M. Eshwar

21BLC1370

Assignment-2

Aim :- To explain the Components of Kali Linux

Introduction :-

[Kali Linux](https://www.kali.org/) (formerly known as *[BackTrack Linux](https://www.backtrack-linux.org/)*) is an [open-source](https://www.kali.org/docs/policy/kali-linux-open-source-policy/), [Debian-based Linux](https://www.kali.org/docs/policy/kali-linux-relationship-with-debian/) distribution aimed at advanced Penetration Testing and Security Auditing. It [does this by](https://www.kali.org/features/) providing common tools, configurations, and automations which allows the user to focus on the task that needs to be completed, not the surrounding activity.

Kali Linux is mainly used for advanced Penetration Testing and Security Auditing. Kali contains several hundred tools which are geared towards various information security tasks, such as Penetration Testing, Security research, Computer Forensics and Reverse Engineering.

Components in Kali Linux:-

1. Information Gathering:-

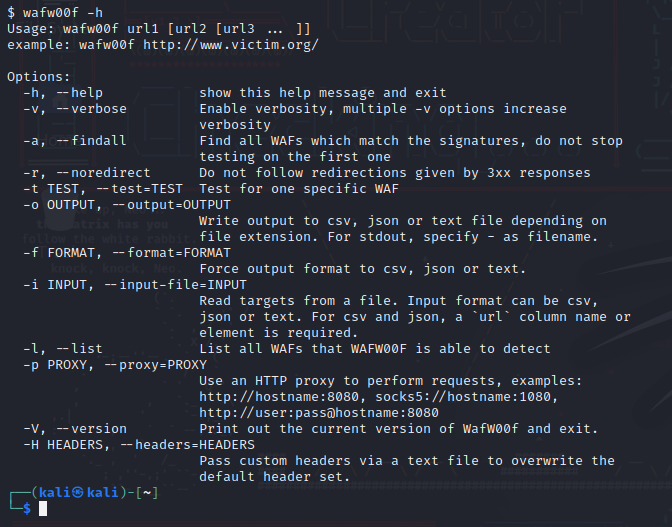
This category includes tools used for everything from identifying all the devices on a network enumerating to linking a network interface controller's media access control address with an IP address to identifying open ports on targeted servers. Kali Linux information gathering tools include scanners, such as Nmap and Wireshark, as well as information planning platforms that integrate the leading tools, often with GUIs for more comprehensive functionality.

