Hunting for Subdomains

Subdomains are like separate rooms or sections within a main website or domain. Just like how a house has different rooms for different purposes (bedroom, kitchen, living room, etc.), a website can have subdomains to organize different areas or functions.

To explain with an example, let's say the main website is www.zomato.com. This is like the main entrance or living room of the website. Now, the website owner may want to have a separate section for their blog, online store, or support center. Instead of cramming everything into the main website, they can create:

- blog.zomato.com (for the blog section)
- store.zomato.com (for the online store)
- support.zomato.com (for customer support)

In information gathering phase -

Subdomains can reveal a wealth of information about an organization's infrastructure, services, and internal operations. By identifying subdomains, we can uncover forgotten or misconfigured assets, potential entry points for further reconnaissance, and even undiscovered vulnerabilities that could be exploited.

- **Pen Test Tools** - https://pentest-tools.com/information-gathering/find-subdomains-of-domain
- **Sub Domain Finder** - https://subdomainfinder.c99.nl
- **Finding subdomains with harvester**

```
python3 theHarvester.py -d domain.com -l 500 -b all
```

- **Finding subdomains using subfinder**

```
subfinder -d <domain>
```

- **Finding subdomains using subfinder**

```
python3 sublist3r.py -d zomato.com
```

- **Subdomain Bruteforcing with Knockpy**

https://t.me/learningnets

```
knockpy <domain> -w <wordlist>
```

- **Subdomain bruteforcing with puredns.**

```
wget
https://raw.githubusercontent.com/trickest/resolvers/main/resolvers.txt
```

```
puredns bruteforce wordlist.txt example.com -r resolvers.txt -w output.txt
```

- **Subdomain bruteforcing with wfuzz**

```
wfuzz -u https://streamio.htb -H "Host: FUZZ.streamio.htb" -w
~/Desktop/Wordlist/SecLists/Discovery/DNS/subdomains-top1million-5000.txt
--sc 200,202,204,301,302,307,403
```

- **Certificates (Can discover potential subdomains)**- https://crt.sh/

Now this uses a very different approach to find out the subdomains of a website. It uses a website SSL certificates and use it find other hosts that are related to it.

- **Dig by Google (Potential Subdomain takeover)** - https://toolbox.googleapps.com/apps/dig/#CNAME/

-> If there is no organization or authority in the CNAME

---

https://t.me/learningnets