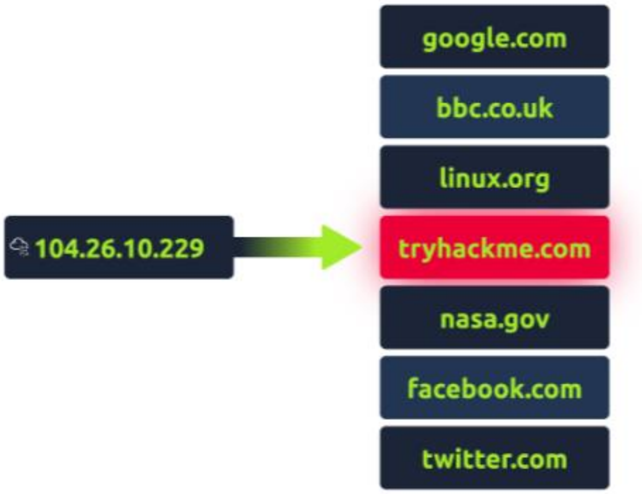
Introduction

The Domain Name System (DNS) is a critical component of the internet's infrastructure, acting as the bridge between human-friendly domain names and machine-friendly IP addresses. Understanding DNS is essential for anyone involved in internet technology, network administration, or cyber security. This report delves into the intricacies of DNS, exploring its structure, functionality, and different types of DNS records. The aim is to provide a clear understanding of how DNS works and its role in the seamless operation of the internet.

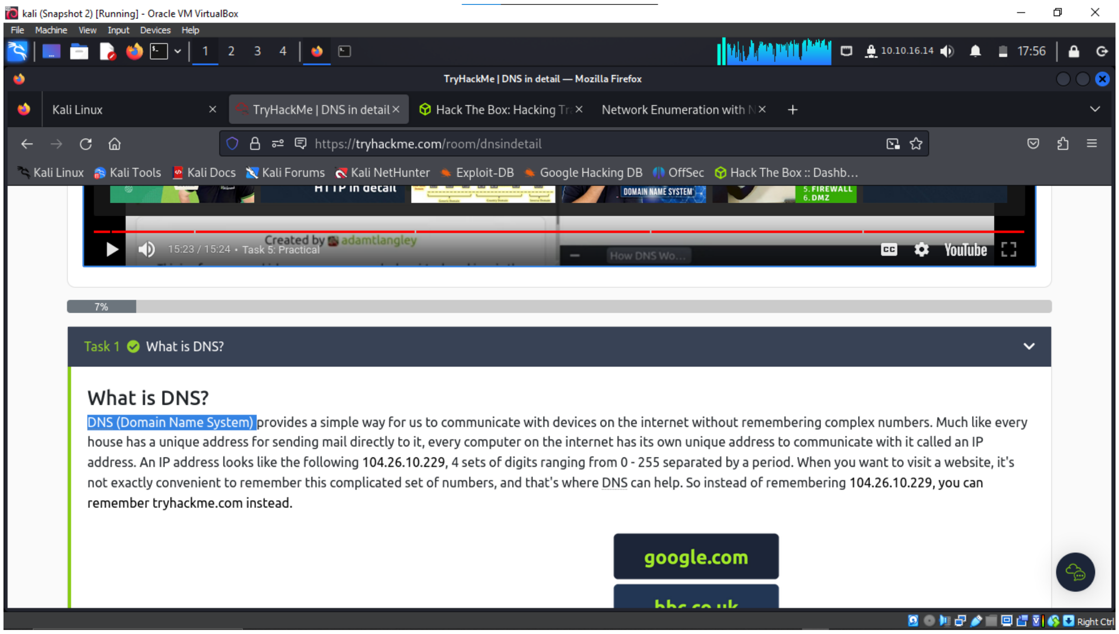
https://tryhackme.com/p/Damiano254

Task 1: What is DNS?

Explanation:
DNS (Domain Name System) is akin to the internet's phone book, translating domain names, which are easy for humans to remember, into IP addresses that computers use to identify each other on the network. This system makes it possible to access websites without needing to remember complex numerical addresses.



Question: What does DNS stand for?
Answer: Domain Name System


kali (Snapshot 2) [Running] - Oracle VM VirtualBox
TryHackMe | DNS in detail — Mozilla Firefox
Kali Linux
TryHackMe | DNS in detail
Hack The Box: Hacking Tr
Network Enumeration with N
https://tryhackme.com/room/dnsindetail
15:23 / 15:24 • Task 5: Practical
Created by adamtlangley
7%

Task 1 What is DNS?

What is DNS?

DNS (Domain Name System) provides a simple way for us to communicate with devices on the internet without remembering complex numbers. Much like every house has a unique address for sending mail directly to it, every computer on the internet has its own unique address to communicate with it called an IP address. An IP address looks like the following 104.26.10.229, 4 sets of digits ranging from 0 - 255 separated by a period. When you want to visit a website, it's not exactly convenient to remember this complicated set of numbers, and that's where DNS can help. So instead of remembering 104.26.10.229, you can remember tryhackme.com instead.

