Section 1.1.6 Computer Networks Fundamentals

DNS
{Domain Name System}

Cracking OSCP: Your Roadmap to Ethical Hacking Success

Socials: HackProKP

Github: https://github.com/at0m-b0mb/Cracking-OSCP-Your-Roadmap-to-Ethical-Hacking-Success

Complete Youtube Playlist: https://www.youtube.com/watch?v=MvkNbn8i2so&list=PLyrv3TPh3ejYNZipa0OIUvkdjHeUTRJ3J&index=1&t=0s

WHAT'S DNS?

The **Domain Name System** (DNS) is a **hierarchical** and **distributed naming system** for computers, services, and other resources on the Internet.

It's a crucial component of the internet that **translates human-readable domain names** into **IP addresses** and vice versa.

DNS serves as the **phonebook** of the **internet**. It translates domain names (like www.example.com) into IP addresses (like 192.0.2.1) that computers use to identify each other on the network.

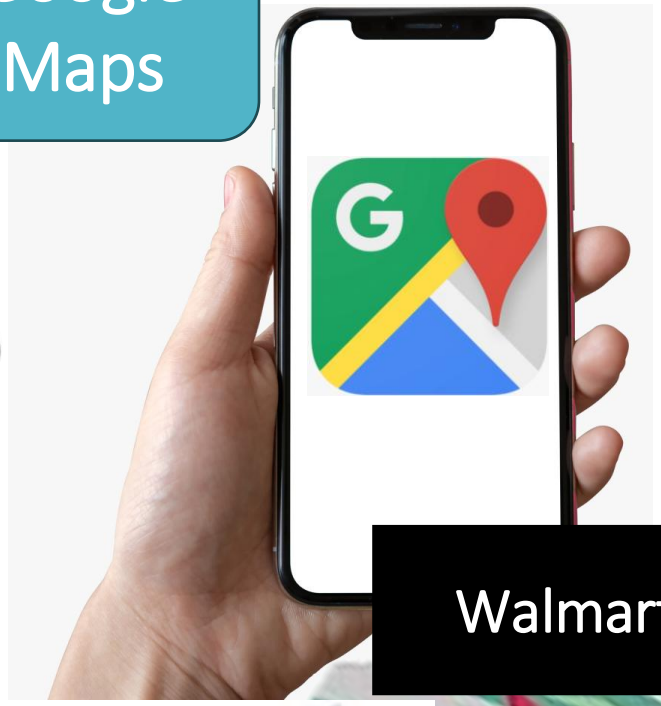
Billy

Wants the new COD Game

Smart

Walmart !!!!

Where is Walmart??



Walmart Address: XXXXXXXXXXXX

Yuppie!!!


TCL
CALL OF DUTY
MODERN
WARFARE
III


PS5
CALL OF DUTY
MODERN
WARFARE
III
18

Hierarchy of DNS:

DNS operates in a hierarchical structure, organized into zones and domains.

At the top level, there are the **root servers**, which store information about the authoritative name servers for top-level domains (TLDs) like **.com, .org, .net**, etc.

Beneath the TLDs are second-level domains (SLDs), which are further divided into subdomains.

Components of DNS:

DNS Resolver: This is the client-side component of DNS. When you type a domain name into a web browser, the resolver is responsible for querying DNS servers to find the corresponding IP address.

DNS Server: These servers store DNS records and respond to DNS queries from resolvers. There are several types of DNS servers, including:

1. Root Servers
2. TLD Servers
3. Authoritative DNS Servers
4. Recursive DNS Servers:

Components of DNS:

