NAME :- M Om Nivas REG NO :- 21BCE9706

E-Mail :- omnivas.21bce9706@vitapstudent.ac.in

Ai For Cyber Security With Ibm Qrador

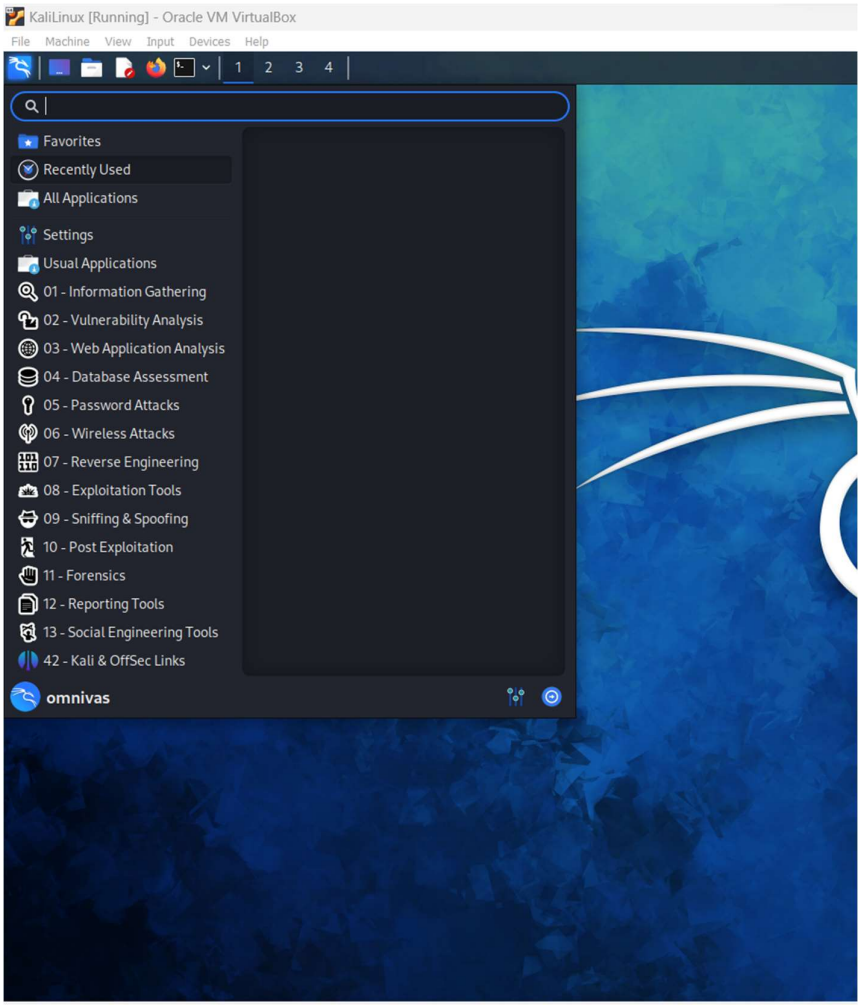
Weekly

Assignment – 2

Exploring Tools in Kali Linux :-

There are total 13 Default Applications in Kali Linux

There are some tools like NESSUS , NMAP , METASPLOIT , WIRESHARK , BURPSUITE, SQLMAP, JOHN THE RIPPER and CLANT.

