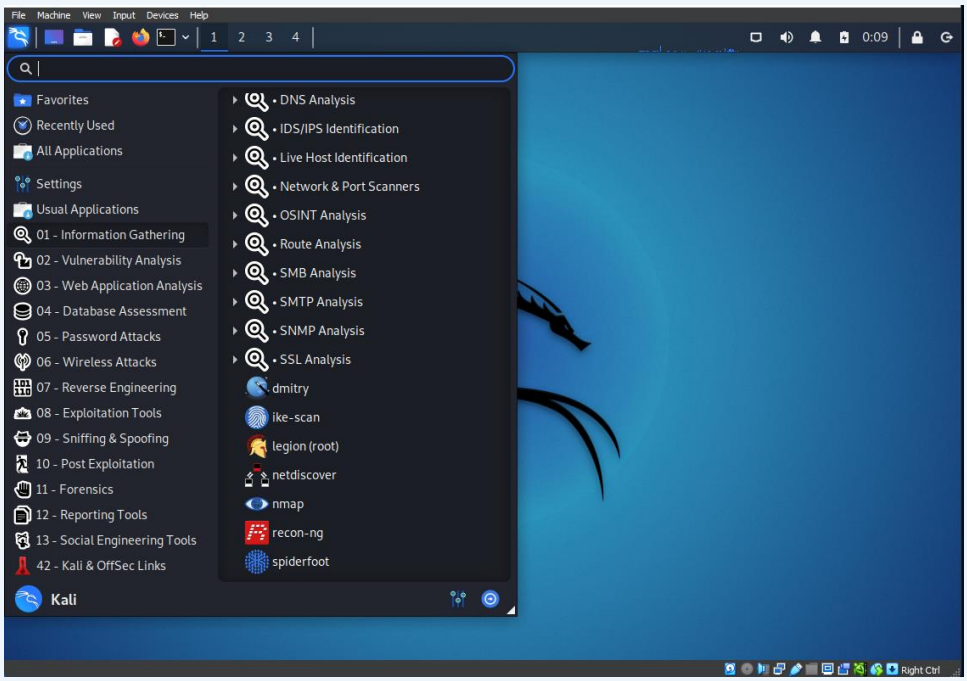
Practical 2

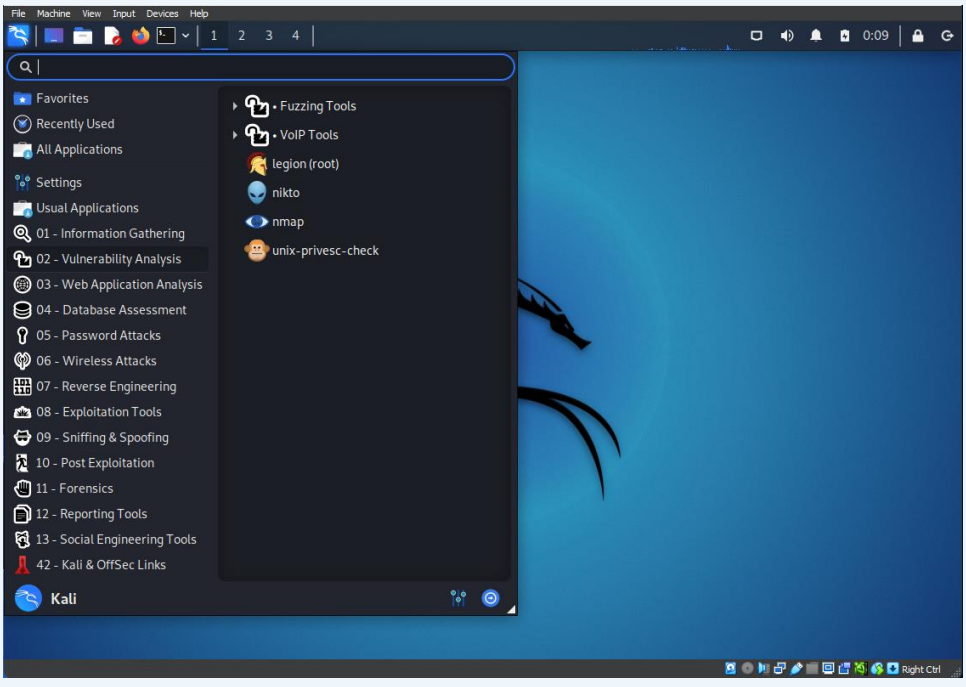
Devasy Patel

20BCE057

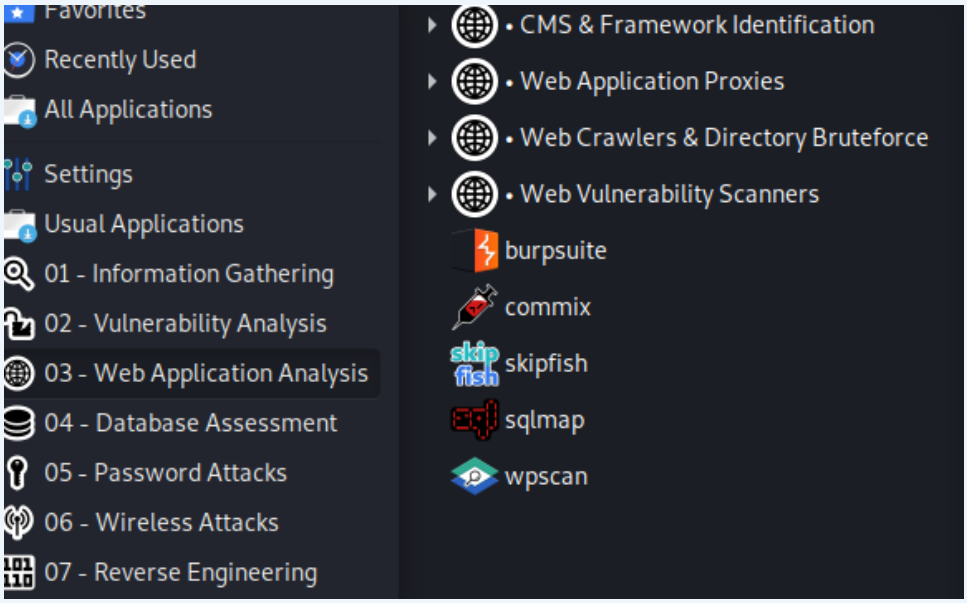
EHVA

1. **Nmap**: It is a network exploration and security auditing tool. It can be used to discover hosts and services on a computer network, thus creating a “map” of the network.