Types of Information Gathering:-

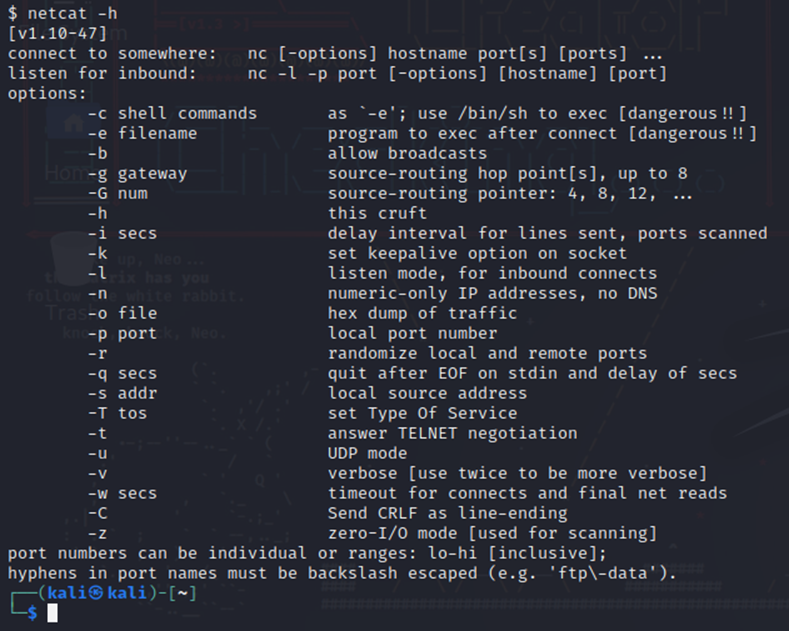
* DNS Analysis



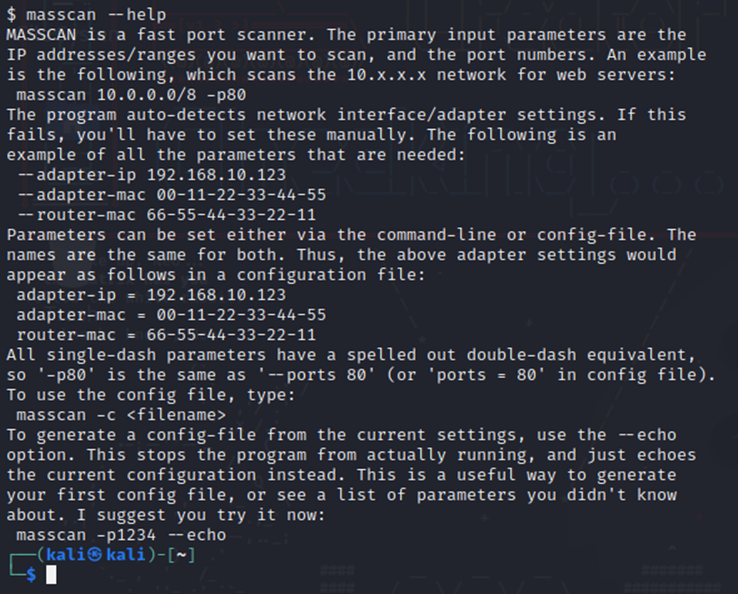
* IDS/IPS Analysis



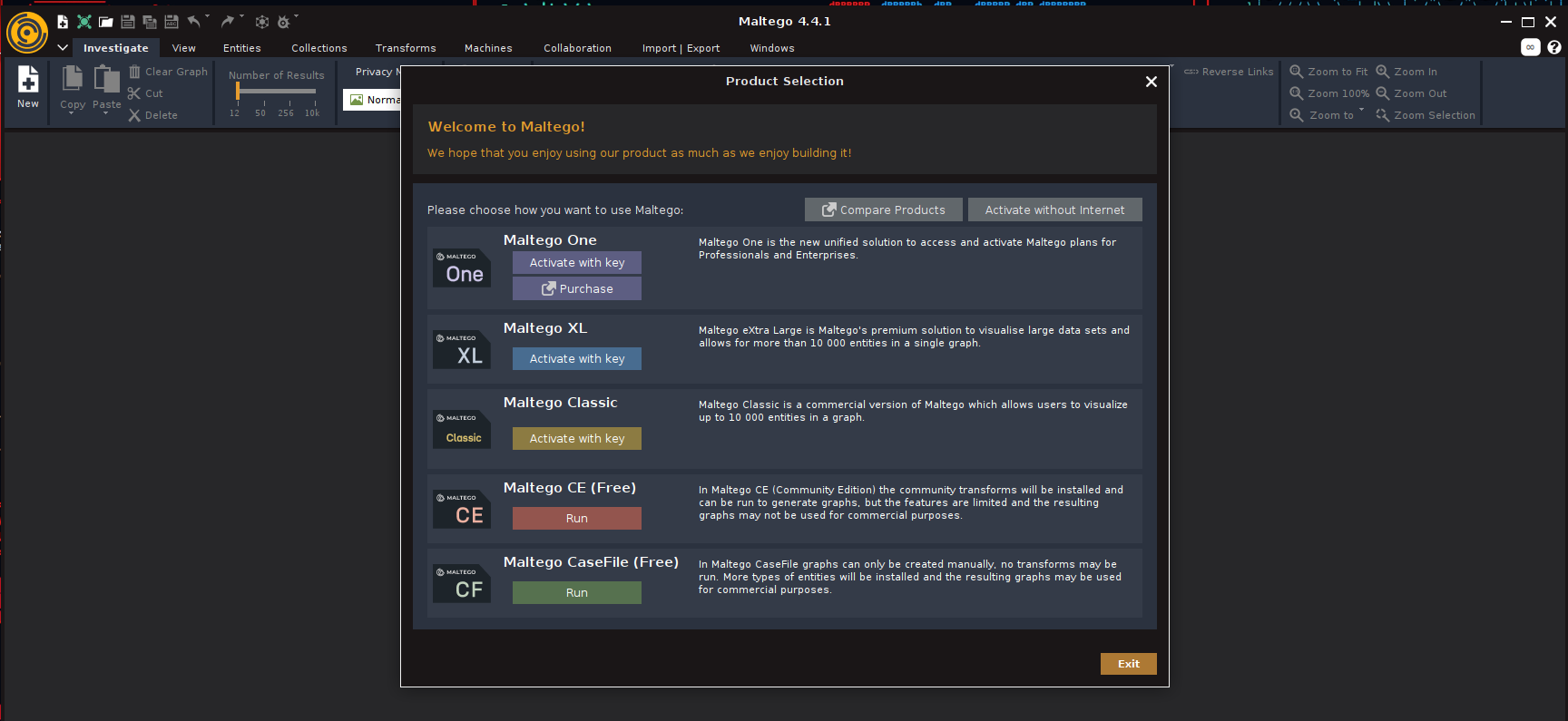
* Live Host Identification



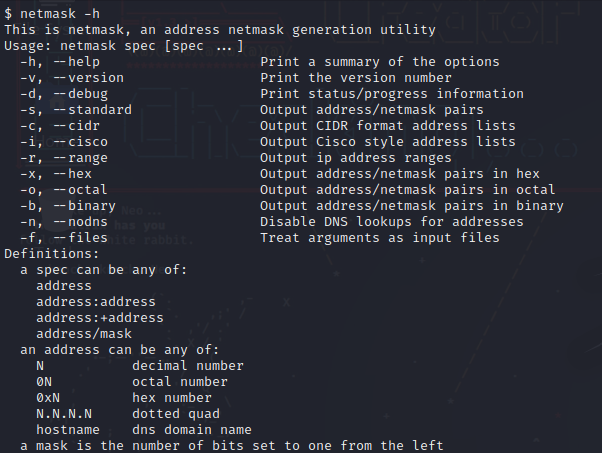
* Network and port Scanners



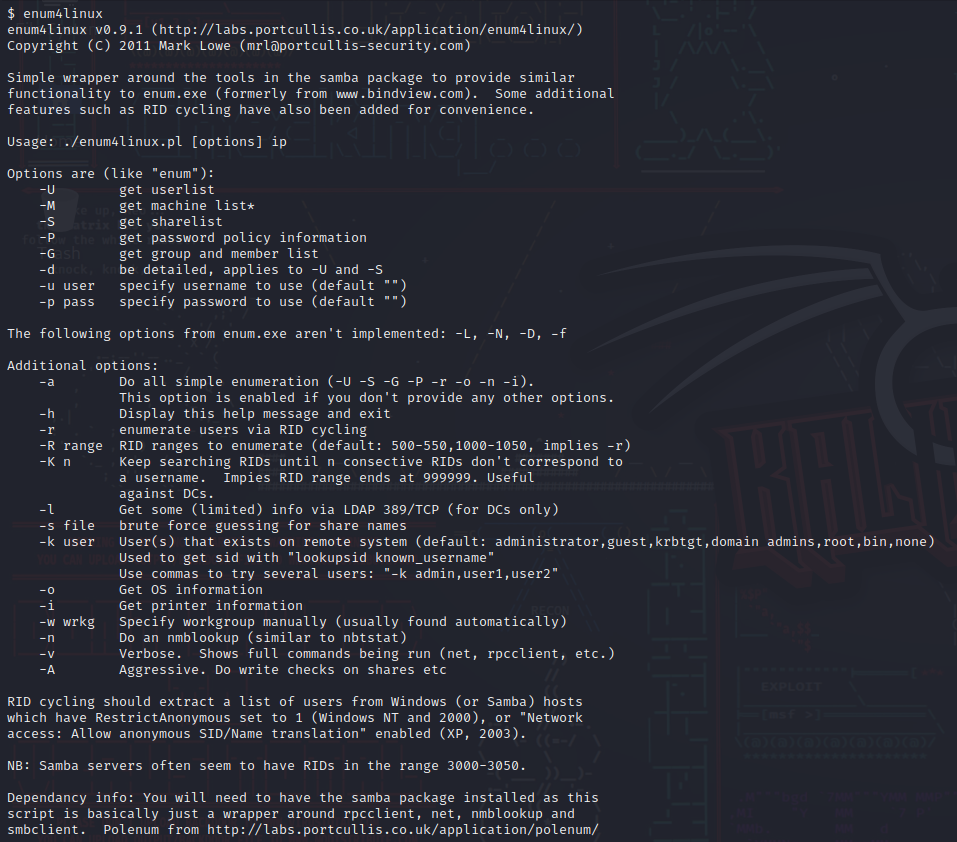
* OSINT Analysis



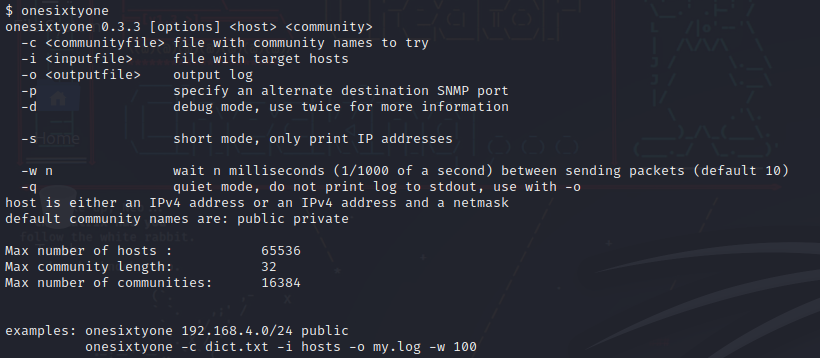
* Route Analysis



* SMB Analysis



* SMTP Analysis
* SNMP Analysis



* SSL Analysis

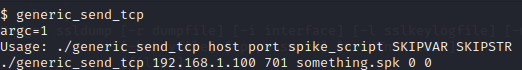