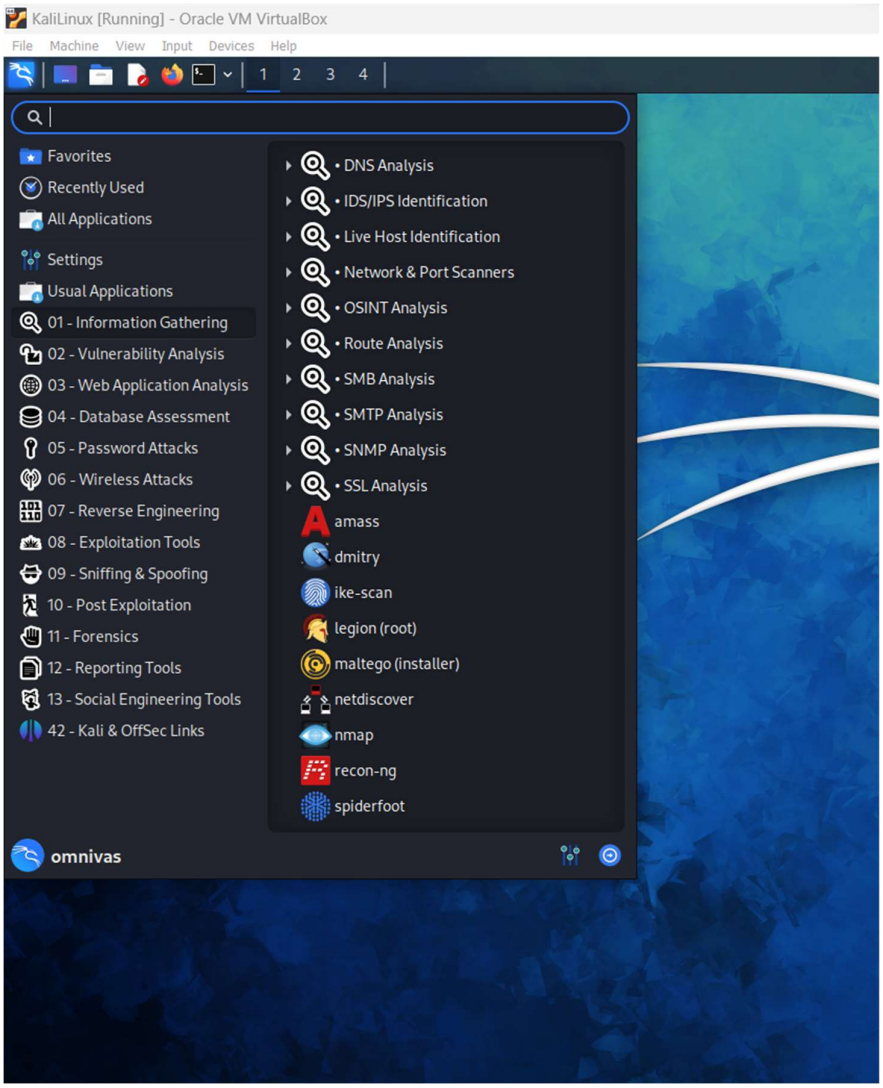


1- Information Gathering :-

In Information Gathering we have several tools like amass, Dmitry, ike-scan, legion, nmap (Network Scanner) etc.

NAMP :-

Nmap is a network scanner created by Gordon Lyon. Nmap is used to discover hosts and services on a computer network by sending packets and analyzing the responses. Nmap provides a number of features for probing computer networks, including host discovery and service and operating system detection.

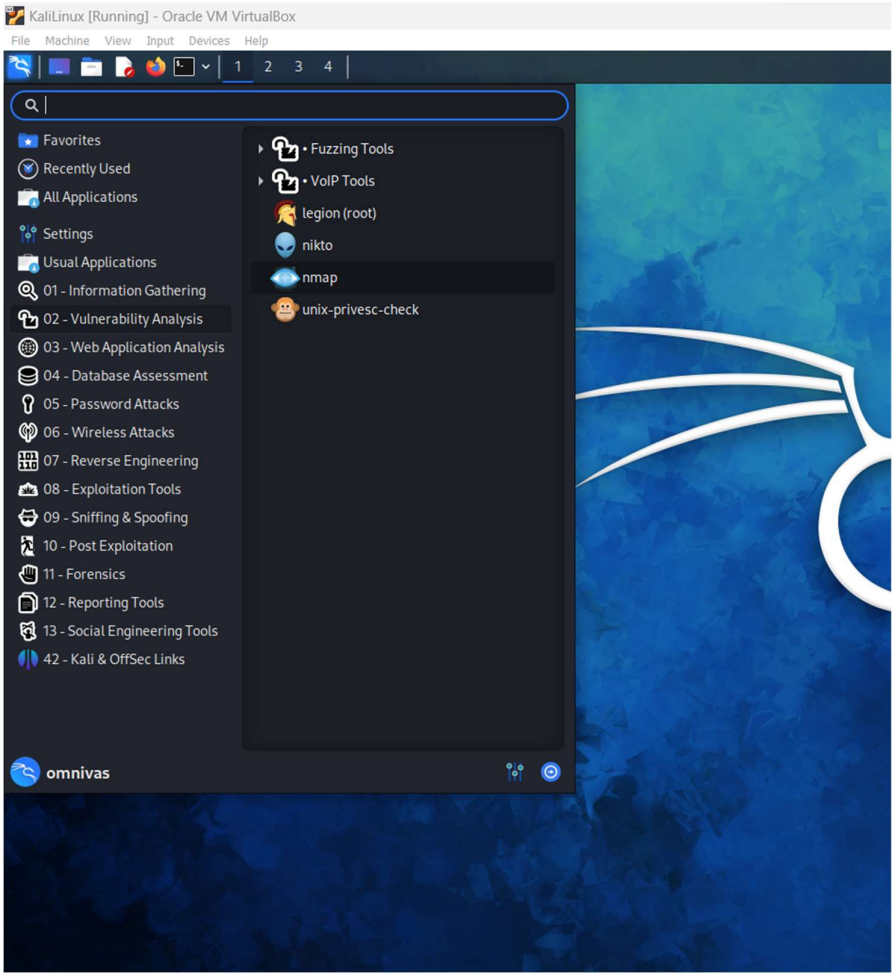


2- Vulnerability Analysis :-

In Vulnerability Analysis we have tools like legion(root), nikto, nmap, unix-privesc-check.

NIKTO :-

Nikto performs over 6000 tests against a website. The large number of tests for both security vulnerabilities and mis-configured web servers makes it a go to tool for many security professionals and systems administrators. It can find forgotten scripts and other hard to detect problems from an external perspective.

