**Assignment Day - 2**

**1. Information Gathering Or Recon**

**Active Recon:** Active reconnaissance is a type of computer attack in which an intruder engages with the targeted system to gather information about vulnerabilities. This may be through automated scanning or manual testing using various tools like ping, traceroute, netcat etc. This type of recon requires that attacker interact with the target. This recon is faster and more accurate, however it also makes much more noise. Since the attacker have to interact with the target to gain information, there’s an increased chance that the recon will get caught by a firewall or one of the network security devices. (Intrusion Detection Systems, network firewalls, etc.)

Tools Used: Nmap, Metasploit and etc.

**Passive Recon:** Passive reconnaissance is an attempt to gain information about targeted computers and networks without actively engaging with the systems. It is a gathering the information without alerting victim. If the victim host alerted then it drastically increases security against the attack.

Tools Used: Wireshark, Shodan and etc.

**2. Google dorking (Passive Recon):** Google dorking, also called Google hacking is a technique that uses Google Search and other Google applications to find security holes in the configuration and computer code that websites are using. Google dorking could also be used for OSINT.

Ex: 1. intitle:login

2. inurl:admin

3. filetype:pdf

4. site:flipkart.com

5. intext:password

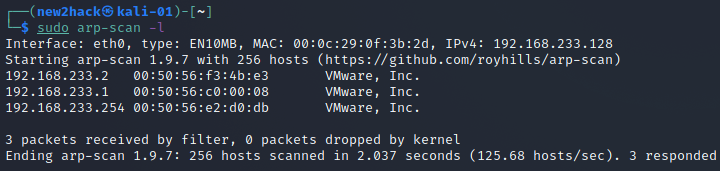
6. "Test to search"

use hyphen (-) to exclude the search type

**3. Google Hacking Database (GHDB):** The GHDB is an index of search queries (we call them dorks) used to find publicly available information, intended for pen-testers and security researchers.

https://www.exploit-db.com/

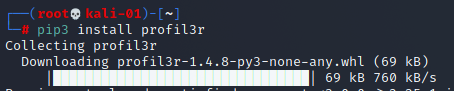
**4. ARP-Scan:** Arp-scan is a command line utility for Linux that can be used to scan the network of a certain interface for alive hosts. It shows the ip address and mac addresses of all the hosts/nodes found.

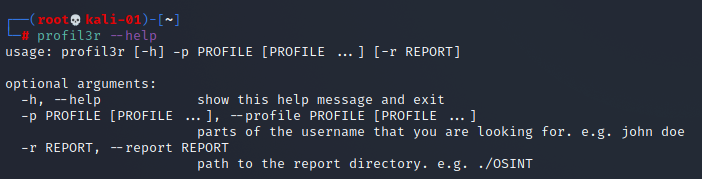


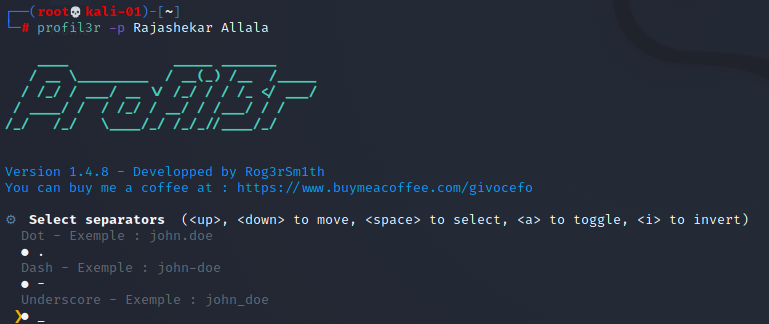
**5. OSINT (Passive Recon):** OSINT (OSINT, for Open Source INTelligence) techniques are the methods and tools used to acquire information that is widely available and useful for supporting intelligence analysts.

