# The Harvester Tool for ****FootPrinting/Reconnaissance****

**Footprinting/Reconnaissance:**Footprinting (also known as reconnaissance) is the technique used for gathering information about computer systems and the entities they belong to. To get this information, a hacker might use various tools and technologies.

**the Harvester:**The objective of this program is to gather emails, subdomains, hosts, employee names, open ports and banners from different public sources like search engines, PGP key servers and SHODAN computer database.



Here we will use this tool to search for information about Infosectrain organization

**the Harvester options**

-d: Domain to search or company name

-b: data source: Google, GoogleCSE, Bing, Bing API, PGP, LinkedIn, Google- profiles, people123, jigsaw, Twitter, Google+, all

-s: Start in result number X (default: 0)

-v: Verify hostname via DNS resolution and search for virtual hosts

-f: Save the results into an HTML and XML file

-n: Perform a DNS reverse query on all ranges discovered

-c: Perform a DNS brute force for the domain name

-t: Perform a DNS TLD expansion discovery

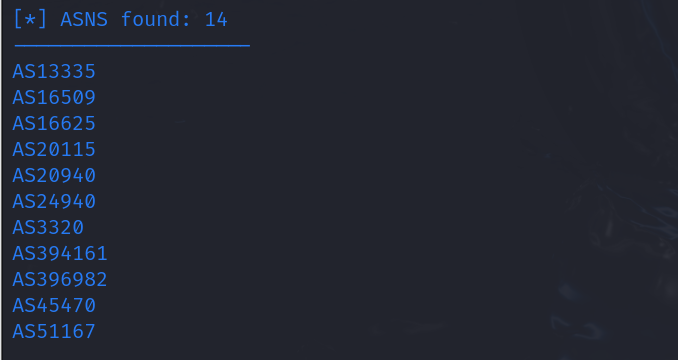
-e: Use this DNS server

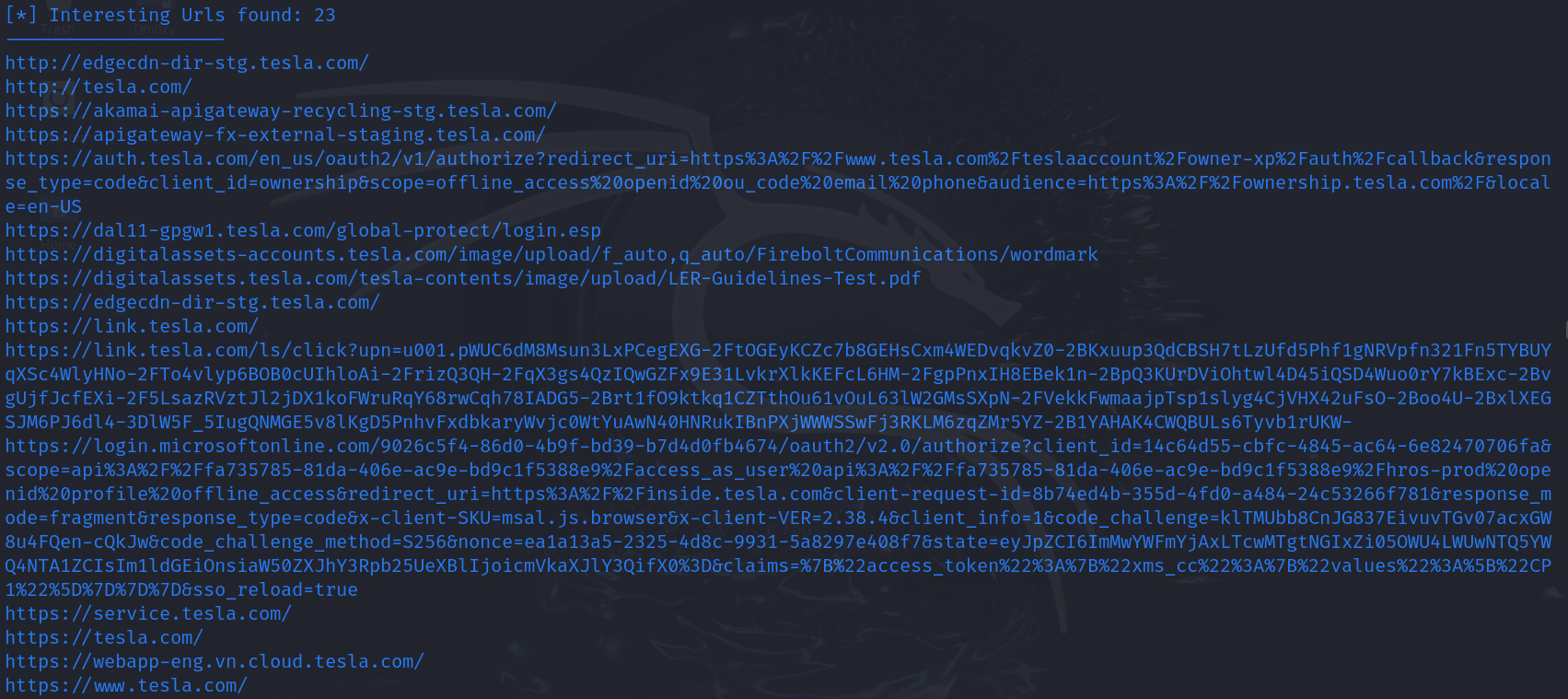
-l: Limit the number of results to work with(bing goes from 50 to 50 results,

