1.Introdução

DNS (*Domain Name System*) fornece uma maneira simples de nos comunicarmos com dispositivos na Internet sem lembrar de números complexos. Assim como cada casa tem um endereço exclusivo para enviar correspondência diretamente para ela, cada computador na Internet tem seu próprio endereço exclusivo para se comunicar, chamado endereço IP.

Um endereço IP se parece com 104.26.10.229, 4 conjuntos de dígitos variando de 0 a 255 separados por um ponto. Quando você deseja visitar um site, não é exatamente conveniente lembrar esse complicado conjunto de números, e é aí que o DNS pode ajudar. Então, em vez de lembrar 104.26.10.229, você pode lembrar tryhackme.com.

Um servidor DNS é um computador com um bando de dados contendo os endereços IP públicos associados aos nomes dos sites para os quais um endereço IP leva um usuário.

O trabalho de um **DNS Nameserver** é armazenar todos os registros DNS de um domínio. Quando alguém envia uma solicitação relacionada ao seu DNS, o servidor vai retornar toda a informação necessária sobre ele, permitindo que essa pessoa encontre o seu site. Na prática, os endereços de **Nameservers** são usados para apontar um domínio para uma conta de hospedagem através dos serviços de DNS.

2.TLD (Top-Level Domain)

Um TLD é a parte mais à direita de um nome de domínio. Assim, por exemplo, o TLD tryhackme.com é .com. Existem dois tipos de TLD, gTLD (*Generic Top Level)* e ccTLD (*Country Code Top Level Domain*).

Historicamente, um gTLD pretendia informar ao usuário a finalidade do nome de domínio; por exemplo, um .com seria para fins comerciais, .org para uma organização, .edu para educação e .gov para governo. E um ccTLD foi usado para fins geográficos, por exemplo, .ca para sites baseados no Canadá, .co.uk para sites baseados no Reino Unido e assim por diante. Devido a essa demanda, há um influxo de novos gTLDs que vão desde .online, .club, .website, .biz e muitos mais.

https://data.iana.org/TLD/tlds-alpha-by-domain.txt

2.1 Second Level Domain

Tomando tryhackme.com como exemplo, a parte .com é o TLD e tryhackme é o domínio de segundo nível. Ao registrar um nome de domínio, o domínio de segundo nível é limitado a 63 caracteres + o TLD e só pode usar a-z 0-9 e hífens.

2.2 Subdomain

Um **subdomínio** fica no lado esquerdo do domínio de segundo nível usando um ponto final para separá-lo; por exemplo, no nome admin.tryhackme.com a parte admin é o subdomínio. Um nome de subdomínio tem as mesmas restrições de criação de um Domínio de Segundo Nível, sendo limitado a 63 caracteres e só pode usar a-z 0-9 e hifens (não pode começar ou terminar com hífens ou ter hífens consecutivos).

Você pode usar vários subdomínios divididos com pontos para criar nomes mais longos, como jupiter.servers.tryhackme.com. Mas o comprimento deve ser mantido em 253 caracteres ou menos. Não há limite para o número de subdomínios que você pode criar para o seu nome de domínio. Porém, o DNS não é apenas para sites e existem vários tipos de registro DNS.

3.DNS recursivo

Em uma situação em que uma solicitação é enviada de maneira recorrente, um servidor pode pedir a outros servidores para atender à solicitação em nome do cliente. Isso é o que chamamos de DNS recursivo.

3.1 A record

Esses registros são resolvidos para endereços IPv4, por exemplo 104.26.10.229

3.2 AAAA record

Esses registros são resolvidos para endereços IPv6, por exemplo 2606:4700:20::681a:be5

3.3 CNAME record

Esses registros são resolvidos para outro nome de domínio, por exemplo, a loja online TryHackMe tem o nome de subdomínio store.tryhackme.com que retorna um registro CNAME lojas.shopify.com.

3.4 NS record

Servidor de domínio, especifica servidores DNS para domínio ou subdomínio. Pelo menos, dois registros NS devem ser definidos para cada domínio. Geralmente, um principal e outro secundário.

3.5 MX (Mail eXchanger) record

Esses registros são resolvidos para o endereço dos servidores que gerenciam o e-mail do domínio que você está consultando. Por exemplo, uma resposta de registro MX para tryhackme.com seria algo como alt1.aspmx.l.google.com. Esses registros também vêm com um sinalizador de prioridade. Isso informa ao cliente em que ordem os servidores devem ser testados, o que é perfeito para caso o servidor principal fique inativo e o e-mail precise ser enviado para um servidor de backup.

3.6 PTR (PoinTeR)

Aponta para o domínio reverso a partir de um endereço IP

3.7 SOA (Start Of Authority)

Indica o responsável por respostas autoritárias a um domínio, ou seja, o responsável pelo domínio. Também indica outras informações úteis como número serial da zona, replicação e outros.

3.8 TXT record

Os registros TXT são campos de texto livre onde qualquer dado baseado em texto pode ser armazenado. Os registros TXT têm vários usos, mas alguns dos mais comuns podem ser listar servidores que têm autoridade para enviar um email em nome do domínio (isso pode ajudar na batalha contra spam e emails falsificados). Eles também podem ser usados para verificar a propriedade do nome de domínio ao se inscrever em serviços de terceiros.

4.Como funciona um request DNS

1. Quando você solicita um nome de domínio, seu computador primeiro verifica o cache local para ver se você consultou o endereço recentemente; caso contrário, será feita uma solicitação ao seu servidor DNS recursivo.

2. Um servidor DNS recursivo geralmente é fornecido pelo seu ISP, mas você também pode escolher o seu próprio. Este servidor também possui um cache local de nomes de domínio pesquisados recentemente. Se um resultado for encontrado localmente, ele será enviado de volta ao seu computador e sua solicitação terminará aqui. Se a solicitação não puder ser encontrada localmente, começa uma jornada para encontrar a resposta correta, começando pelos servidores DNS raiz da Internet.

3. Os servidores raiz atuam como a espinha dorsal do DNS da Internet; o trabalho deles é redirecioná-lo para o servidor de domínio de nível superior correto, dependendo da sua solicitação. Se, por exemplo, você solicitar www.tryhackme.com, o servidor raiz reconhecerá o domínio de nível superior .com e encaminhará você para o servidor TLD correto que lida com endereços .com

4. O servidor TLD mantém registros de onde encontrar o servidor autorizado para responder à solicitação DNS. O servidor autoritativo também é conhecido como servidor de nomes do domínio. Por exemplo, o servidor de nomes para tryhackme.com é kip.ns.cloudflare.com e uma.ns.cloudflare.com. Freqüentemente, você encontrará vários servidores de nomes para um nome de domínio para atuar como backup no caso de um deles cair.

5. Um servidor DNS autoritativo é o servidor responsável por armazenar os registros DNS de um nome de domínio específico e onde seriam feitas quaisquer atualizações nos registros DNS do seu nome de domínio. Dependendo do tipo de registro, o registro DNS é então enviado de volta ao servidor DNS recursivo, onde

uma cópia local será armazenada em cache para solicitações futuras e então retransmitida de volta ao cliente original que fez a solicitação. Todos os registros DNS vêm com um valor TTL (Time To Live). Este valor é um número representado em segundos para o qual a resposta deve ser salva localmente até que você precise procurá-la novamente.