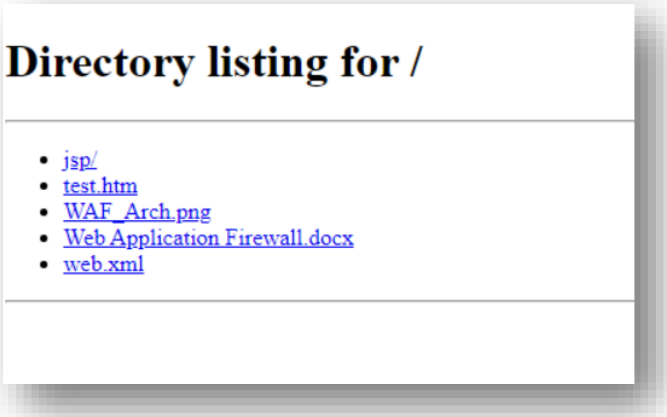
EnDa Subdomain Enumeration Tool (SubDM)

EnDa Subdomain Enumeration tool (EnDa SubDM) is an ethical hacking tool, an essential for penetration testers who are testing a private or a public webserver. This program was coded in Python programming language and it's the first step of creating the most powerful and organized PenTester Kit for white-hat hackers. I want to create this for more than one operating system, Linux (Debian) which runs python scripts on Bash Shells, for windows and any other operating systems with pythons. This kit must be in a USB and when you need it you can plug-in the USB driver and use it, without having the problem of operating systems. On windows you can run the executable and it will be much easier.

This tool can be used in CTF Challenges (Catch the flag -> More info here) which starts with an black-box (a vulnerable machine about which you have the least information) and the first step is to harvest most information that you can harvest with OSINT or more other protocols. Sometimes, the administrators of web-servers can create a custom subdomain which helps the group of developers to access the files and the directories of webserver main folder, which is a serious vulnerability. There are some methods to secure it, but, some lazy administrators just create a minimal secured secret subdomain, with random characters or in many times, with a common subdomain name (like development, developers, develop, execute, run, assets, folders, directories, images, files, databases or more others that can be found in a wordlist with 1000 lines, which means that you can find a serious vulnerability with only max. of 1000 scans).



Directory listing for /

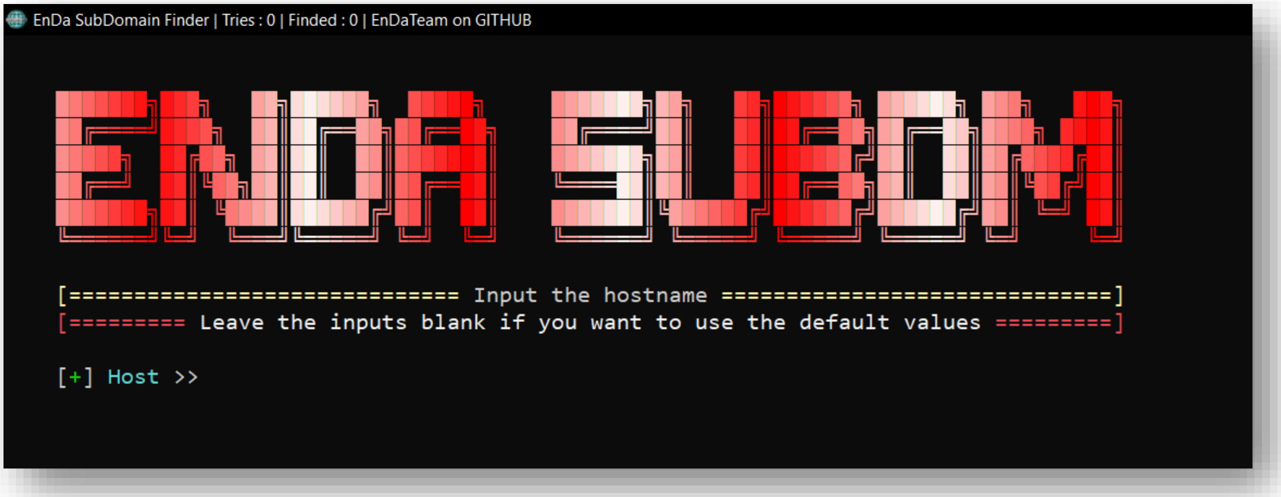
- jsp/
- test.htm
- WAF_Arch.png
- Web Application Firewall.docx
- web.xml

->> This is an example of vulnerable subdomain, which has a **CNAME DNS Redirection** to https://www.{host}/assets which can be only accessed with a cookie and access with this subdomain is bypassing it.