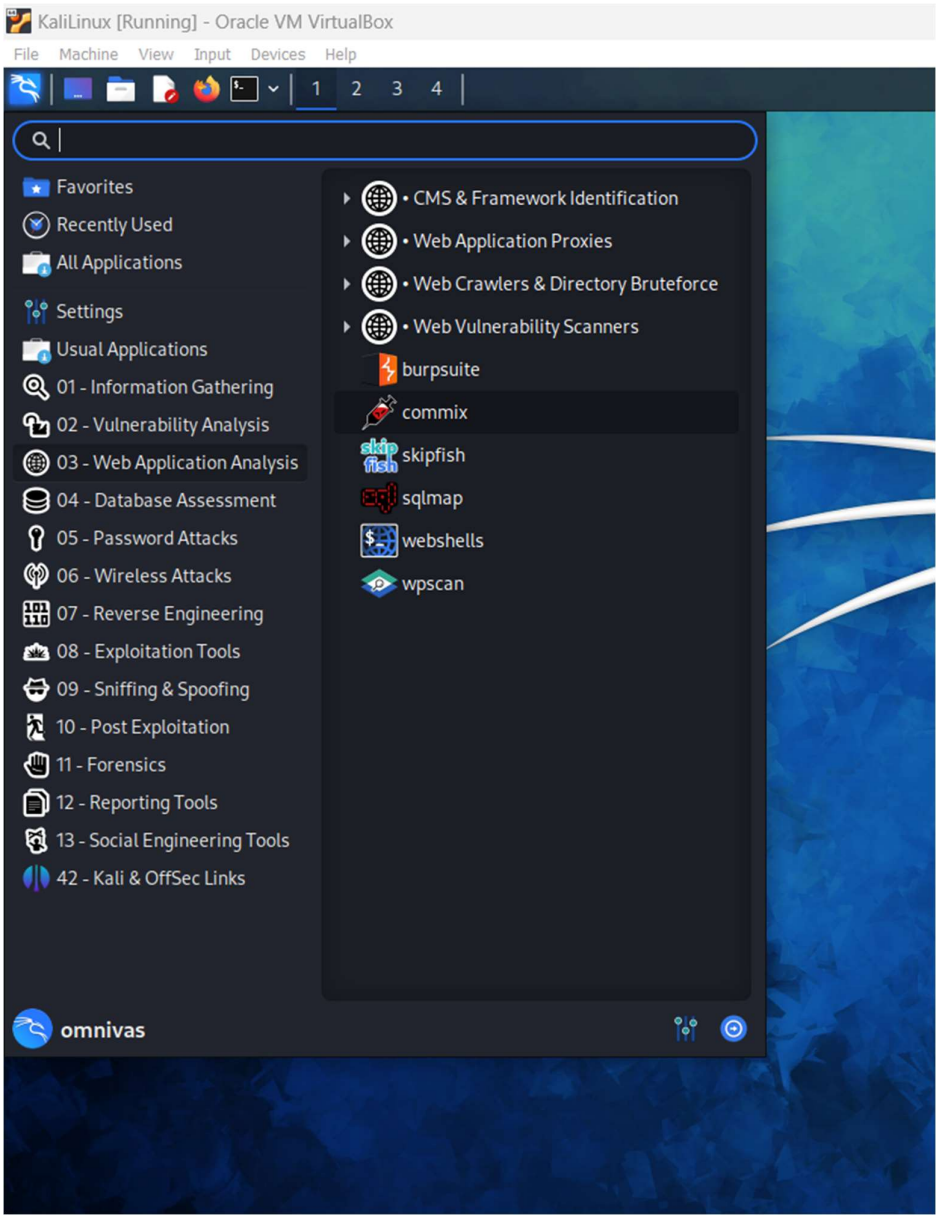


3-Web Application Analysis :-

In this we have tools like burpsuite, commix, skipfish, sqlmap, webshells and webscan.

BURP SUITE :-

Burp Suite is a software security application used for penetration testing of web applications. Both a free and a paid version of the software are available. The software is developed by the company PortSwigger.