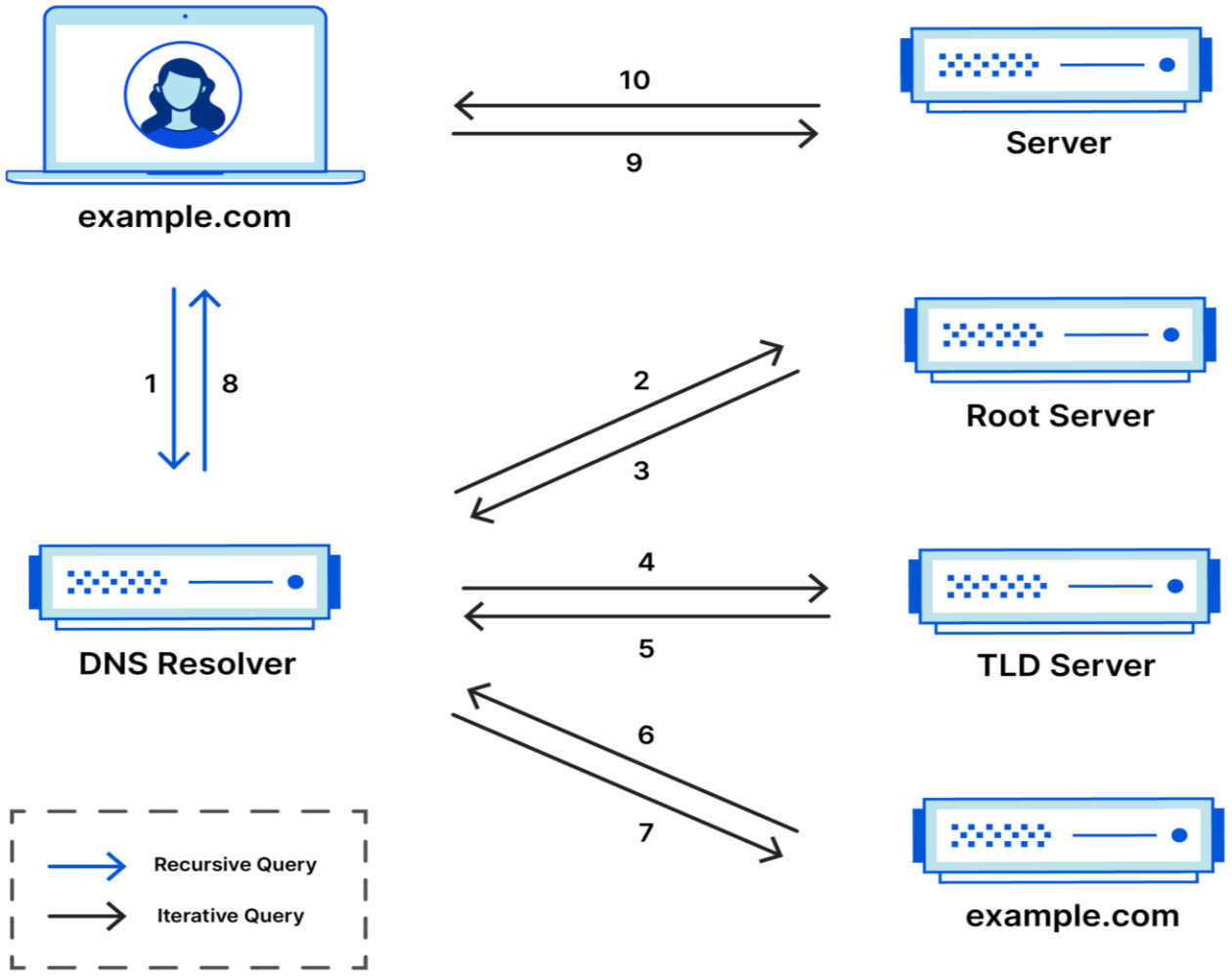
- **Root Servers:** These servers are responsible for directing queries to the appropriate TLD servers.
- **TLD Servers:** They manage top-level domain information.
- **Authoritative DNS Servers:** These servers store DNS records for specific domains and provide authoritative responses to queries about those domains.
- **Recursive DNS Servers:** These servers perform DNS resolution on behalf of clients, recursively querying other DNS servers until they find the IP address associated with a domain name.

DNS Record:

Common types of DNS records include:

- **A Record:** Maps a domain name to an IPv4 address.
  Example: example.com A 192.0.2.1
- **AAAA Record:** Maps a domain name to an IPv6 address.
  Example: example.com AAAA 2001:0db8:85a3:0000:0000:8a2e:0370:7334
- **CNAME Record:** Creates an alias for a domain name (canonical name). Example: www.example.com CNAME example.com
- **MX Record:** Specifies the mail servers responsible for receiving email on behalf of a domain. Example: example.com MX 10 mail.example.com
- **TXT Record:** Stores arbitrary text data, often used for verification or authentication purposes. Example: example.com TXT "v=spf1 ip4:192.0.2.0/24 -all"

Complete DNS Lookup and Webpage Query



https://www.cloudflare.com/learning/dns/what-is-dns/

DNS Resolution Process:

1. When you type a domain name into your web browser, your DNS resolver sends a query to a recursive DNS server.
2. The recursive DNS server starts by querying the root servers to find the authoritative name servers for the appropriate TLD.
3. It then queries the TLD servers to find the authoritative name servers for the domain.
4. Finally, it queries the authoritative name servers for the domain to obtain the IP address associated with the domain name.
5. Once the IP address is obtained, it is cached by the recursive DNS server for future use, and the resolver can then connect to the desired IP address.

DNS Caching:

To improve performance and reduce DNS query traffic, DNS servers cache the results of previous queries.

Caching occurs at various levels, including the resolver, recursive DNS servers, and even within ISP networks.

Cached DNS records have a **time-to-live** (TTL) value, which specifies how long the record can be stored before it expires and must be refreshed.

DNS Security:

DNS is vulnerable to various attacks, such as **DNS spoofing**, **cache poisoning**, and **DNS amplification attacks.**

To mitigate these risks, several security measures have been developed, including **DNSSEC** (Domain Name System Security Extensions), which adds cryptographic signatures to DNS records to ensure their integrity and authenticity.

DNS TOOLS

Windows Commands:

1. nslookup: This command-line tool is used to query DNS servers and obtain domain name or IP address information.

Syntax: nslookup domain or IP

Example: nslookup www.youtube.com

2. ipconfig /flushdns: This command is used to flush the DNS resolver cache on a Windows machine.

Syntax: ipconfig /flushdns

Flushing the DNS cache can be useful for troubleshooting DNS resolution issues.

3. ipconfig /displaydns: This command displays the contents of the DNS resolver cache on a Windows machine.

Syntax: ipconfig /displaydns

It shows a list of resolved DNS entries along with their TTL (Time-to-Live) values.

DNS TOOLS

Linux Commands:

1. dig: dig (domain information groper) is a flexible tool for interrogating DNS name servers.

Syntax: dig domain

Example: dig www.youtube.com

2. host: This command is used to perform DNS lookups and display the corresponding IP addresses.

Syntax: host domain

Example: host www.youtube.com

3. nslookup: Although more common on Windows, nslookup is also available on Linux systems.

Syntax: nslookup domain

Example: nslookup www.youtube.com

Thank You!

Please Like 👍 and Subscribe 📖 to never miss a video 🎥

And to help me with the Algorithm 🤖

And It’s completely Free!!! 💵

Love you guys ❤️