The reasons why I created this tool are this:

- Harvest more information about the black-box
- Find the perfect subdomain to take over it (only with GitHub)
- Find some unpublished useful new functions of a web-application
- Find a subdomain to bypass the login system of admins
- Get access to developer privileges at start

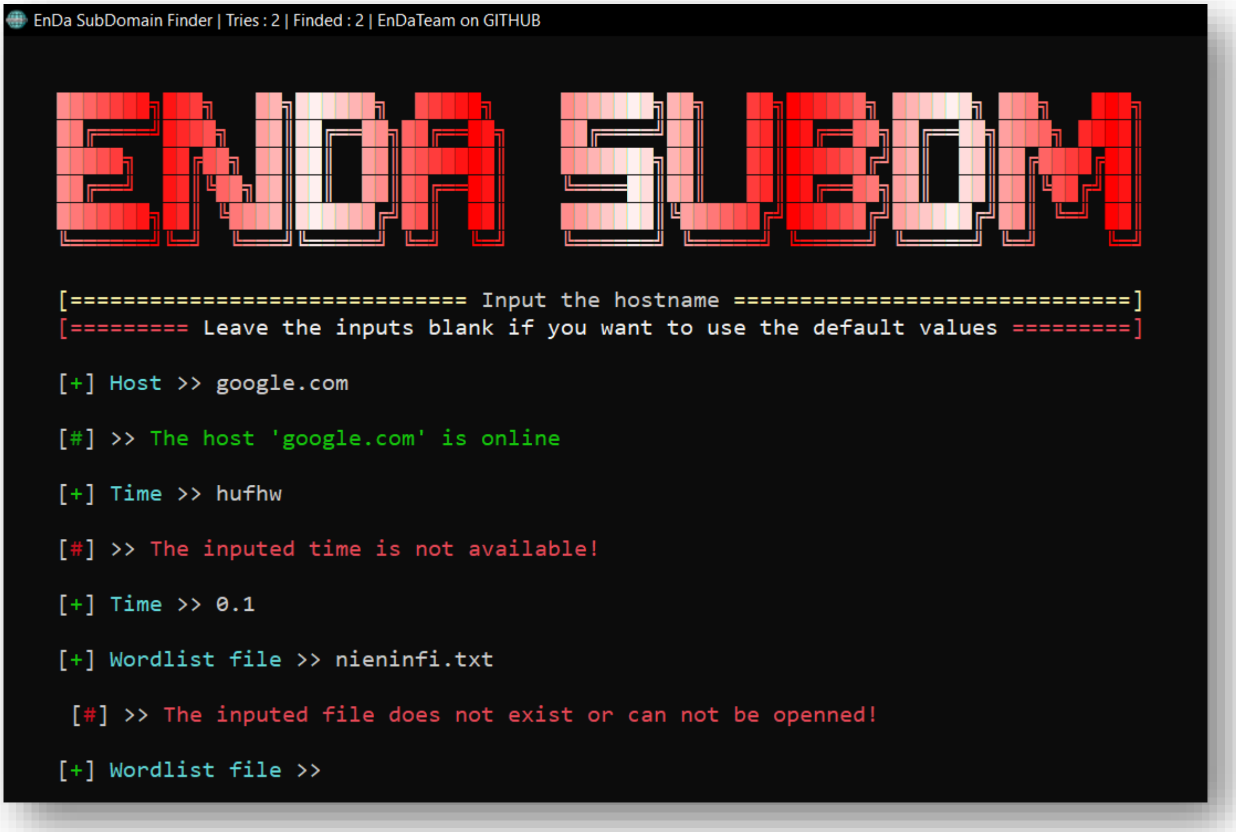
EnDa SubDM is a simple program, created with a challenge: Create a useful hacking tool in 2 hours (including debugging, coding, documentation etc.). This is published on GitHub as user EnDaTeam, the team I created for coding.