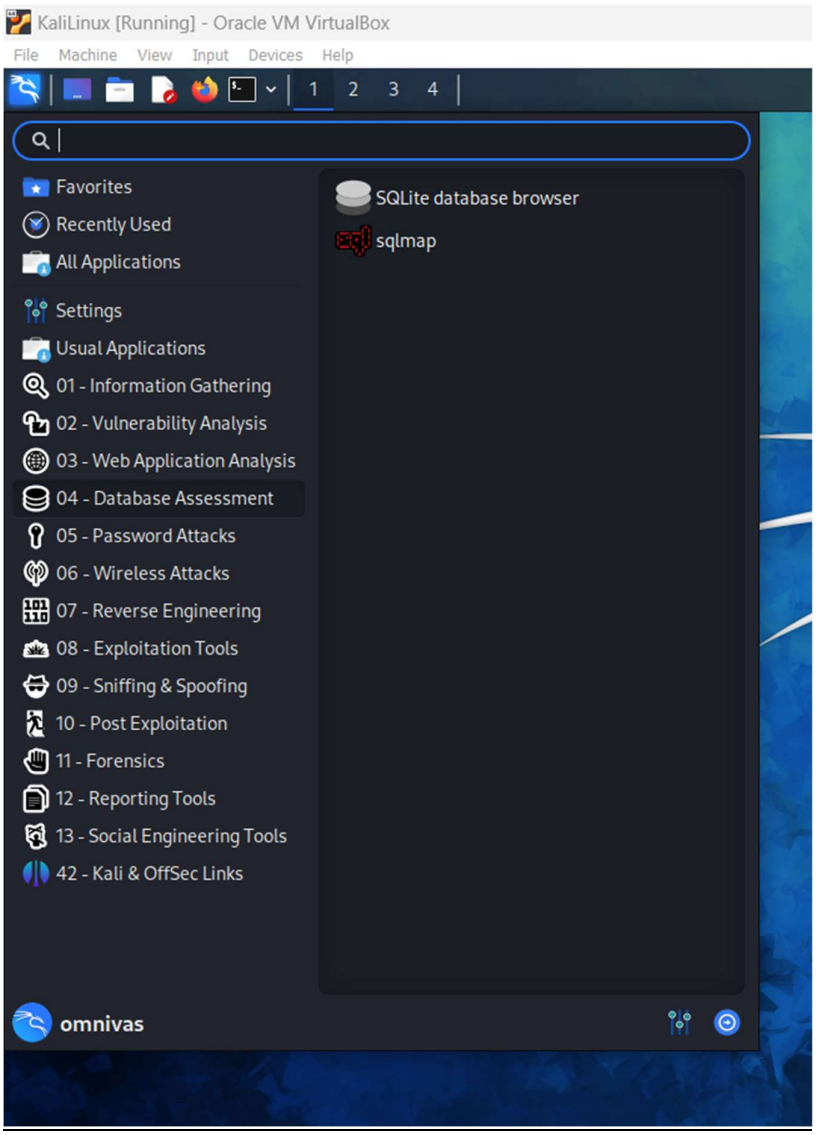


4-Database Assessment :-

In Database Assessment we have tools like sqlmap.

SQL MAP :-

sqlmap is an open source penetration testing tool that automates the process of detecting and exploiting SQL injection flaws and taking over of database servers. It comes with a powerful detection engine, many niche features for the ultimate penetration tester and a broad range of switches lasting from database fingerprinting, over data fetching from the database, to accessing the underlying file system and executing commands on the operating system via out-of-band connections.



5-Password Attacks :-

In Password Attacks we have tools like cewl, crunch, hashcat, hydra, john, medusa, ncrack, ophcrack and wordlists.

John The Ripper :-

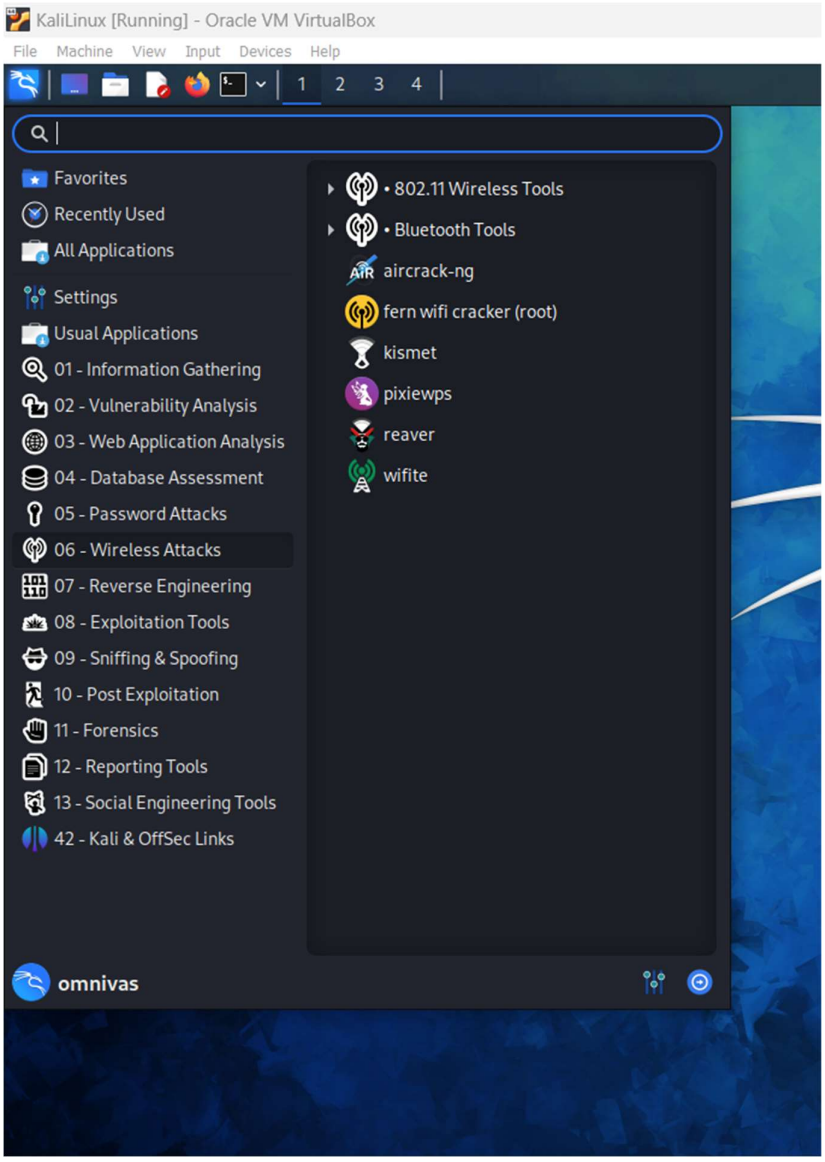
John the Ripper is a free password cracking software tool. Originally developed for the Unix operating system, it can run on fifteen different platforms.