Task 2: Domain Hierarchy

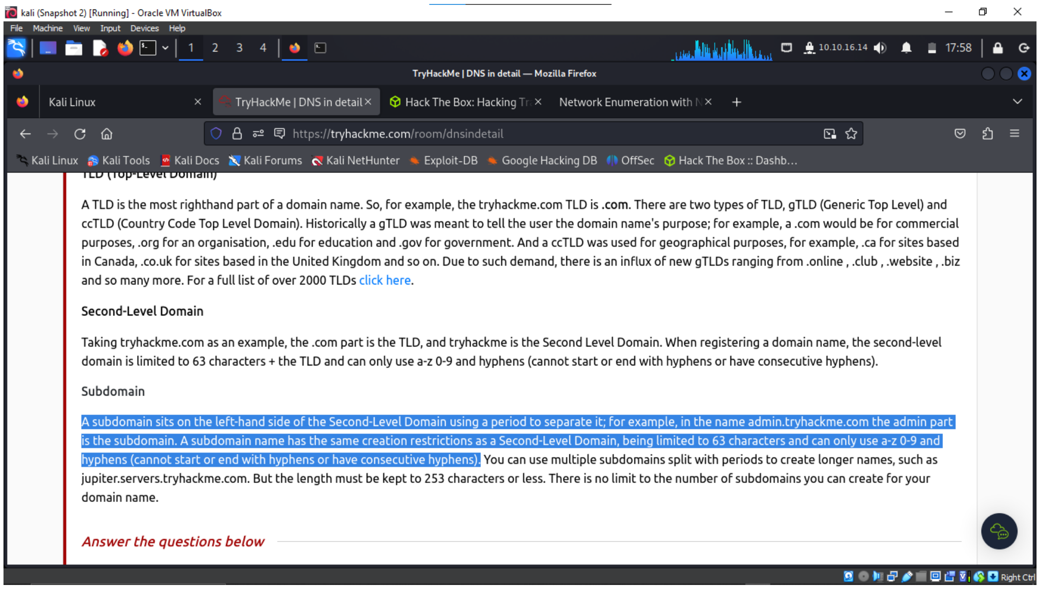
Explanation:

The domain hierarchy is an organized structure of domain names. It includes:

- **TLD (Top-Level Domain):** The rightmost part of a domain, like .com or .org.
- **Second-Level Domain:** The part of the domain to the left of the TLD, such as 'google' in google.com.
- **Subdomain:** A domain that is part of a larger domain, like 'mail' in mail.google.com.

Questions & Answers:

1. **Maximum length of a subdomain:** 63 characters


kali (Snapshot 2) [Running] - Oracle VM VirtualBox
TryHackMe | DNS in detail — Mozilla Firefox
Kali Linux
TryHackMe | DNS in detail
Hack The Box: Hacking Tr
Network Enumeration with N
https://tryhackme.com/room/dnsindetail

TLD (Top-Level Domain)

A TLD is the most righthand part of a domain name. So, for example, the tryhackme.com TLD is **.com**. There are two types of TLD, gTLD (Generic Top Level) and ccTLD (Country Code Top Level Domain). Historically a gTLD was meant to tell the user the domain name's purpose; for example, a .com would be for commercial purposes, .org for an organisation, .edu for education and .gov for government. And a ccTLD was used for geographical purposes, for example, .ca for sites based in Canada, .co.uk for sites based in the United Kingdom and so on. Due to such demand, there is an influx of new gTLDs ranging from .online , .club , .website , .biz and so many more. For a full list of over 2000 TLDs click here.

Second-Level Domain

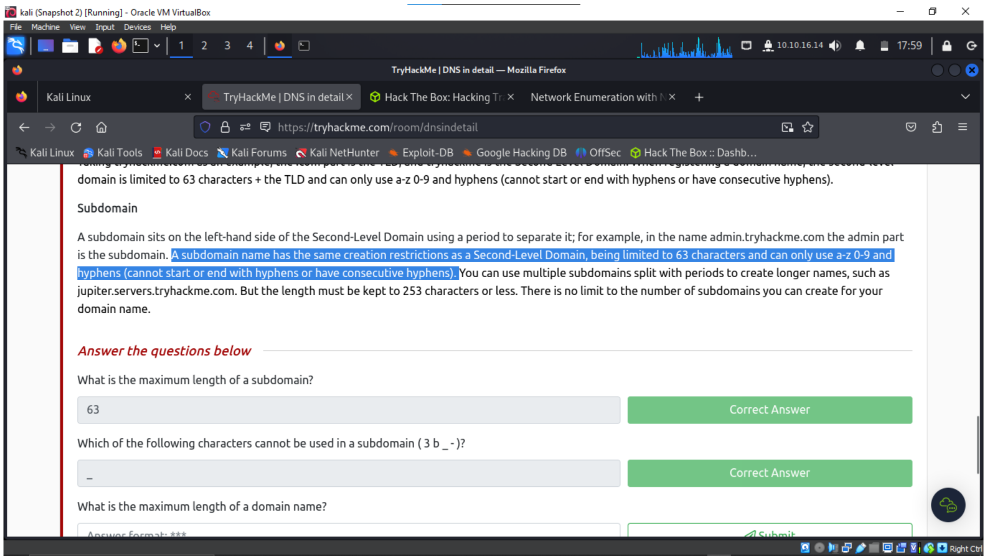
Taking tryhackme.com as an example, the .com part is the TLD, and tryhackme is the Second Level Domain. When registering a domain name, the second-level domain is limited to 63 characters + the TLD and can only use a-z 0-9 and hyphens (cannot start or end with hyphens or have consecutive hyphens).

Subdomain

A subdomain sits on the left-hand side of the Second-Level Domain using a period to separate it; for example, in the name admin.tryhackme.com the admin part is the subdomain. A subdomain name has the same creation restrictions as a Second-Level Domain, being limited to 63 characters and can only use a-z 0-9 and hyphens (cannot start or end with hyphens or have consecutive hyphens). You can use multiple subdomains split with periods to create longer names, such as jupiter.servers.tryhackme.com. But the length must be kept to 253 characters or less. There is no limit to the number of subdomains you can create for your domain name.

Answer the questions below

2. **Characters not used in a subdomain:** '_'


kali (Snapshot 2) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
10.10.16.14
17:59
TryHackMe | DNS in detail — Mozilla Firefox
Kali Linux
TryHackMe | DNS in detail
Hack The Box: Hacking Tr
Network Enumeration with N
https://tryhackme.com/room/dnsindetail
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Hack The Box :: Dashb…
Right Ctrl

domain is limited to 63 characters + the TLD and can only use a-z 0-9 and hyphens (cannot start or end with hyphens or have consecutive hyphens).

