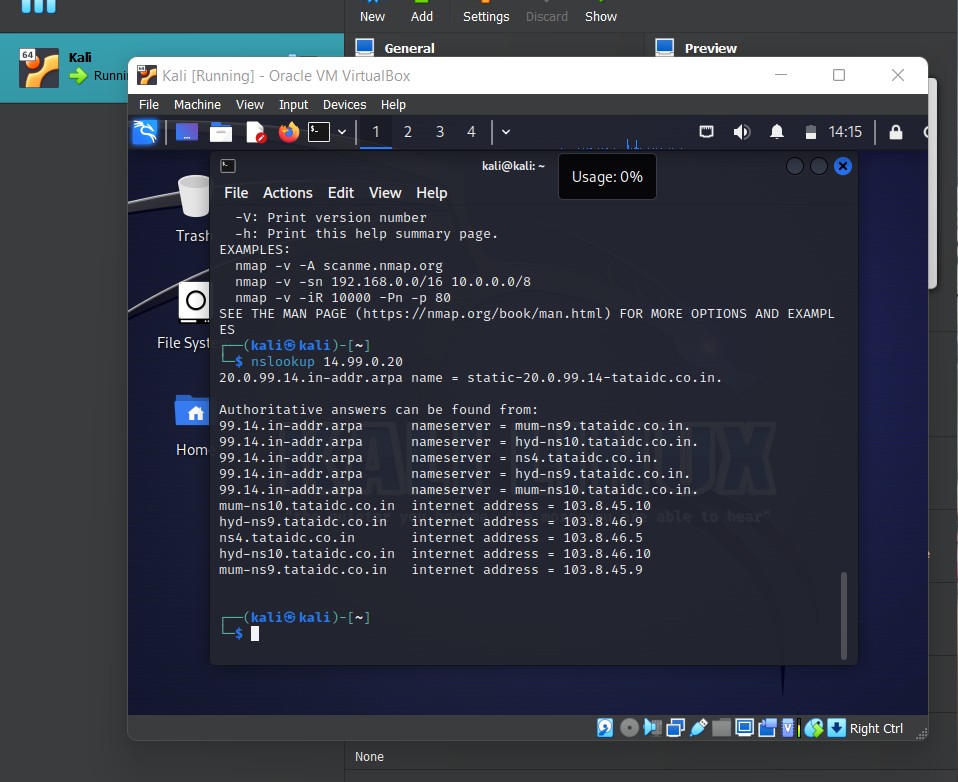
Assignment 2

**Perform and explain the first 10 types of tools on Kali Linux**

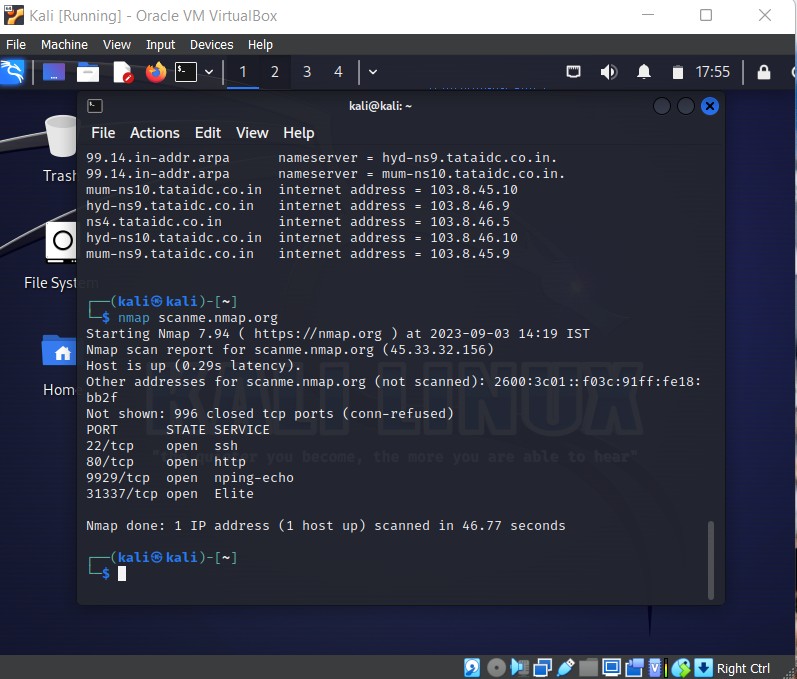
# Information gathering applications

**Nmap** is a network scanner that can be used to discover hosts and services on a network.

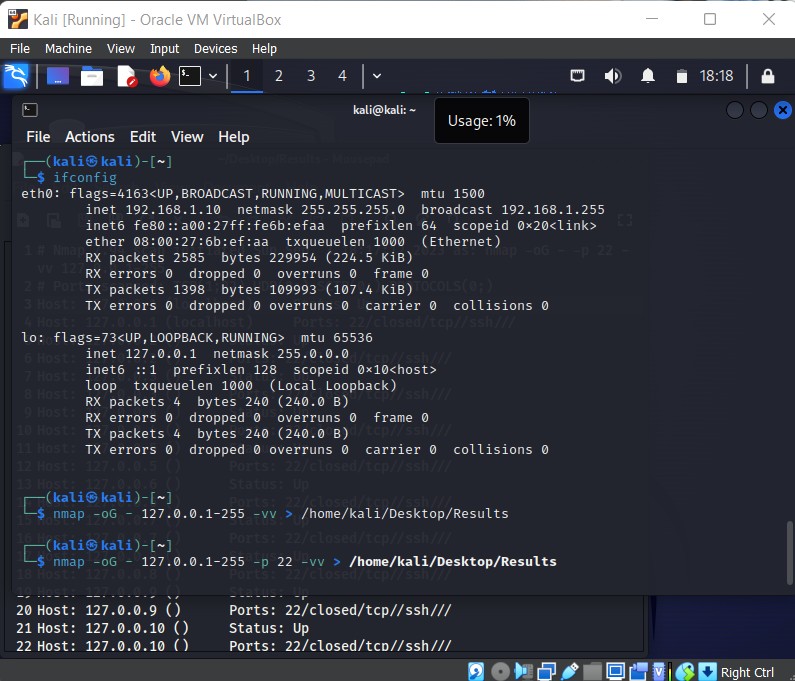
Performing the nslookup command on an ip found on nirsoft

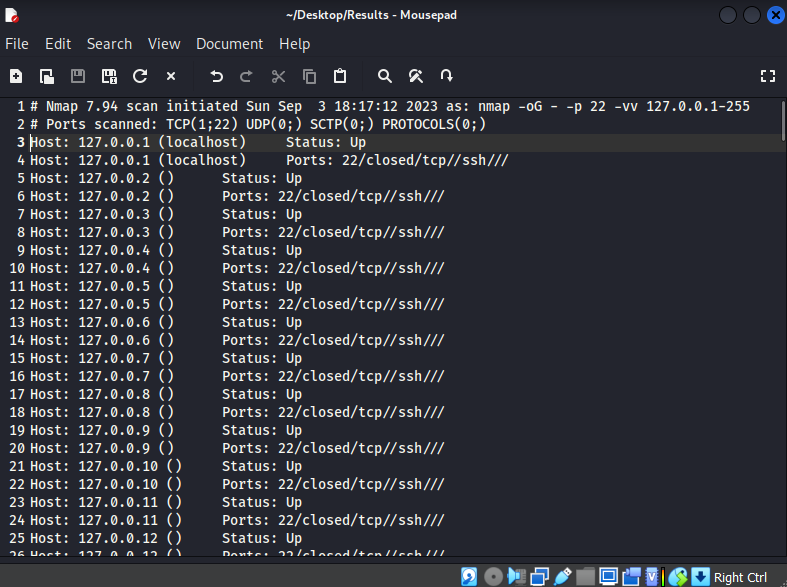


Scanning the website [scanme.nmap.org](http://scanme.nmap.org/), it will also give us the latency and the ports

