Documentation

Tools Used:

1. Knockpy (Active)
2. Censys (Passive)
3. Subfinder (Passive)
4. Assetfinder (Passive)

About Tools:

1. **Knockpy** : Knockpy is a Active Python tool that can be used for enumerating subdomains of a given domain name using a wordlist. It does this by sending DNS queries for each name in the wordlist and checking whether the domain name exists or not. Knockpy also provides functionality to perform port scanning on the discovered subdomains and determine which ports are open.

   The official Knockpy GitHub repository (https://github.com/guelfoweb/knock) contains the tool's documentation, installation instructions, usage examples, and information about the project's development.

2. **Censys subdomain finder** : Censys.io (www.censys.io) is a web-based search platform for assessing attack surface for Internet connected devices. The tool can be used not only to identify Internet connected assets and Internet of Things/Industrial Internet of Things (IoT/IIoT), but Internet-connected industrial control systems and platforms.
   The link of github repository of Censys subdomain finder:
   https://github.com/vkvbit/censys-subdomain-finder

3. **Assetfinder**: Assetfinder is a Go-based Passive tool to find related domains and subdomains that are potentially related to a given domain from a variety of sources including Facebook, ThreatCrowd, Virustotal and more.
   The link of github repository of assetfinder:
   https://github.com/tomnomnom/assetfinder

4. **Subfinder** : Subfinder is an open-source Passive tool used for subdomain enumeration, which is the process of discovering subdomains associated with a given domain name. It does this by querying multiple sources, such as search engines, certificate transparency logs, and public DNS servers, to gather as much information as possible about the target domain.
   The link of github repository of subfinder:
   https://github.com/projectdiscovery/subfinder

API Endpoints:

To create a request: http://4.227.244.76/search
To see subdomains of domain: http://4.227.244.76/getsubdomainresult
To see subdomains & their IP address: http://4.227.244.76/getcompleteresult

Note: All the endpoints are POST method.

Format of API body data: (JSON)

Example format of JSON body:

```
{
    “domains”: [“website.com”, “example.com”]
}
```