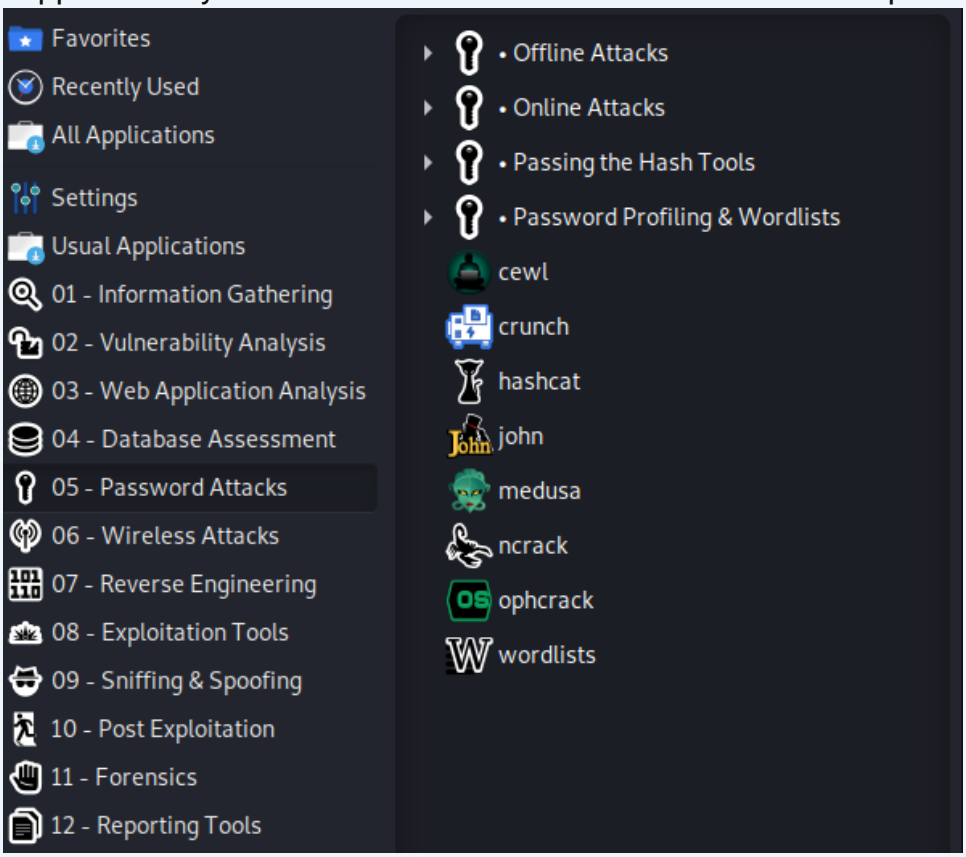




2. **sqlmap**: It is an open-source penetration testing tool that automates the process of detecting and exploiting SQL injection flaws and taking over of database servers.



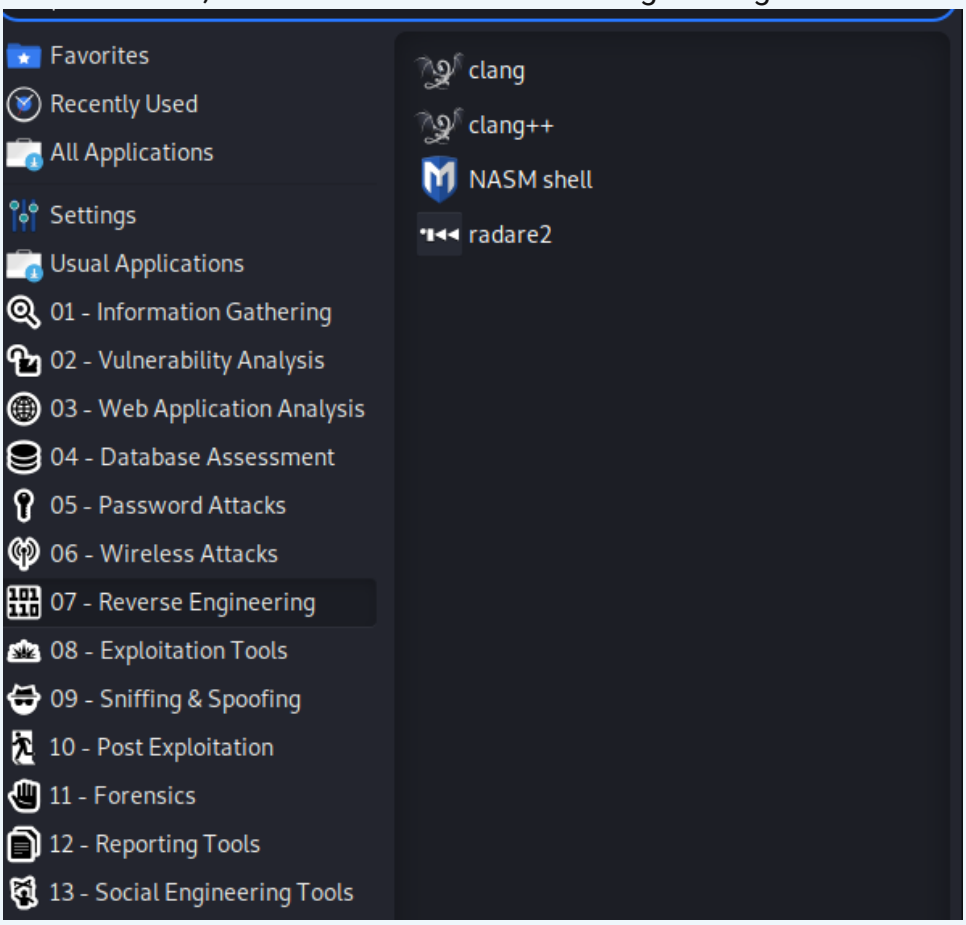
3. **medusa**: It is a speedy, massively parallel, modular, login brute-forcer that supports many services which allow remote authentication as possible.



