ASSIGNMENT 2

Overview of the Assignment:

To explore 10 tools in Kali Linux, one from each different section of tools like information gathering, vulnerability analysis, wireless attacks etc. and write about them or show the action.

KALI LINUX TOOLS

1. Information Gathering:

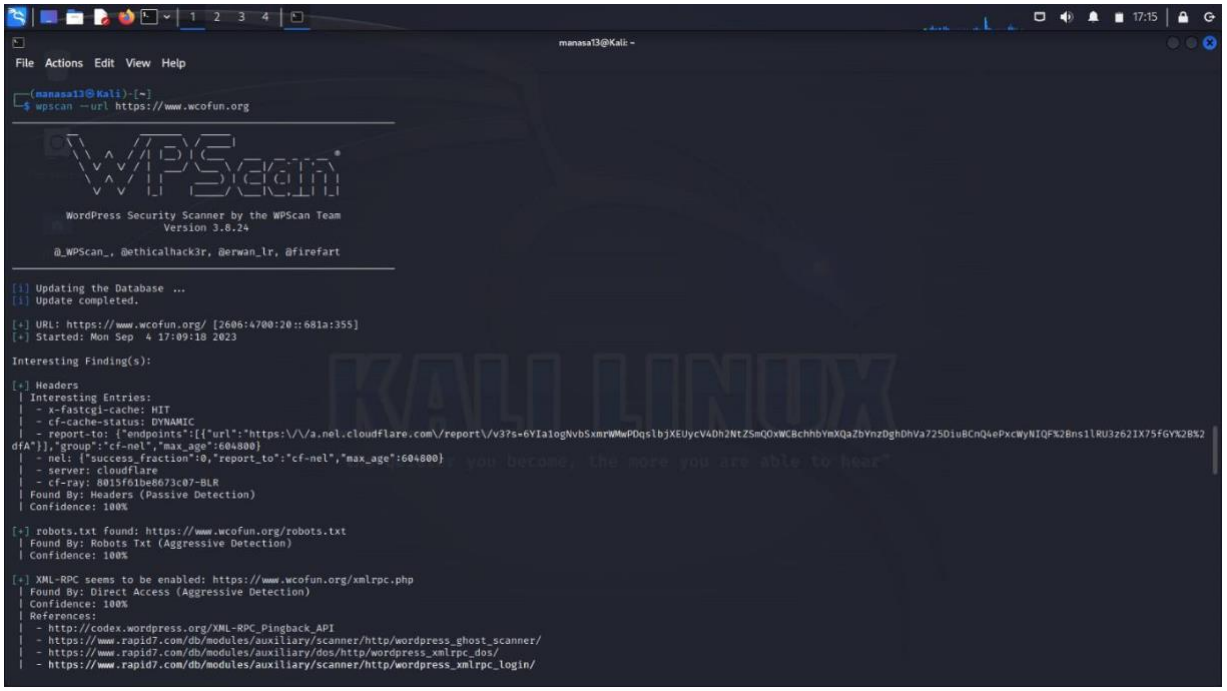
For information gathering, a tool named dnsenum is used. It is a command-line tool used for DNS (Domain Name System) enumeration and information gathering. It is typically used by security professionals, network administrators, and ethical hackers to gather information about a target domain's DNS configuration.

