AI WITH CYBER SECURITY

ASSIGNMENT-2

SHREYA SINGH

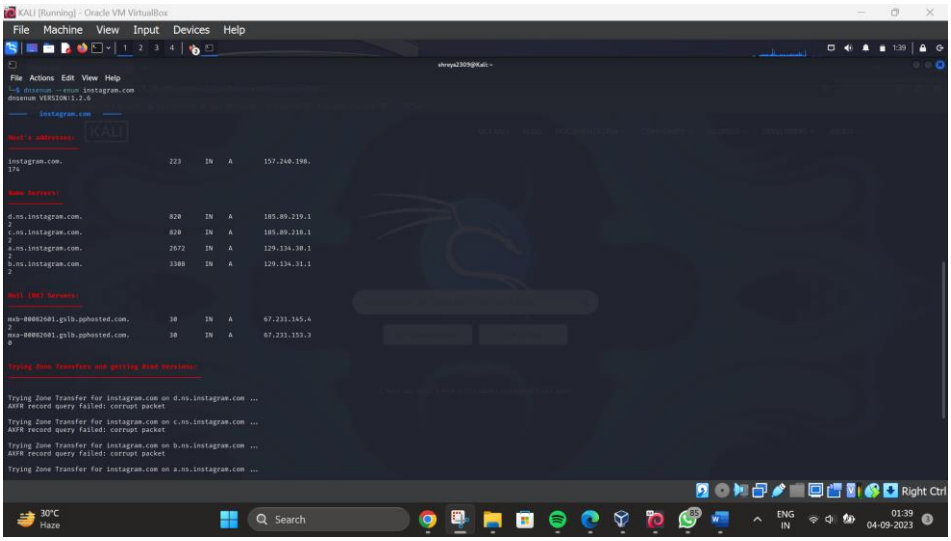
1. **INFORMATION GATHERING**

   It is a method used by analysts to determine the needs of customers and users. Techniques that provide safety, utility, usability, learnability, etc. for collaborators result in their collaboration, commitment, and honesty. Various tools and techniques are available, including public sources such as Whois, nslookup which can help hackers to gather user information. This step is very important because while performing attacks on any target information (such as his pet name, best friend's name, age, or phone number to perform password guessing attacks(brute force) or other kinds of attacks) are required.

   Information gathering can be classified into the following categories:

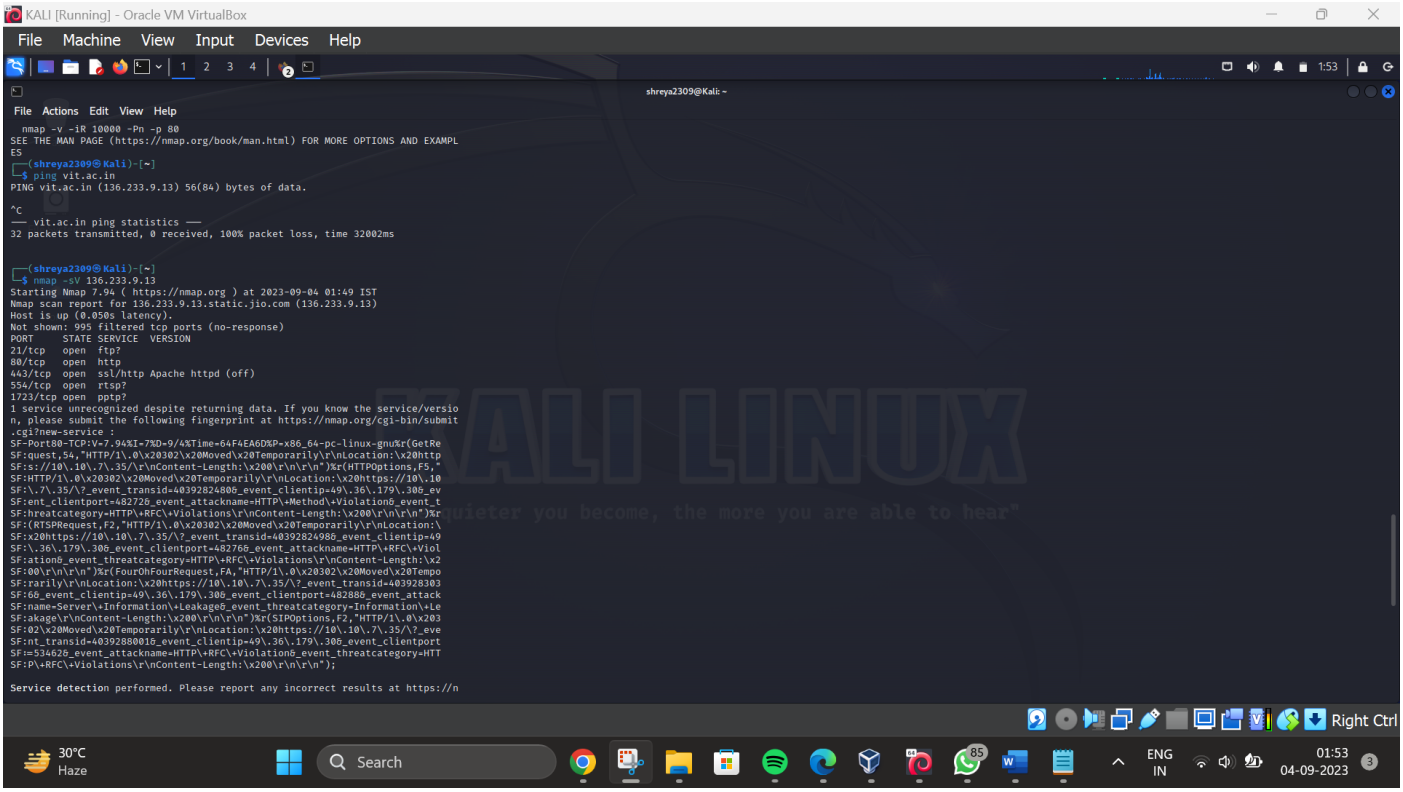
   Footprinting
   Scanning
   Enumeration
   Reconnaissance

   - **DNSENUM**



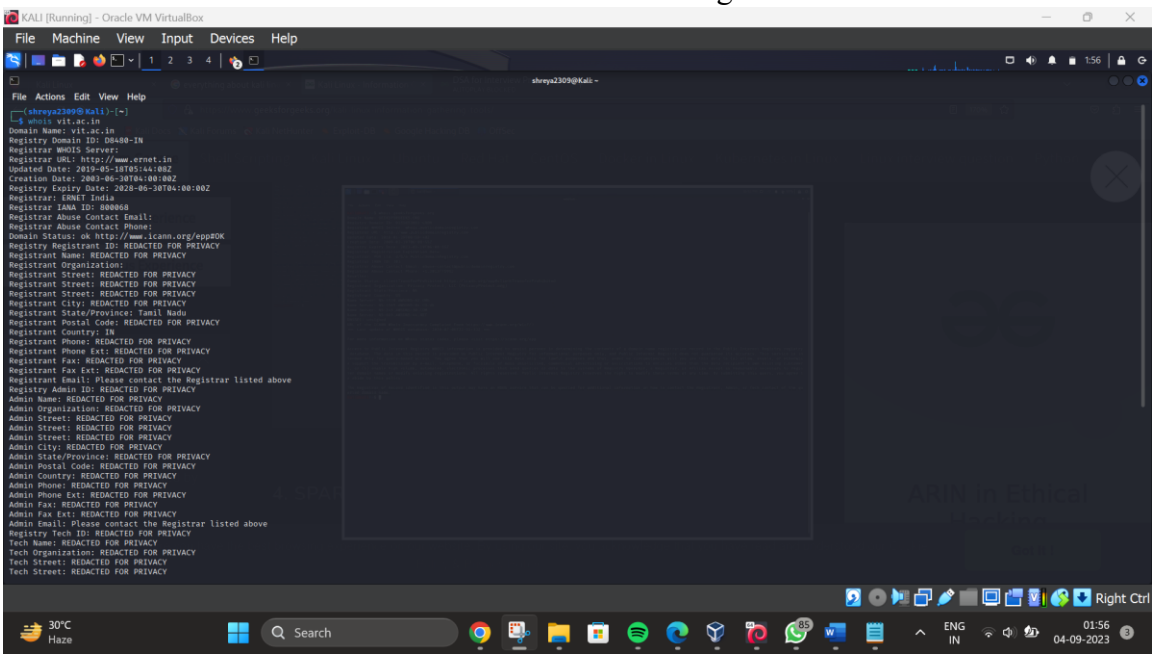
   - **NMAP TOOL**

     Nmap is an open-source network scanner that is used to recon/scan networks. It is used to discover hosts, ports, and services along with their versions over a network. It sends packets to the host and then analyzes the responses in order to produce the desired results. It could even be used for host discovery, operatingsystem detection, or scanning for open ports. It is one of the most popular reconnaissance tools.