4. **kismet**: It is a wireless network and device detector, sniffer, wardriving tool, and WIDS (wireless intrusion detection) framework.

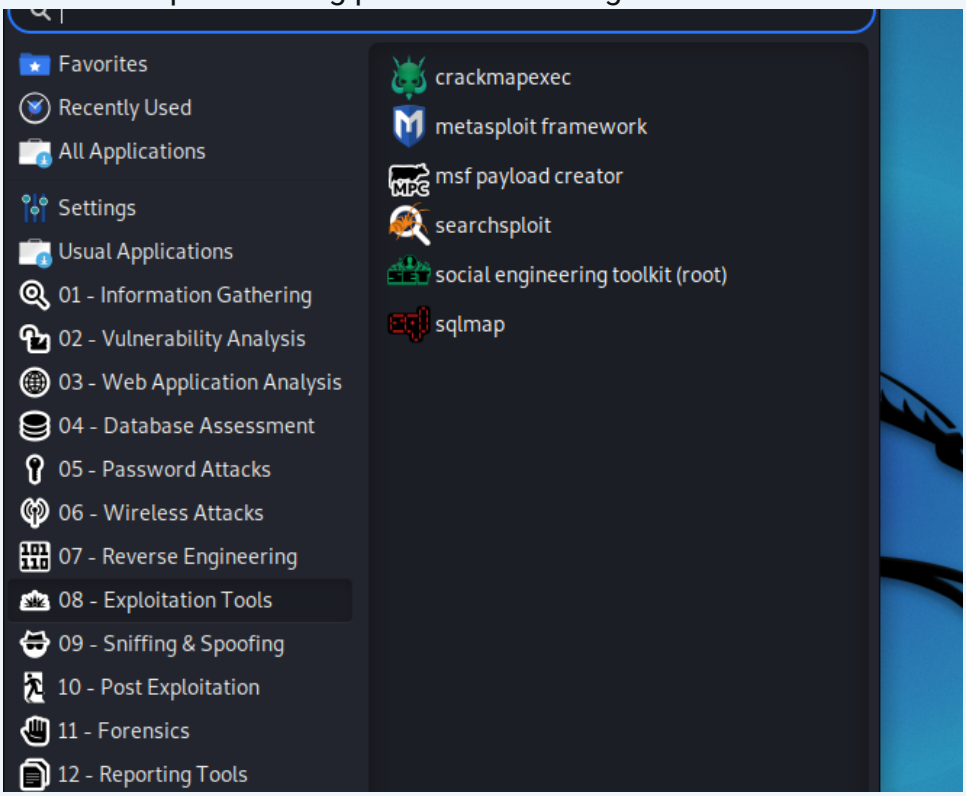
5. **NASM Shell**: NASM Shell is an interactive assembler and disassembler that is mainly used for x86 and x86-64 architectures. Assemblers like NASM Shell allow security researchers and penetration testers to analyze and understand low-level

machine code, which is crucial for reverse engineering and vulnerability analysis.



6. **searchsploit**: Searchsploit is a command-line utility used to search for known exploits in the Exploit Database (exploit-db.com). It is part of the Exploit Database project and assists penetration testers in finding existing exploits for specific vulnerabilities. This tool streamlines the process of identifying and using

available exploits during penetration testing.



7. **Wireshark**: It is a network protocol analyzer that lets you see what is happening on your network at a microscopic level.