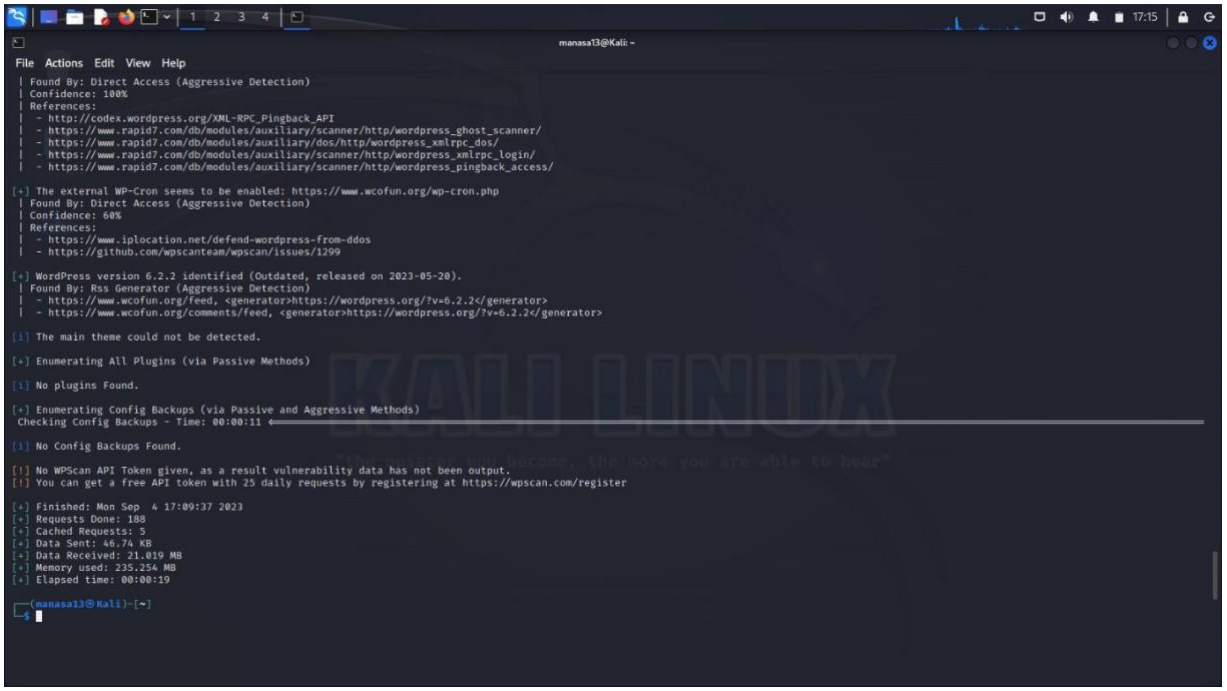
For this, I have used www.wcofun.org website.

2. Vulnerability Analysis:

For vulnerability analysis, nmap tool is used. Nmap (Network Mapper) is a widely used open-source tool for network discovery and vulnerability analysis. It is primarily used for network scanning, mapping, and fingerprinting, but it can also assist in vulnerability assessment.

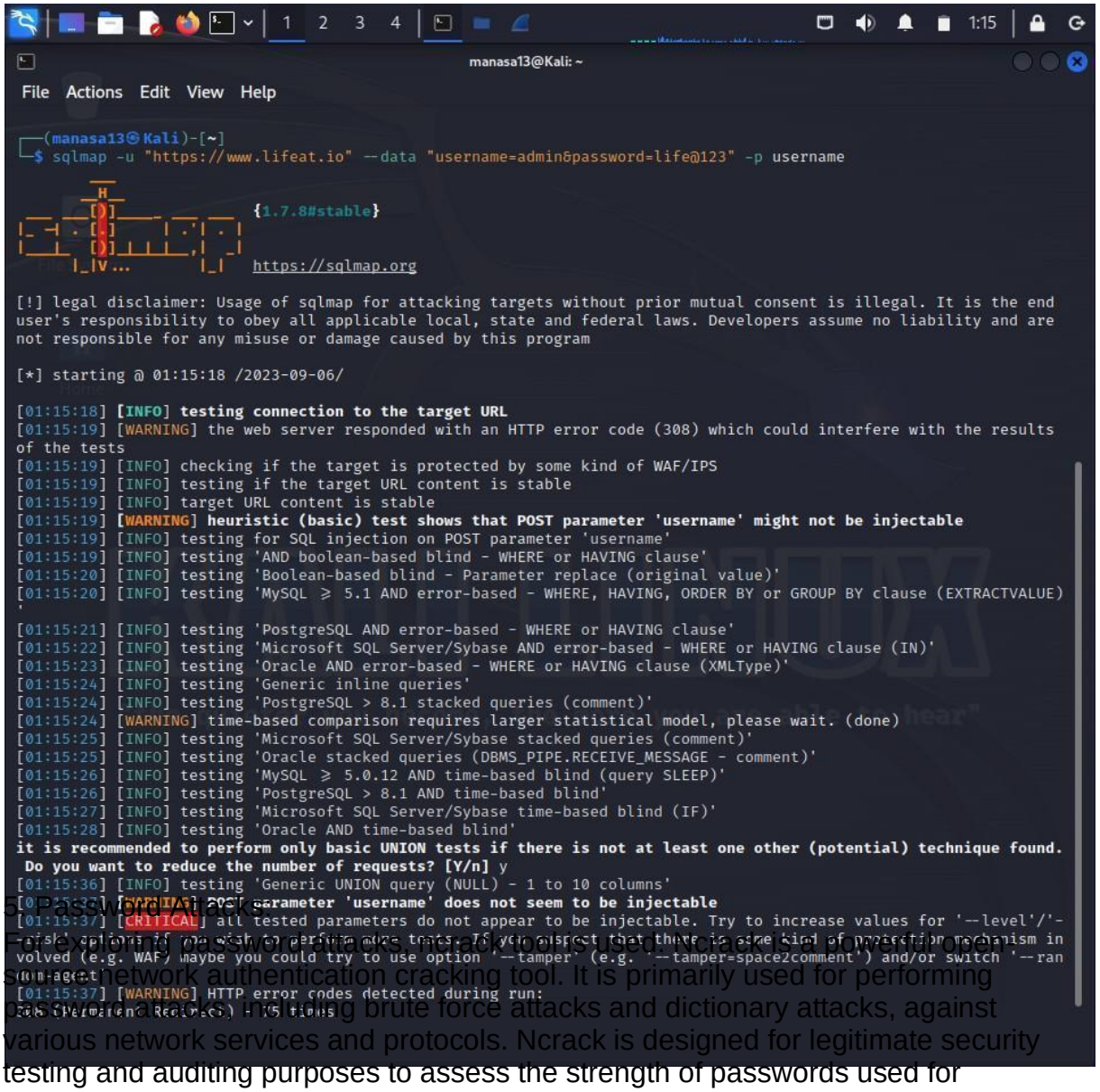
3. Web Application Analysis:
For Web Application Analysis, a tool named wpscan is used. WPScan is a popular open-source security scanner specifically designed for WordPress websites. It is used for identifying vulnerabilities, misconfigurations, and security issues in WordPress installations. It can be a valuable tool for security professionals, website administrators, and penetration testers to assess the security posture of WordPress sites.