Subdomain

A subdomain sits on the left-hand side of the Second-Level Domain using a period to separate it; for example, in the name admin.tryhackme.com the admin part is the subdomain. A subdomain name has the same creation restrictions as a Second-Level Domain, being limited to 63 characters and can only use a-z 0-9 and hyphens (cannot start or end with hyphens or have consecutive hyphens). You can use multiple subdomains split with periods to create longer names, such as jupiter.servers.tryhackme.com. But the length must be kept to 253 characters or less. There is no limit to the number of subdomains you can create for your domain name.

Answer the questions below

What is the maximum length of a subdomain?

63

Correct Answer

Which of the following characters cannot be used in a subdomain (3 b _ -)?

_

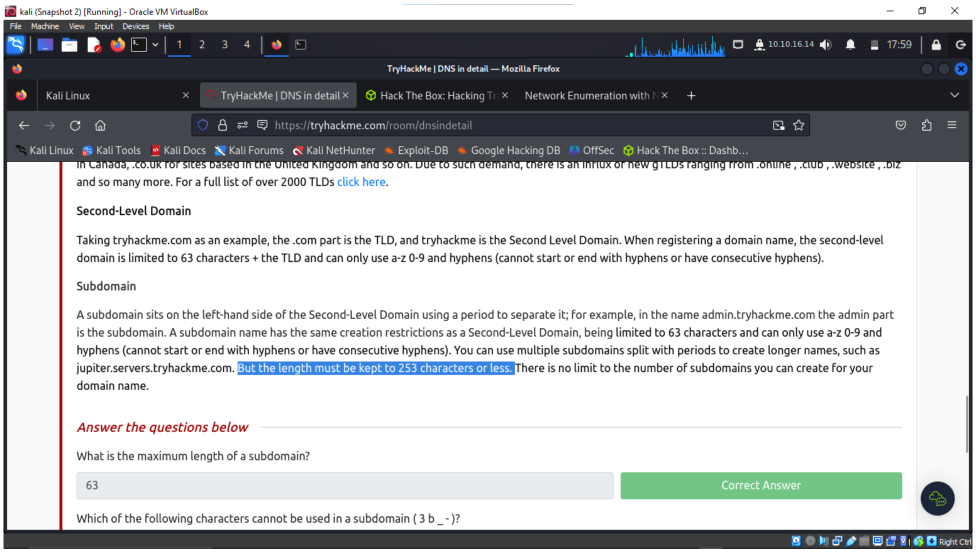
Correct Answer

What is the maximum length of a domain name?

Answer format: ***

Submit

3. **Maximum length of a domain name:** 253 characters


kali (Snapshot 2) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
10.10.16.14
17:59
TryHackMe | DNS in detail — Mozilla Firefox
Kali Linux
TryHackMe | DNS in detail
Hack The Box: Hacking Tr
Network Enumeration with N
https://tryhackme.com/room/dnsindetail
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Hack The Box :: Dashb…
Right Ctrl

in Canada, .co.uk for sites based in the United Kingdom and so on. Due to such demand, there is an influx of new gTLDs ranging from .online , .club , .website , .biz and so many more. For a full list of over 2000 TLDs click here.

Second-Level Domain

Taking tryhackme.com as an example, the .com part is the TLD, and tryhackme is the Second Level Domain. When registering a domain name, the second-level domain is limited to 63 characters + the TLD and can only use a-z 0-9 and hyphens (cannot start or end with hyphens or have consecutive hyphens).

Subdomain

A subdomain sits on the left-hand side of the Second-Level Domain using a period to separate it; for example, in the name admin.tryhackme.com the admin part is the subdomain. A subdomain name has the same creation restrictions as a Second-Level Domain, being limited to 63 characters and can only use a-z 0-9 and hyphens (cannot start or end with hyphens or have consecutive hyphens). You can use multiple subdomains split with periods to create longer names, such as jupiter.servers.tryhackme.com. But the length must be kept to 253 characters or less. There is no limit to the number of subdomains you can create for your domain name.

Answer the questions below

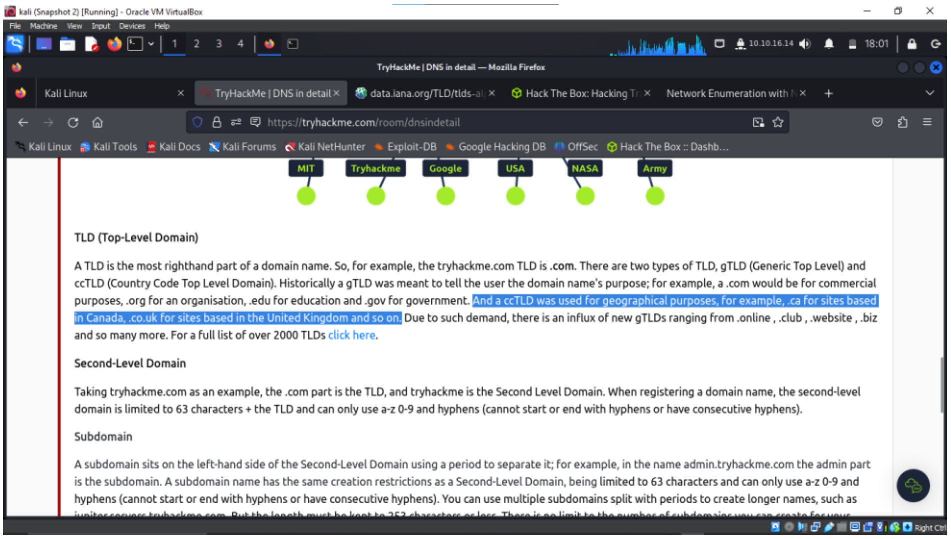
What is the maximum length of a subdomain?