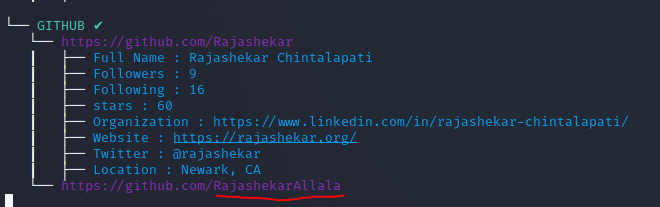
**6. Profil3r:** Profil3r is an OSINT tool that allows you to find potential profiles of a person on social networks, as well as their email addresses. This program also alerts you to the presence of a data leak for the found emails.

https://github.com/Rog3rSm1th/Profil3r



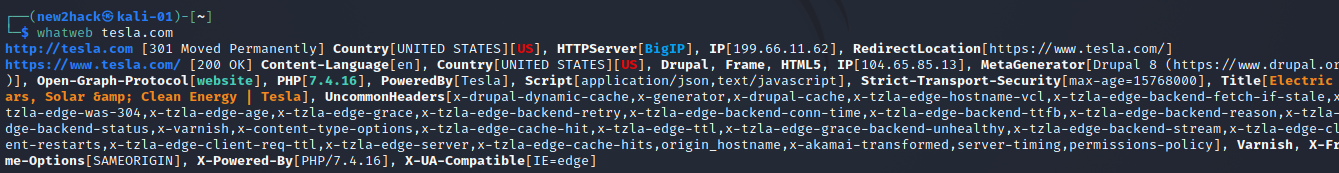




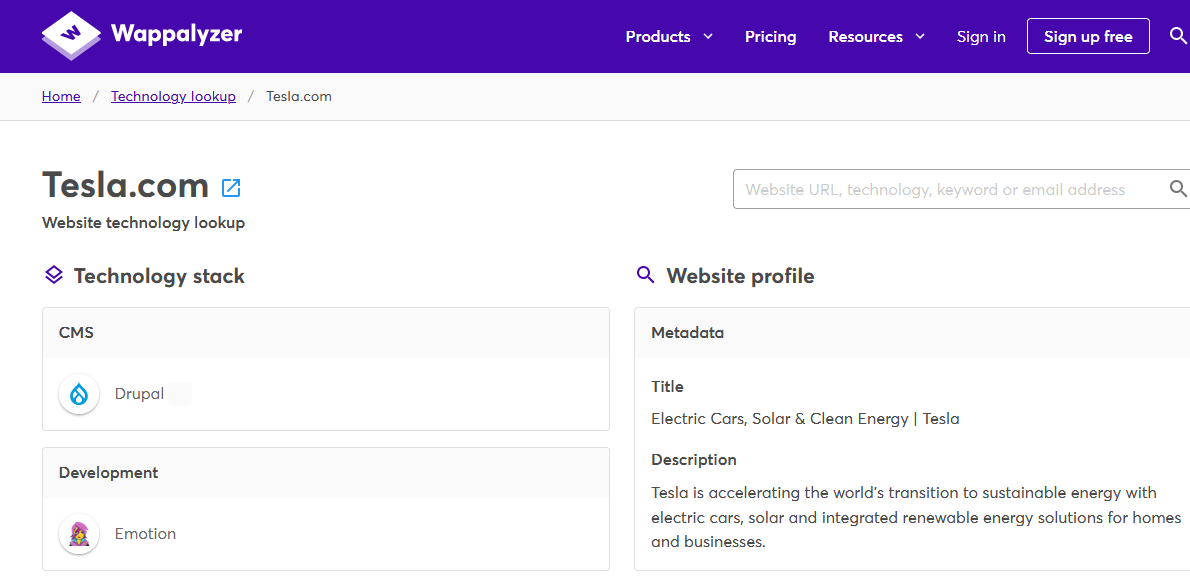


**7. Website Information:**

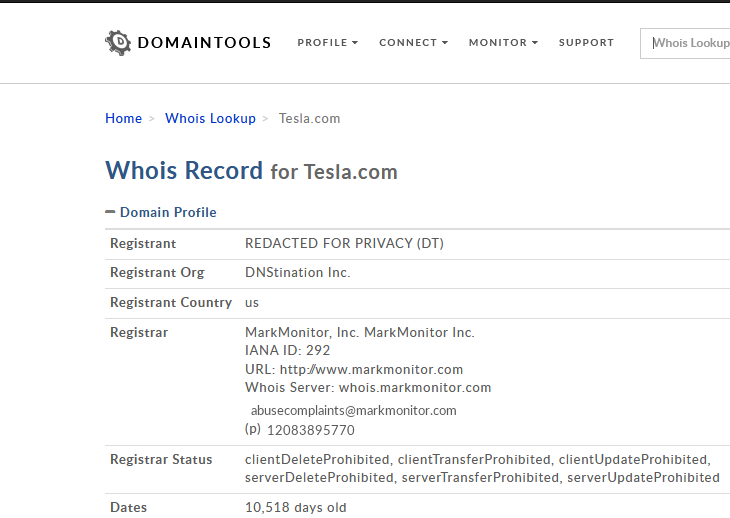
**i. Whatweb <Website\_URL>**



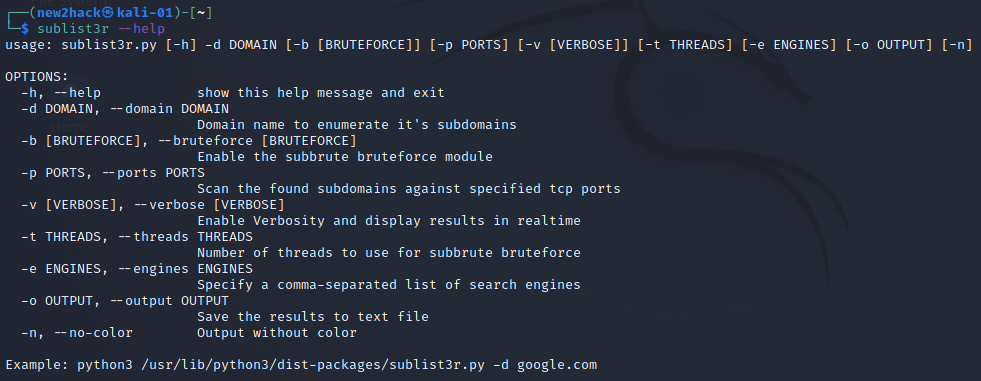
**ii. https://www.wappalyzer.com**



**iii. https://whois.domaintools.com/**

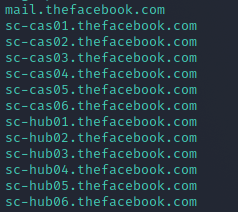


**iv. sublist3r**





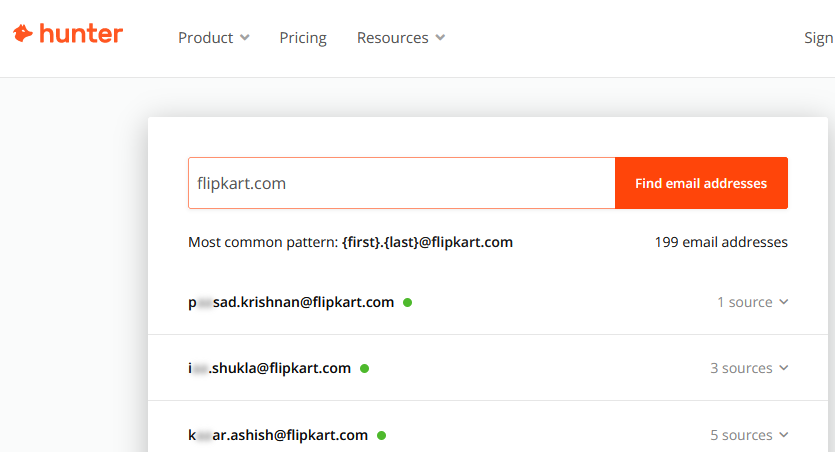
Few of the sub domains



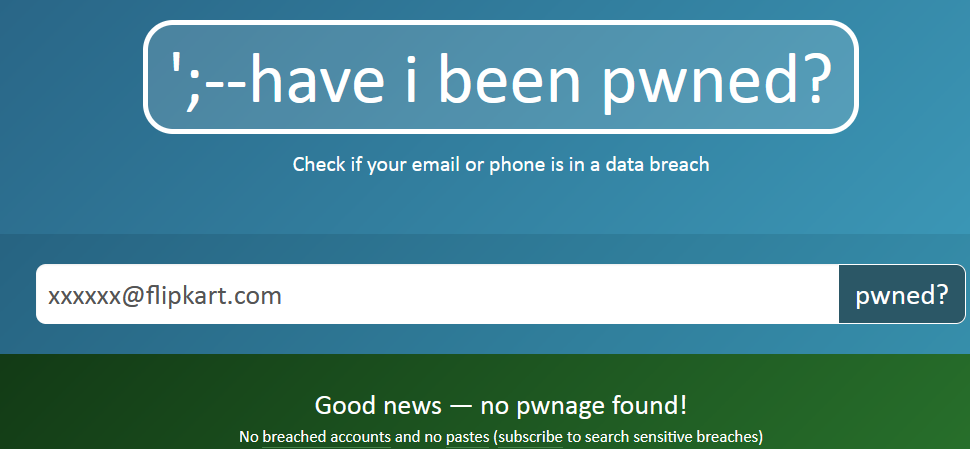
