'une des plus courantes consiste à répertorier les serveurs autorisés à envoyer des e-mails au nom du domaine (ce qui peut aider à lutter contre le spam et les e-mails frauduleux). Ils peuvent également être utilisés pour vérifier la propriété du nom de domaine lors de l'inscription à des services tiers.

Tâche 4 : Faire une demande

Que se passe-t-il lorsque vous effectuez une requête DNS ?

1. Lorsque vous demandez un nom de domaine, votre ordinateur vérifie d'abord son **cache local** pour voir si vous avez récemment recherché cette adresse. Si ce n'est pas le cas, une requête est envoyée à votre serveur DNS récursif.

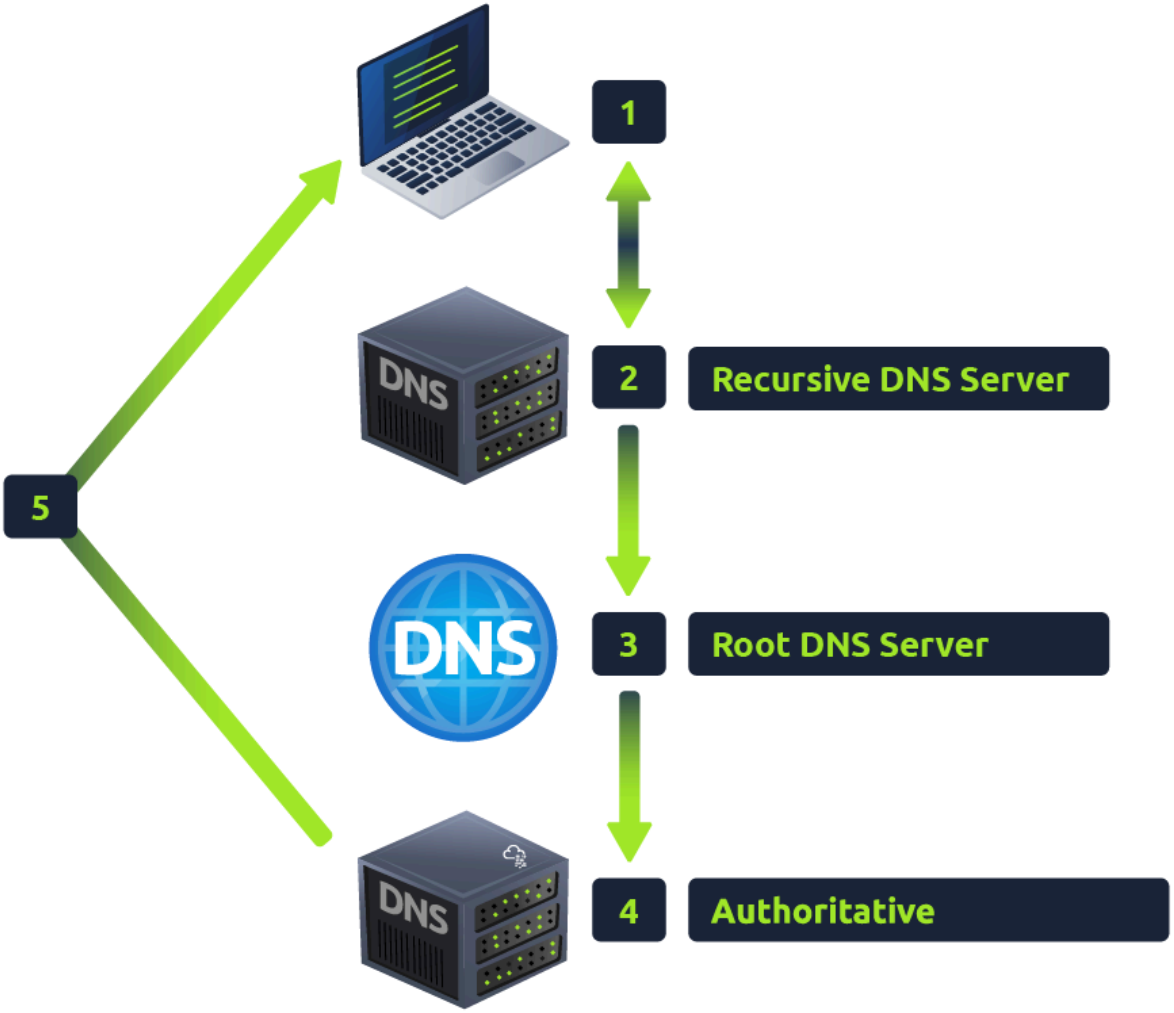
2. Un **serveur DNS récursif** est généralement fourni par votre FAI, mais vous pouvez également choisir le vôtre. Ce serveur dispose également d'un cache local des noms de domaine récemment recherchés. Si un résultat est trouvé localement, il est renvoyé à votre ordinateur et votre requête s'arrête là (c'est courant pour les services populaires et très sollicités tels que Google, Facebook ou Twitter). Si la requête ne peut être trouvée localement, un parcours commence pour trouver la bonne réponse, en commençant par les serveurs DNS racines d'Internet.

3. **Les serveurs racine** agissent comme la colonne vertébrale DNS d'Internet ; leur rôle est de vous rediriger vers le serveur de domaine de premier niveau approprié, en fonction de votre requête. Si, par exemple, vous demandez www.tryhackme.com, le serveur racine reconnaîtra le domaine de premier niveau .com et vous redirigera vers le serveur TLD approprié qui traite les adresses .com.

4. **Le serveur TLD** contient des enregistrements indiquant où trouver le serveur faisant autorité pour répondre à la requête DNS. Le serveur faisant autorité est souvent appelé « serveur de noms » pour le domaine. Par exemple, les serveurs de noms pour tryhackme.com sont kip.ns.cloudflare.com et uma.ns.cloudflare.com. Vous trouverez souvent plusieurs serveurs de noms pour un nom de domaine, qui servent de sauvegarde en cas de panne de l'un d'entre eux.

5. Un serveur DNS faisant autorité est le serveur chargé de stocker les enregistrements DNS d'un nom de domaine particulier et sur lequel toute mise à jour des enregistrements DNS de votre nom de domaine serait effectuée. Selon le type d'enregistrement, l'enregistrement DNS est ensuite renvoyé au serveur DNS récursif, où une copie locale sera mise en cache pour les requêtes futures, puis retransmise au client d'origine qui a effectué la requête. Les enregistrements DNS sont tous accompagnés d'une valeur TTL (Time To Live). Cette valeur est un nombre représenté en secondes qui indique la durée pendant laquelle la réponse doit être enregistrée localement jusqu'à ce que vous deviez

la rechercher à nouveau. La mise en cache évite d'avoir à effectuer une requête DNS à chaque fois que vous communiquez avec un serveur.



Tâche 5 : Pratique

À l'aide du site Web situé à droite, nous pouvons créer des requêtes DNS et afficher les résultats. Le site Web vous indiquera également la commande à exécuter sur votre propre ordinateur si vous souhaitez effectuer vous-même les requêtes.

FIN