63

Correct Answer

Which of the following characters cannot be used in a subdomain (3 b _ -)?

4. **Type of TLD for .co.uk:** ccTLD


kali (Snapshot 2) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
10.10.16.14
18:01
TryHackMe | DNS in detail — Mozilla Firefox
Kali Linux
TryHackMe | DNS in detail
data.iana.org/TLD/tlds-al
Hack The Box: Hacking Tr
Network Enumeration with N
https://tryhackme.com/room/dnsindetail
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Hack The Box :: Dashb…
MIT
Tryhackme
Google
USA
NASA
Army
Right Ctrl

TLD (Top-Level Domain)

A TLD is the most righthand part of a domain name. So, for example, the tryhackme.com TLD is **.com**. There are two types of TLD, gTLD (Generic Top Level) and ccTLD (Country Code Top Level Domain). Historically a gTLD was meant to tell the user the domain name's purpose; for example, a .com would be for commercial purposes, .org for an organisation, .edu for education and .gov for government. And a ccTLD was used for geographical purposes, for example, .ca for sites based in Canada, .co.uk for sites based in the United Kingdom and so on. Due to such demand, there is an influx of new gTLDs ranging from .online , .club , .website , .biz and so many more. For a full list of over 2000 TLDs click here.

Second-Level Domain

Taking tryhackme.com as an example, the .com part is the TLD, and tryhackme is the Second Level Domain. When registering a domain name, the second-level domain is limited to 63 characters + the TLD and can only use a-z 0-9 and hyphens (cannot start or end with hyphens or have consecutive hyphens).

Subdomain

A subdomain sits on the left-hand side of the Second-Level Domain using a period to separate it; for example, in the name admin.tryhackme.com the admin part is the subdomain. A subdomain name has the same creation restrictions as a Second-Level Domain, being limited to 63 characters and can only use a-z 0-9 and hyphens (cannot start or end with hyphens or have consecutive hyphens). You can use multiple subdomains split with periods to create longer names, such as jupiter.servers.tryhackme.com. But the length must be kept to 253 characters or less. There is no limit to the number of subdomains you can create for your

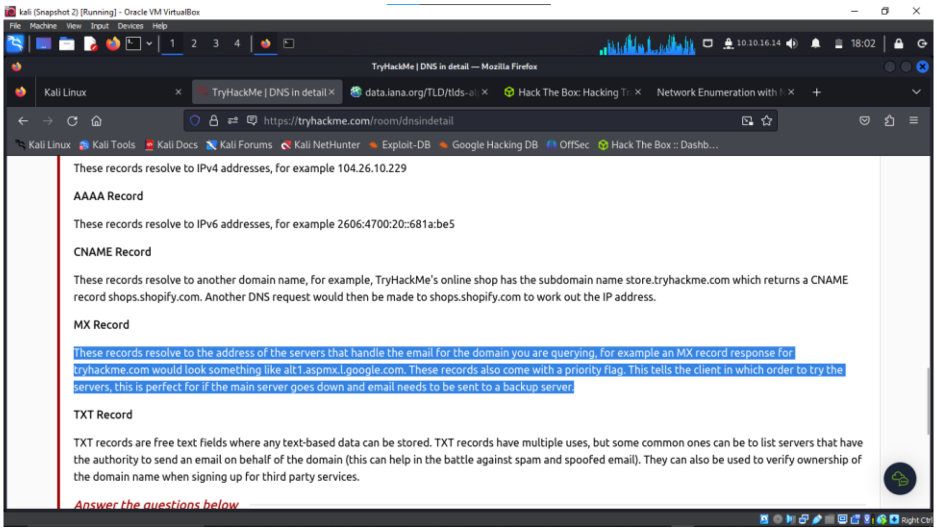
Task 3: DNS Record Types

Explanation:

Various DNS records serve different purposes, like directing web traffic, email, and other services.

Questions & Answers:

1. **Record for email direction:** MX Record


kali (Snapshot 2) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
TryHackMe | DNS in detail — Mozilla Firefox
Kali Linux
TryHackMe | DNS in detail
data.iana.org/TLD/tlds-al
Hack The Box: Hacking Tr
Network Enumeration with N
https://tryhackme.com/room/dnsindetail
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Hack The Box :: Dashb…
18:02
Right Ctrl

These records resolve to IPv4 addresses, for example 104.26.10.229

AAAA Record

These records resolve to IPv6 addresses, for example 2606:4700:20::681a:be5

CNAME Record

These records resolve to another domain name, for example, TryHackMe's online shop has the subdomain name store.tryhackme.com which returns a CNAME record shops.shopify.com. Another DNS request would then be made to shops.shopify.com to work out the IP address.

MX Record

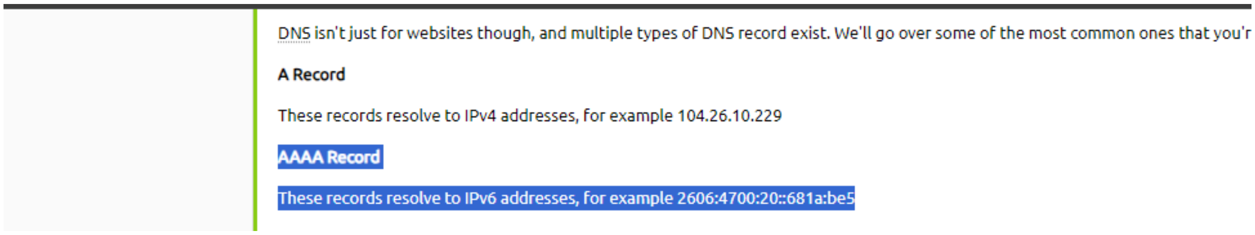
These records resolve to the address of the servers that handle the email for the domain you are querying, for example an MX record response for tryhackme.com would look something like alt1.aspmx.l.google.com. These records also come with a priority flag. This tells the client in which order to try the servers, this is perfect for if the main server goes down and email needs to be sent to a backup server.

