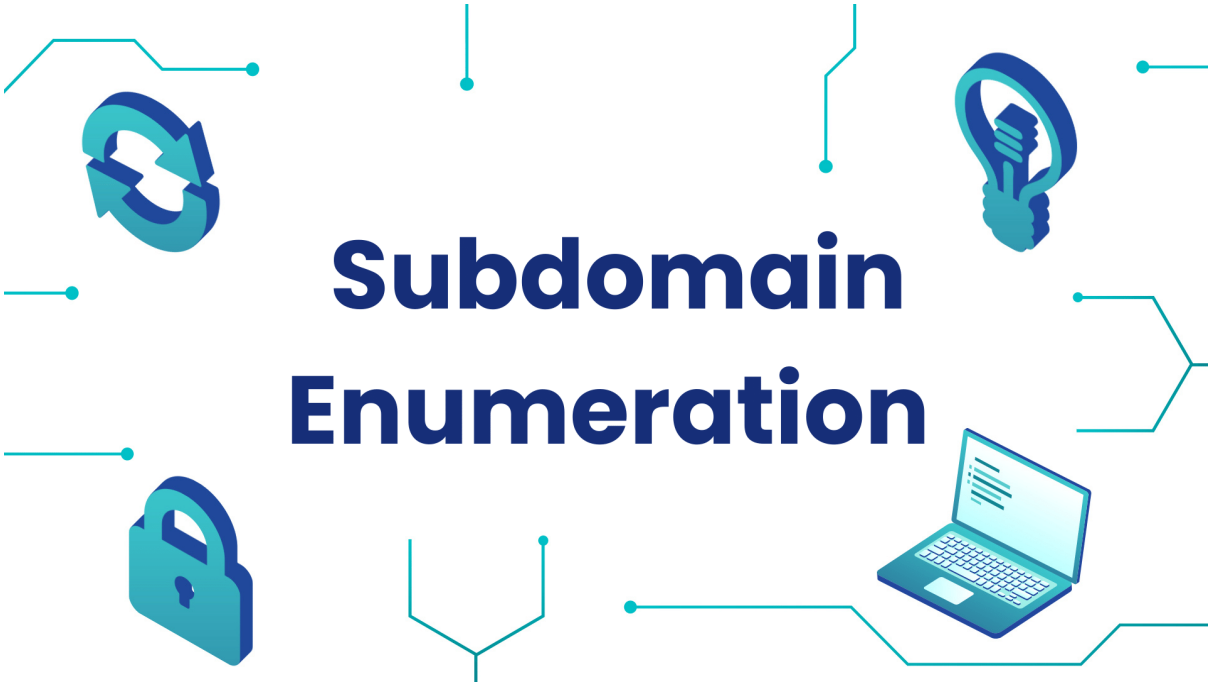
SUBDOMAIN ENUMERATION



SUBDOMAIN ENUMERATION

Subdomain Enumeration is a process to discover or identify the subdomain that is associated with particular domain. This is an essential step in cybersecurity that often use to in bug hunting and penetration tester. Basically this process helps to identify potential entry point and vulnerabilities in the domain.

IMPORTANCE OF SUBDOMAIN ENUMERATION

1. **Attack Surface Discovery:** Subdomains may represent different services, applications and functionalities of the domain. By identifying these things, a penetration tester may get an insight on expanded surface area which have potential entry points or vulnerabilities in subdomains.

2. **Vulnerability Assessment:** It is possible that different domains may host on different server or infrastructure so there are chances that the security postures may vary for any domain. So this helps in assessment to find potential vulnerabilities.

3. **Risk Management:** It is essential to know the complete scope of the domain's subdomain. In this case if security team finds any security issue in any domain then they can prioritize the case to resolve the issue as soon as possible and fix it.

4. **Phishing and Social Engineering:** It is easy for hackers to implement Phishing attack and social engineering when they have subdomain details. They monitor the account and wait for the correct time to implement these attacks for specific domains.

5. **Bug Bounty Hunting:** Security researchers and bug bounty hunters often perform subdomain enumeration to identify weakness in the subdomain so that they can report the issue in order to fix the security related concern for the specific domain.

