Subdomain enumeration is one of the major parts of Reconnaissance. In-fact we can term it as the primary step to start with any Bug Bounty Program. So, in this post, I'll share with you the step-by-step guide to use a tool in Kali Linux for enumerating the Sub Domains.

The tool I am using for the purpose is sublist3r. Sublist3r is a great tool for finding the sub-domains of any web application. This tool is written in python language. Although you can run it on both Windows and Linux environment but I highly recommend you to use Kali because it's more convenient as well as kali will provide you many other tools for the hacking purpose.

SETTING UP:

I will guide you the installation and usage in Kali Linux. But, As I mentioned earlier, you can run it in windows environment too, I suggest you should use Kali because it has most of the tools needed by Hackers for penetration testing as well as some pre-installed packages in order to execute scripts.

You can use Kali Linux in 4 different ways:
1- Dual Boot
2- Bootable USB Live
3- Bootable USB Persistent
4- Virtual Box

DUAL BOOT

Dual Boot means you can use your base operating system and Kali Linux by sharing the same hardware. This is basically installing multiple OS in a single computer. This will be a good decision if you have sufficient hard disk space.

The procedure is similar to installing any other OS. Since it's a dual boot so you need to create a partition on your hard drive. It'll be convenient. However, you can check out some videos on youtube also.

BOOTABLE USB (LIVE MODE)

You can also use Kali Linux on Live mode. Here, live mode means you don’t need to install it on your PC. You can directly start working on it. But everything is temporary.

One thing you need to keep in mind while using kali on live mode is that you can’t save anything. So whatever application or scripts you downloaded/updated will last until you reboot your system.

BOOTABLE USB (PERSISTENT SOLUTION)

If you want your live USB bootable to save your progress each time, then you can also use live bootable persistent mode. But the procedure includes some extra steps so I recommend you to go through with some guide. A 32 GB pen-drive will be enough for the same.

The main advantage of using it is that you can use the same operating system along with the files in multiple different computers with your USB stick. I use this option personally as I need to switch between my desktop and my laptop very often.

VIRTUAL BOX

Virtual Box is one of the most used methods. Here, you can run Kali Linux inside your windows OS on virtual box software. This has its own demerits. It’ll slow down the system’s speed. However, you can use it in the starting phase.

The concept behind is that you’ll download a virtual box software and install another operating system inside it. It’ll dedicate a particular memory size for the same. For the learning phase, it’s ok to use it but if you are working professionally, I would not recommend this. use live persistent instead.

SUBLIST3R: QUICK INTRO

In this section, I'll give you a quick introduction to this tool sublist3r. Although there are various other techniques available to scan sub-domains, by using this script is just amazing. This tool is best because:

1. Enumerating sub-domains from 10+ services which include major search engines such as Google.
2. Integrated with Sub-Brute script so that you can perform Brute-force to get hidden sub-domains which are not available in public resources.
3. Finding subdomains for a specific port.
4. Finding Sub-domains from specific Search Engine.

HANDS-ON WITH SUBLIST3R

This is not a primary tool of Kali Linux so, you need to install it in order to execute. To do this just write the below command on your terminal.

```
git clone https://github.com/aboul3la/Sublist3r.git
```

Now it'll start cloning.

Once the process will get finished, navigate to the sublist3r directory with the following command: cd Sublist3r

Now you can start working on enumerating the sub-domains. So, you need to type the below command for that.

```
python  sublist3r.py -d pranjalsinghal.in
```

The above command has 3 important things. I have written python in the beginning as the script is python based. Secondly, -d is used as an argument to define the domain name. I can write any domain name such as xyz.com only after -d.