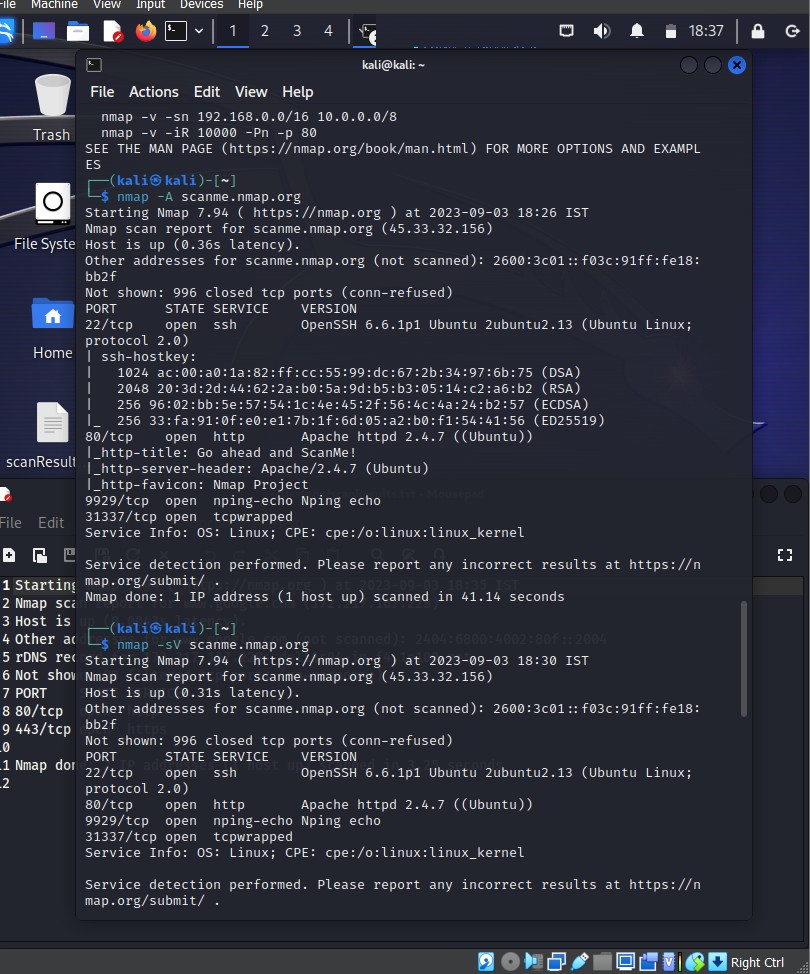


Now we are getting the network ip configuration using ifconfig and then using that we found out all the ports available on the ip, then we targeted a specific port and saved all the info on a file “results”

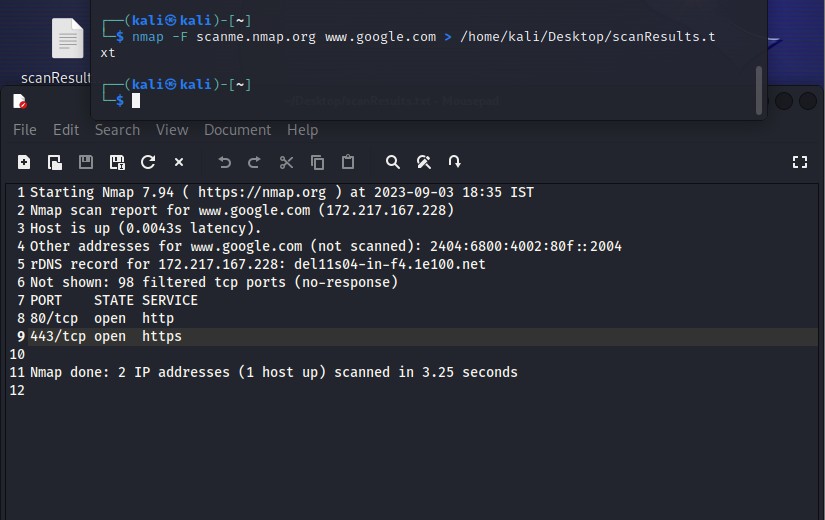




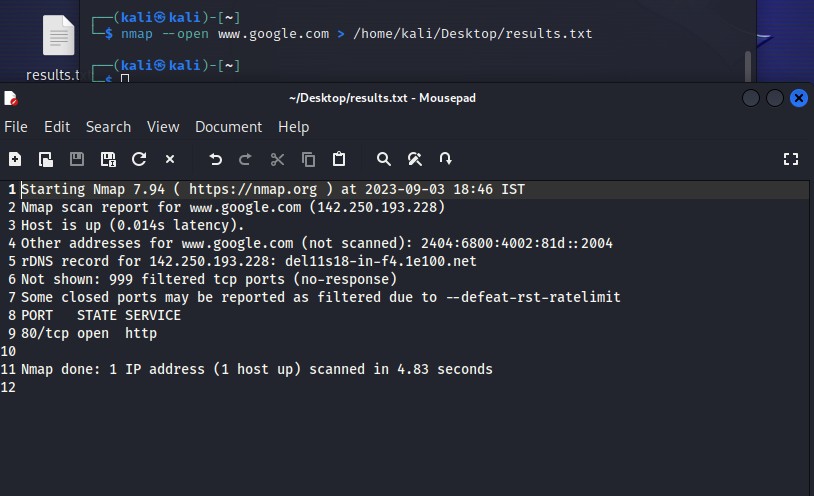
Then we can also perform aggresive searches using -A, we can also scan for versions on open services using -sV only:



We can also fast search for the open ports only, in this it only scans 100 ports not 1000, we use the -F command. Results are stored in a file called “scanResults”:



We can also just scan for open ports and filter all the other ports using —open:



**TheHarvester** is a tool that can be used to collect information about email addresses, social media profiles, and other online accounts.

**WhatWeb** is a tool that can be used to identify the technologies used on a website.

**SpiderFoot** is a tool that can be used to collect information about a target from a variety of

sources, including social media, public records, and WHOIS databases.