- **WHOIS lookup**
  whois is a database record of all the registered domains over the internet. It is used for many purposes, a few of them are listed below.

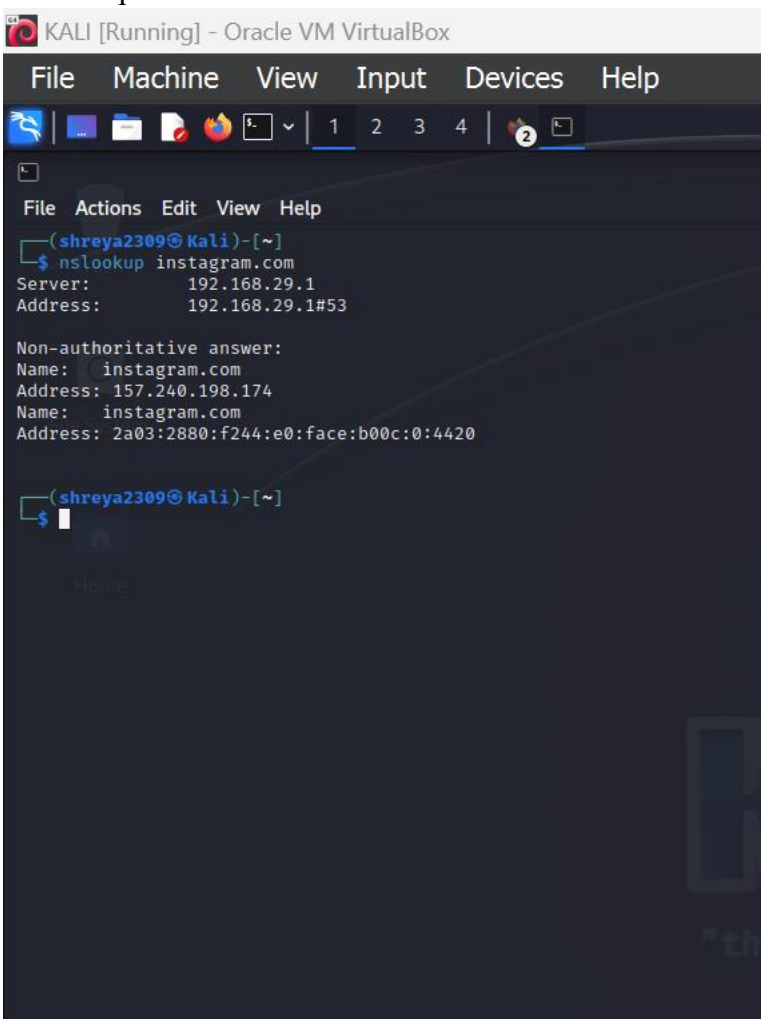
  It is used by Network Administrators in order to identify and fix DNS or domain-related issues.
  It is used to check the availability of domain names.
  It is used to identify trademark infringement.
  It could even be used to track down the registrants of the Fraud domain.



- **Nslookup**
  nslookup stands for nameserver lookup, which is a command used to get the information from the DNS server. It queries DNS to obtain a domain name, IP address

mapping, or any other DNS record. It even helps in troubleshooting DNS-related problems. It is used for many purposes, a few of them are listed below.

To get the IP address of a domain.
For reverse DNS lookup
For lookup for any record
Lookup for an SOA record
Lookup for an ns record
Lookup for an MX record
Lookup for a txt record



2. **Vulnerability Analysis**
   - **Nikto**

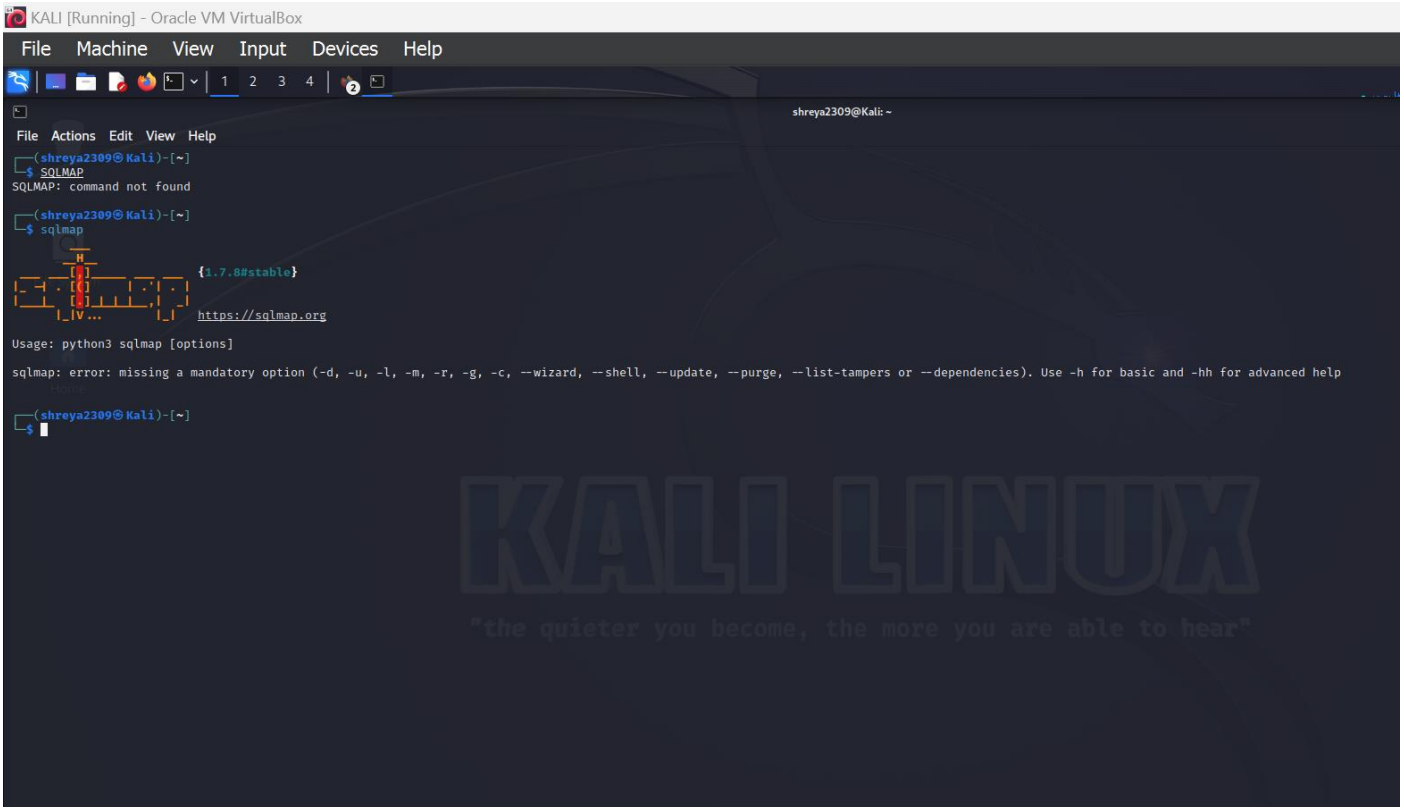
     Nikto is an Open Source software written in Perl language that is used to scan a web-server for vulnerability that can be exploited and can compromise the server. It can also check for outdated version details of 1200 servers and can detect problems with specific version details of over 200 servers. It comes packed with many features, a few of them are listed below.