TXT Record

TXT records are free text fields where any text-based data can be stored. TXT records have multiple uses, but some common ones can be to list servers that have the authority to send an email on behalf of the domain (this can help in the battle against spam and spoofed email). They can also be used to verify ownership of the domain name when signing up for third party services.

Answer the questions below

2. **Record handling IPv6 addresses:** AAAA Record



DNS isn't just for websites though, and multiple types of DNS record exist. We'll go over some of the most common ones that you'r

A Record

These records resolve to IPv4 addresses, for example 104.26.10.229

AAAA Record

These records resolve to IPv6 addresses, for example 2606:4700:20::681a:be5

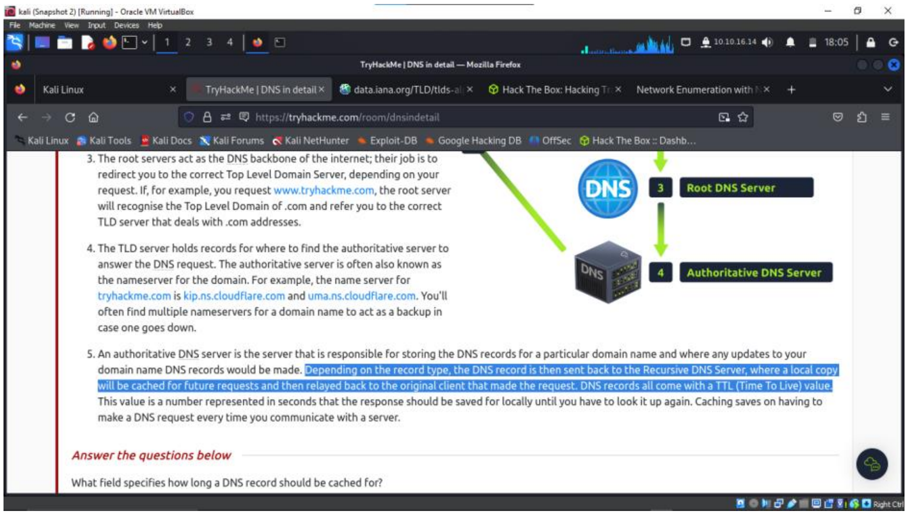
Task 4: Making A DNS Request

Explanation:

The process of making a DNS request involves several steps, from checking the local cache to querying the root and TLD servers, and finally getting the required information from the authoritative DNS server.

Questions & Answers:

1. **Field specifying DNS record cache duration:** TTL


kali (Snapshot 2) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
TryHackMe | DNS in detail — Mozilla Firefox
Kali Linux
TryHackMe | DNS in detail
data.iana.org/TLD/tlds-al
Hack The Box: Hacking Tr
Network Enumeration with N
https://tryhackme.com/room/dnsindetail
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Hack The Box :: Dashb…
18:05
DNS
3
Root DNS Server
DNS
4
Authoritative DNS Server
Right Ctrl

3. The root servers act as the DNS backbone of the internet; their job is to redirect you to the correct Top Level Domain Server, depending on your request. If, for example, you request www.tryhackme.com, the root server will recognise the Top Level Domain of .com and refer you to the correct TLD server that deals with .com addresses.

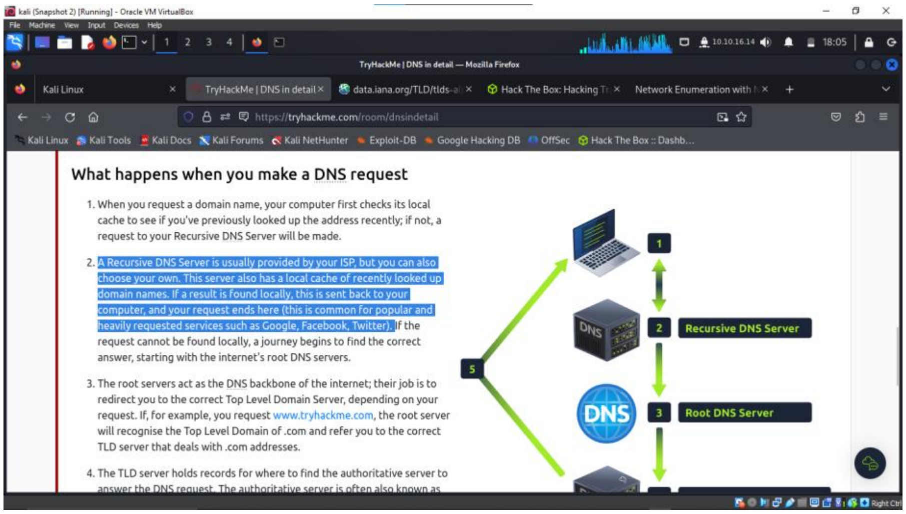
4. The TLD server holds records for where to find the authoritative server to answer the DNS request. The authoritative server is often also known as the nameserver for the domain. For example, the name server for tryhackme.com is kip.ns.cloudflare.com and uma.ns.cloudflare.com. You'll often find multiple nameservers for a domain name to act as a backup in case one goes down.

5. An authoritative DNS server is the server that is responsible for storing the DNS records for a particular domain name and where any updates to your domain name DNS records would be made. Depending on the record type, the DNS record is then sent back to the Recursive DNS Server, where a local copy will be cached for future requests and then relayed back to the original client that made the request. DNS records all come with a TTL (Time To Live) value. This value is a number represented in seconds that the response should be saved for locally until you have to look it up again. Caching saves on having to make a DNS request every time you communicate with a server.

Answer the questions below

What field specifies how long a DNS record should be cached for?