# Web Application Analysis

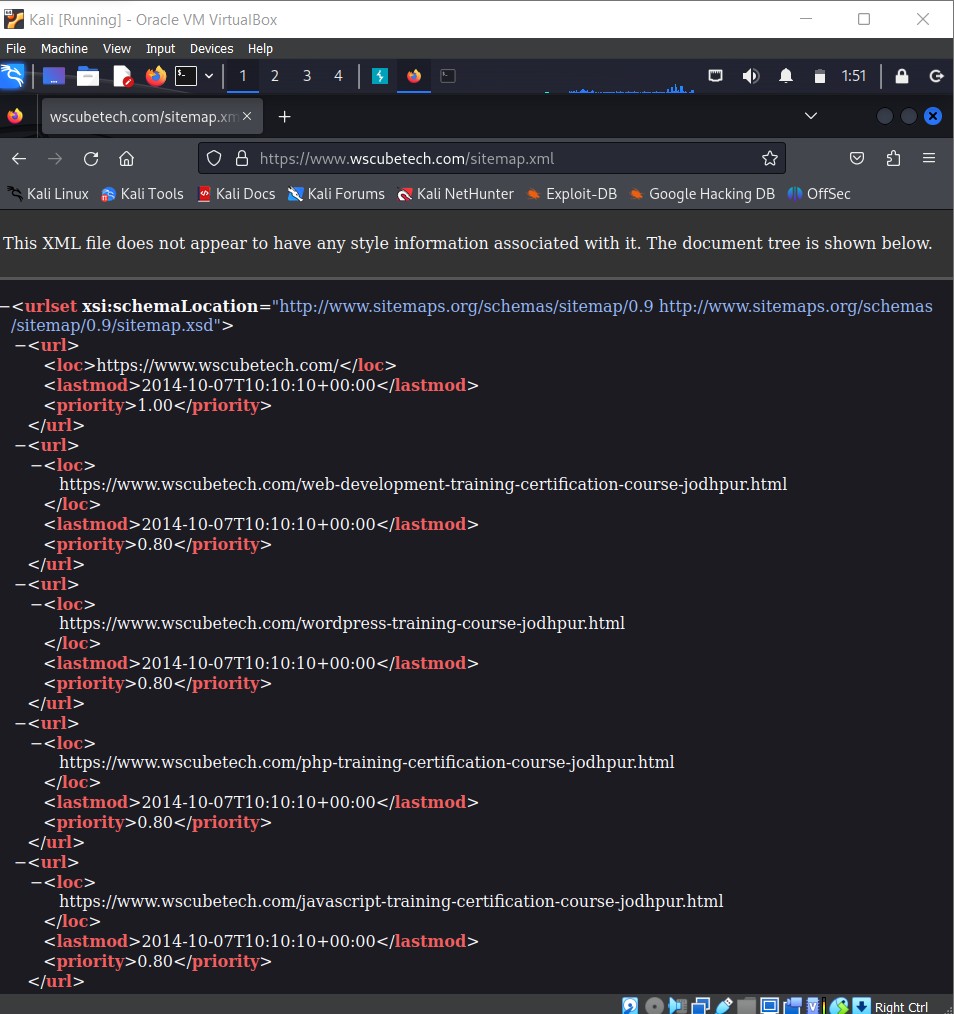
**Nikto** is a web scanner that can be used to identify vulnerabilities in web applications.

**Wapiti** is another web scanner that is similar to Nikto.

**Burp Suite** is a comprehensive web application security testing suite that includes a variety of tools for scanning, fuzzing, and exploiting vulnerabilities.

In this first we change the kali browser proxy to the burp proxy so that the burp can get the information about the sites we are visiting.

We can access the sitemap which is public if it has any of the private domain information or try to access Robot.txt file which contains all the domains that the developer don’t want the public to know.



Now we can find all the information in the proxy of the Burp Suite from the requests in the browser:

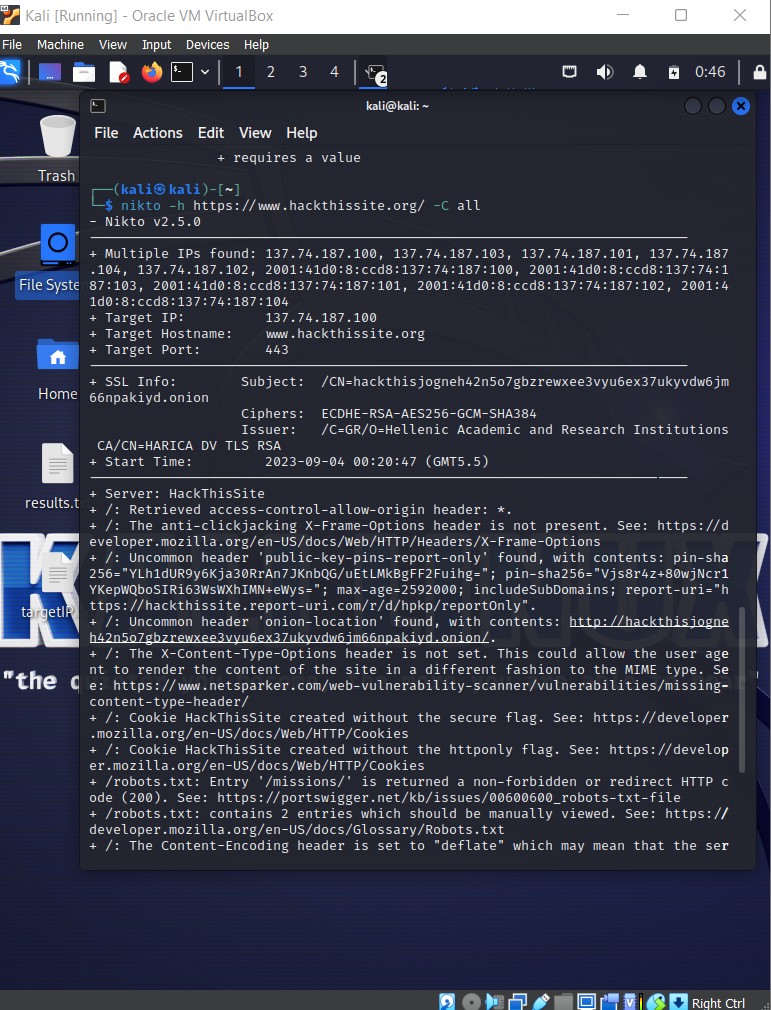


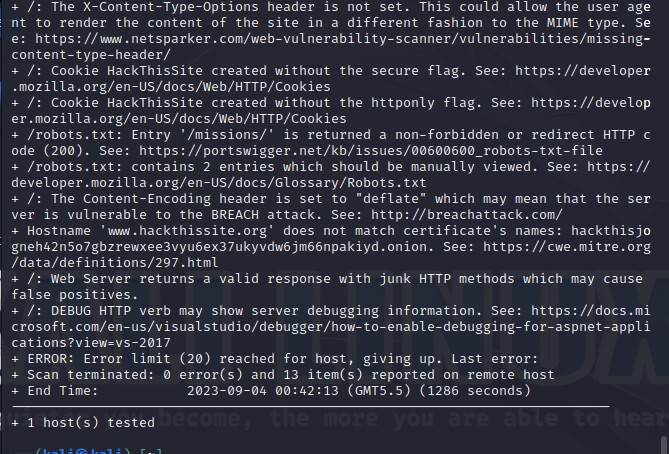
# Vulnerability analysis applications

**Metasploit Framework** is a penetration testing framework that includes a variety of tools for exploiting vulnerabilities.

**Nikto:** Nikto is a web scanner that can be used to identify vulnerabilities in web applications. It is a free and open-source tool that is available for Windows, macOS, and Linux. Nikto can be used to scan for a variety of vulnerabilities, including outdated software, misconfigurations, dangerous files, server-side include vulnerabilities, cross- site scripting vulnerabilities and SQL injection vulnerabilities.

We are finding vulnerabilities in [https://www.hackthissite.org/](http://www.hackthissite.org/)





From this output we can see various vulnerabilities that might be exploitable:

**The anti-clickjacking X-Frame-Options header is not present.** This means that the website is vulnerable to clickjacking attacks,

which can be used to trick the user into clicking on a malicious link.

**The X-Content-Type-Options header is not set.** This means that the website is vulnerable to content-type sniffing

attacks, which can be used to inject malicious content into the website.

**Cookie HackThisSite created without the httponly flag.** This means that the cookie can be accessed by JavaScript, which could allow an attacker to steal it.

**Cookie HackThisSite created without the secure flag.** This means that the cookie can be sent over an unencrypted connection, which could allow an attacker to steal it.

**Entry '/missions/' is returned a non-forbidden or redirect HTTP code (200).** This means that the robots.txt file is not being enforced, which could allow an attacker to access sensitive pages.

**The Content-Encoding header is set to "deflate" which may mean that the server is vulnerable to the BREACH attack.** This attack can be used to steal cookies and other sensitive information.

**contains 2 entries which should be manually viewed.** This means that there are two entries in the robots.txt file that

should be reviewed to make sure they are not allowing unauthorized access to the website.

# Hostname 'www.hackthissite.org' does not match certificate's names: hackthisjogneh42n5o7gbzrewxee3vyu6ex37ukyvdw6jm66npakiyd.onion.