6-Wireless Attacks :-

In Wireless Attacks we have tools like aircrack-ng, fern wifi cracker (root), kismet, pixiwps, reaver and wifite.

WIFITE :-

> Wifite is a tool to audit WEP or WPA encrypted wireless networks. It uses aircrack-ng, pyrit, reaver, tshark tools to perform the audit.
>
> This tool is customizable to be automated with only a few arguments and can be trusted to run without supervision.

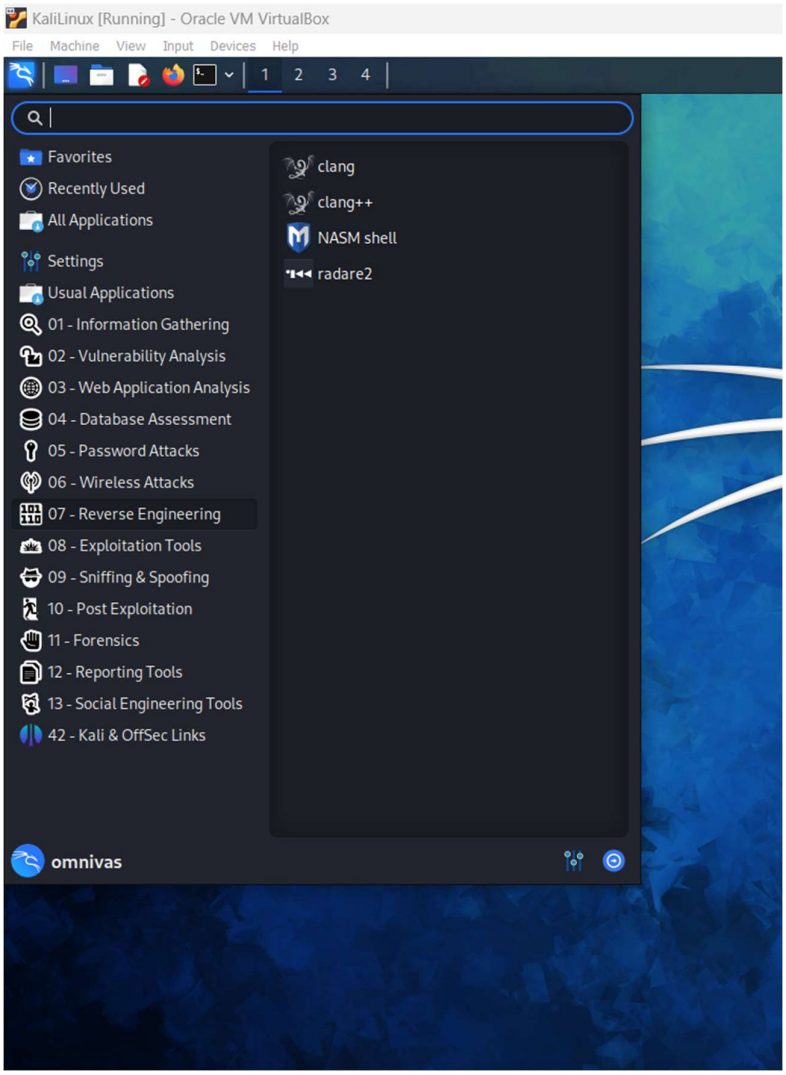


7-Reverse Engineering :-

in Reverse Engineering we have tools like clang, clang++, NASM shell and radre2.

CLANG :-

Clang is a compiler front end for the C, C++, Objective-C, and Objective-C++ programming languages, as well as the OpenMP, OpenCL, RenderScript, CUDA, SYCL, and HIP frameworks. It acts as a drop-in replacement for the GNU Compiler Collection, supporting most of its compilation flags and unofficial language extensions.



