**💻As part of the hacking or penetration testing phase, the second phase is information gathering, and it is critical to understand the target👾**

**🤖Let’s begin with the best information gathering tools.** ❓

**🤔 Nmap – The Network Mapper:** Nmap, the Network mapper, is a free, open-source tool for vulnerability scanning and network discovery. It is designed to quickly scan massive networks, however works fine against single hosts. 🌐

**🎯Whois**: whois is used to gather the information about website they gather contacts, mails, IP address, and so on this tool is very useful to gather the information. 👌

**🥷Ip2location**: ip2location is useful tool to gather information about IP address. 🙌

**🕵️Netcraft:** This tool is very useful to gather information about technologies used in website and know about there OS. ⌛

**👍Hunter.io:** Hunting for email addresses is a great tool for gathering mail. ⚡

**🧑‍🎓**[**Shodan.io**](http://shodan.io/)**:** Shodan is the first search engine for internet-connected devices that allows you to search any website or any corporation whether the IP address is disclosed publicly or not. Sometimes the public IP provides you with username and password. ✨

**🔎Ping**: By using ping you can determine whether a target is communicable with your system or not, or find out if the target has IPv4 or IPv6. 📕

**📌Recon-ng:** recon-ng can gather many information such as IP, URLs, Mail, Number, Social media accounts and so on. 🦹

**❕Th3inspector**:Th3inspector is an powerful open source information gathering tool available on Github through which you can easily find much information about the target such as server details, whois lookup, target IP location, phone number, email address, sub-domains etc. 💬

**🥇Red Hawk:** Red Hawk is another open source information gathering tool available on github. It supports many scans & features like basic scan, web server detection, cms detection, whois lookup, geo-ip lookup, grab banners, dns lookup, subnet calculatorsub-domain scanner, reverse ip lookup & CMS detection. 🔒

**🤔Sandmap:** [Sandmap](https://github.com/trimstray/sandmap) is a open source tool which supports network and system reconnaissance using the massive Nmap engine. It provides a easy user-friendly interface, automates and accelerates scanning and permits you to simply use several advanced scanning techniques. 🎉

###### 🎯Devploit – Information Gathering Tool: [Devploit](https://github.com/joker25000/Devploit) is a simple python script to Information Gathering. Features of devploit are DNS lookup, Whois lookup, Geo-IP lookup, subnet lookup, Port scanner, Extract links, Zone transfer, HTTP header, Host finder, IP-locator, Traceroute, host DNS finder, reverse IP lookup, Subdomain finder. 🙌

###### 🤖ZenMap: Zenmap is the official GUI version of Nmap scanner. It is a multi-platform free and open source application which aims to make Nmap easy for beginners to use while providing advanced features for experienced Nmap users. 🤔

🎉 **Maltego:** Maltego is the all-in-one tool for link analysis. Maltego offers real-time data mining and information gathering, as well as the representation of this information on a node-based graph, making patterns and multiple order connections between said information easily identifiable. **👾**

**📌Wireshark:** Wireshark is a network protocol analyzer, or an application that captures packets from a network connection, such as from your computer to your home office or the internet. Packet is the name given to a discrete unit of data in a typical Ethernet network. Wireshark is the most often-used packet sniffer in the world. **🤖**

## **💻Tcpdump:** Tcpdump is a free data-network packet analyzer that works on the CLI interface. It allows users to see, read, or capture network traffic being transmitted over a network that is attached to the computer. 🦹

## **👍Raccoon:** [Raccoon](https://github.com/evyatarmeged/Raccoon) is a widely used reconnaissance and intelligence collecting tool focusing on ease of use. It can gather DNS records, retrieving WHOIS information, obtain TLS information, investigate WAF presence, and even do subdomain enumeration. Each scan generates a separate file. ⚡

🔎Using these tools, you can gather the useful information because they are very useful and powerful. Check out more blogs for more information. ❕

https://who.is/whois/senselearner.com

https://mxtoolbox.com/SuperTool.aspx?action=a%3asenselearner.com&run=toolpage

https://www.whois.com/whois/senselearner.com

https://sitereport.netcraft.com/?url=http://senselearner.com

https://www.hackingarticles.in/beginner-guide-website-footprinting/

https://builtwith.com/senselearner.com

https://mxtoolbox.com/SuperTool.aspx?action=a%3asenselearner.com&run=toolpage

https://whois.domaintools.com/senselearner.com

https://mxtoolbox.com/SuperTool.aspx?action=asn%3asenselearner.com&run=toolpage

https://pentest-tools.com/website-vulnerability-scanning/discover-hidden-directories-and-files

https://nanonets.com/website-scraper

https://www.lantechsoft.com/web-data-extractor.html

https://web.archive.org/web/\*/senselearner.com\*

https://iplocation.io/website-server-software/162.250.126.19