This means that the website is using a certificate that is not valid

for the domain name. This could be a sign of a man-in-the-middle attack.

**DEBUG HTTP verb may show server debugging information.** This means that the website is returning debugging information to

users. This information could be used by an attacker to exploit the website.

# Web Server returns a valid response with junk HTTP methods which

**may cause false positives.** This means that the website is returning a valid response to HTTP

methods that it should not be responding to. This could be a sign of a vulnerability.

**Vega** is a graphical vulnerability scanner that is easy to use.

**Nessus** is a vulnerability scanner that can be used to identify vulnerabilities in a variety of systems and applications.

**OpenVAS** is another vulnerability scanner that is similar to Nessus.

# Database Assessment applications

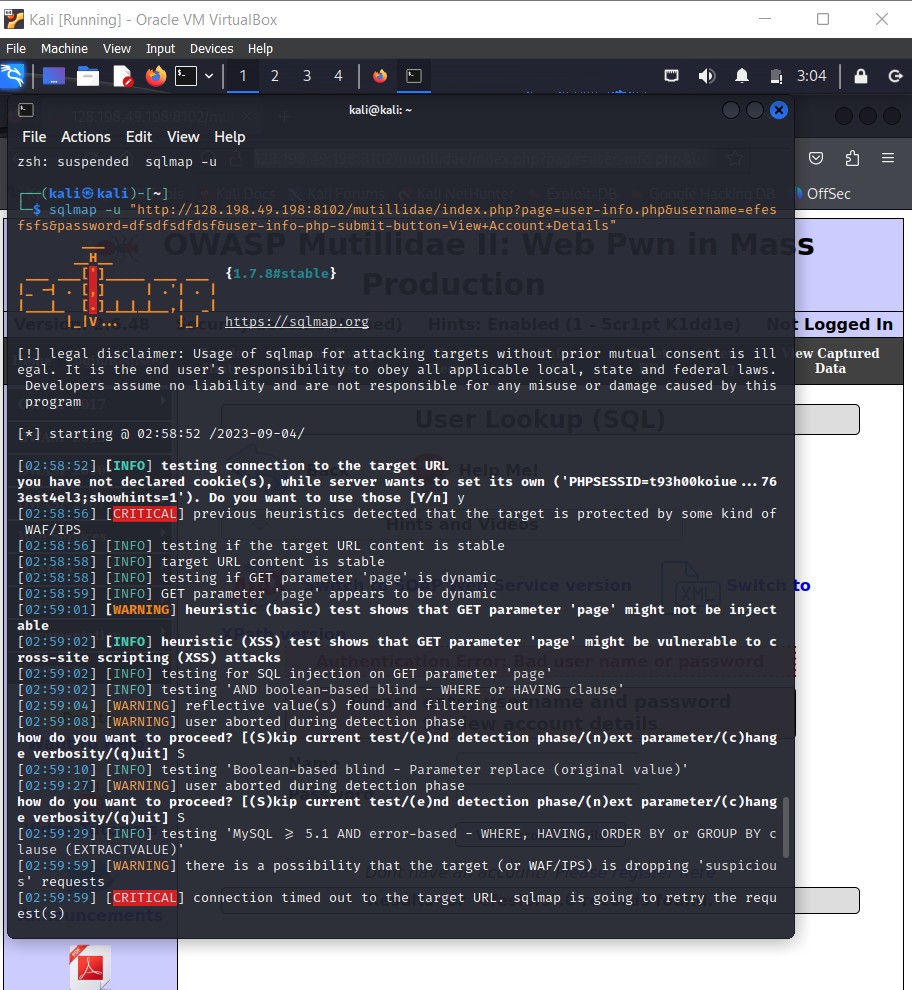
**SQLMap** is a tool that can be used to automate the process of identifying and exploiting SQL injection vulnerabilities.

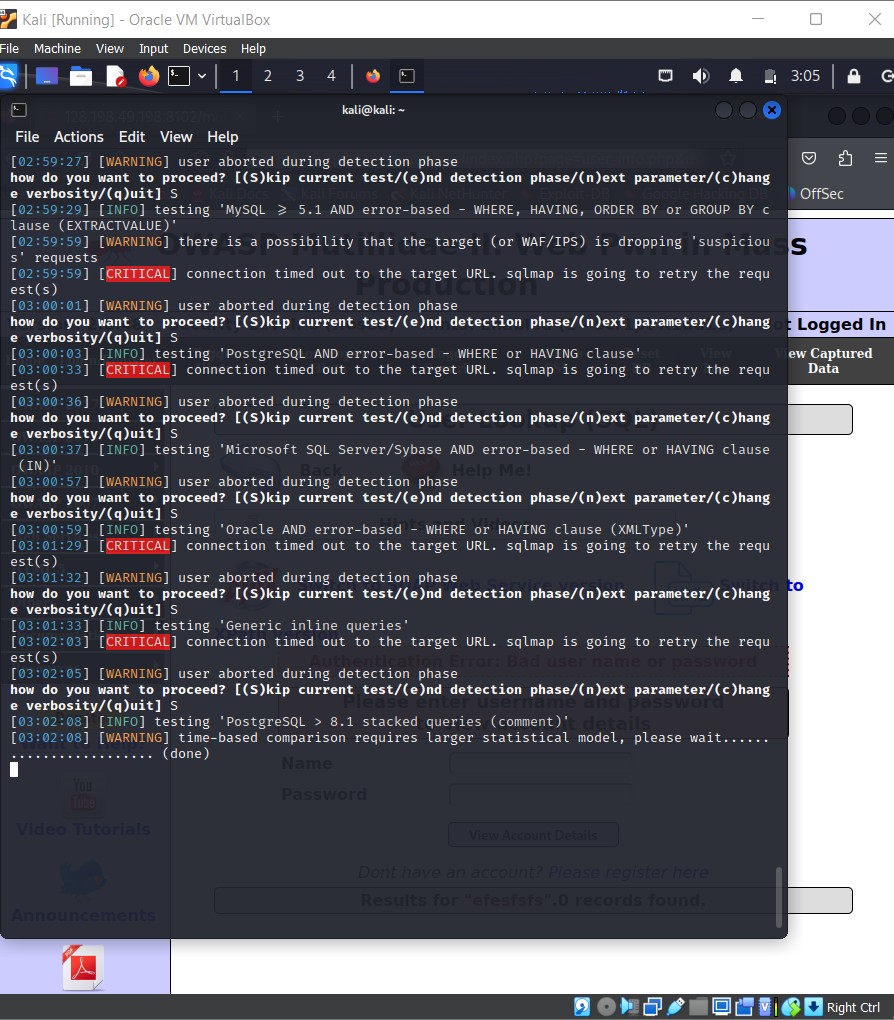
A simple test to check whether your website is vulnerable would be to replace the value in the get request parameter with an asterisk (\*).