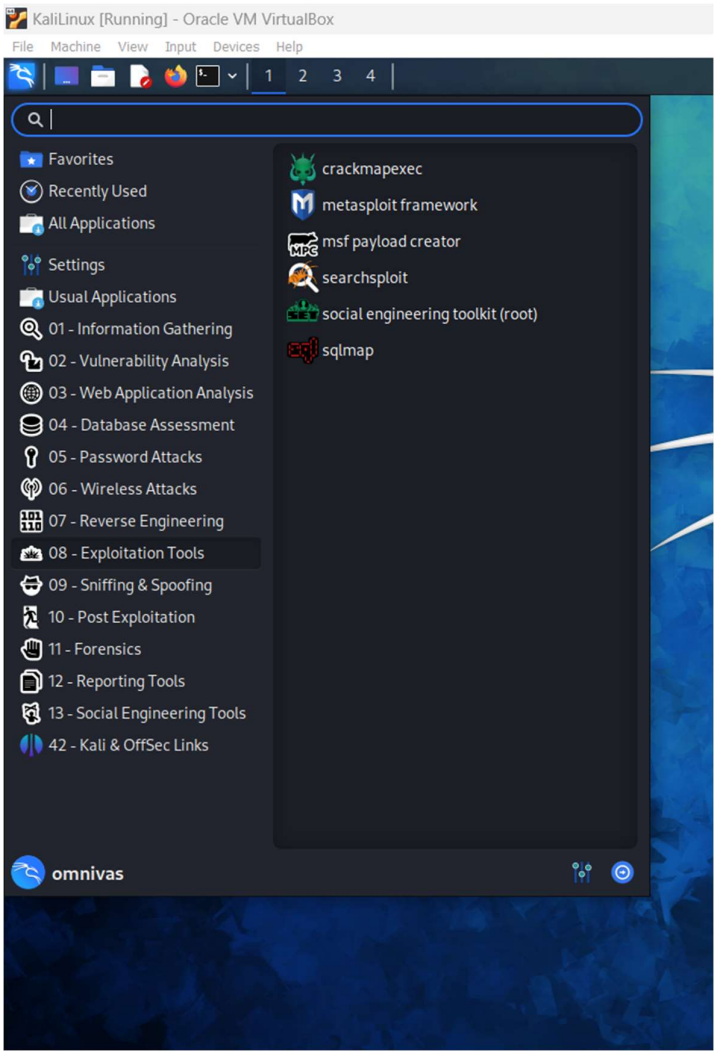
8-Exploitation Tools :-

In Exploitation Tools we have tools like crackmapexec, Metasploit framwork, msf payload creator, searchsploit, social engineering toolkit and sqlmap.

METASPLOIT FRAMEWORK :-

The Metasploit framework is a very powerful tool which can be used by cybercriminals as well as ethical hackers to probe systematic vulnerabilities on networks and servers. Because it's an open-source framework, it can be easily customized and used with most operating systems.

With Metasploit, the pen testing team can use ready-made or custom code and introduce it into a network to probe for weak spots. As another flavor of threat hunting, once flaws are identified and documented, the information can be used to address systemic weaknesses and prioritize solutions.

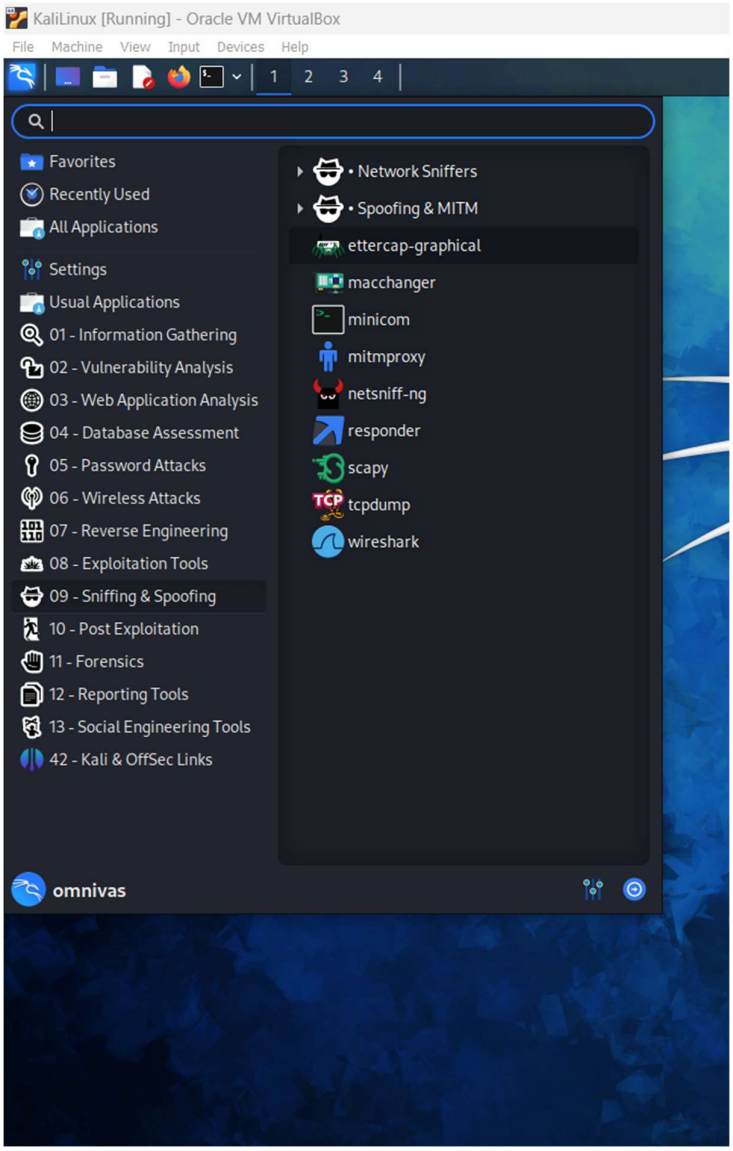


9-Sniffing & Spoofing :-

In Sniffing & Spoofing we have tools like Ettercap-graphical, macchanger, minicom, mitmproxy, netsniff-ng, responder, scapy, tcpdump and wireshark.

