Chapter 4

Puzzle of Hacking and Sub-domain

UNDERSTANDING SUB-DOMAIN IN HACKING

Sub-domains play a critical role in ethical hacking. When hackers target sub-domains, they often find vulnerabilities that help them understand the weaknesses of a website. Many websites even host their admin panels on sub-domains, making it easier for hackers to gain access to the entire website through these entry points.

WHY SUB-DOMAINS ARE IMPORTANT IN HACKING

Sub-domains are vital in hacking because they often house the admin panels and other sensitive parts of a website. By targeting these sub-domains, hackers can gain access to areas that are otherwise not exposed through the main website. When hackers break into the admin panel via these sub-domains, they can control the entire website and

compromise all its data. This makes sub-domain discovery a key skill in ethical hacking.

DIFFERENCE BETWEEN A DOMAIN AND A SUB-DOMAIN

Let's break this down using a simple analogy:

- **Domain**: Think of a domain as the main address of a website, like "*earth.com*." It's unique and helps users access a specific site.
- **Sub-domain**: A sub-domain is a part of that domain. It is created by adding a prefix in front of the domain name. For example, "*moon.earth.com*" is a sub-domain where "*moon*" is added to "*earth.com*."

A REAL-LIFE ANALOGY

Think of the *earth.com* domain as a planet in a galaxy. The moon becomes a satellite of the planet. Now, "*moon.earth.com*" would be a sub-domain of *earth.com*, just as the moon orbits the earth.

Just like how ISRO discovered valuable resources on the moon (water, for instance), hackers often discover valuable data or access points hidden within sub-domains. In the same way ISRO found treasures on the moon, ethical hackers can uncover vulnerabilities and sensitive data within these sub-domains that can be used to improve security.

WHY WE NEED TO STUDY SUB-DOMAINS FOR HACKING

In hacking, sub-domains are like hidden treasures. They hold potential for finding weak spots in a website's infrastructure. Understanding how to locate and examine sub-domains helps ethical hackers gain valuable insight into the structure of a website, making it easier to spot vulnerabilities. For example, many websites host their admin panels on

sub-domains like "*admin.domain.com*." If a hacker gains access to this sub-domain, they could potentially access the entire website's admin area.

FINDING SUB-DOMAINS USING SUBLISTER AND WEBSITES

Now we will learn two effective methods to find sub-domains: using a tool called Sublister and through online sub-domain finder websites.

Using Sublister Tool

The Sublister tool acts like a virtual rover, scanning the main domain and discovering its sub-domains. Here's how to use it in Kali Linux:

Step 1: Open Kali Linux
If you haven't already set up Kali, refer to the detailed guide provided in the second part of this course.

Step 2: Open the Terminal
Once Kali is up and running, open the terminal where we will enter commands.

Step 3: Install Sublister
To install Sublister, type the following command:

```
sudo apt install sublist3r
```

Press Enter. The installation process will begin, and within a few seconds, Sublister will be installed.

Step 4: Run Sublister
Now that the tool is installed, you can use it by typing the following:

```
sublist3r -d <domain_name>
```

Replace <*domain_name*> with the actual domain you want to scan for sub-domains. Be sure to remove "*http://*" or "*https://*" when typing the domain name.

Step 5: View Sub-domains

Once you press Enter, the tool will start processing. Within about 30 seconds, it will show you all the sub-domains related to the domain you specified.

This method is quick and effective for discovering sub-domains on any domain.

USING SUB-DOMAIN FINDER WEBSITE

Apart from using the Sublister tool, you can also find sub-domains through online websites dedicated to sub-domain discovery. These websites work in a similar way by scanning the domain and listing its sub-domains.

Step 1: Visit the Website
Open *https://subdomainfinder.c99.nl/*

Step 2: Enter the Domain
Type the domain name (e.g., example.com) into the search box (without "*http://*" or "*https://*").

Step 3: View Results
The website will show the sub-domains for the entered domain.

This method can be a simple alternative if you don't want to use Kali Linux or if you're looking for a quick solution.

CONCLUSION

Now, you know two ways to find sub-domains: using the Sublister tool in Kali Linux or exploring online sub-domain finder websites. Both methods are effective, and you can choose the one that suits your needs best.

By ScripterJee