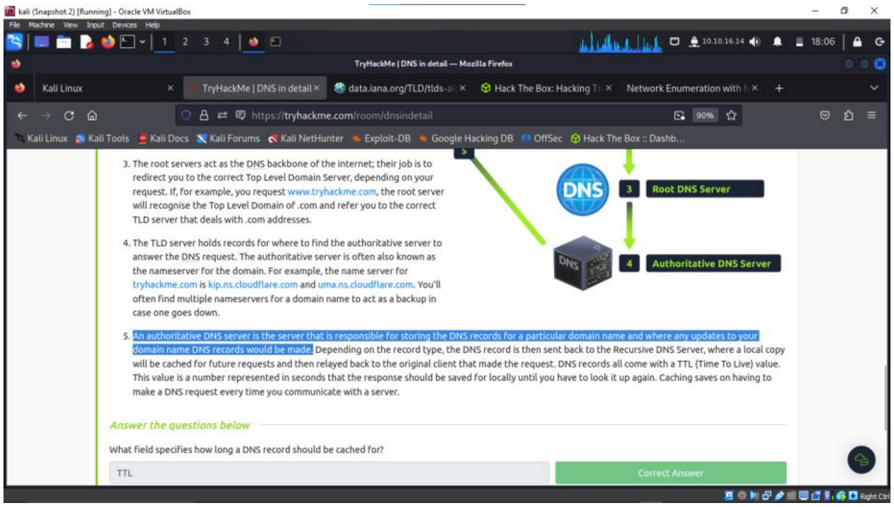
2. **Type of DNS Server typically provided by ISP:** Recursive DNS Server


kali (Snapshot 2) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
10.10.16.14
18:05
TryHackMe | DNS in detail — Mozilla Firefox
Kali Linux
TryHackMe | DNS in detail
data.iana.org/TLD/tlds-al
Hack The Box: Hacking Tr
Network Enumeration with N
https://tryhackme.com/room/dnsindetail
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Hack The Box :: Dashb...
1
2
Recursive DNS Server
DNS
3
Root DNS Server
5
Right Ctrl

What happens when you make a DNS request

1. When you request a domain name, your computer first checks its local cache to see if you've previously looked up the address recently; if not, a request to your Recursive DNS Server will be made.
2. A Recursive DNS Server is usually provided by your ISP, but you can also choose your own. This server also has a local cache of recently looked up domain names. If a result is found locally, this is sent back to your computer, and your request ends here (this is common for popular and heavily requested services such as Google, Facebook, Twitter). If the request cannot be found locally, a journey begins to find the correct answer, starting with the internet's root DNS servers.
3. The root servers act as the DNS backbone of the internet; their job is to redirect you to the correct Top Level Domain Server, depending on your request. If, for example, you request www.tryhackme.com, the root server will recognise the Top Level Domain of .com and refer you to the correct TLD server that deals with .com addresses.
4. The TLD server holds records for where to find the authoritative server to answer the DNS request. The authoritative server is often also known as

3. **Server holding all records for a domain:** Authoritative DNS Server


kali (Snapshot 2) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
10.10.16.14
18:06
TryHackMe | DNS in detail — Mozilla Firefox
Kali Linux
TryHackMe | DNS in detail
data.iana.org/TLD/tlds-al
Hack The Box: Hacking Tr
Network Enumeration with N
https://tryhackme.com/room/dnsindetail
90%
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Hack The Box :: Dashb...
DNS
3
Root DNS Server
DNS
4
Authoritative DNS Server
Right Ctrl

3. The root servers act as the DNS backbone of the internet; their job is to redirect you to the correct Top Level Domain Server, depending on your request. If, for example, you request www.tryhackme.com, the root server will recognise the Top Level Domain of .com and refer you to the correct TLD server that deals with .com addresses.
4. The TLD server holds records for where to find the authoritative server to answer the DNS request. The authoritative server is often also known as the nameserver for the domain. For example, the name server for tryhackme.com is kip.ns.cloudflare.com and uma.ns.cloudflare.com. You'll often find multiple nameservers for a domain name to act as a backup in case one goes down.
5. An authoritative DNS server is the server that is responsible for storing the DNS records for a particular domain name and where any updates to your domain name DNS records would be made. Depending on the record type, the DNS record is then sent back to the Recursive DNS Server, where a local copy will be cached for future requests and then relayed back to the original client that made the request. DNS records all come with a TTL (Time To Live) value. This value is a number represented in seconds that the response should be saved for locally until you have to look it up again. Caching saves on having to make a DNS request every time you communicate with a server.

Answer the questions below

What field specifies how long a DNS record should be cached for?

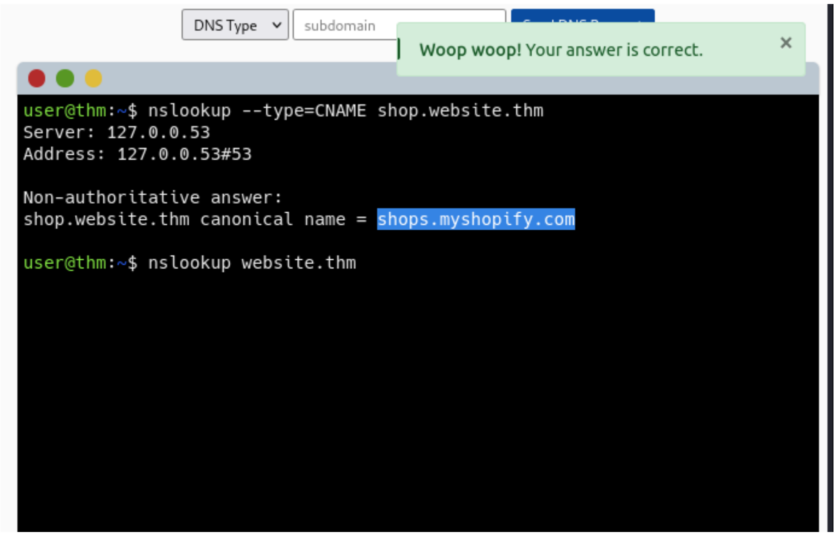
TTL

Correct Answer

Task 5: Practical Application

Questions & Answers:

