DNS

- DNS refer to domain name system
- every device connected to the internet has a gateway
- to get the IP of the website we use **nslookup** command in linux
  - nslookup google.com

    nslookup google.com

    Server: 8.8.8.8

    Address: 8.8.8.8#53

    Non-authoritative answer:

    Name: google.com

    Address: 142.250.201.14

    Name: google.com

    Address: 2a00:1450:4006:80e::200e
  - nslookup yahoo.com

    Server: 8.8.8.8

    Address: 8.8.8.8#53

    Non-authoritative answer:

    Name: yahoo.com

    Address: 74.6.231.20

    Name: yahoo.com

    Address: 74.6.143.25

    Name: yahoo.com

    Address: 74.6.231.21

    Name: yahoo.com

    Address: 98.137.11.163

    Name: yahoo.com

    Address: 98.137.11.164

    Name: yahoo.com

    Address: 74.6.143.26

    Name: yahoo.com

Address: 2001:4998:44:3507::8000

Name: yahoo.com

Address: 2001:4998:44:3507::8001

Name: yahoo.com

Address: 2001:4998:124:1507::f000

Name: yahoo.com

Address: 2001:4998:24:120d::1:1

Name: yahoo.com

Address: 2001:4998:124:1507::f001

Name: yahoo.com

Address: 2001:4998:24:120d::1:0

Known Attacks on DNS

- DNS Poisoning
- Subdomain Takeover
- DNS Cache Snooping
- DNS Amplification Attacks (DDOS)

dnschef command in linux

- allow you to make fake DNS

```
DNSChef is a highly configurable DNS proxy for Penetration Testers and Malware
Analysts. A DNS proxy (aka "Fake DNS") is a tool used for application network
traffic analysis among other uses. For example, a DNS proxy can be used to fake
requests for "badguy.com" to point to a local machine for termination or
interception instead of a real host somewhere on the Internet.
```

Different DNS types

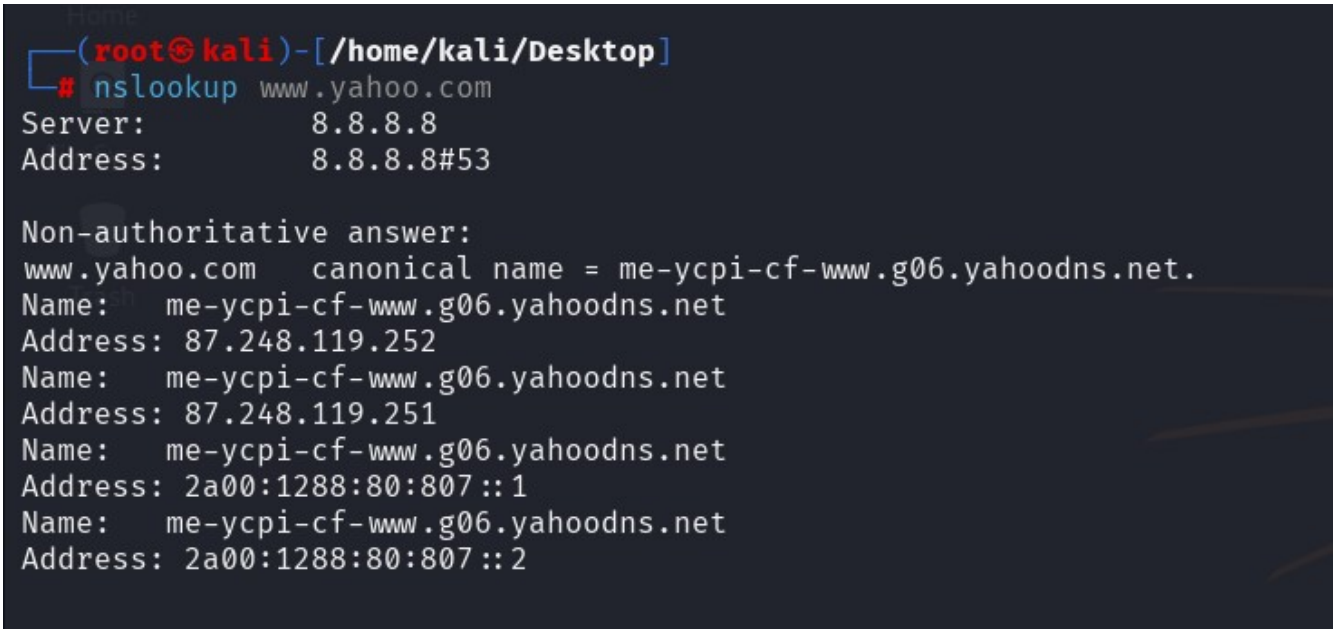
Record Type	Description
A	These are the subdomains like [**www.yahoo.com**], subdomains called A records, there are many ways to show the all A records (subdomains) like **sublister** tool example: **dig @8.8.8.8 www.yahoo.com**
AAAA	Matches a domain name to an IPV6 address. DNS AAAA records are exactly like DNS A records except they store a domain's IPV6 address instead of its IPV4 address. IPV6 is the latest version of the internet protocol (IP)

MX	The MX record directs emails to a mail exchange server. MX record indicate how email messages should be routed in accordance with the simple mail transfer protocol (SMTP, the standard protocol for all email)
CNAME	Alias → Subdomain Takeover a type of DNS record that maps an alias name to a true or canonical domain name. CNAME records are typically used to map a subdomain such as WWW or mail to the domain hosting that subdomain's content
PTR	Provide the domain name associated with an IP address. A DNS PTR record is exactly the opposite of 'A' record which provide the IP address associated with a domain name. A PTR records are used in reverse DNS lookup

Tools

- dig, nslookup, mxtoolboc.com

Example about CNAME: nslookup www.yahoo.com



Subdomain Takeover

- **dig @8.8.8.8 MX www.google.com**
- **dig @8.8.8.8 A www.yahoo.com**
- **dig @8.8.8.8 PTR 74.6.143.25** **// PTR usually used with the IP address**
- **dig PTR 142.251.12.113** **// PTR usually used with the IP address**

Subdomain takeover is a type of security vulnerability that occurs when a subdomain (e.g., `sub.example.com`) points to an external service (like GitHub Pages, Heroku, AWS, etc.), but the resource or account associated with that service has been deleted or is no longer in use—**yet the DNS record still exists**.

How it works:

1. A company sets up a subdomain (`blog.example.com`) to point to a third-party service (e.g., GitHub Pages).
2. Later, they remove the GitHub repository or the GitHub Pages site.
3. However, they **forget to delete the DNS CNAME or A record** that points `blog.example.com` to GitHub.
4. An attacker finds that `blog.example.com` is pointing to GitHub, but there's no content hosted.
5. The attacker creates a GitHub repository with the same name and **claims control** over `blog.example.com`.

Example:

blog.example.com -> blog-user.github.io

If `blog-user` deletes their GitHub Pages repository, and the DNS still points to GitHub, **anyone** can register `blog-user` and control `blog.example.com`.

Common services vulnerable to subdomain takeovers:

- GitHub Pages
- Heroku
- AWS S3 buckets
- Azure
- Shopify
- Bitbucket
- WordPress (managed hosting)

How to prevent it:

- Regularly audit your DNS records.
- Remove DNS entries for services no longer in use.
- Use automated tools to scan for dangling subdomains.
- Monitor third-party services and integrations.