DNS Bruteforcing & Subdomain Enumeration

What is DNS Bruteforcing ?

DNS Bruteforcing is a technique used to discover subdomains or hostnames associated with a target domain. It involves systematically generating and sending a large number of DNS queries to find valid subdomains.

Imagine you have a company website example.com. So, During DNS bruteforcing, you would try querying the DNS server with different combinations of words and phrases, like:

- www.example.com
- mail.example.com
- support.example.com
- blog.example.com
- etc.

The goal is to find subdomains that resolve to valid IP addresses and are actively used by the target organization. This can uncover hidden or forgotten subdomains that we might have missed with our subdomain hunting before.

- **Peform DNS bruteforcing & Subdomain Enumeration with dnsmap**

```
dnsmap zomato.com -w subdomain-brute.txt
```

- **DNS Bruteforcing with Nmap**

```
nmap -p 53 --script dns-brute zonetransfer.me
```

Remember, this is also kinda a active information gathering because we are sending some sort of request to the target. However, these requests can be ruled out as normal traffic if we don't overload the target server with our request.