**v. theHarveter**



**v. https://hunter.io/**



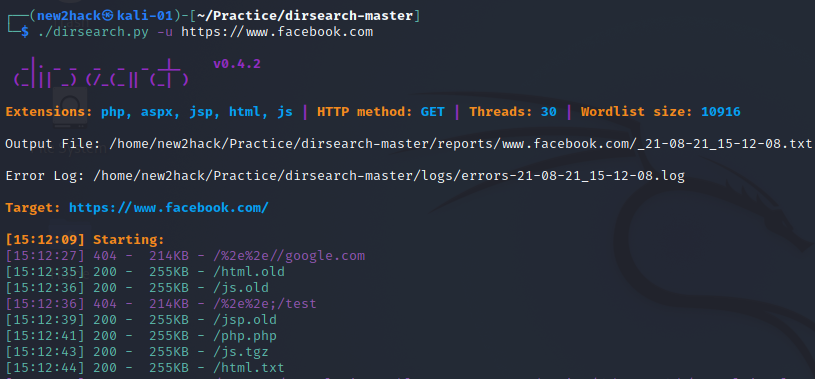
**vi. https://haveibeenpwned.com/**



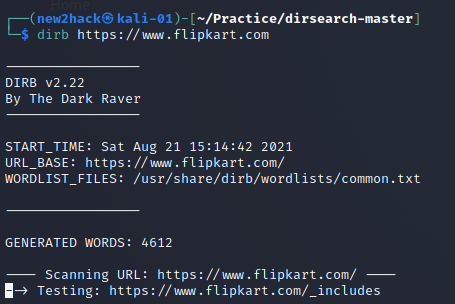
**8. Scanning: Scanning for vulnerabilities in a Website/Web application**

**i. dirsearch:** Dirsearch, written in python is a command-line website directory scanner. It has a lot of features making it the complete winner in terms of performance: It includes Multithreading, making it faster than any other site scanner tool. It performs Recursive brute-forcing. It has HTTP proxy support.

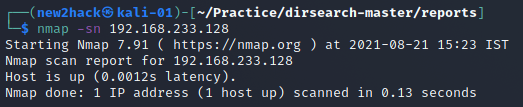
https://github.com/maurosoria/dirsearch

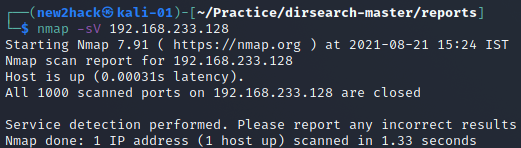


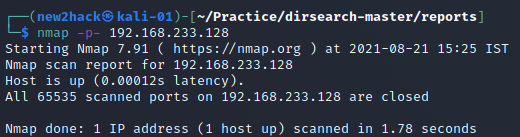
**ii. DIRB:** DIRB is a Web Content Scanner. It looks for existing (and/or hidden) Web Objects. It basically works by launching a dictionary-based attack against a web server and analyzing the response. ... It doesn't search vulnerabilities nor does it look for web contents that can be vulnerable.



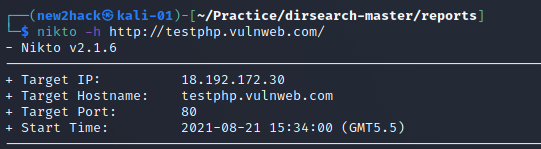
**iii. Nmap:** Nmap is used to discover hosts and services on a computer network by sending packets and analyzing the responses.







**iv. Nikto:** Nikto is a free software command-line vulnerability scanner that scans web servers for dangerous files/CGIs, outdated server software and other problems. It performs generic and server type specific checks. It also captures and prints any cookies received.



vi. acunetix/nessus/netsparker/ vega - Vulnerability scanning tools