Here we are going to do the sql injection on “http://128.198.49.198:8102/mutillidae/index.php?page=user-

info.php&username=efesfsfs&password=dfsdfsdfdsf&user-info-php-submit- button=View+Account+Details”

Now we will use the sqlmap -u command to perform SQL injection:





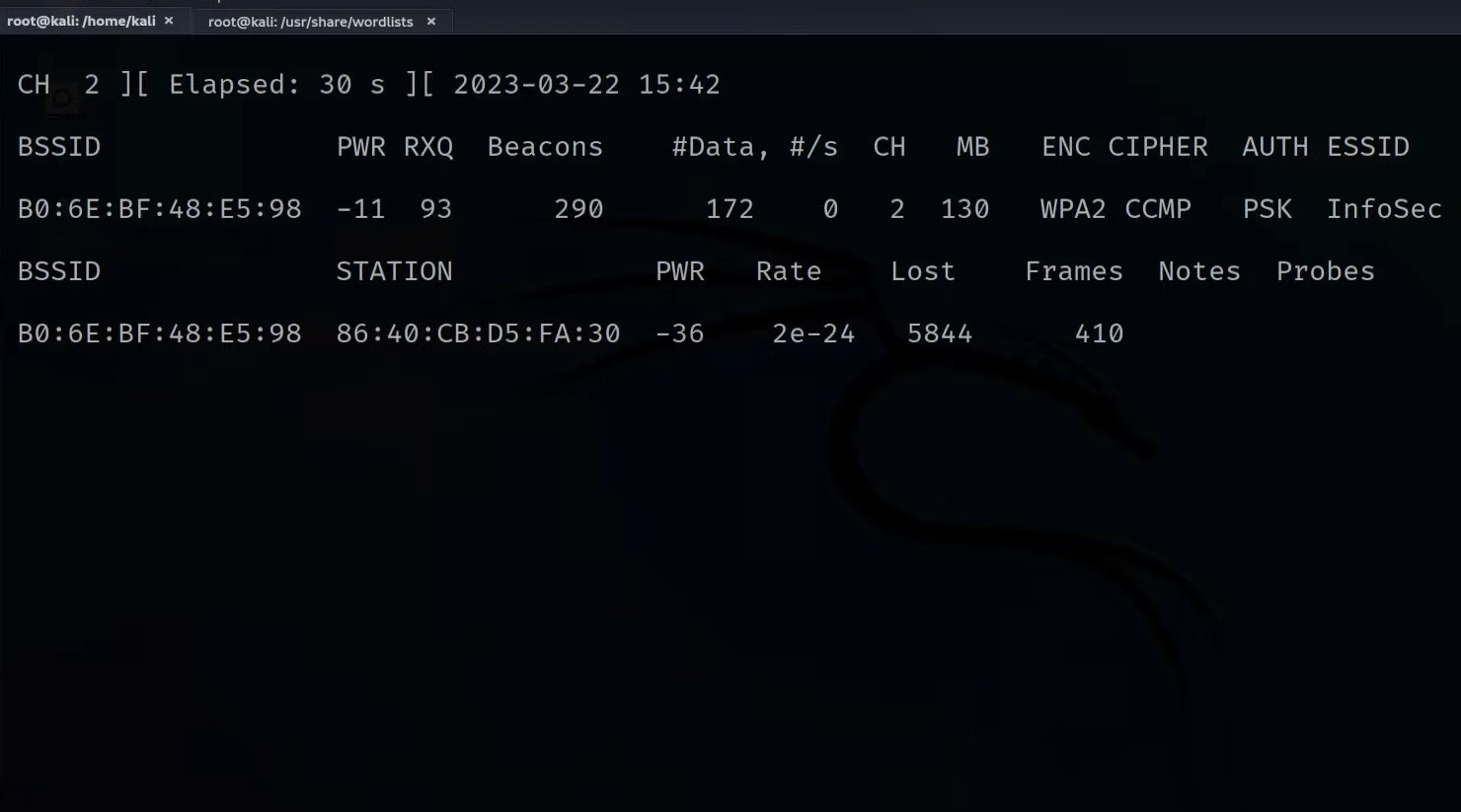
**SQLite Data Browser** is a database assessment tool that can be used to view and edit SQLite databases. It is a graphical user interface (GUI) tool that is easy to use, even for users who are not familiar with SQLite.

# Wireless Attacks

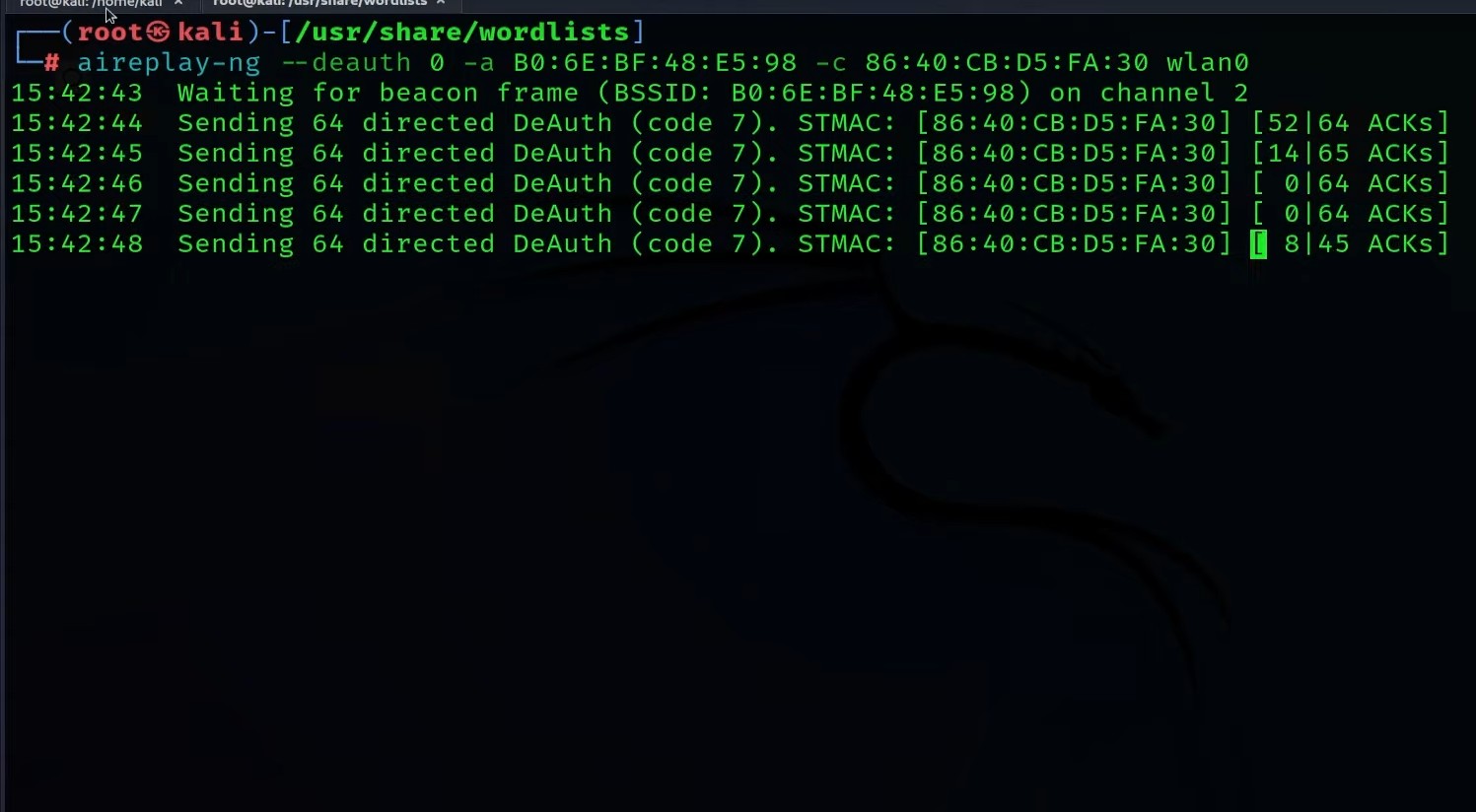
**Aircrack-ng** is a suite of tools that can be used to crack wireless passwords.