EnDa SubDomain Finder | Tries : 0 | Finded : 0 | EnDaTeam on GITHUB
ENDA SUBDM

```
[============================== Input the hostname ==============================]
[========= Leave the inputs blank if you want to use the default values =========]

[+] Host >>
```

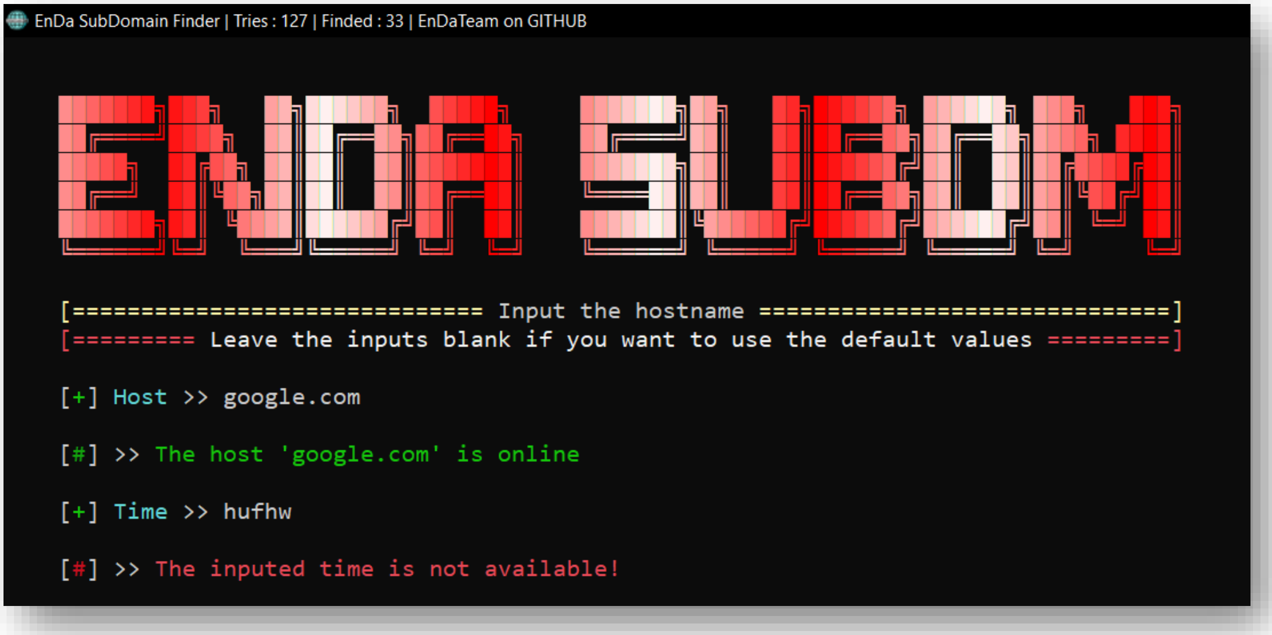
The program is starting with a clean-up of console, a banner (the colors are randomized), some information about the tool and a fancy input where you can set the host that you want to harvest. It has a special function for windows users: It adds a title at top where you can see how many tries of finding a valid subdomain the tool did, how many subdomains are valid and a promotion of EnDaTeam. It has a simple verifier of host, if it is on or not, but is like bit of buggy and it does not work properly for now.