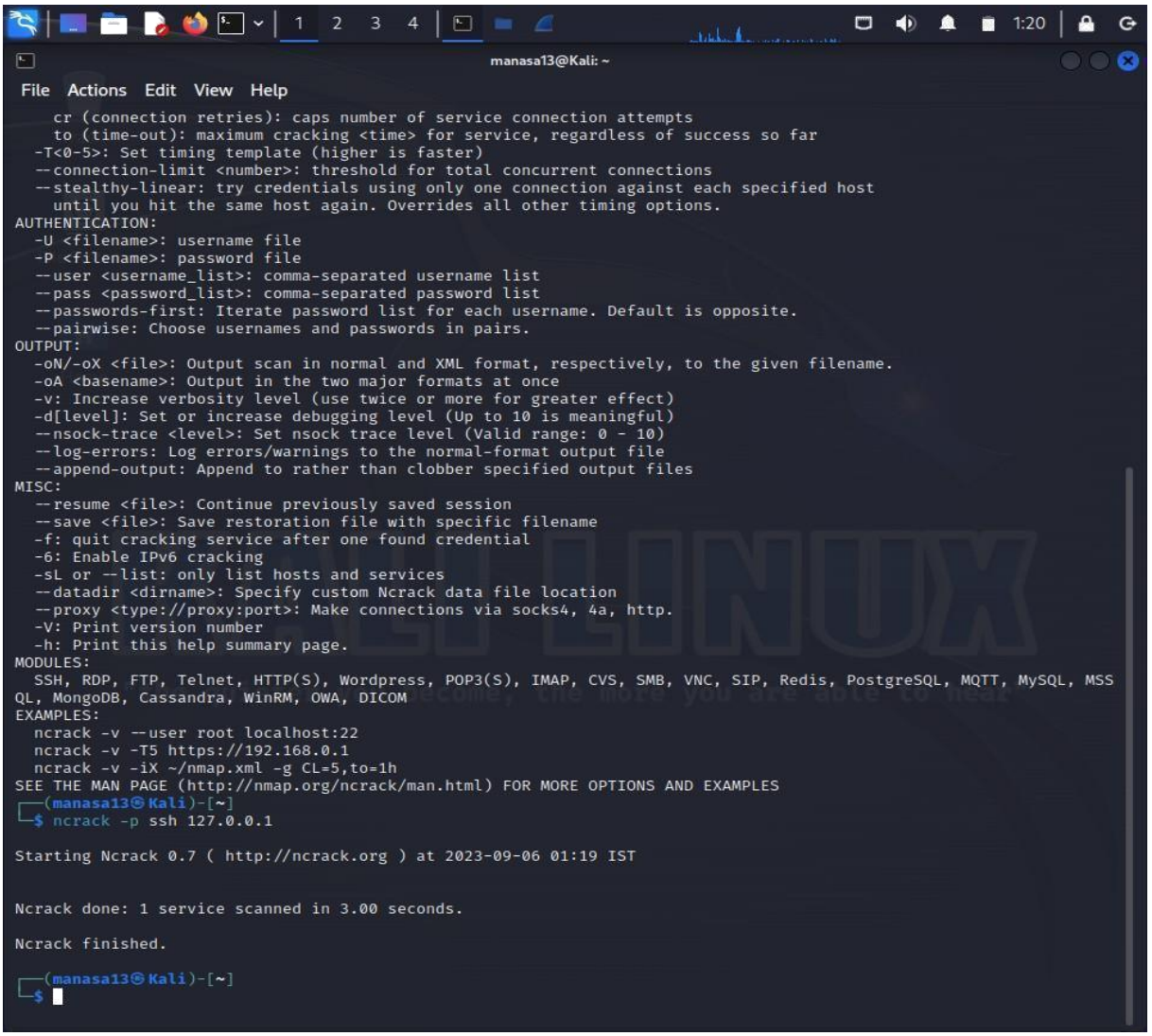
4. Database Assessment:
For Database Assessment, sqlmap tool is used. sqlmap is a popular open-source tool used for automated penetration testing and database assessment. Its primary purpose is to detect and exploit SQL injection vulnerabilities in web applications and their underlying