1. Vulnerability Analysis:-

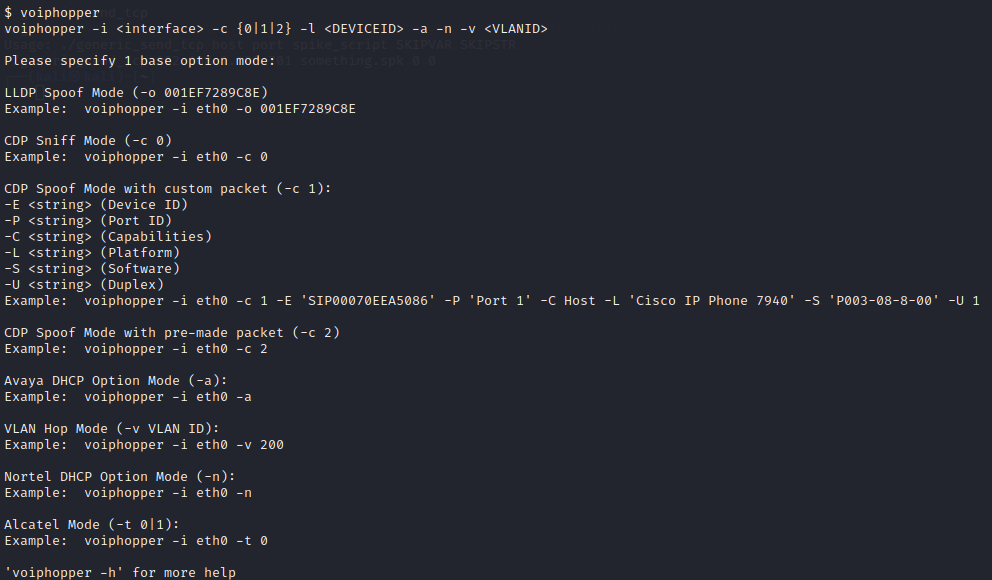
Vulnerability Analysis is one of the most important phases of Hacking. It is done after Information Gathering and is one of the crucial steps to be done while designing an application. The cyber-world is filled with a lot of vulnerabilities which are the loopholes in a program through which hacker executes an attack. These vulnerabilities act as an injection point or a point that could be used by an attacker as a launchpad to execute the attack.