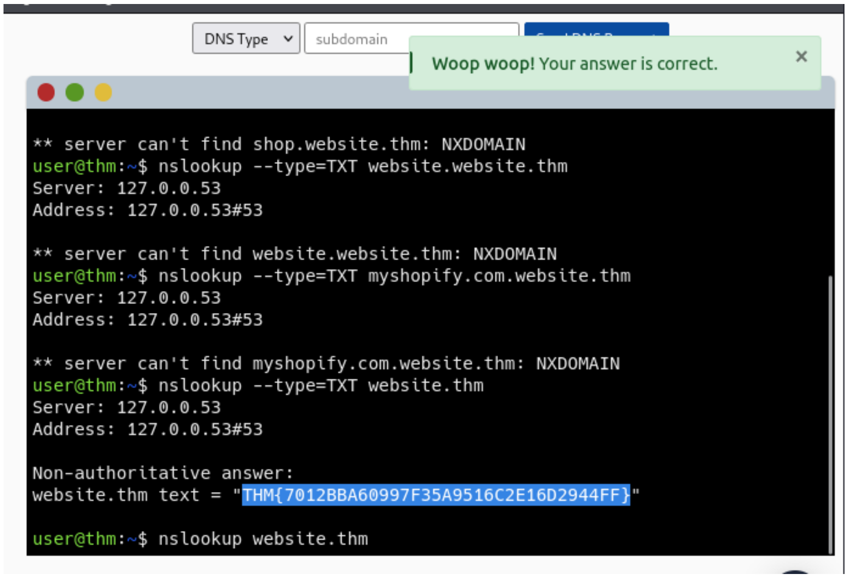
1. **CNAME of shop.website.thm:** shops.myshopify.com



Woop woop! Your answer is correct.

```
user@thm:~$ nslookup --type=CNAME shop.website.thm
Server: 127.0.0.53
Address: 127.0.0.53#53

Non-authoritative answer:
shop.website.thm canonical name = shops.myshopify.com

user@thm:~$ nslookup website.thm
```

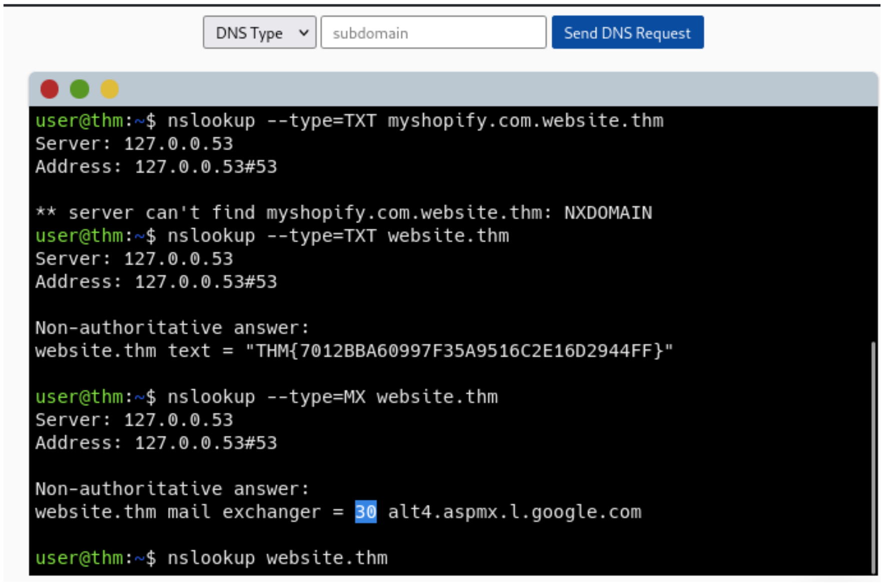
2. **TXT record value of website.thm:** THM{7012BBA60997F35A9516C2E16D2944FF}



Woop woop! Your answer is correct.

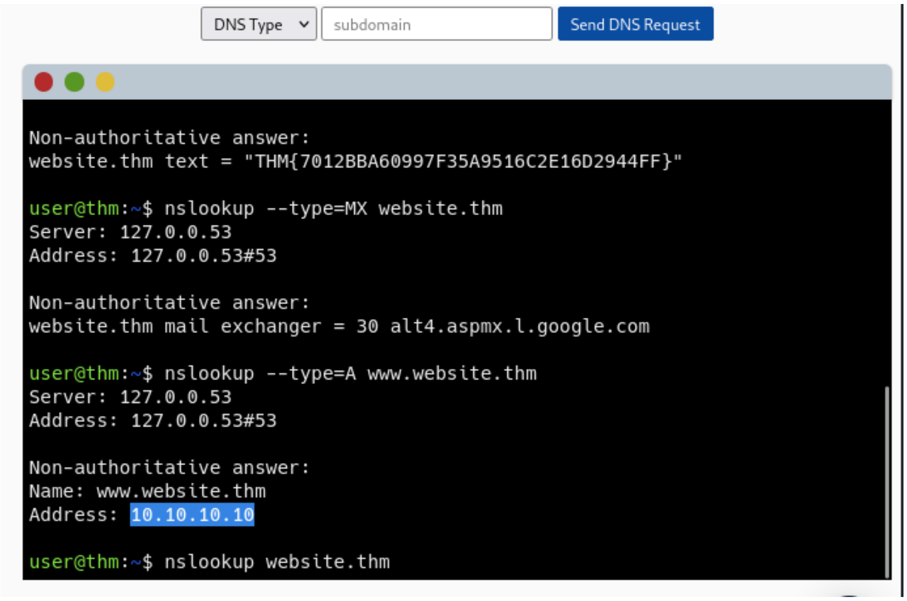
```
** server can't find shop.website.thm: NXDOMAIN
user@thm:~$ nslookup --type=TXT website.website.thm
Server: 127.0.0.53
Address: 127.0.0.53#53

** server can't find website.website.thm: NXDOMAIN
user@thm:~$ nslookup --type=TXT myshopify.com.website.thm
Server: 127.0.0.53
Address: 127.0.0.53#53

** server can't find myshopify.com.website.thm: NXDOMAIN
user@thm:~$ nslookup --type=TXT website.thm
Server: 127.0.0.53
Address: 127.0.0.53#53

Non-authoritative answer:
website.thm text = "THM{7012BBA60997F35A9516C2E16D2944FF}"

user@thm:~$ nslookup website.thm
```