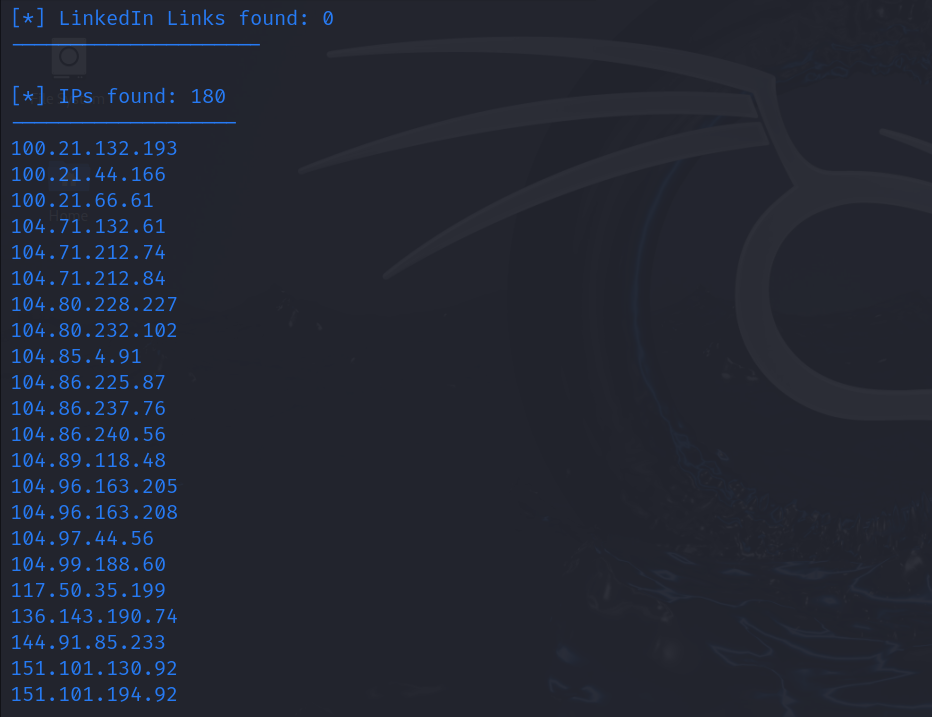
-h: use SHODAN database to query discovered hosts

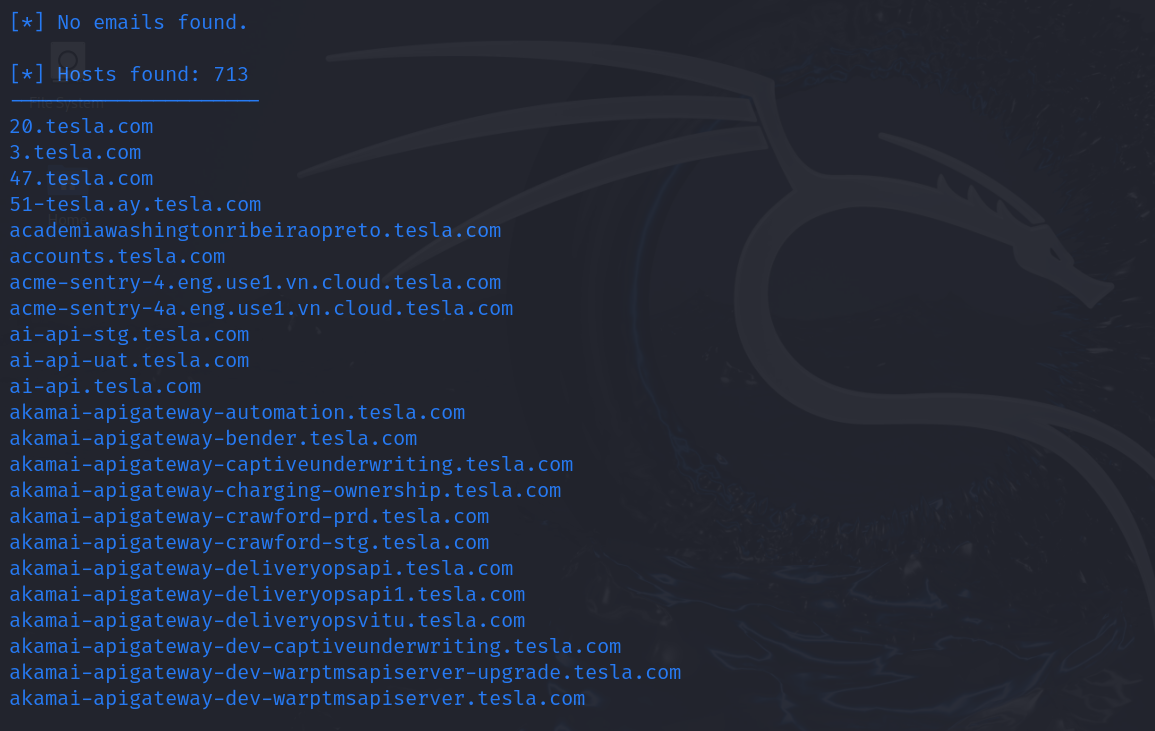
Command: theHarvester -d tesla.com -l 50 -b all











these are the important information( host, IP addresses & URLs) I got using this tool.

theHarvester may return too much information to go through, for better readability, you can write the output to an HTML file:

Command: theHarvester -d tesla.com -l 50 -b all -f report

The file will be exported in your home folder in Kali Machine.

Note: If you having trouble to export the HTML file, keep in mind it's a huge amount of information being collected, you can reduce the search engines/sources, instead to use them all at once.

theHarvester is a valuable tool for OSINT which allows to quickly discover a good amount of data, especially email addresses. Remember that you need to verify information: for example, it could be that an employer is not working anymore on a certain company, but his email address is still present on the web and so it will be returned in the results.