TOOLS TO PERFORM SUBDOMAIN ENUMERATION

There are online tools available on internet that provide subdomain details i.e., **DNSDUMPSTER & Security Trails**, these are the best tools that provide details regarding the subdomain as mentioned above. However, using different tools can also provide slightly different results which is a valuable information and we can also say a unique diamond from a mine. Today we are using tools in kali linux which is mentioned below.

- **Assetfinder:** This tool is integrated in a way that it works in conjunction with different engines and gather information related with subdomains for further analysis and testing purpose.

GUIDE TO INSTALL ASSETFINDER TOOL IN KALI LINUX

1. **Open Terminal.**
    - You can open the terminal by clicking on terminal icon or open by using the keyboard shortcut **Ctrl + Alt + T.**
2. **Make Sure You Have Go Language Installed**.
    - You can check the version by using the following command.

      go version
3. **Install Assetfinder Tool.**
    - You can install the Assetfinder tool by using the following command.

      Apt install Assetfinder
4. **Run Assetfinder.**
    - You can run the assetfinder tool by using the following command.

      Assetfinder vulnweb.com

SCREENSHOT OF LIVE USEAGE OF ASSFETFINDER TOOL

SCREENSHOT: STEP 1,2 & 3.

SCREENSHOT: STEP 4.

- **Turbolister:** Turbolist3r is a python based tool so make sure the python packages are installed in your system in order to run this tool properly. As this tool is an open source free to use tool as well as powerful tool. Turbolist3r is the tool for Subdomain enumeration. It is the fork of the tool Sublist3r. This tool also allows brute-forcing of the subdomains using the subbrute tool utility.

  Subdomain Enumeration is the crucial step for expanding the target scope. The functionality or features cannot be compressed in a single domain so the subdomains are created to split the functionality. These Subdomains can have some crucial information about the target domain. So to detect this Subdomains automation should be done, as Manual identification becomes complex.

GUIDE TO INSTALL TURBOLISTER TOOL IN KALI LINUX

1. **Open Terminal.**

    - You can open the terminal by clicking on terminal icon or open by using the keyboard shortcut **Ctrl + Alt + T.**

2. **Install Turbolister Tool.**

    - You can install the Assetfinder tool by using the following command.

      git clone https://github.com/fleetcaptain/Turbolist3r.git

3. **Run cd Turbolister.**

    - You can run the following command to change the directory to Turbolister.

      Cd Turbolister

4. **Run Ls command.**

    - You can run ls command to list down the files existing in the Turbolister.

      Ls

5. **Install Requirements.txt File.**

    - Follow the below command to install the requirements.txt file.