**Kismet** is a tool that can be used to sniff wireless traffic and identify vulnerable networks.

Monitoring devices:



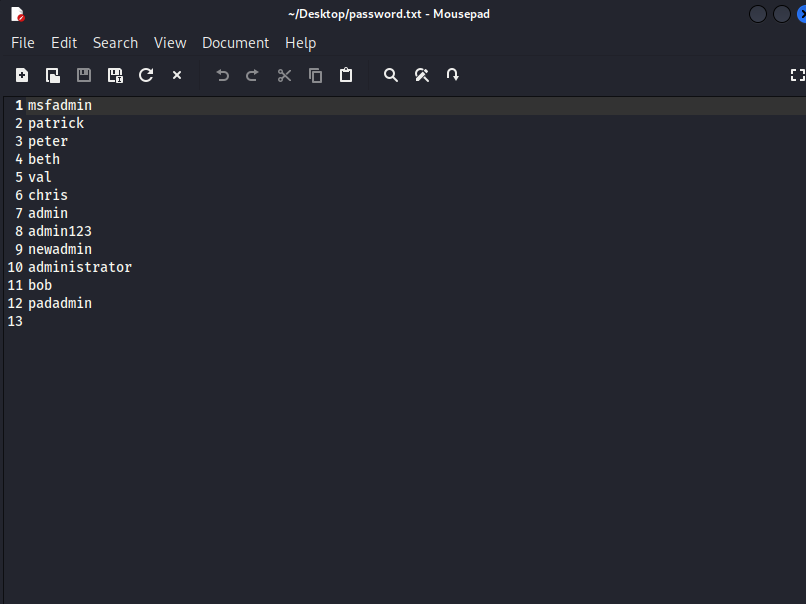
Deauthentication attacks can be done now based on the acquired information:



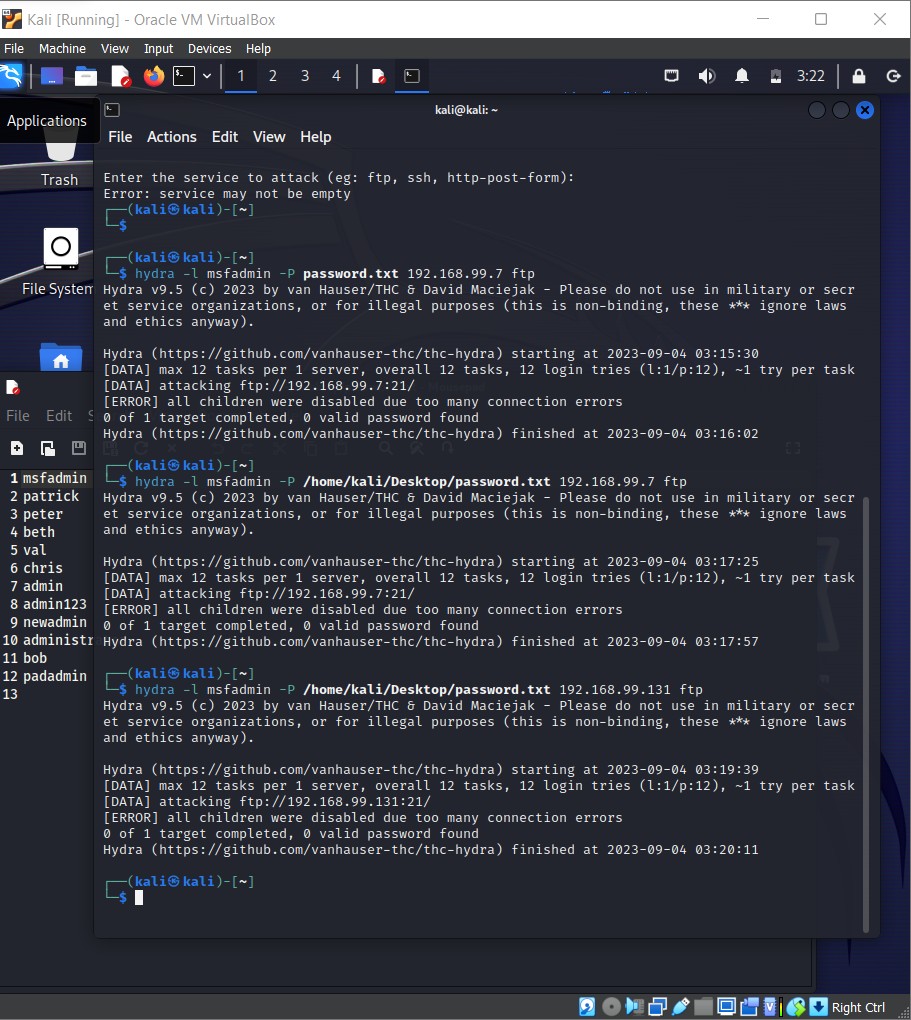
# Password Attacks

**Hydra** is a tool that can be used to perform brute-force password attacks against a variety of protocols, including HTTP, FTP, SSH, and Telnet. It can be used to crack passwords by trying a large number of possible passwords until it finds one that works.

First we created a password text file in which we got all the possible passwords



Now we will proceed using the brute force approach:



**Hashcat** is another password cracking tool that is similar to John the Ripper.

**Aircrack-ng** is a suite of tools that can be used to crack wireless passwords.

# Reverse Engineering applications

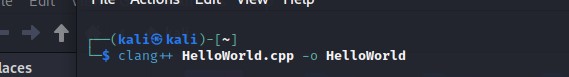
**Clang** can be used for reverse engineering in Kali Linux by decompiling binaries into their source code. This can be useful for understanding how a program works or for finding vulnerabilities.

Once **clang++** is installed, you can use it to compile C++ code.

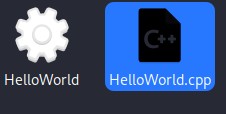
Here we have written a simple C++ code for printing hello world:



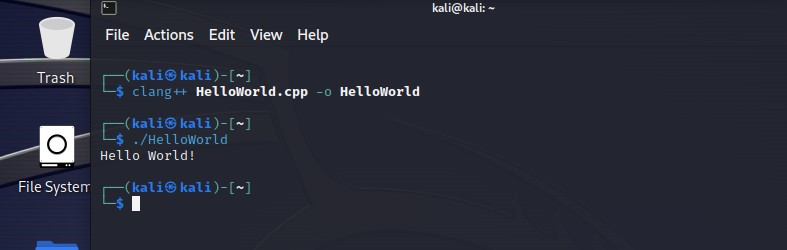
Then we will compile this C++ program using clang++:



After the command, we get the compiled C++ in the directory:



To get the output of the code, we can get the output in the terminal:

