**Anubis – Subdomain enumeration and information gathering tool**

**Anubis Overview:**

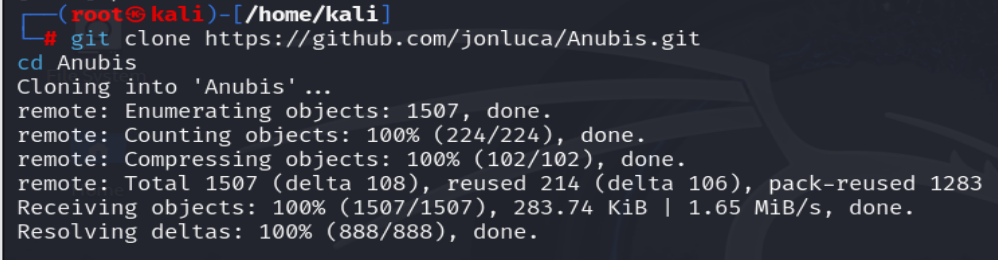
Anubis is a powerful information-gathering tool, particularly valuable during the initial stages of penetration testing. It specializes in discovering subdomains using various modules that employ an advanced wordlist for brute force attacks. Available for free on GitHub, Anubis is open-source, meaning you can download and use it without any cost.

This tool is designed to aid in the reconnaissance of subdomains for websites and web applications. Finding subdomains on HTTPS sites or web applications can be challenging, but Anubis simplifies this process, identifying subdomains for both HTTP and HTTPS sites. Written in Python, it requires Python to be installed on your Kali Linux system.

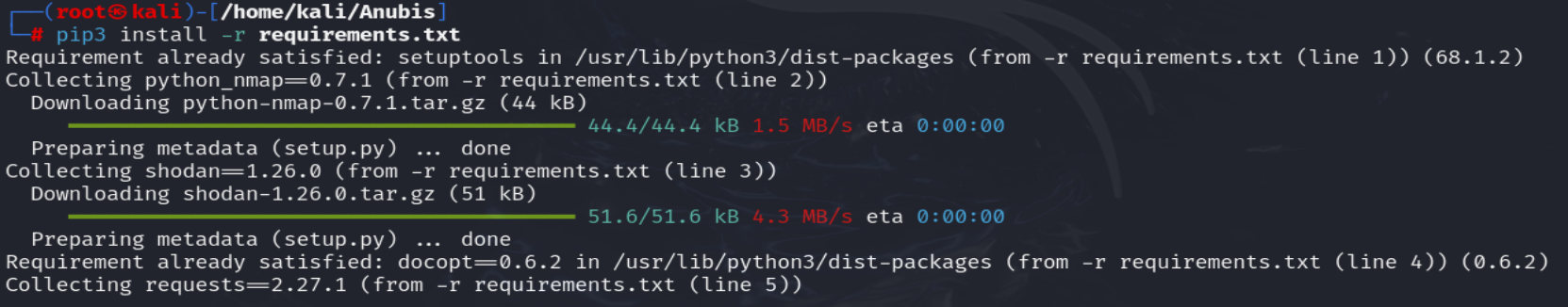
Anubis features an intuitive user interface reminiscent of Metasploit 1 and Metasploit 2, making it straightforward and user-friendly. This familiar interface enhances its usability, allowing security researchers to efficiently conduct their reconnaissance tasks.

**Installation**

**Step 1:**Use the following command to install the tool in your operating system and use the second command to move into the directory of the tool.



