Preface

I have made this report file on the topic of **Passive Reconnaissance**. I have tried my best to elucidate all the relevant details to the topic to be included in the report.

My efforts and wholehearted co-corporation of each and every one has ended on a successful note. My sincere gratitude to CYBERSAPEINS and thanks them for providing me the reinforcement, confidence and most importantly the track of the topic.

Passive Reconnaissance

Passive reconnaissance, also known as passive information gathering or footprinting, is a crucial phase in cybersecurity and intelligence gathering. Unlike active reconnaissance, which involves direct interaction with the target system and may trigger alerts to the target system, passive reconnaissance relies on collecting information without directly engaging the target. This method involves analyzing publicly available data, such as domain registrations, social media profiles, online forums, and other sources to build a thorough understanding of the target's digital footprint.

Passive Reconnaissance Tools

I would like to share a curated list of Passive Reconnaissance Tools that are publicly accessible on the internet, along with their respective URLs for convenient access:

- **Shodan**: A search engine for finding devices connected to the internet. https://www.shodan.io/

- **Social Mapper:** A powerful tool that they can even search the information about the anonymous person on the internet by using his/her face without knowing the actual name of the person.

- **TheHarvester:** A tool for gathering email account, subdomains, virtual host, open ports and banners. It is pre-built in Kali Linux.

- **Whois Lookup:** Tool that provides information about domain registration. https://www.whois.com/whois/

- **DNSDumpster:** Gathers information about a domain, including subdomains and associated IP addresses. https://dnsdumpster.com/

- **Google Advance Search:** Advanced operators can be used for targeted searches. https://www.google.com/advanced_search

- **Google Dork:** It exposes the sensitive information about companies, websites and individuals.

- **SpiderFoot:** This tool is an open source intelligence automation tool which gather information about target system. i.e., IP address, domain name, hostname, network subnet, email address, person's name and ASN.

- **Tinfoleak:** This tool is use to extract information on twitter and other social media i.e., tweets, geo-location and user profiles. https://github.com/vaguileradiaz/tinfoleak.git

- **Bing Dork:** It is just like google dork which narrow downs the search and provide information which is not easily accessible.

- **GhostRecon:** This is a passive subdomain enumeration tool. It is available on GitHub and you can access it through this link.

- **Dork Genius:** Dork genius is a powerful AI tool which customs advance search for Google, Bing & DuckDuckGo. https://dorkgenius.com/