     Full support for SSL
     Looks for subdomains
     Supports full HTTP Proxy
     Outdated component report
     Username Guessing

- **Burpsuite**
  Burp Suite is one of the most popular web application security testing software. It is used as a proxy, so all the requests from the browser with the proxy pass through it. And as the request passes through the burp suite, it allows us to make changes to those requests as per our need which is good for testing vulnerabilities like XSS or SQLi or even any vulnerability related to the web. Kali Linux comes with burp suite community edition which is free but there is a paid edition of this tool known as burp suite professional which has a lot many functions as compared to burp suite community edition.

  I used burpsuite in the previous assignment to carry put different vulnerabilities

- **SQL MAP**
  SQLMap is an open-source tool that is used to automate the process of manual SQL injection over a parameter on a website. It detects and exploits the SQL injection parameters itself all we have to do is to provide it with an appropriate request or URL. It supports 34 databases including MySQL, Oracle, PostgreSQL, etc.



- **ZENMAP**
  It uses the Graphical User Interface. It is a great tool for network discovery and security auditing. It does the same functions as that of the Nmap tool or in other words, it is the graphical Interface version of the Nmap tool. It uses command line Interface. It is a free utility tool for network discovery and security auditing. Tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime are considered really useful by systems and network administrators.

3. WEB APPLICATION ANALYSIS

- **MALTEGO**
  Maltego is a platform developed to convey and put forward a clear picture of the environment that an organization owns and operates. Maltego offers a unique perspective to both network and resource-based entities which is the aggregation of information delivered all over the internet – whether it's the current configuration of a router poised on the edge of our network or any other information, Maltego can locate, aggregate and visualize this information. It offers the user with unprecedented information which is leverage and power.

Maltego's Uses:

It is used to exhibit the complexity and severity of single points of failure as well as trust relationships that exist currently within the scope of the infrastructure.

It is used in the collection of information on all security-related work. It will save time and will allow us to work more accurately and in a smarter way.

It aids us in thinking process by visually demonstrating interconnected links between searched items.

It provides a much more powerful search, giving smarter results.

It helps to discover "hidden" information.

- **WHATWEB**

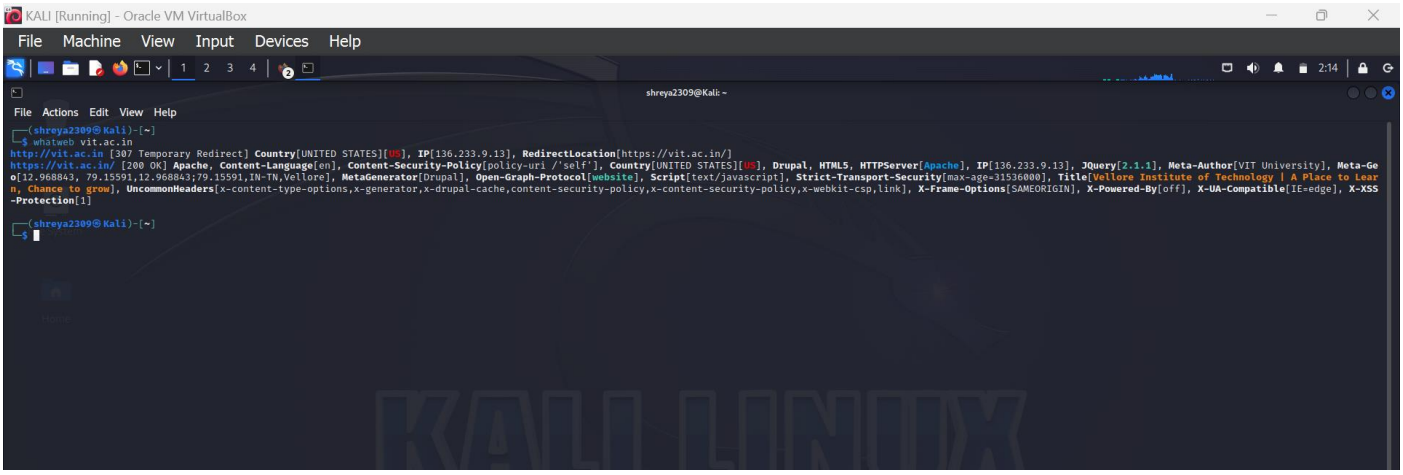
Whatweb is an acronym of "what is that website".It is used to get the technologies which a website is using, these technologies might me content management system(CMS), Javascript Libraries, etc. It is used for many purposes, a few of them are listed below.

To get the Content Management System is used by a web application

To get the Web Server details being used by the web application

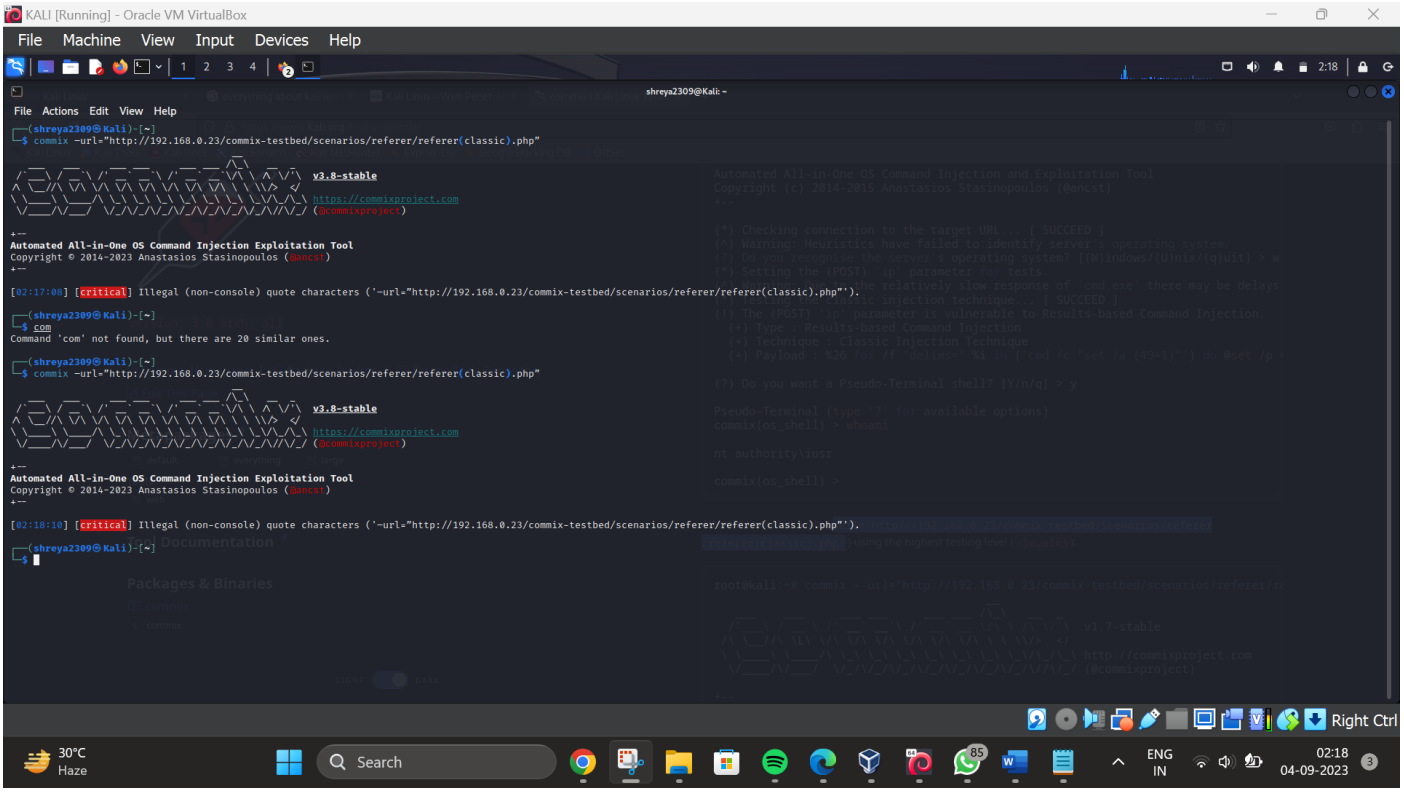
To get the embedded devices attached to the web application

It consists of 1700+ plugins and every plugin is used to recognize something different.