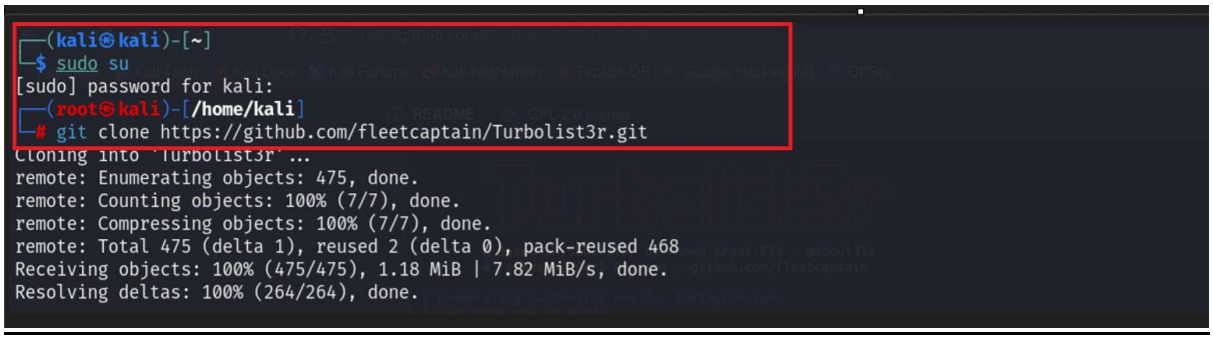
      Pip install –r requirements.txt

6. **Run the Turbolister Tool.**

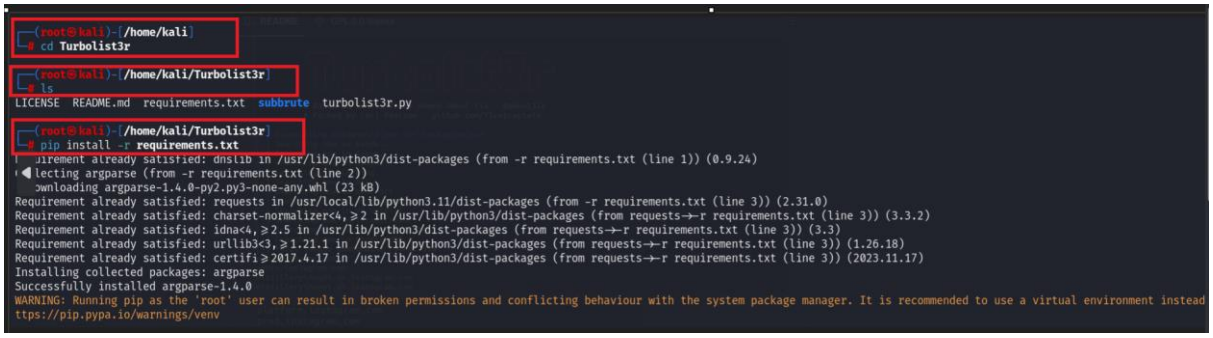
    - By following the below command you can run the tool to get the information about target domain.

      python turbolist3r.py -b vulnweb.com

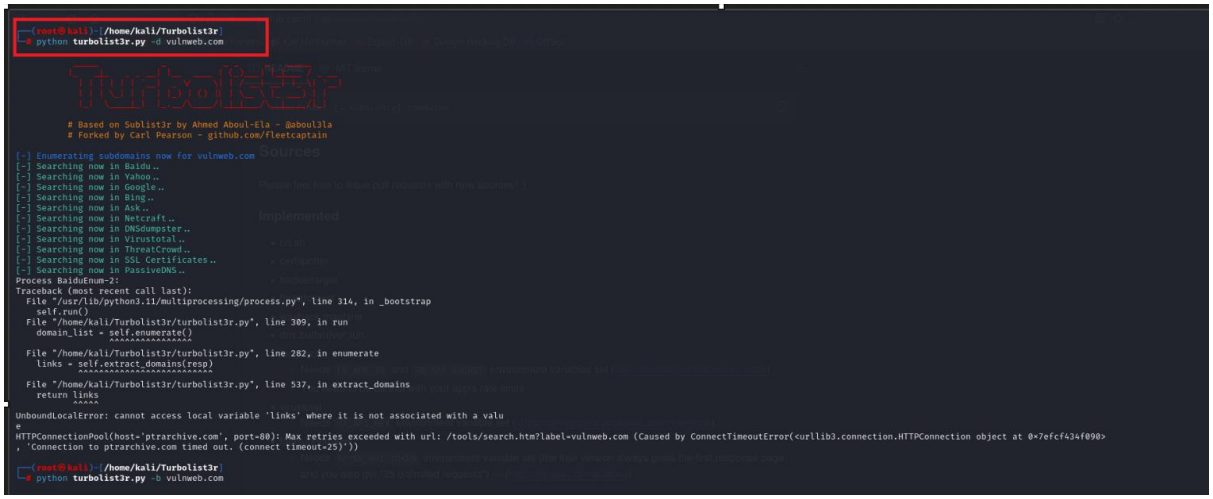
SCREENSHOT OF LIVE USAGE OF TURBOLISTER TOOL



SCREENSHOT: STEP 1 & 2.



SCREENSHOT: STEP 3, 4 & 5.



SCREENSHOT: STEP 6.

REFERENCES

https://www.geeksforgeeks.org/turbolist3r-subdomain-enumeration-tool/

https://www.briskinfosec.com/tooloftheday/toolofthedaydetail/Turbolist3r-Tool-Web-Application-Subdomain-Discover

https://chat.openai.com/