Types of Vulnerability Analysis:-

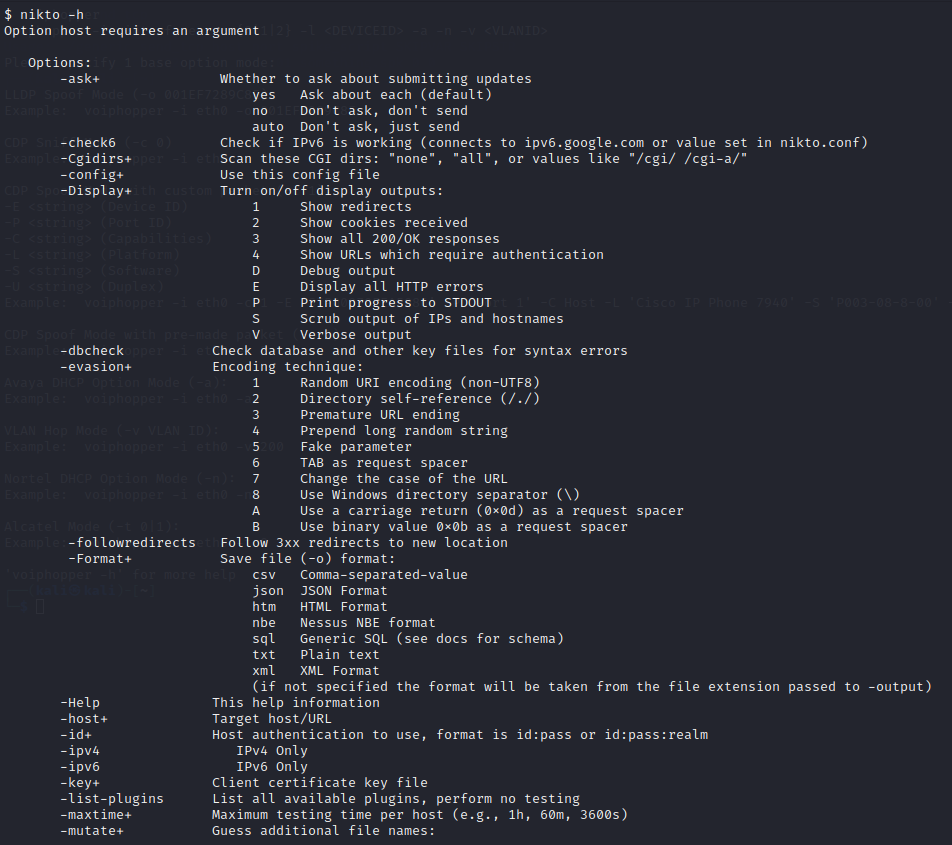
* Fuzzing Tools



* VoIP Tools



* Nmap

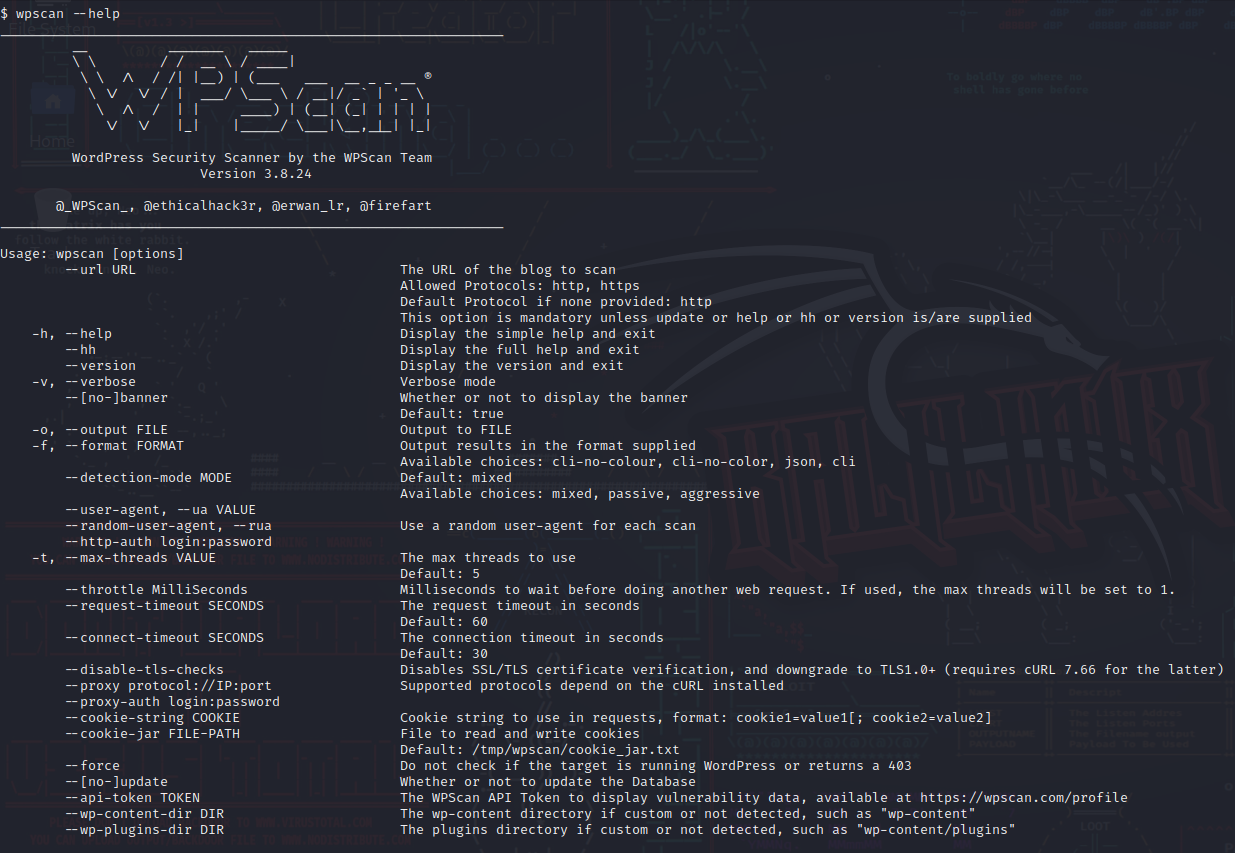


1. Web application analysis:-

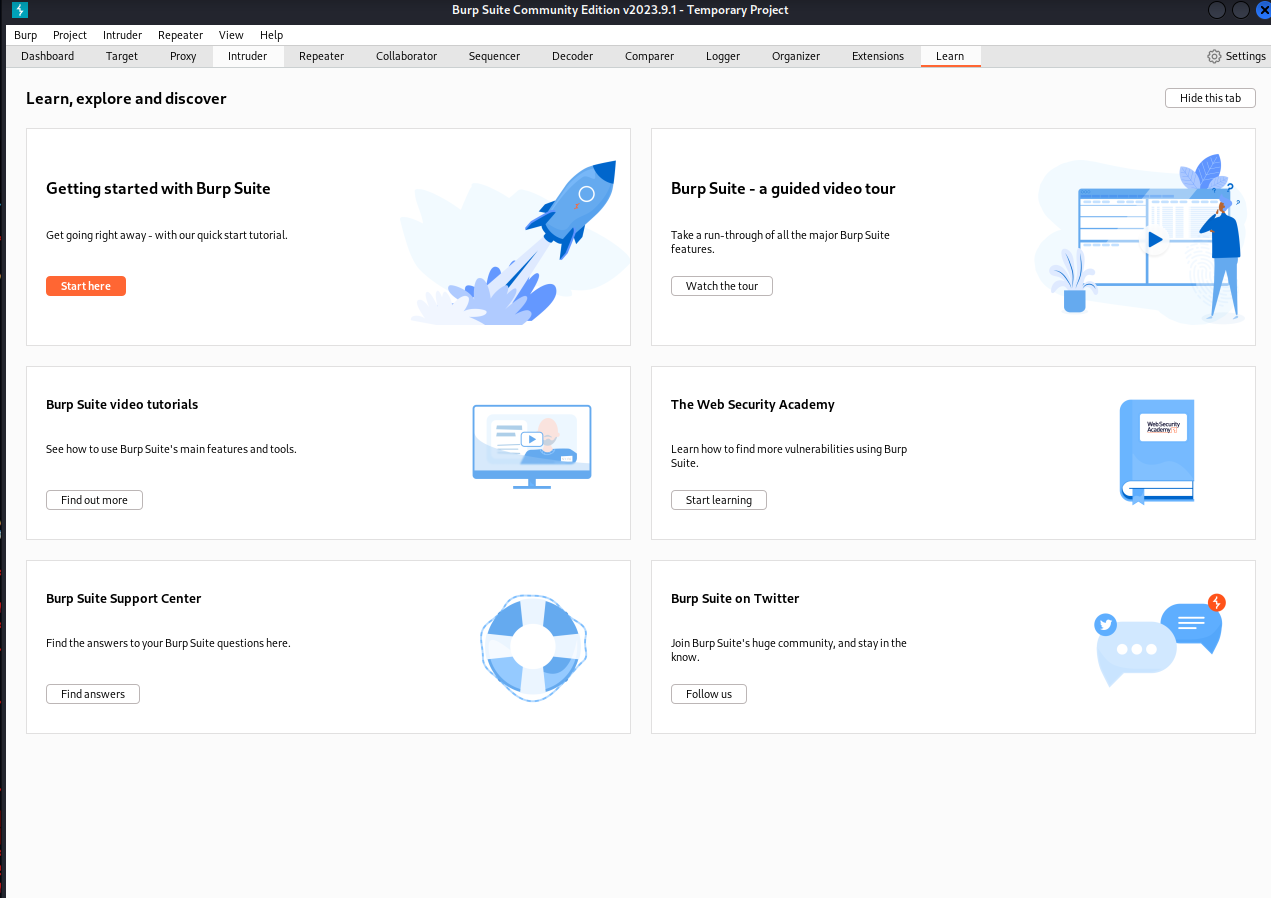
This category covers a lot of ground, and like everything in Kali, tools exist for almost any pen testing or red-teaming exercise involving web applications. While OWASP is a rich cybersecurity platform for network attacks and defenses included with Kali, OWASP Zed Attack Proxy is just one of the many utilities available for attacking web apps.