databases. SQL injection is a common attack vector where malicious SQL statements are inserted into input fields of a web application to manipulate the database or gain unauthorized access to sensitive data.



5. Password Attacks:

Ncrack is a high-speed network authentication cracking tool. It is primarily used for performing password attacks, including brute force attacks and dictionary attacks, against various network services and protocols. Ncrack is designed for legitimate security testing and auditing purposes to assess the strength of passwords used for authentication on network services.

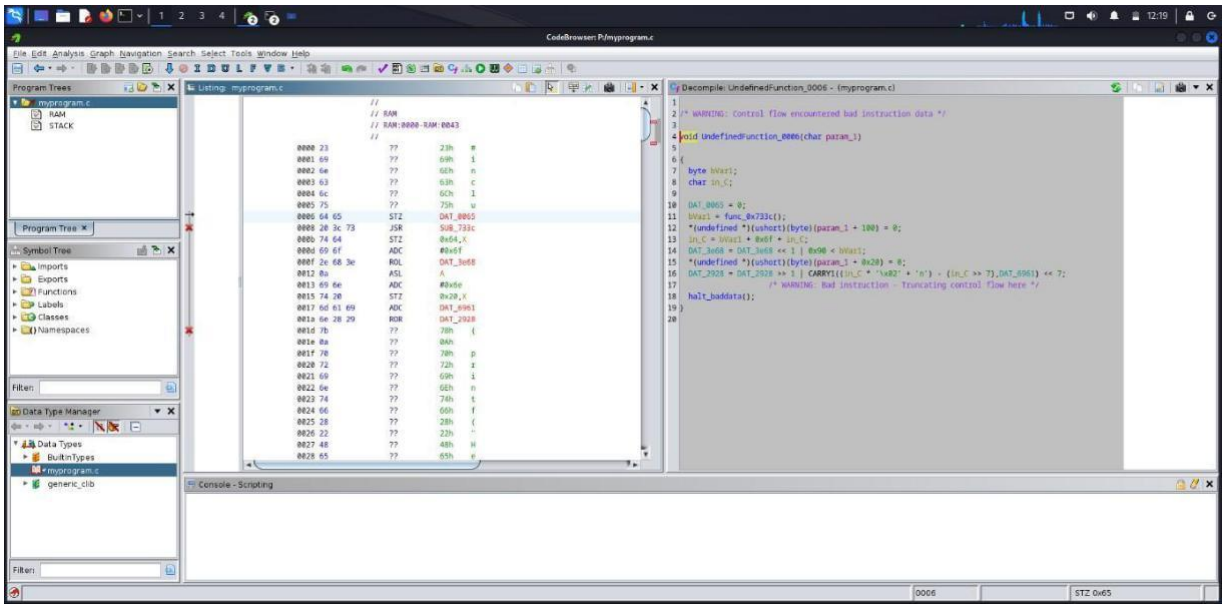


6. Wireless Attacks:

For exploring wireless attacks, wifite tool is used. Wifite is a popular wireless auditing tool available in Kali Linux. It is designed to automate various wireless attacks, including WEP and WPA/WPA2-PSK cracking, using a combination of well-known attack methods.