- **COMMIX**

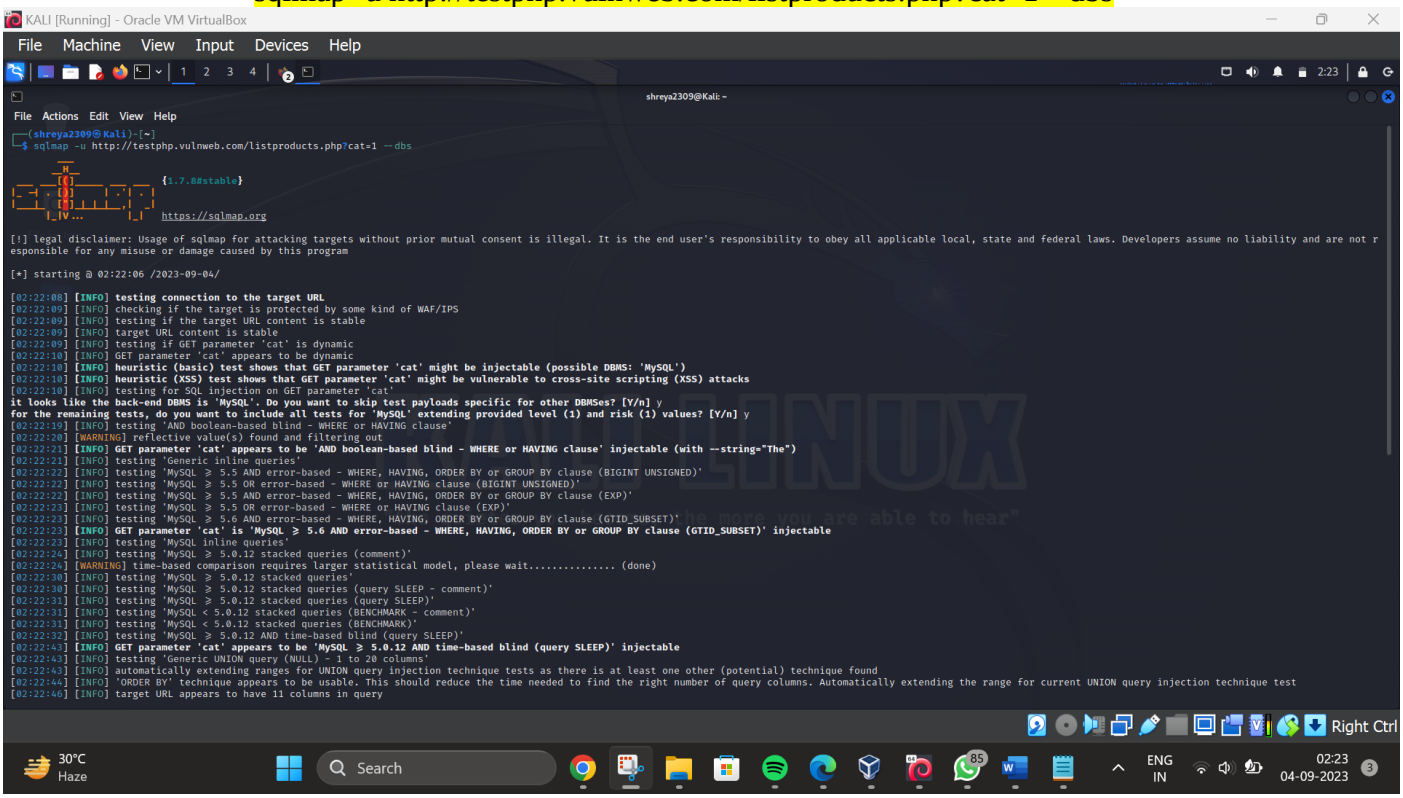
Command injection exploiter (commix) is an automated tool written in Python that is pre-compiled in Kali Linux **to perform various OS commands if the application is vulnerable to command injection**. It allows attackers to inject into any specific vulnerable parts of the application, or even into an HTTP header.