Types of Web Application Analysis:-

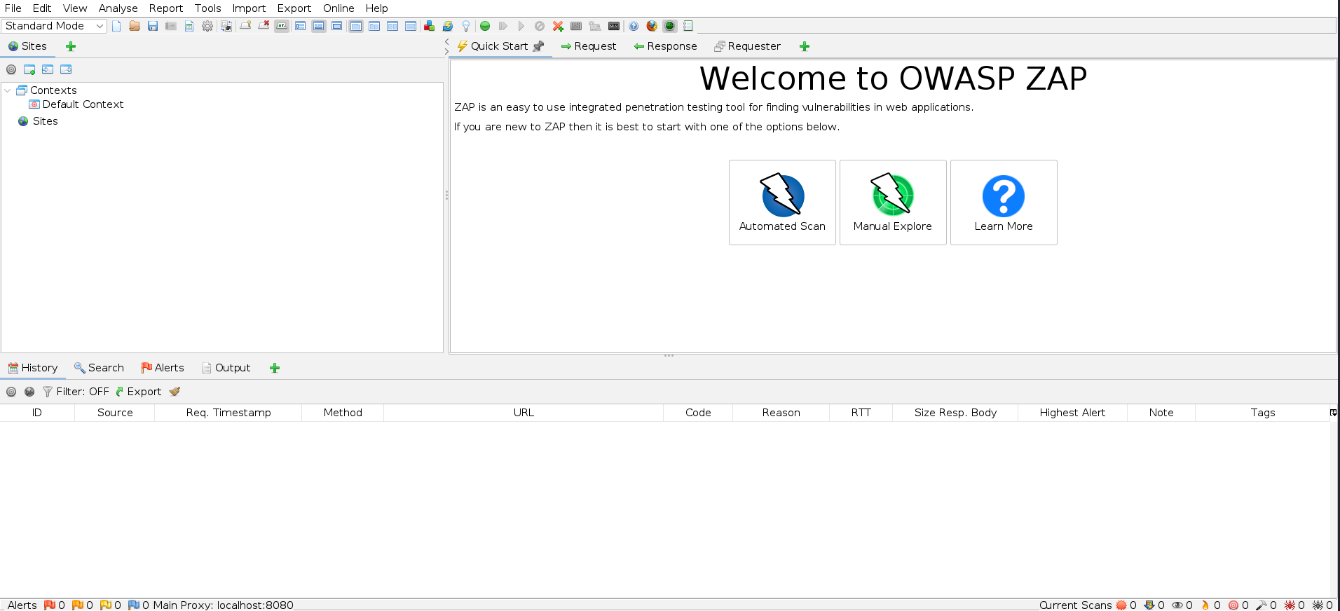
* CMS and Frame work Identification.



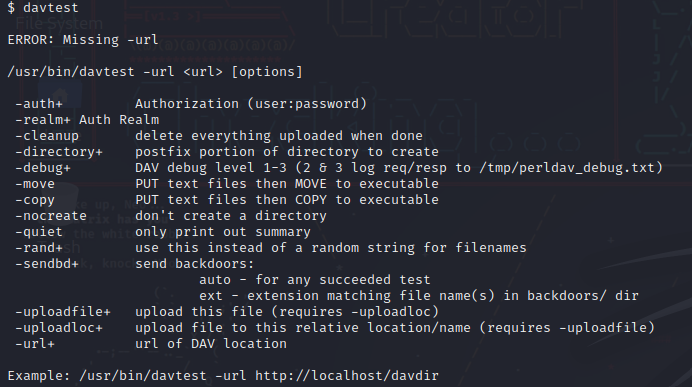
* Web Application Proxies



* Web Crawlers and Directory Bruteforce.



* Web Vulnerability Scanners



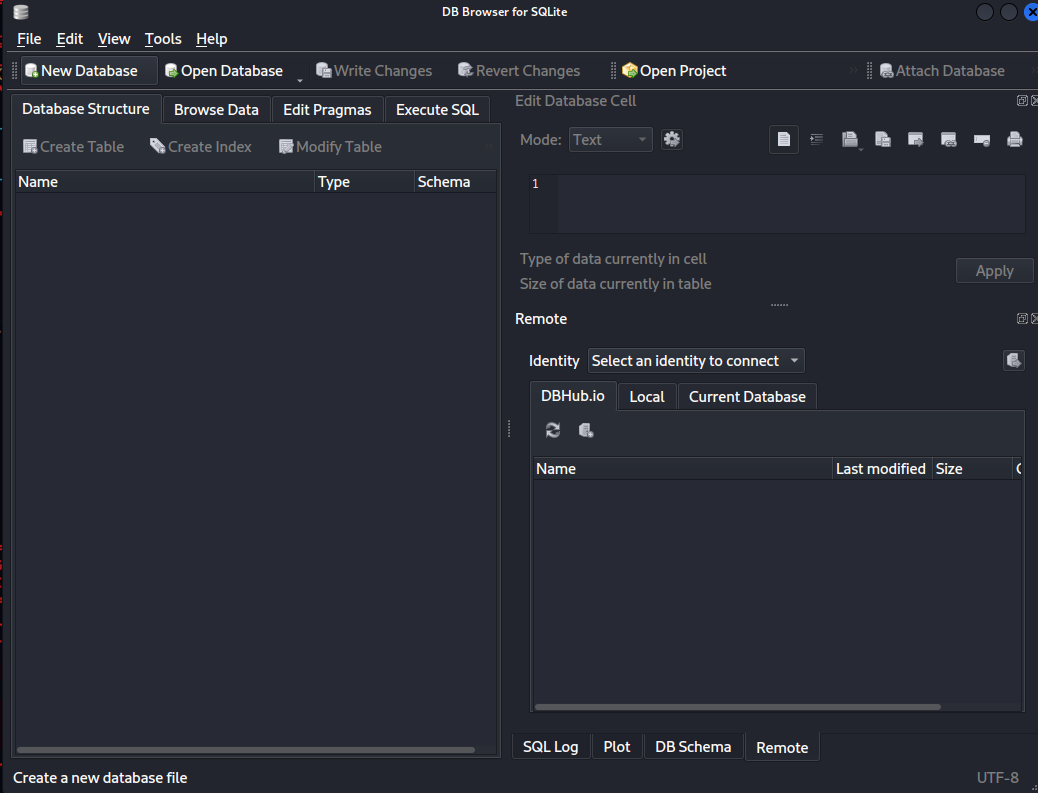
1. Database assessment:-

As the amount of data generated by the business as well as the increasing number of attacks and database breaches, it is more important than ever to keep our data safe. Today's businesses ignore their databases, oblivious to the fact that gaining access to their data is one of a hostile individual's goals (typically their crown jewels). Freepik Heartland Payment Systems (worth $ 300 million), Talk Talk, and Archos are just a few of the well-known data breaches where the SQL injection vulnerability was used to obtain access to client data.

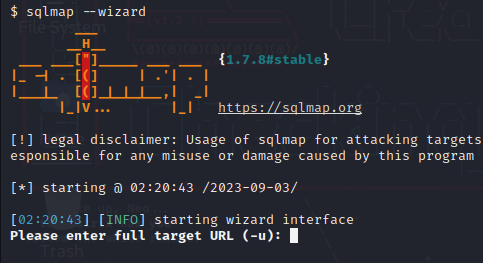
There are numerous advantages of carrying out a database security assessment. In Kali Linux, there are various tools that we can use to perform a database security assessment in our IT environment.