EnDa SubDomain Finder | Tries : 2 | Finded : 2 | EnDaTeam on GITHUB

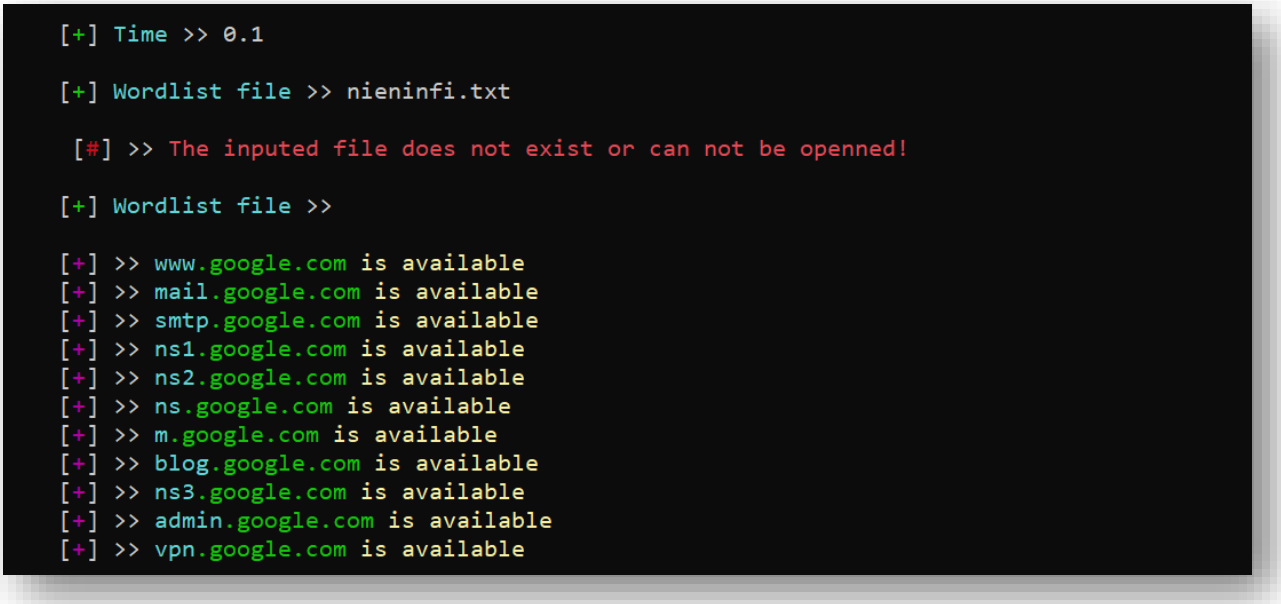
```
[============================== Input the hostname ==============================]
[========= Leave the inputs blank if you want to use the default values =========]

[+] Host >> google.com

[#] >> The host 'google.com' is online

[+] Time >> hufhw

[#] >> The inputed time is not available!

[+] Time >> 0.1

[+] Wordlist file >> nieninfi.txt

 [#] >> The inputed file does not exist or can not be openned!

[+] Wordlist file >>
```

You can add the time sleep between the scans, you can leave it blank for the default value of 0.1 second. If you input an invalid time, like a string, an error message is going to appear. You can add a wordlist as well, you can use the default one which can be accessed with leaving empty (without value). If you want to add a custom wordlist, just create it at the same directory of the program and input the path or the name of created wordlist (with extension as well). If the file does not exist, an error message will appear.