WIRESHARK :-

Wireshark is a free and open-source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education. Originally named Ethereal, the project was renamed Wireshark in May 2006 due to trademark issues.

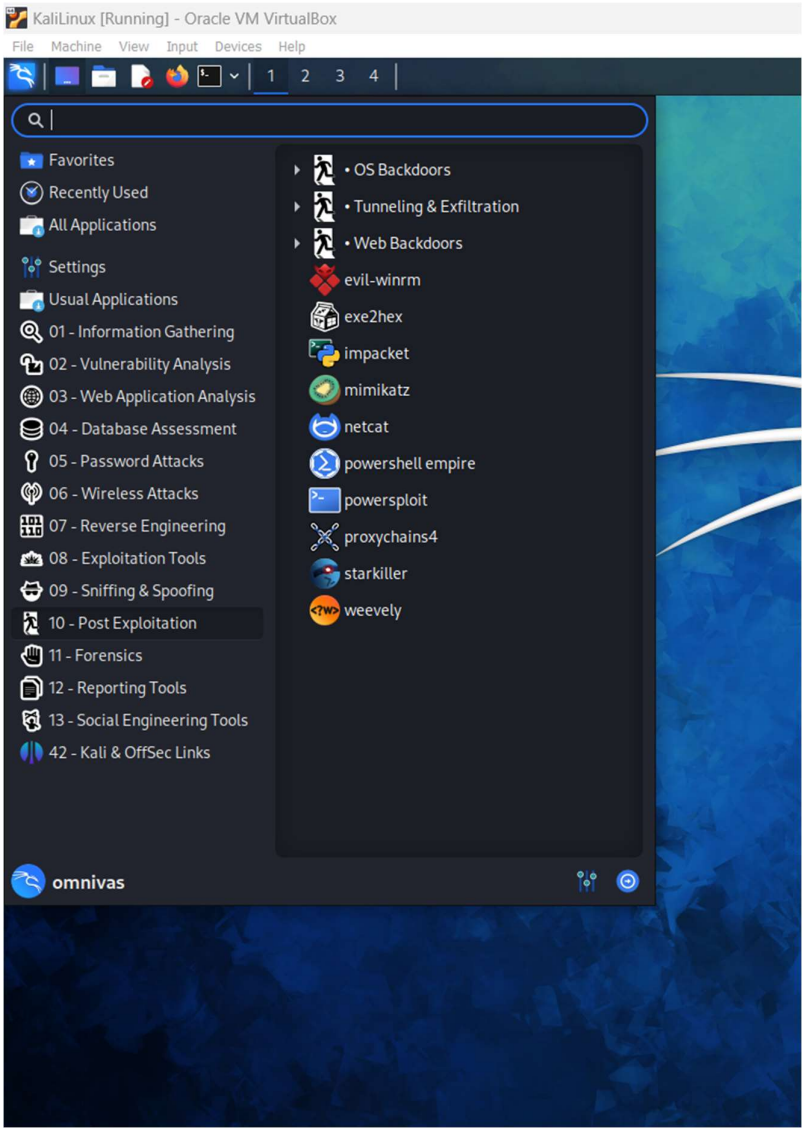


10-Post Exploitation :-

In Post Exploitation we have tools like evil-winrm, exe2hex, impacket, mimikatz, netcat, powershell empire and weevely.

NETCAT :-

Netcat or NC is a utility tool that uses TCP and UDP connections to read and write in a network. It can be used for both attacking and security. In the case of attacking. It helps us to debug the network along with investigating it. It runs on all operating systems.