Types of Database Assessment:-

* SQLite Database Browser



* Sqlmap

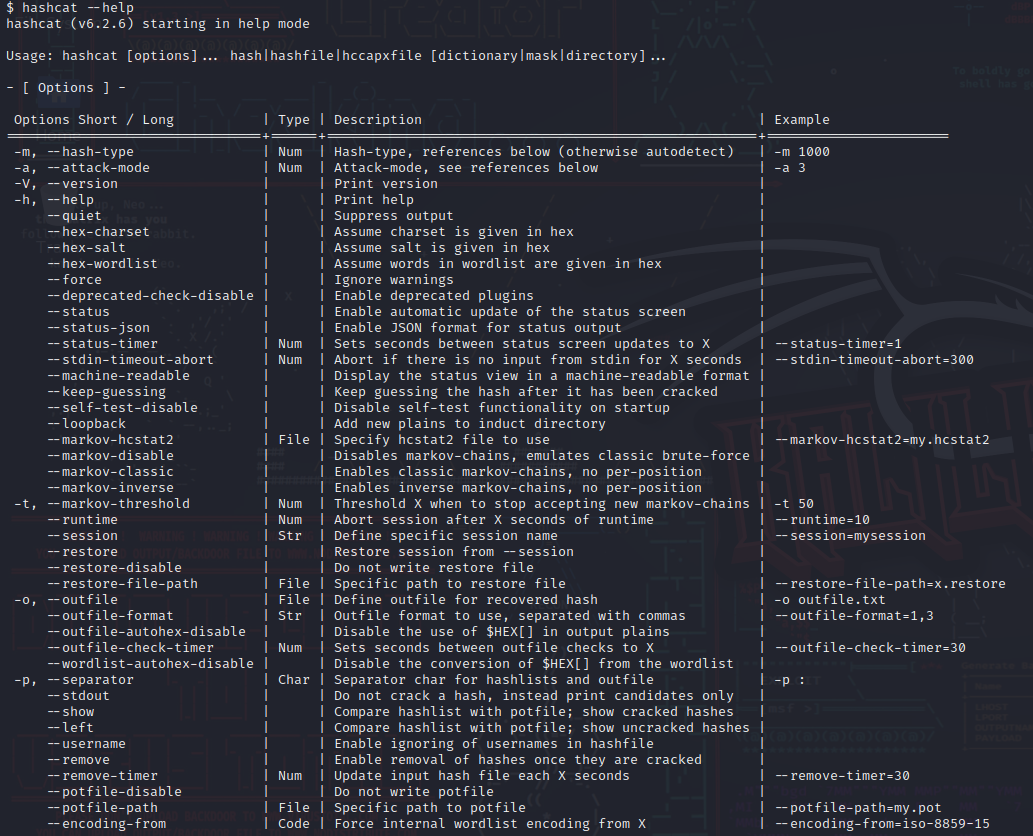


1. Password attacks:-

This category includes standalone password cracker tools, such as Hydra, Ncrack, Hashcat and John the Ripper. It also includes utilities that help increase the effectiveness of any password cracker, such as Crunch, a program for generating wordlists; Ophcrack, a program that uses rainbow tables to crack Windows passwords; and more.