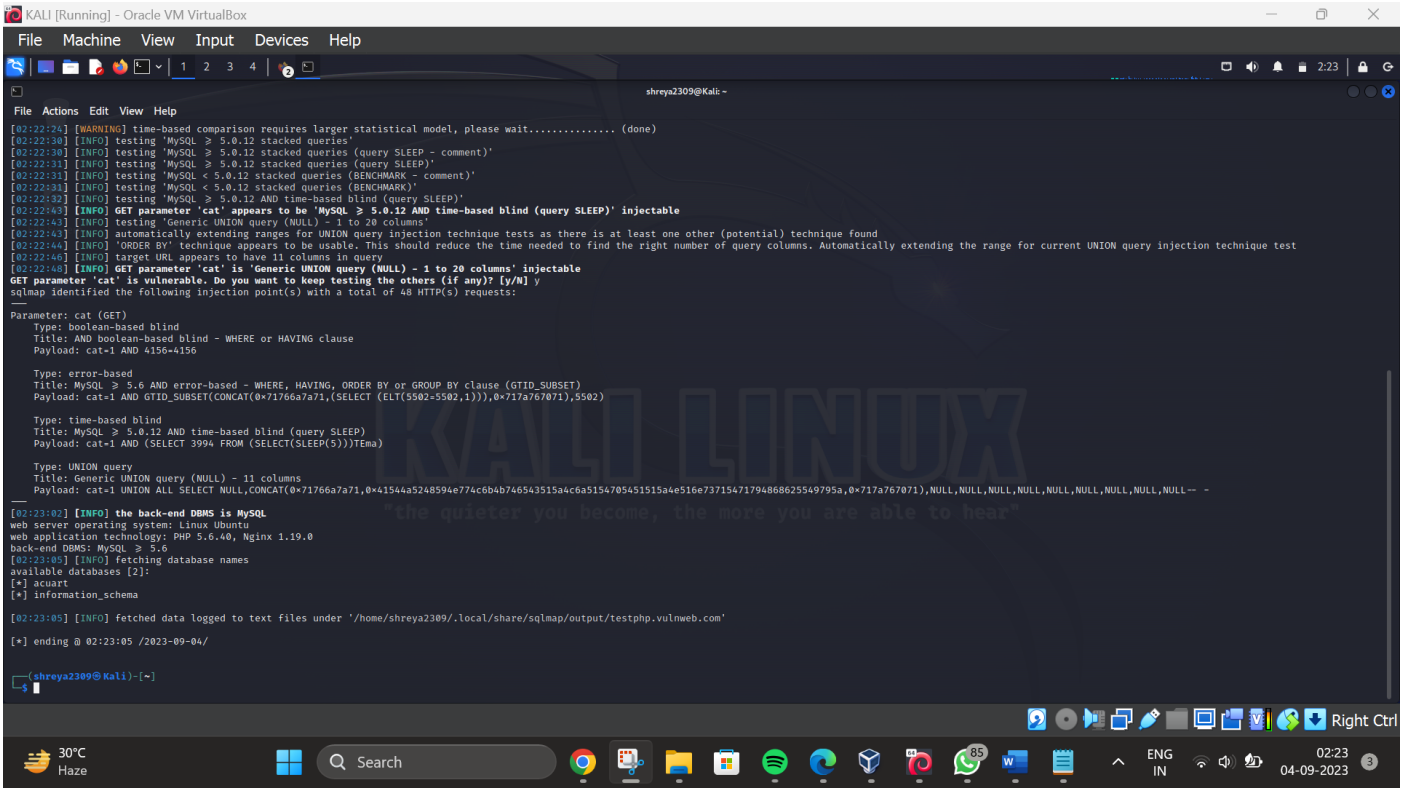


4. DATABASE ASSESSMENT

- **SQLMAP**

sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 --dbs

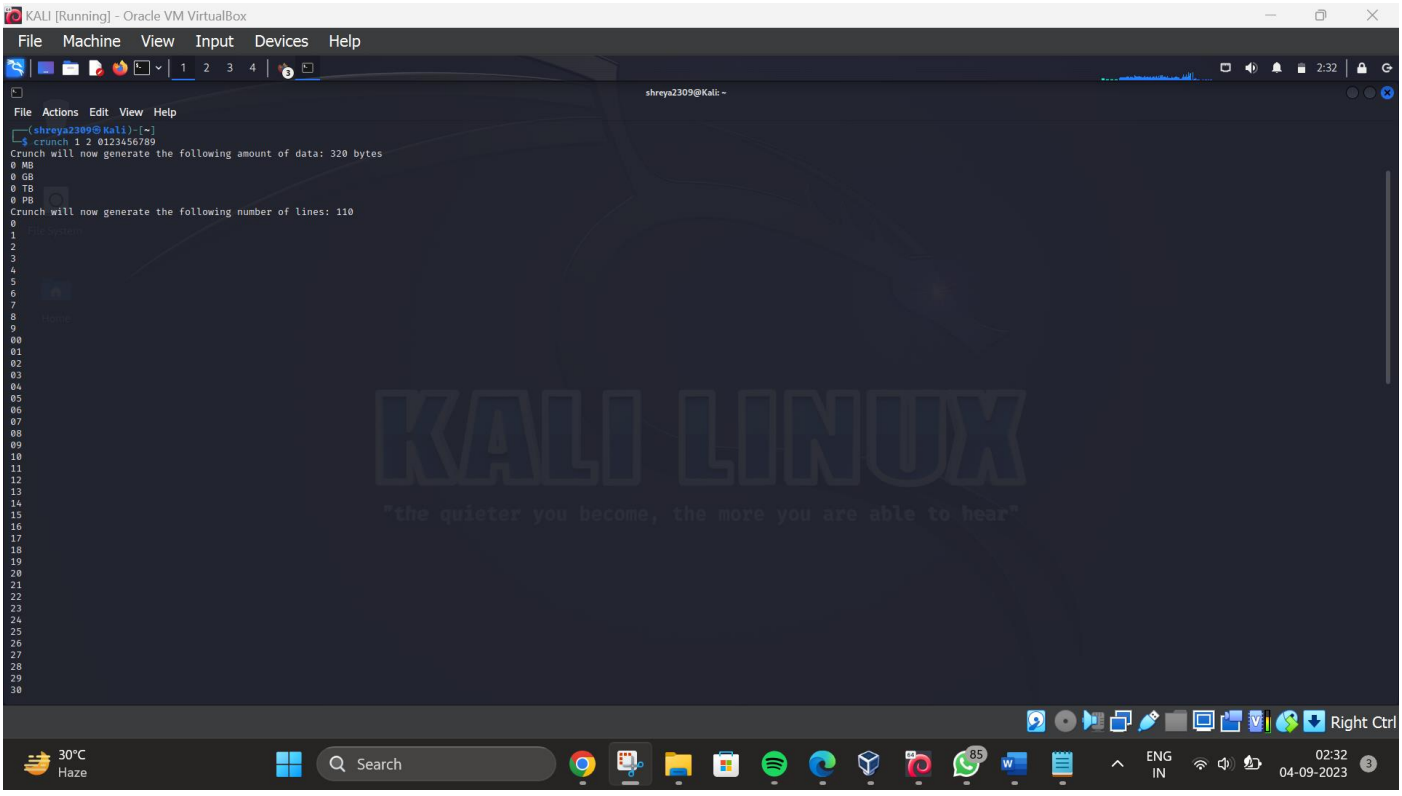




5. PASSWORD CRACKING

- **CRUNCH**

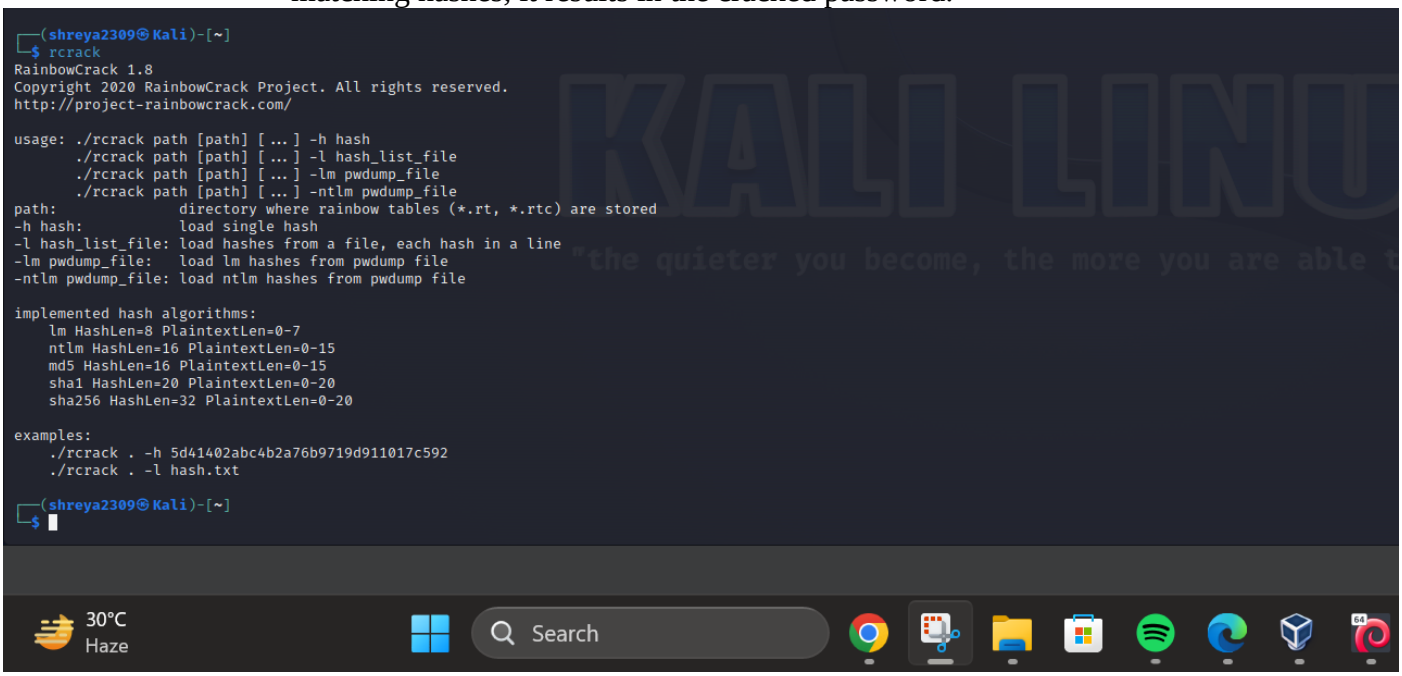
  crunch is a wordlist generating tool that comes pre-installed with Kali Linux. It is used to generate custom keywords based on wordlists. It generates a wordlist with permutation and combination. We could use some specific patterns and symbols to generate a wordlist.