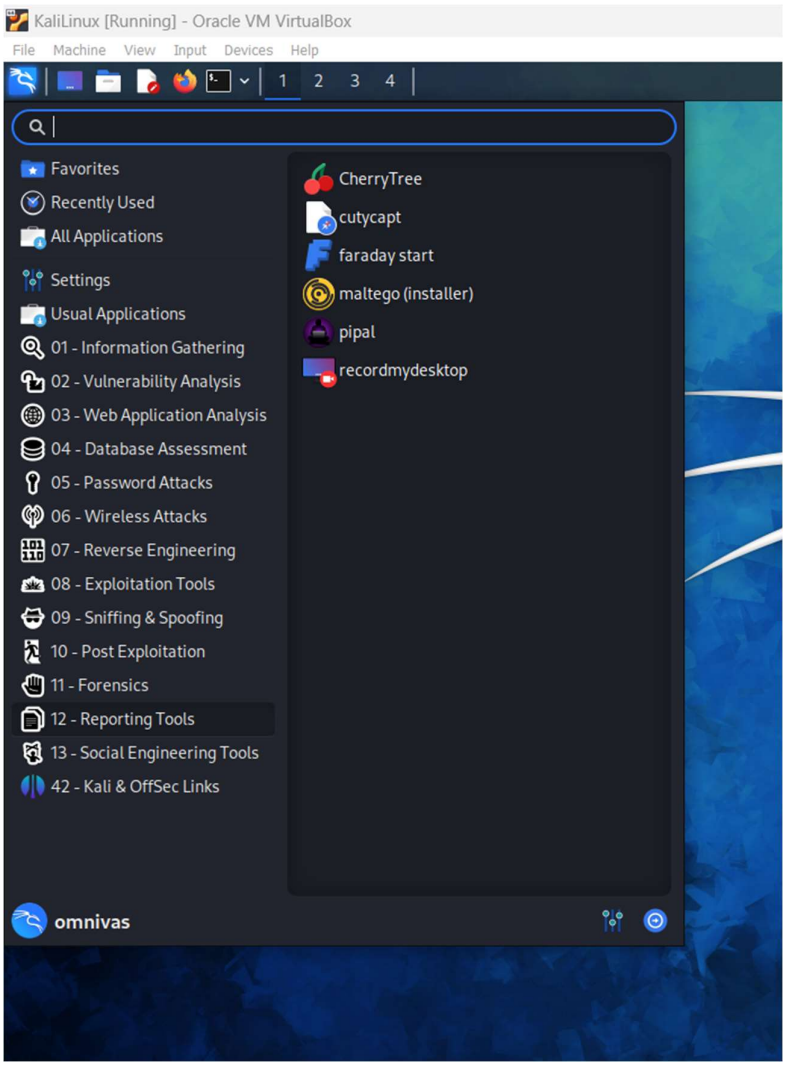


11-Forensics :-

In Forensics we have tools like autopsy, binwalk, bulk_extractor and hashdeep.

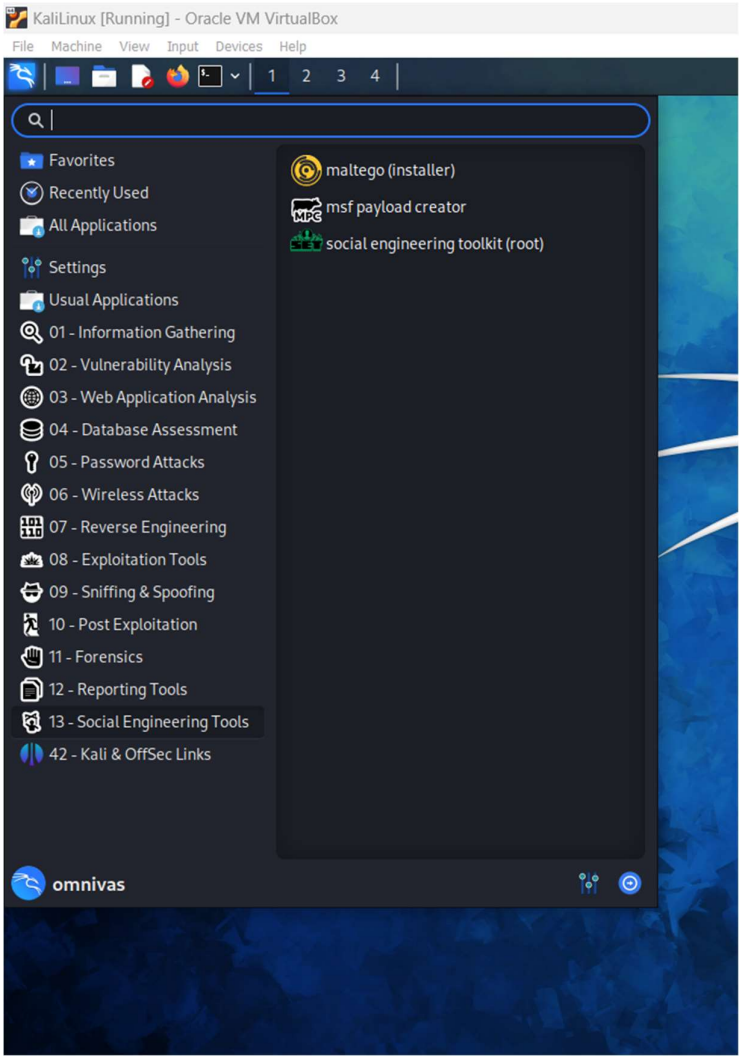
12-Reporting Tools :-

In Reporting Tools we have tools like cherry Tree, cutycapt, faraday start, maltego and pipal.



13-Social Engineering Tools :-

In Social Engineering Tools we have like maltego, msf payload creator and Social Engineering Toolkit.



END