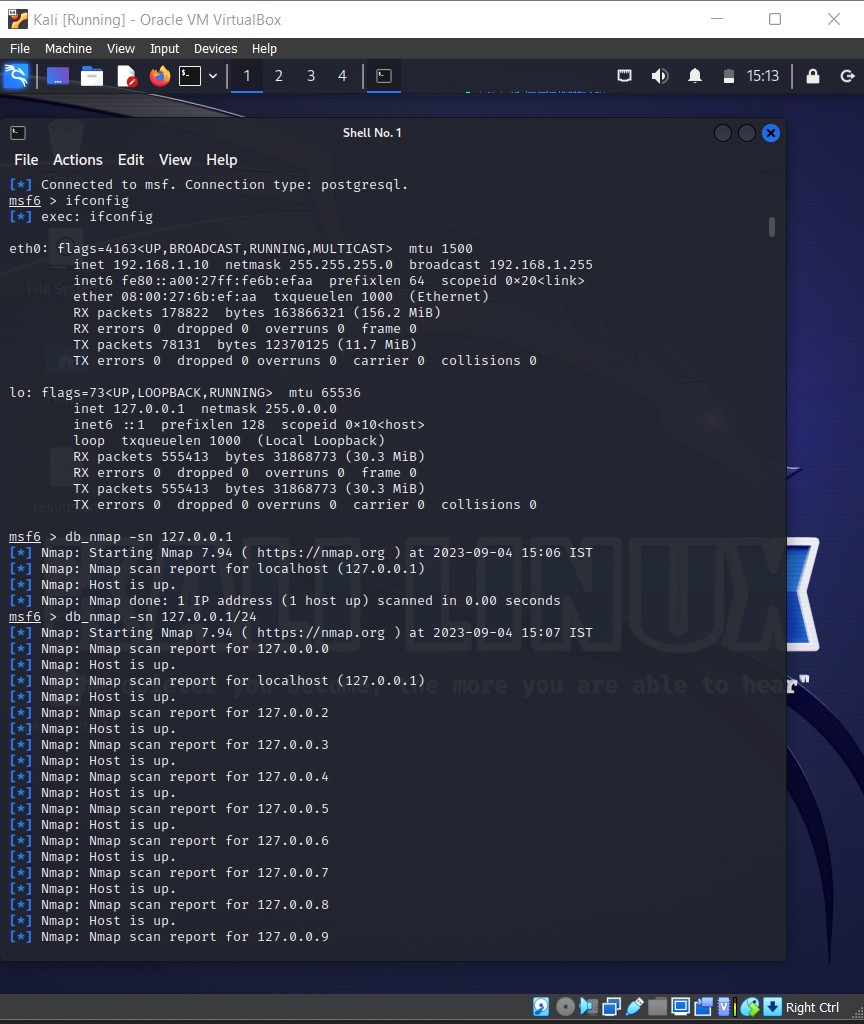


**Radare2** is a free and open-source reverse engineering framework. It can be used to disassemble, debug, analyze, patch, and manipulate binaries. This can be useful for understanding how a program works or for finding vulnerabilities.

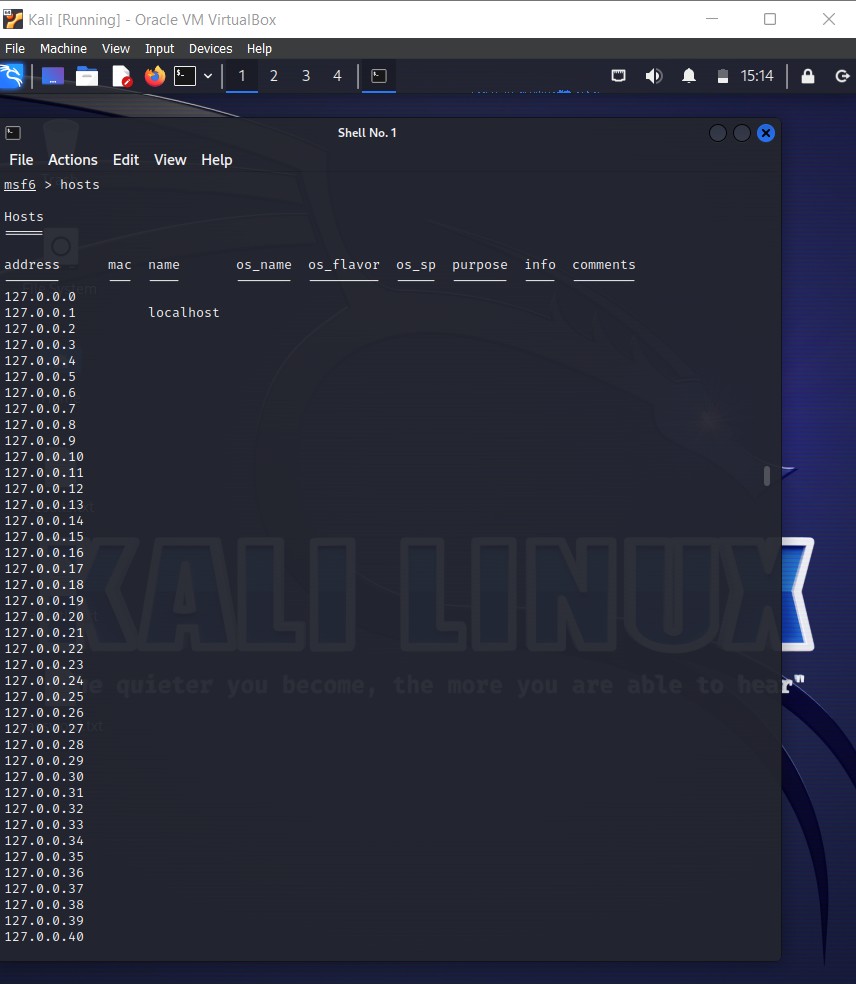
# Exploitation Tools

**Metasploit Framework** is a penetration testing framework that includes a variety of tools for exploiting vulnerabilities.

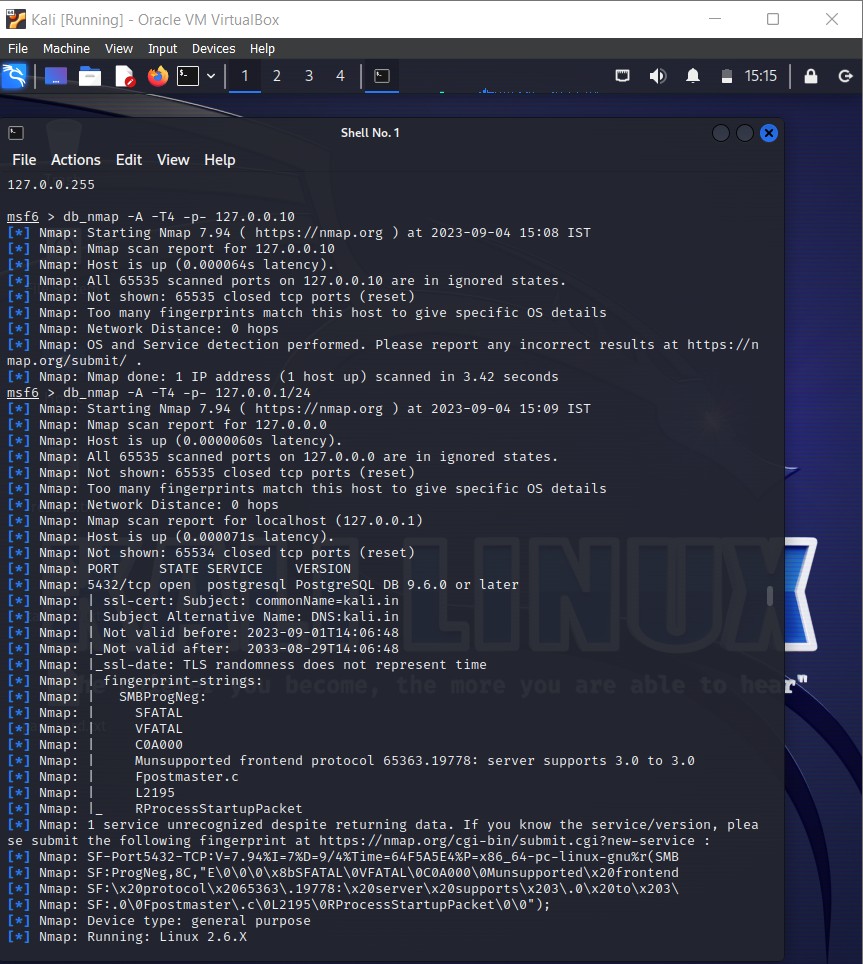
We can use various tools here. Here we are using nmap to get all the ports on our ip:



We can then get the hosts on our ip:



Scanning the 127.0.0.1/24 Subnet using db\_nmap:



The scan results show that all 25 hosts in the subnet are up. However, the OS and version information for most of the hosts could not be determined because there were too many matching fingerprints. This is likely because the hosts are running common operating systems, such as Linux or Windows.

The only host for which the OS and version information could be determined is the localhost (127.0.0.1). This host is running Linux 2.6.32, which is a relatively old version of Linux.

The scan also found that the localhost is running a PostgreSQL database server on port 5432. This is a popular open-source database that is used for a variety of applications.