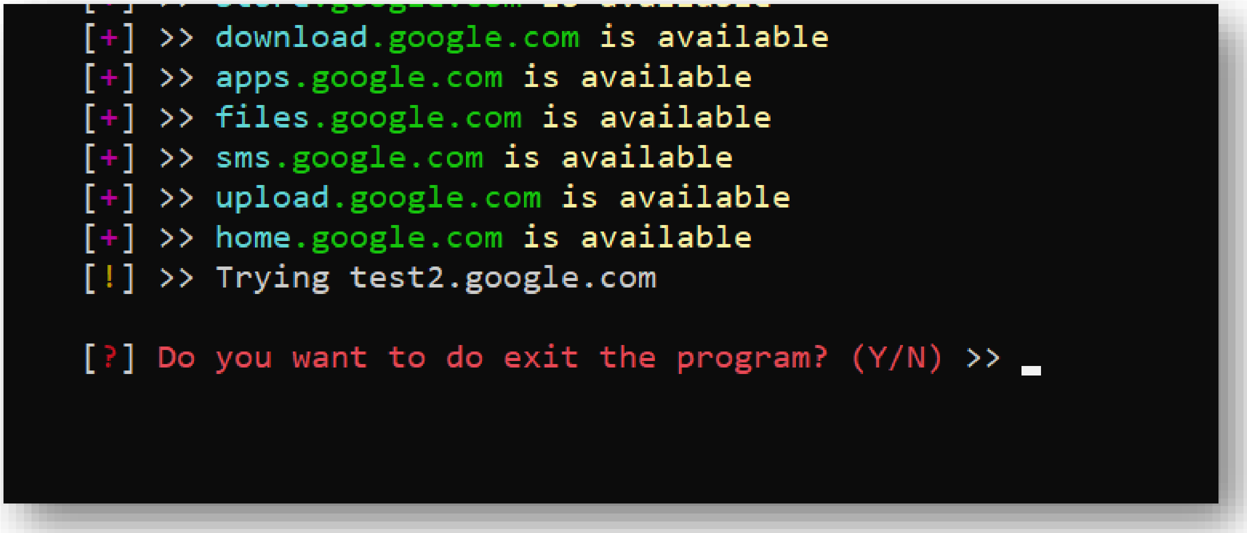
EnDa SubDomain Finder | Tries : 127 | Finded : 33 | EnDaTeam on GITHUB

```
[============================== Input the hostname ==============================]
[========= Leave the inputs blank if you want to use the default values =========]

[+] Host >> google.com

[#] >> The host 'google.com' is online

[+] Time >> hufhw

[#] >> The inputed time is not available!
```



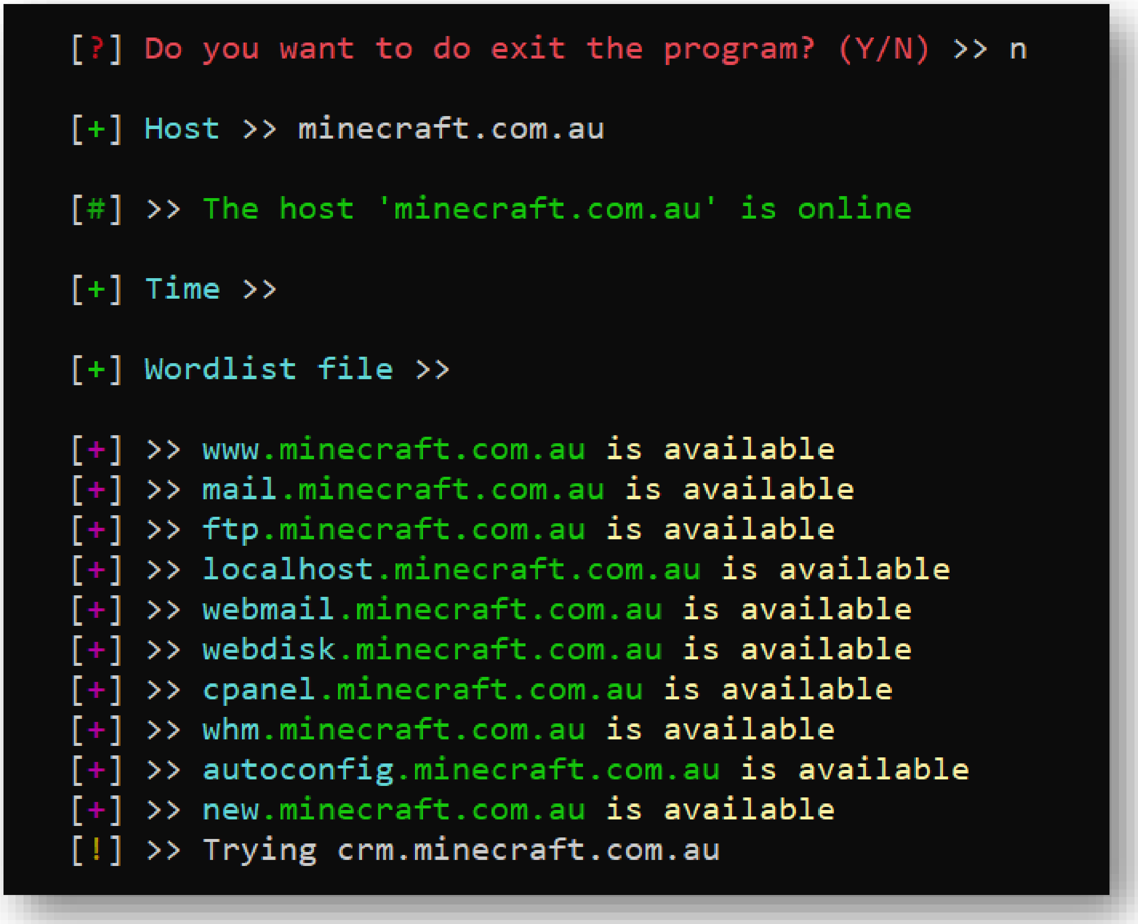
```
[+] Time >> 0.1

[+] Wordlist file >> nieninfi.txt

 [#] >> The inputed file does not exist or can not be openned!

[+] Wordlist file >>

[+] >> www.google.com is available
[+] >> mail.google.com is available
[+] >> smtp.google.com is available
[+] >> ns1.google.com is available
[+] >> ns2.google.com is available
[+] >> ns.google.com is available
[+] >> m.google.com is available
[+] >> blog.google.com is available
[+] >> ns3.google.com is available
[+] >> admin.google.com is available
[+] >> vpn.google.com is available
```