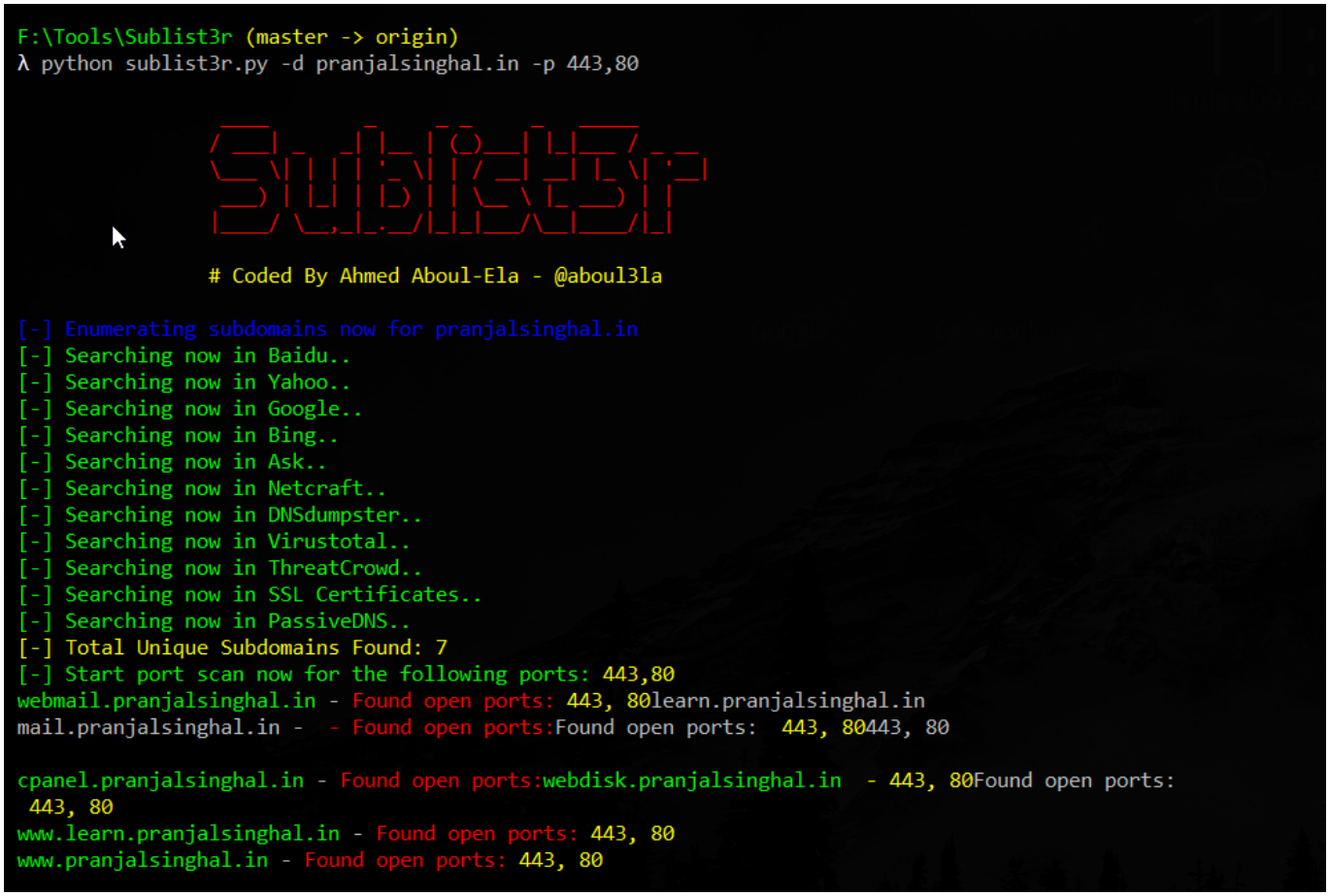
Above is the very basic example of this tool. let's dig deeper.

Suppose we need to find all sub-domains running on port 443. So we can simply do this with below command.

```
python sublist3r.py -d panjalsinghal.in -p 443
```

Now the result will be port-based. It'll scan all the sub-domains using port 443. You can replace this with any other port you want. In fact, you can use multiple port number separated by commas.

```
python sublist3r.py -d pranjalsinghal.in -p 443,80
```



With sublist3r, we can get “selected-service” based results. I mean if you want sub-domains to be scanned on any particular search engine or service (if offered by sublist3r) such as Google or bing then you can do that easily with ‘-e’ parameter. Below is the example

```
python sublist3r.py -d pranjalsinghal.in -p 443,80 -e google
```

We can use multiple services separated by commas as we did previously with the port.

When you’ll run the above commands, you will notice one thing that results aren’t delivered in real-time. so if you want real-time results and also the source of the result, you can use -v command. You should try it while using the brute-force module. for example

```
python sublist3r.py -d pranjalsinghal.in -p 443,80 -e google -v
```

We can also do brute-force of sub-domains by using -b command. This is very useful to discover hidden sub-domains which are not available publicly. You can define a number of threads for the brute-force using -t command To do Bruteforce, use below command.

```
python sublist3r.py -d pranjalsinghal.in -b -v -t 100
```

This will start brute-forcing the sub-domains. But it is time-consuming. So first perform the basic scan then only move on to this module.

After completing the brute force, you might want to save them to start testing one by one. You can save the output using -o command followed by name of the file. For example

```
python sublist3r.py -d pranjalsinghal.in -p 443,80 -e google -v
-o sub.txt
```

The above command will save the output file as sub.txt after performing the scan.

FINAL WORDS

If you are using Windows OS then it might be a bit confusing for you to start with Kali terminal. But from the hacker's point of view, this is really beneficial. Most of the tools are included in Kali which you can use for testing purpose.

Sublist3r is one of the most useful tools. I saw most of the tutorials which explain sublist3r, covered the topic with minimum words by using point to point wordings. They are good for those who have Intermediate knowledge but not suitable for beginners. That's why I decided to cover all the features of this tool in a single post.

If you will follow the tutorial, then I am 100% sure you'll master it very well. Apart from this tool, I will soon make a how-to guide on other important tools too. Please write your valuable comment below. Thanks,

cheers! Happy Hacking <3

ALSO READ: HOW TO BECOME AN ETHICAL HACKER

Pranjal Singhal

I am a freelancer Cybersecurity researcher and a digital marketer. I have already helped Top IT Giants to secure their web applications and maintain a safe environment for their users.

Sharing and Caring is my motive. I love to guide beginners about making a successful career in the cybersecurity industry.