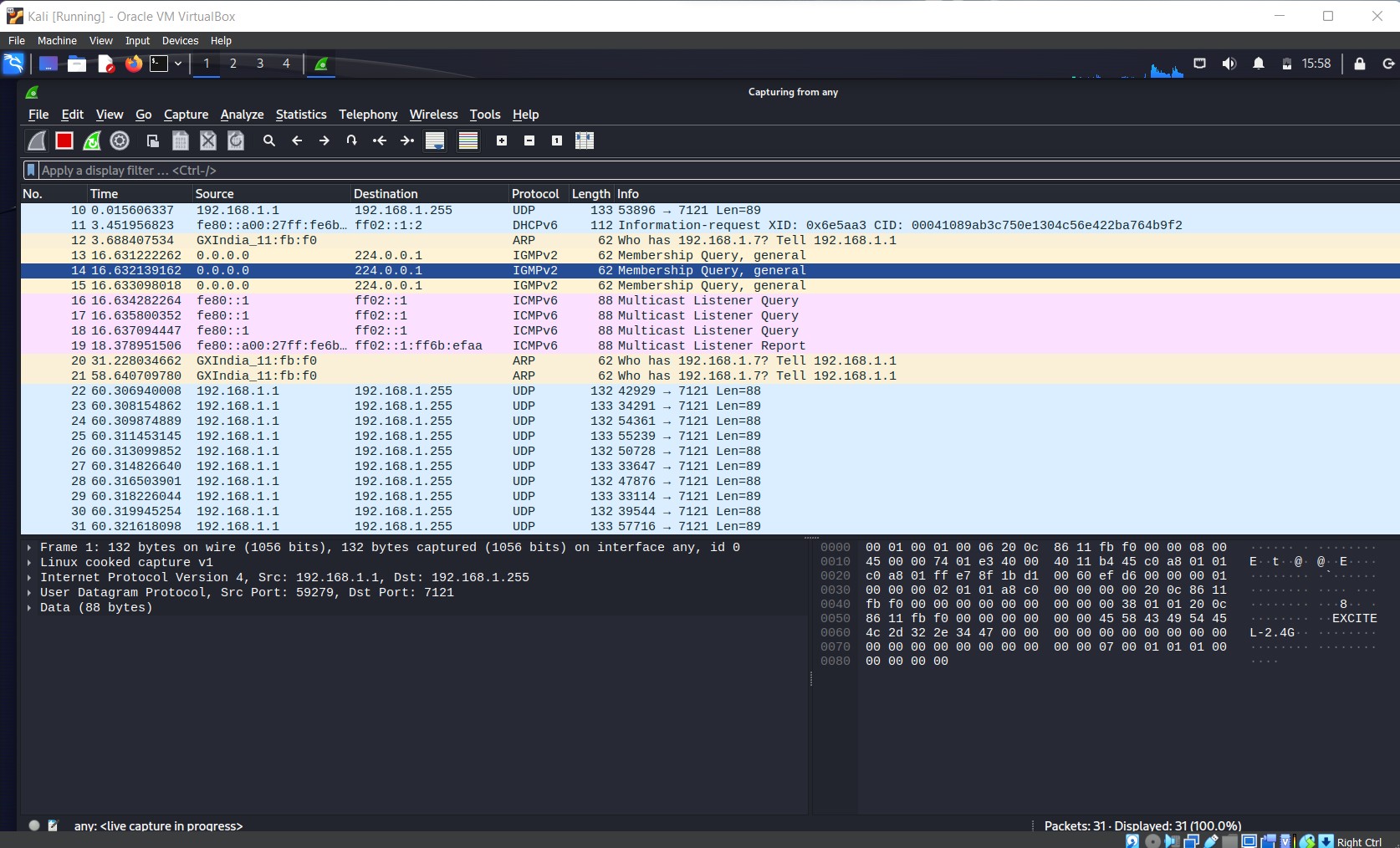
**Nessus** is a vulnerability scanner that can also be used to exploit vulnerabilities.

**OpenVAS** is another vulnerability scanner that can be used to exploit vulnerabilities.

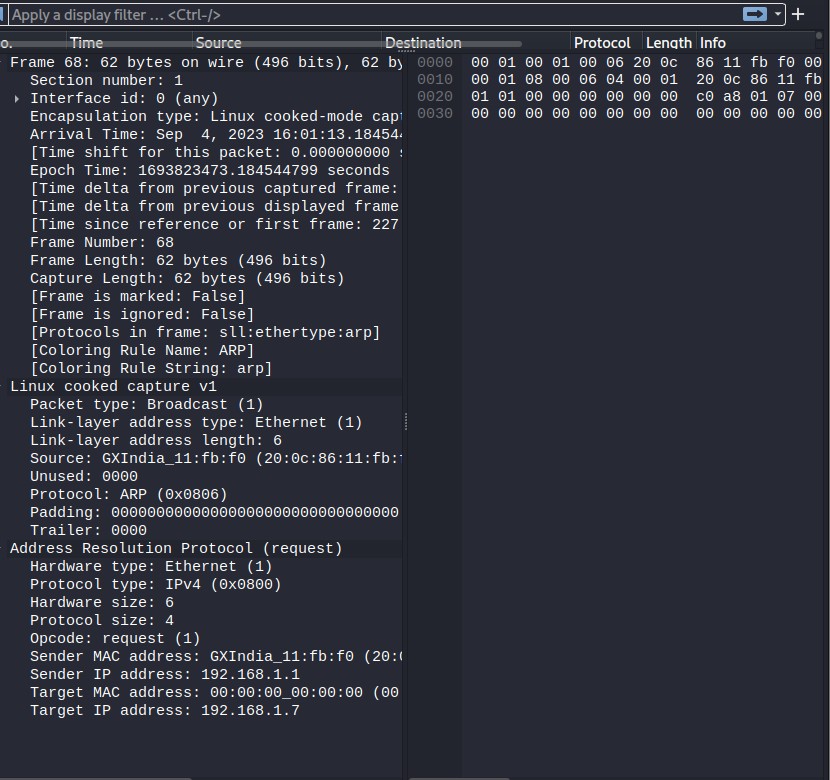
# Sniffing and spoofing

**Wireshark** is a network packet analyzer that can be used to sniff network traffic.

Here I have captured the information of the packets from my wi-fi:



We can get information of a particular packet by simply clicking on the targeted packet:



We can sniff packet and internet traffic using wireshark and initiate attacks like Man in the Middle attack (MITM).

**tcpdump** is a command-line packet analyzer that is similar to Wireshark.

**ettercap** is a tool that can be used to sniff network traffic and perform man-in-the- middle attacks.

# Post Exploitation applications

**Metasploit Framework** includes a variety of tools for post-exploitation, such as keyloggers, backdoors, and shells.

**Impacket** is a library of Python modules that can be used for post-exploitation tasks, such as gathering information about a system and executing commands

**Powershell Empire** is a post-exploitation framework that is based on PowerShell. PowerShell is a powerful scripting language that is commonly used by system administrators to automate tasks. This makes it a valuable tool for attackers, as it allows them to execute commands and scripts on compromised systems without having to know the underlying operating system.

PowerShell Empire includes a variety of modules that can be used to perform post- exploitation tasks. These modules include:

**File download/upload:** This module allows the attacker to download or upload files to the

compromised system. This can be used to steal data or install malware.

**Keylogger:** This module allows the attacker to record all keystrokes made on the compromised

system. This can be used to steal passwords and other sensitive information.

**Remote shell:** This module allows the attacker to create a remote shell on the compromised

system. This allows the attacker to interact with the system as if they were sitting at the keyboard.

**Webcam capture:** This module allows the attacker to capture images from the webcam on the

compromised system. This can be used to spy on the victim.