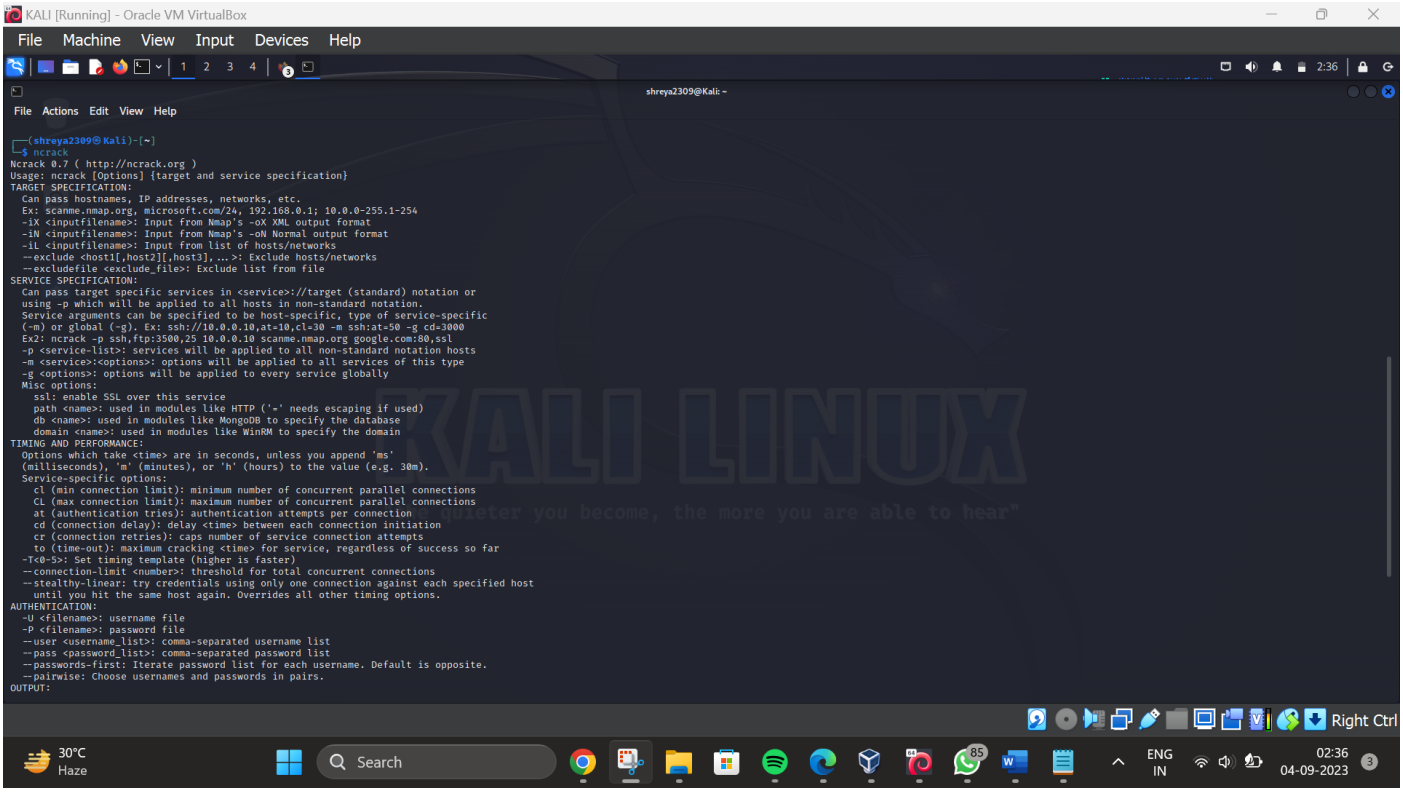
- **RAINBOW CRACK**

  Rainbow crack is a tool that uses the time-memory trade-off technique in order to crack hashes of passwords. It uses rainbow tables in order to crack hashes of passwords. It doesn't use the traditional brute force method for cracking passwords. It

generates all the possible plaintexts and computes the hashes respectively. After that, it matches hash with the hashes of all the words in a wordlist. And when it finds the matching hashes, it results in the cracked password.



- **NCRACK**



- **JOHN THE RIPPER**

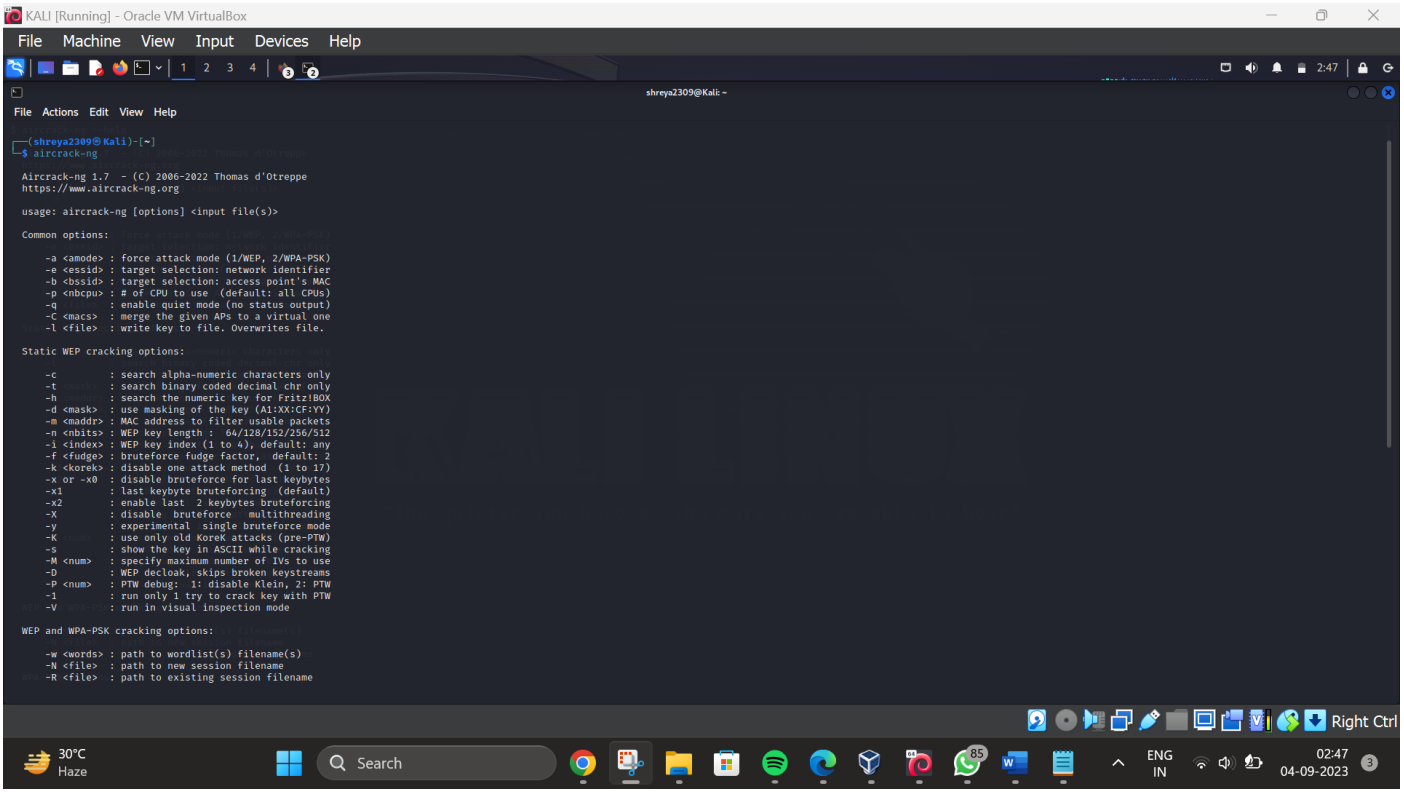
John the Ripper is a great tool for cracking passwords using some famous brute for attacks like dictionary attack or custom wordlist attack etc. It is even used to crack the hashes or passwords for the zipped or compressed files and even locked files as well. It has many available options to crack hashes or passwords.

6. WIRELESS ATTACKS

- **AIRCRACK NG**

Aircrack is an all in one packet sniffer, WEP and WPA/WPA2 cracker, analyzing tool and a hash capturing tool. It is a tool used for wifi hacking. It helps in capturing the package and reading

