CYBER SECURITY

INFORMATION GATHERING TOOLS:

IN KALI:

1. **Nmap :**With Nmap, security professionals can find live hosts on a network and perform port scanning. This app is helpful for many reasons such as identifying open ports which are vulnerable to attack by hackers, or finding the operating system in use so that vulnerabilities may be exploited.
2. **Metasploit:**The Metasploit framework is a powerful tool for cybersecurity professionals while conducting information-gathering tasks. What makes it unique is the fact that it is very easy to use. It can be used by both ethical hackers and cybercriminals to identify vulnerabilities on networks and servers.
3. **Maltego:**Maltego is a tool that gives you the ability to use graph-based data mining, network analysis and visualization tools. It can be used with information-gathering tasks such as building IP ranges, mapping out domains or finding connected devices on your network.
4. **Wireshark :**Wireshark is one of the most well-known and often used packet sniffing tools available today. It is used by cybersecurity professionals, network administrators and hackers to collect information from networks. Network packets contain a wealth of information, and Wireshark captures this data for later analysis. Learning how to use Wireshark is essential if you wish to conduct information gathering on a network.
5. **Netcat:** Netcat is a tool that can be used to create simple connections between hosts. Netcat can also be used in conjunction with the TCP and UDP protocols for things like port scanning or creating backdoor channels. It can read and write data if the appropriate ports are configured. If you

want to be a penetration tester or work in cybersecurity then learning how to use Netcat will be highly beneficial.

6. **BadKarma – Advance Network Reconnaissance Toolkit:** BadKarma is a python3 GTK+ toolkit that aims to help penetration testers throughout all the network infrastructure penetration testing activity phases. It permits testers to save lots of time by having point-and-click access to their toolkits, launch them against single or multiple targets and interact with them through simplified GUIs or Terminals.
   Every task's output is logged beneath a session file in order to assist throughout reporting phase or in a possible incident response scenario. it is additionally accessible a proxychains switch that permit everything go through proxies, and last but not least, each command may be adjusted before the execution by disabling the "auto-execute" checkbox.
7. **Devploit – Information Gathering Tool:** 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.
8. **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.
9. **SANDEEP:** Sandmap is a tool that lets you gather information quickly and easily. With this tool, you can see how people are searching for things online (and which keywords bring them to your site), figure out where those searches are coming from, find out how long people stay on your site, and even see whether the type of device they're using matters in any way.

10. **Raccoon:** 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.Raccoon uses Python's `asyncio` module to conduct most scans asynchronously because most of its scans are autonomous and do not rely on each other's results. For anonymous routing, Raccoon supports Tor/proxy.

11.