3. **Numerical priority of MX record:** 30



```
user@thm:~$ nslookup --type=TXT myshopify.com.website.thm
Server: 127.0.0.53
Address: 127.0.0.53#53

** server can't find myshopify.com.website.thm: NXDOMAIN
user@thm:~$ nslookup --type=TXT website.thm
Server: 127.0.0.53
Address: 127.0.0.53#53

Non-authoritative answer:
website.thm text = "THM{7012BBA60997F35A9516C2E16D2944FF}"

user@thm:~$ nslookup --type=MX website.thm
Server: 127.0.0.53
Address: 127.0.0.53#53

Non-authoritative answer:
website.thm mail exchanger = 30 alt4.aspmx.l.google.com

user@thm:~$ nslookup website.thm
```

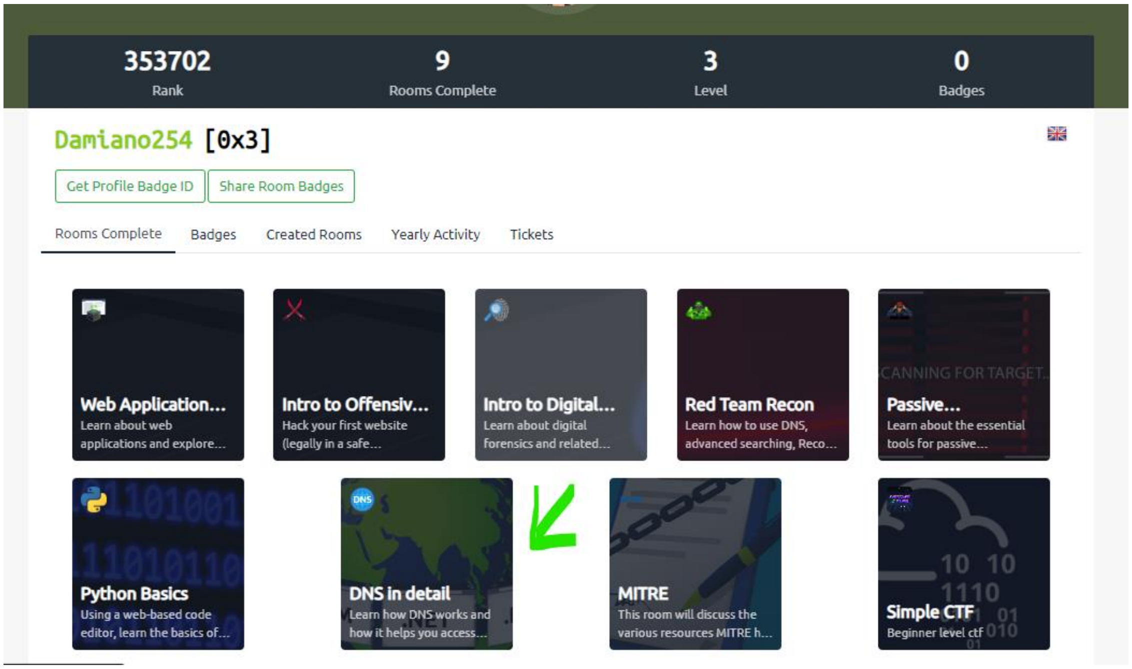
4. **IP address for A record of www.website.thm:** 10.10.10.10



```
Non-authoritative answer:
website.thm text = "THM{7012BBA60997F35A9516C2E16D2944FF}"

user@thm:~$ nslookup --type=MX website.thm
Server: 127.0.0.53
Address: 127.0.0.53#53

Non-authoritative answer:
website.thm mail exchanger = 30 alt4.aspmx.l.google.com

user@thm:~$ nslookup --type=A www.website.thm
Server: 127.0.0.53
Address: 127.0.0.53#53

Non-authoritative answer:
Name: www.website.thm
Address: 10.10.10.10

user@thm:~$ nslookup website.thm
```

Conclusion

DNS is a foundational technology that makes navigating the internet user-friendly and efficient. It's a complex system of hierarchies and records that ensures users can find websites using simple names instead of numerical addresses. The DNS system's reliability and scalability have been key to the growth and usability of the internet. As technology evolves, the importance of understanding and effectively managing DNS will continue to be paramount for ensuring a secure and accessible digital world.



353702 Rank | 9 Rooms Complete | 3 Level | 0 Badges

Damiano254 [0x3]

Web Application... Learn about web applications and explore...

Intro to Offensiv... Hack your first website (legally in a safe...

Intro to Digital... Learn about digital forensics and related...

Red Team Recon Learn how to use DNS, advanced searching, Reco...

Passive... Learn about the essential tools for passive...

Python Basics Using a web-based code editor, learn the basics of...

DNS in detail Learn how DNS works and how it helps you access...

MITRE This room will discuss the various resources MITRE h...

Simple CTF Beginner level ctf