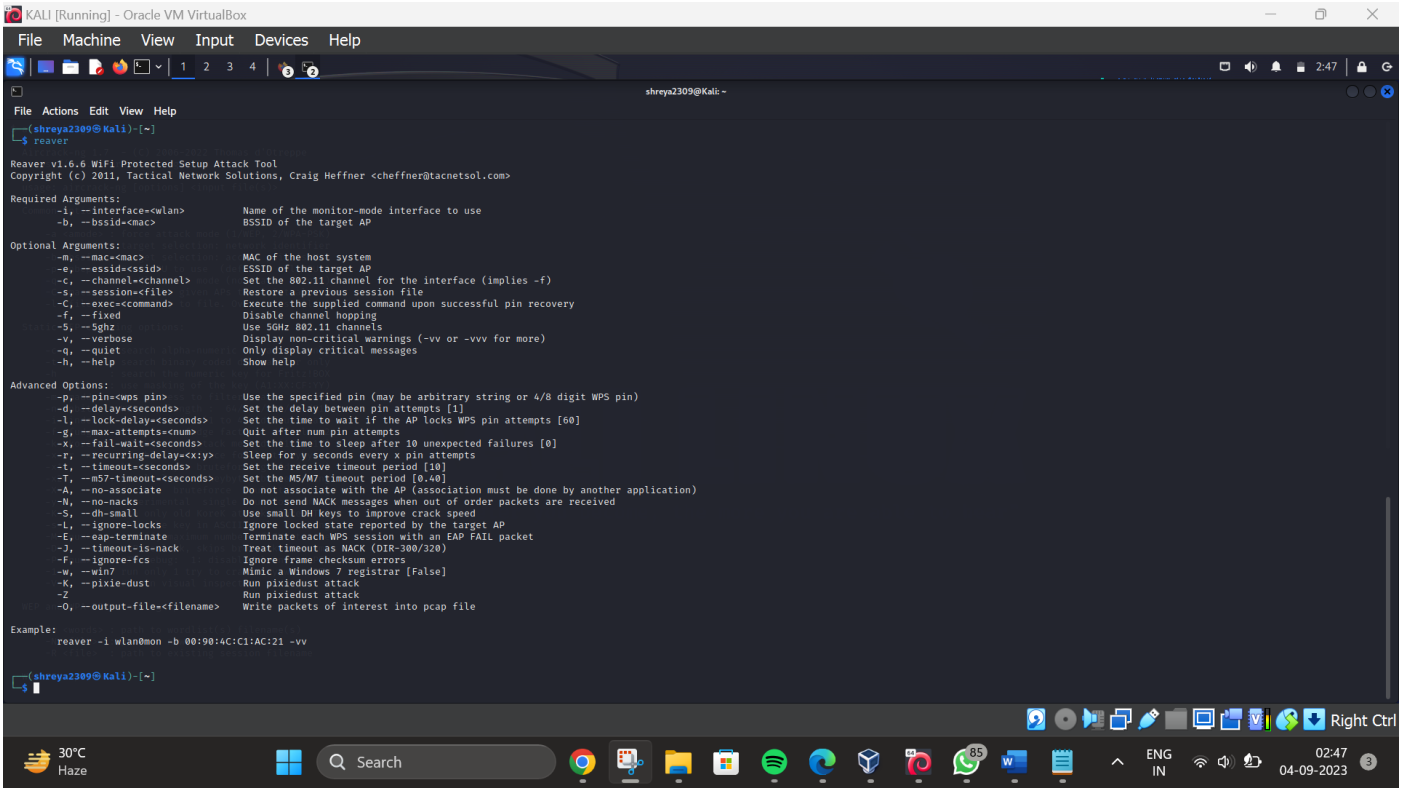
the hashes out of them and even cracking those hashes by various attacks like dictionary attacks. It supports almost all the latest wireless interfaces.



- **REAVER**

  Reaver is a package that is a handy and effective tool to implement a brute force attack against Wifi Protected Setup (WPS) registrar PINs to recover WPA/WPA2 passphrases. It is depicted to be a robust and practical attack against WPS, and it has been tested against a wide variety of access points and WPS implementations. In today's time hacking WPA/WPA2 is exceptionally a tedious job.

  A dictionary attack could take days, and still will not succeed. On average Reaver will take 4-10 hours to recover the target AP's plain text WPA/WPA2 passphrase, depending on the AP. Generally, it takes around half of this time to guess the correct WPS pin and recover the passphrase.



- **WIFITE**

When it comes to wifi Hacking wifite is one of the most useful tools when you have a lot of wireless devices across your location. It is used to crack WEP or WPA/WPS encrypted wireless networks in a row. It could easily be customized to automate the process of multiple wifi hacking. It comes packed with many features, few of them are listed below.

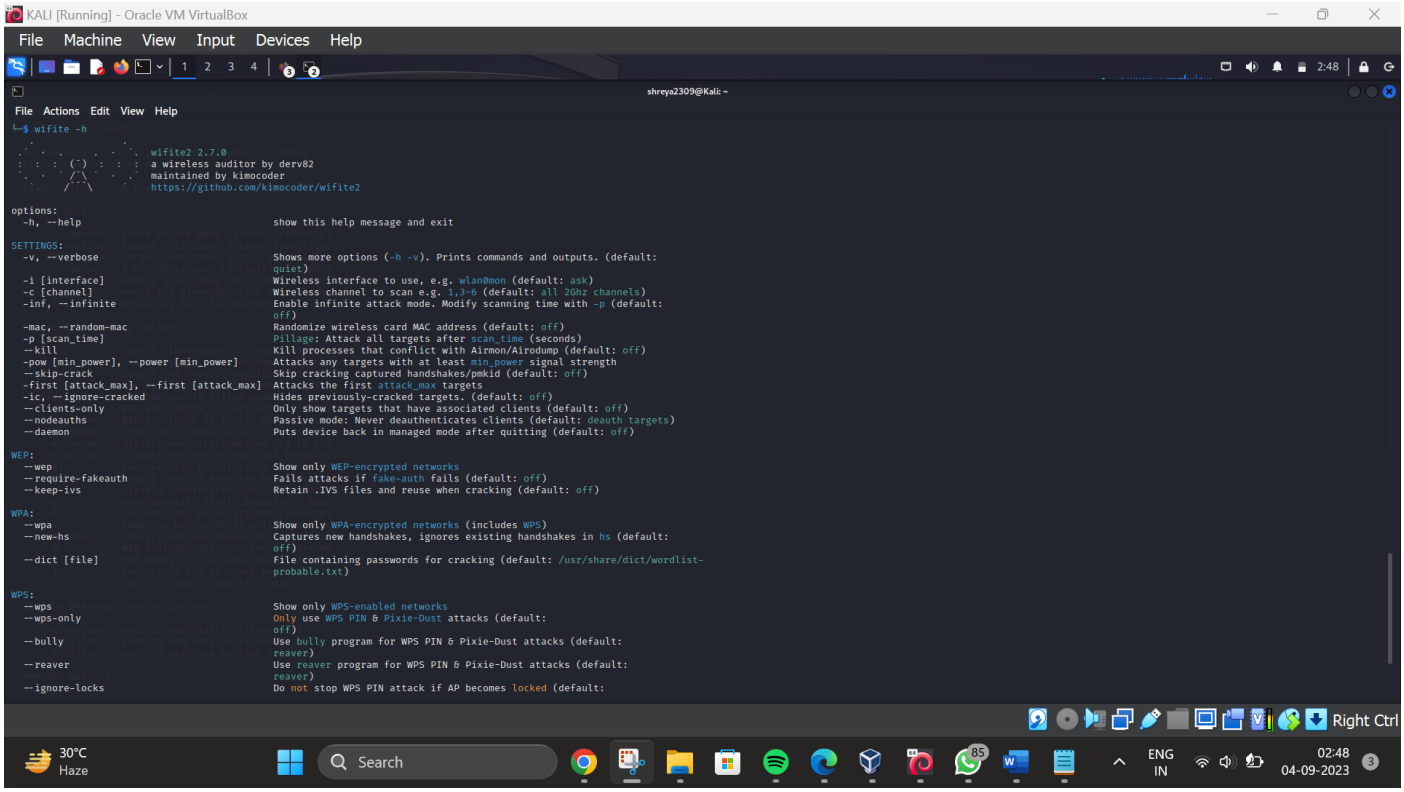
When cracking the passwords for multiple networks it sorts them based on their signal strength.

Packed with a lot of customizing options to improve the effectiveness of the attack.

Changes mac address while attacking to make the attacker anonymous.

If an attacker finds any target not appropriate to be attacked, so it allows the attacker to block the attack for the specific network.

It saves all passwords to a separate file.



- **FERN WIFI CRACKER**

  Fern wifi cracker is used when we want a Graphical User Interface to crack wifi passwords. Fern is a widely used wifi hacking tool designed in Python Programming Language using the Python Qt GUI library. The tools are comfortable to attack wireless networks along with ethernet networks. Fern comes packed with many features, few of them are listed below.

  Used in WEP cracking
  It could perform dictionary attacks for WPA/WPA2/WPS with ease.
  It provides service of an automatic access point attack system.
  May be used to do session hijacking.