The scan will start, the tries and founded numbers from title will be modified and the founded subdomains will be displayed as console lines. After the scan if any subdomains was found, a special message will appear (No subdomain was found!). It has an animation as well, a trying message will be displayed and it will be changed after every scan of subdomains.



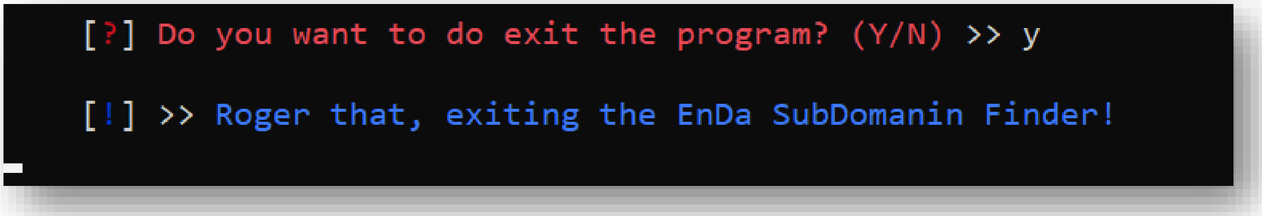
```
[+] >> download.google.com is available
[+] >> apps.google.com is available
[+] >> files.google.com is available
[+] >> sms.google.com is available
[+] >> upload.google.com is available
[+] >> home.google.com is available
[!] >> Trying test2.google.com

[?] Do you want to do exit the program? (Y/N) >> _
```

It has a error catcher for keyboard intrerrupt which ask you a question : Do you want to exit the program. If you do not want to exit it, write “N”, and it will reset the scanner, otherwise type “Y”.



```
[?] Do you want to do exit the program? (Y/N) >> n

[+] Host >> minecraft.com.au

[#] >> The host 'minecraft.com.au' is online

[+] Time >>

[+] Wordlist file >>

[+] >> www.minecraft.com.au is available
[+] >> mail.minecraft.com.au is available
[+] >> ftp.minecraft.com.au is available
[+] >> localhost.minecraft.com.au is available
[+] >> webmail.minecraft.com.au is available
[+] >> webdisk.minecraft.com.au is available
[+] >> cpanel.minecraft.com.au is available
[+] >> whm.minecraft.com.au is available
[+] >> autoconfig.minecraft.com.au is available
[+] >> new.minecraft.com.au is available
[!] >> Trying crm.minecraft.com.au
```

If you want to continue with another scan



```
[?] Do you want to do exit the program? (Y/N) >> y

[!] >> Roger that, exiting the EnDa SubDomanin Finder!
```

If you want to exit the program

! Do not use this tool for unethical proposes !

! The product is licensed !