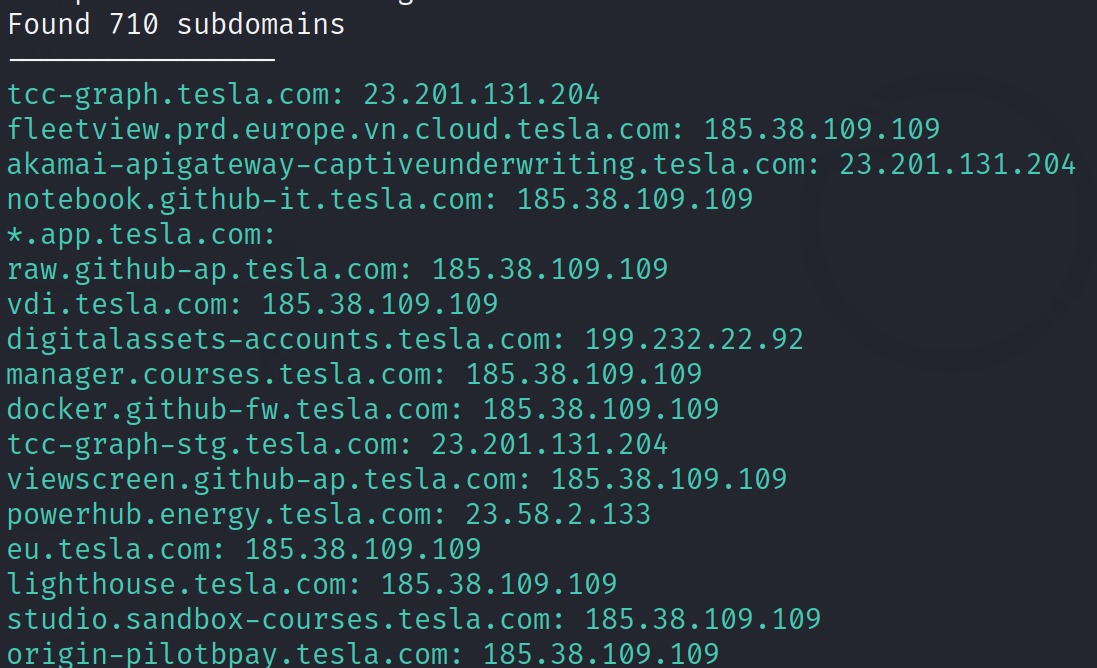
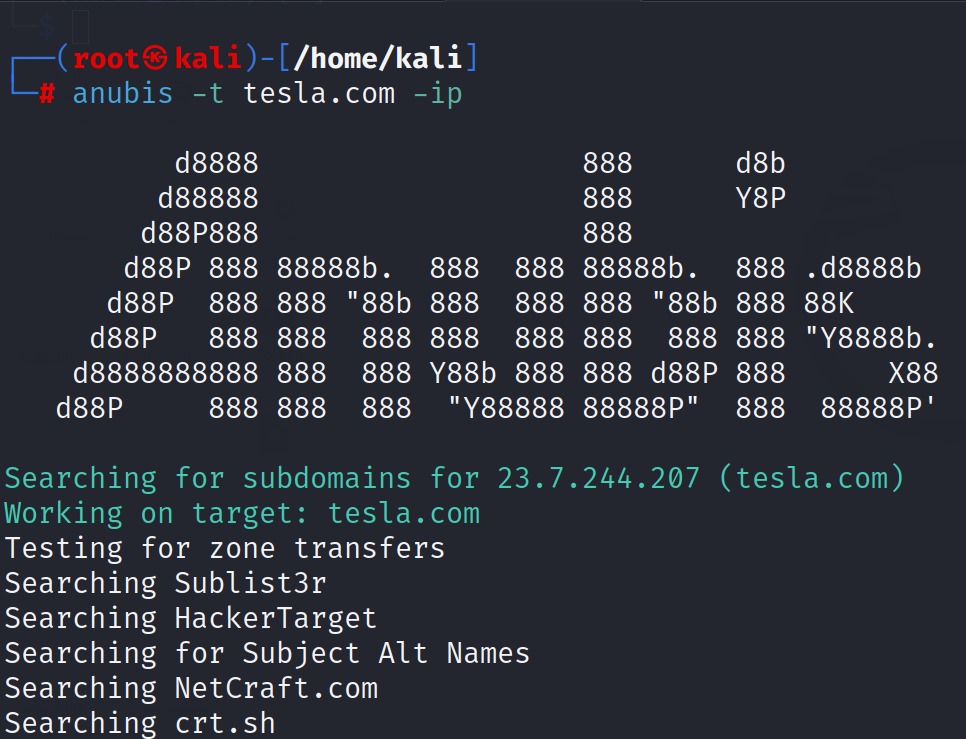
**Step 2:** The tool has been downloaded and installed in your system. Now you have to install the requirements of the tool using the following command.



The requirements have been installed. Now we will see an example to use the tool.

**Usage**

 Find the subdomain of domain geeksforgeeks.com and IP address.



**Summary:**

Anubis simplifies the often-difficult task of identifying subdomains, making it an invaluable tool for security researchers during penetration testing.