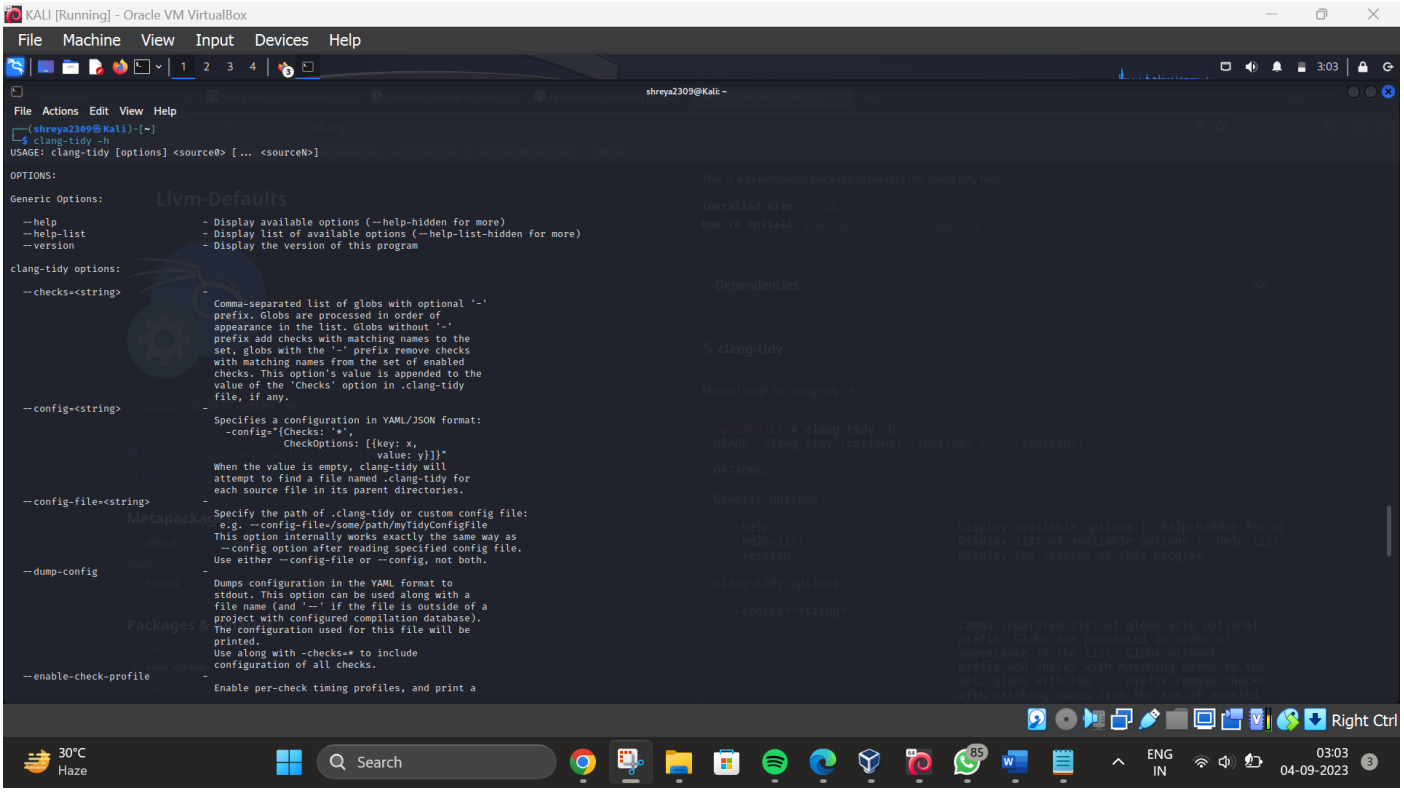
7. REVERSE ENGINEERING

The process of taking a piece of software or hardware and analyzing its functions and information flow so that its functionality and behavior can be understood. Malware is commonly reverse-engineered in cyber defense.

TOOLS USED ARE:

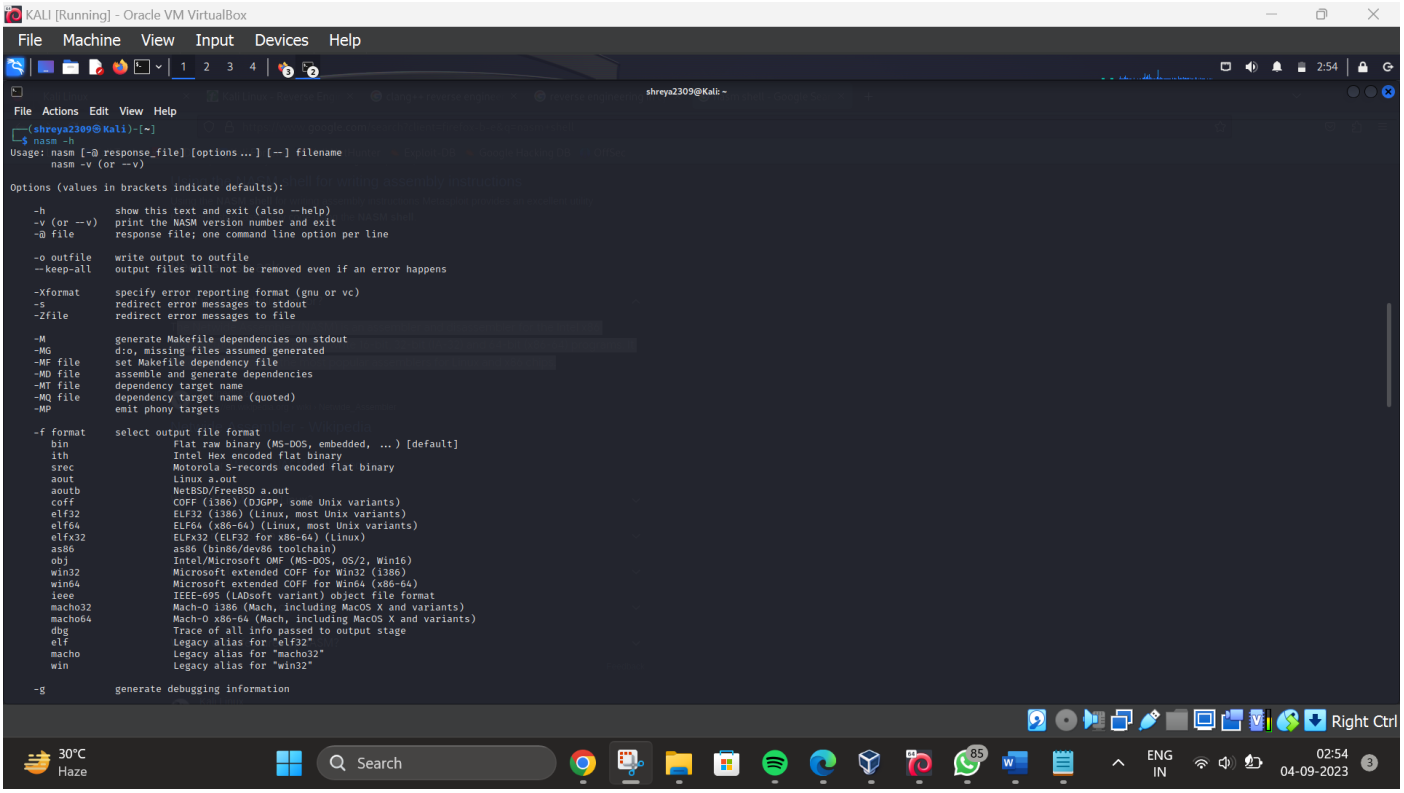
- **CLANG**

  The Clang tool is **a front end compiler that is used to compile programming languages such as C++, C, Objective C++ and Objective C into machine code**. Clang is also used as a compiler for frameworks like OpenMP, OpenCL, RenderScript, CUDA and HIP.



- **CLANG++**
- **NASM SHELL**

  he Netwide Assembler (NASM) is an assembler and disassembler for the Intel x86 architecture. It can be used **to write 16-bit, 32-bit (IA-32) and 64-bit (x86-64) programs**. It is considered one of the most popular assemblers for Linux and x86 chips.



8. EXPLOITATION TOOLS

- **METASPLOIT**

  Metasploit Framework is basically a penetration testing tool that exploits the website and validates vulnerabilities. This tool contains the basic infrastructure, specific content, and tools necessary for penetration testing and vast security assessment. Metasploit Framework is one of the most famous exploitation frameworks and is updated on a regular basis. It can be accessed in the Kali Whisker Menu and launched directly from the terminal. Also here, new exploits are updated as soon as they are published. It contains many tools that are used for creating security workspaces for vulnerability testing and penetration testing systems. It was designed by rapid7 LLC and is completely open-source software and is easy to use.