Types of Password attacks:-

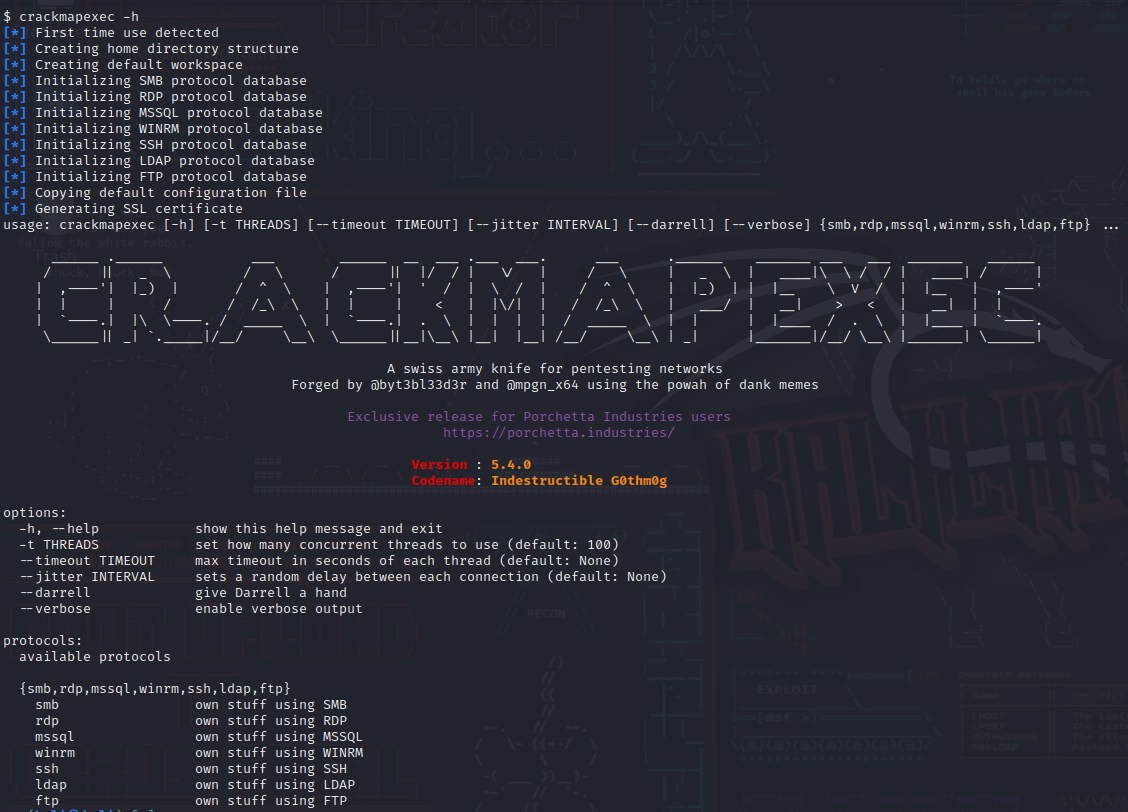
* Offline Attacks



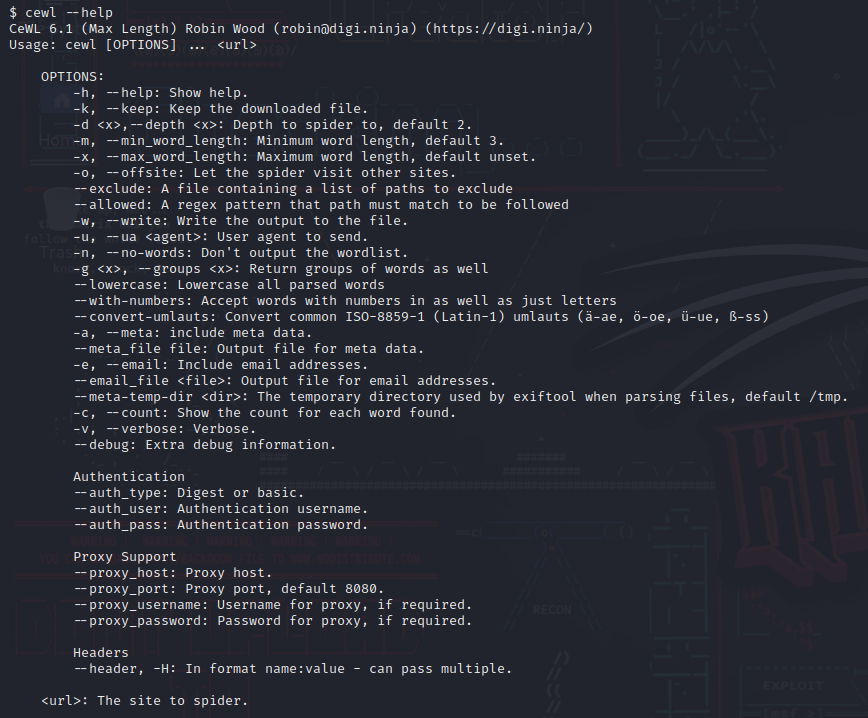
* Online Attacks



* Passing the hash Tools



* Password Profiling and Wordlists

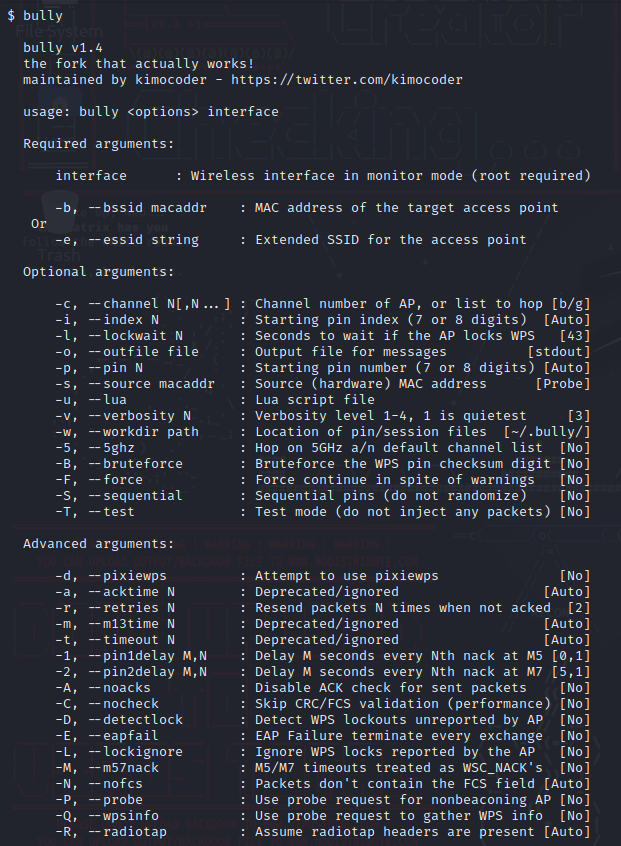


1. Wireless attacks:-

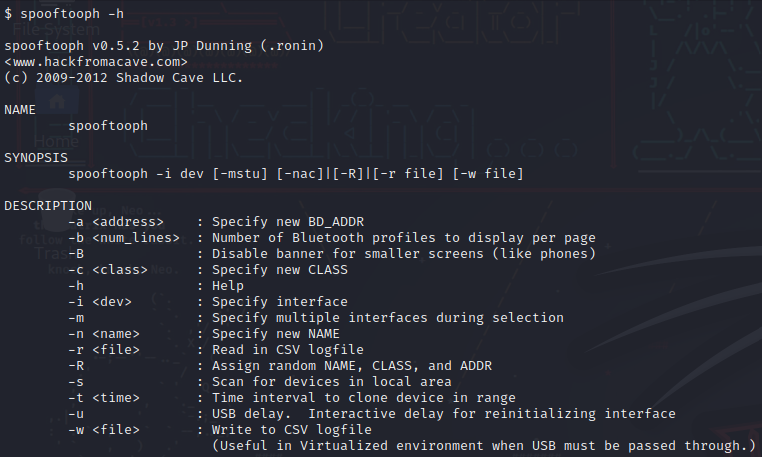
This category includes a broad range of utilities to carry out cybersecurity exercises or hack attacks against wireless systems, including those connected by Bluetooth and Wi-Fi. The top Kali wireless utility is Aircrack-ng, a software suite that includes a network detector, wireless packet sniffer and credential cracking tools used to attack wireless authentication protocols, such as Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access.

Types of Wireless attacks:-

* 802.11 Wireless Tools

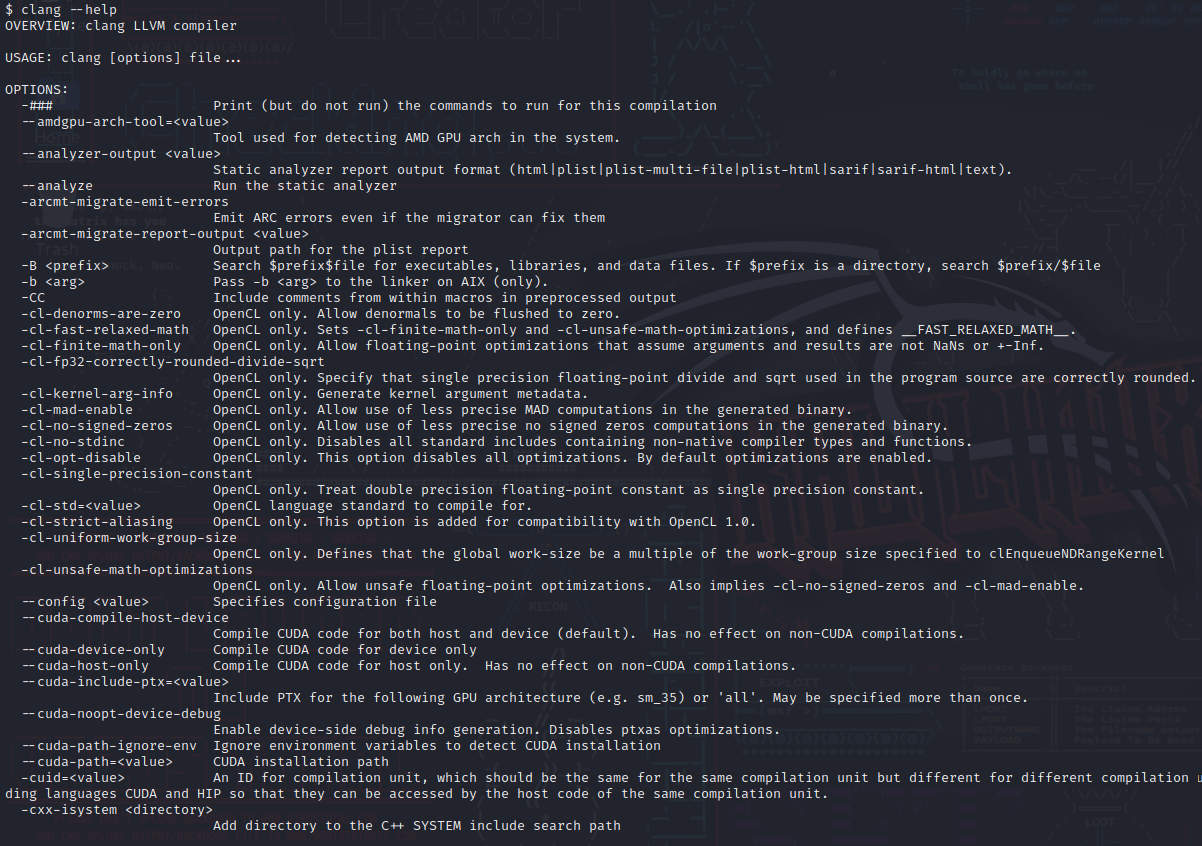


* Bluetooth Tools



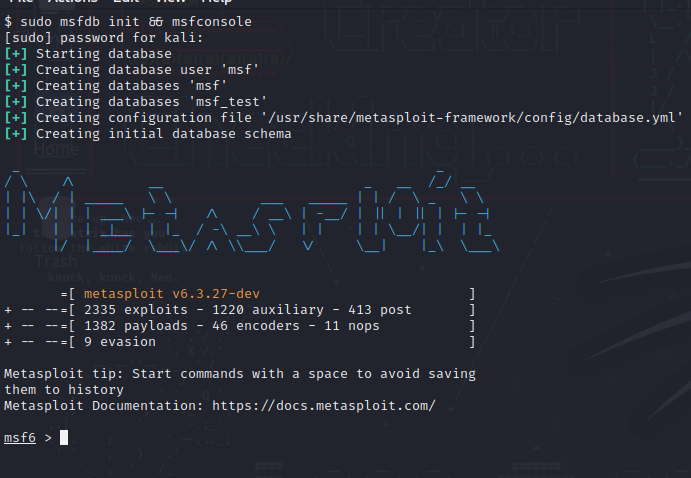
1. Reverse Engineering:-

The purpose of reverse-engineering is to find out how an object or system works. There are a variety of reasons to do this. Reverse-engineering can be used to learn how something works and to recreate the object or to create a similar object with added enhancements.



1. Exploitation Tools:-

After Scanning, information Gathering, and finding a vulnerability comes the main concept of hacking which is Exploitation of the vulnerability. Vulnerability is not that effective if it can not be exploited or it could not cause harm to the application, So in order to get the impact of the vulnerability, we have to exploit also in many cases we have to take down a hacker’s or a spammer’s website. So we have to find a vulnerability on the website and have to exploit it. Kali Linux comes packed with 300+ tools for cybersecurity and penetration testing out of which many of the tools are used to exploit these vulnerabilities.

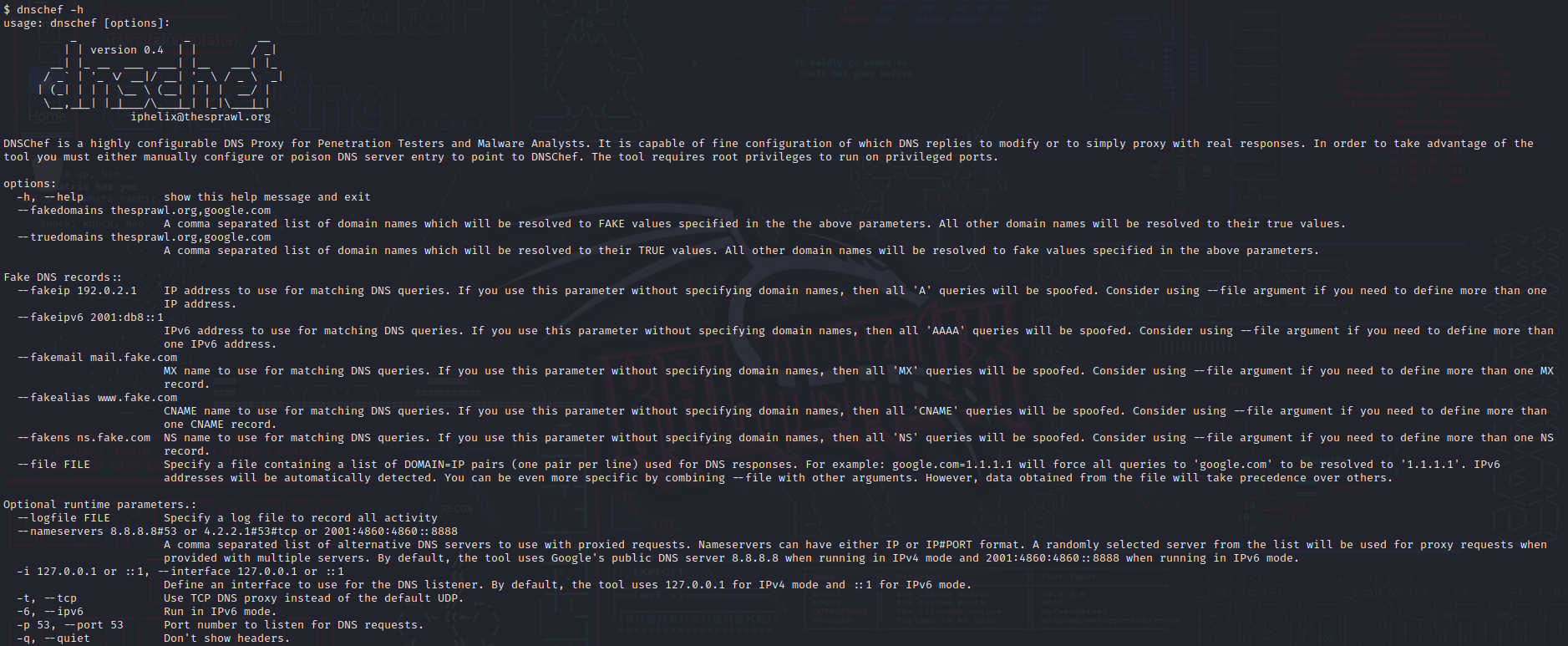


1. Sniffing and Spoofing:-

Sniffing is the process of intercepting and collecting network traffic as it passes over a digital network. Spoofing is the act of disguising a communication from an unknown source as being trustworthy. Using a packet analyzing (sniffing) or spoofing tool, intercept network traffic.

Types of Sniffing and Spoofing:-

Network Sniffers



* Spoofing and MITM