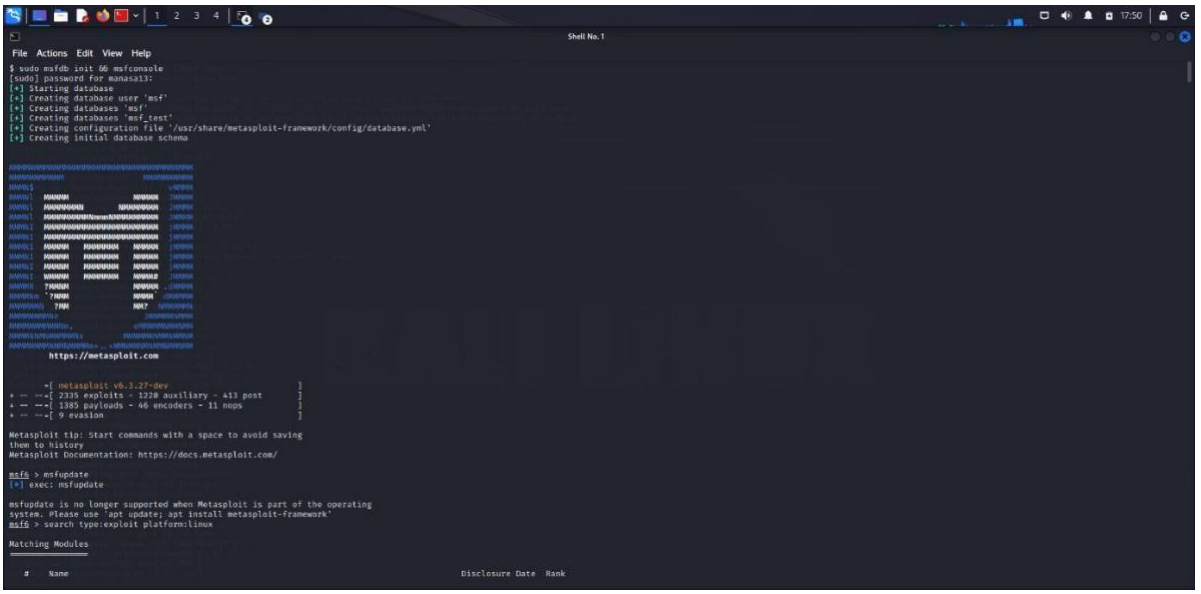
7. Reverse Engineering:

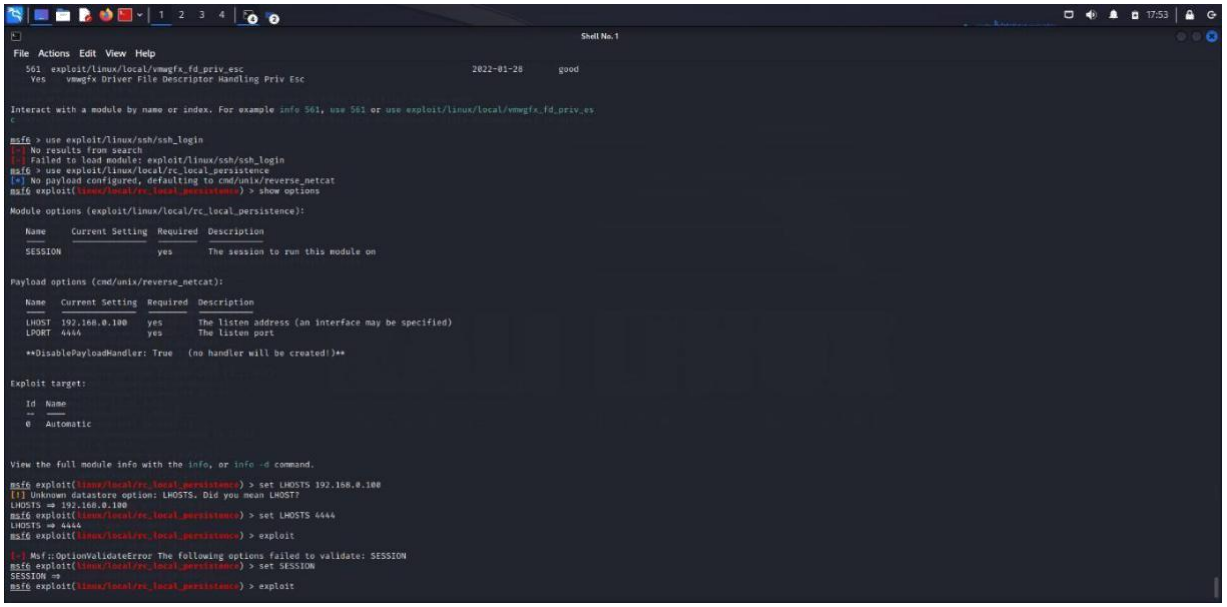
For Reverse engineering, Clang and Ghidra are used. Clang is a popular open-source C and C++ compiler front end that is part of the LLVM project. Ghidra is a powerful open-source software reverse engineering framework developed by the National Security Agency (NSA).



8. Exploitation Tools:

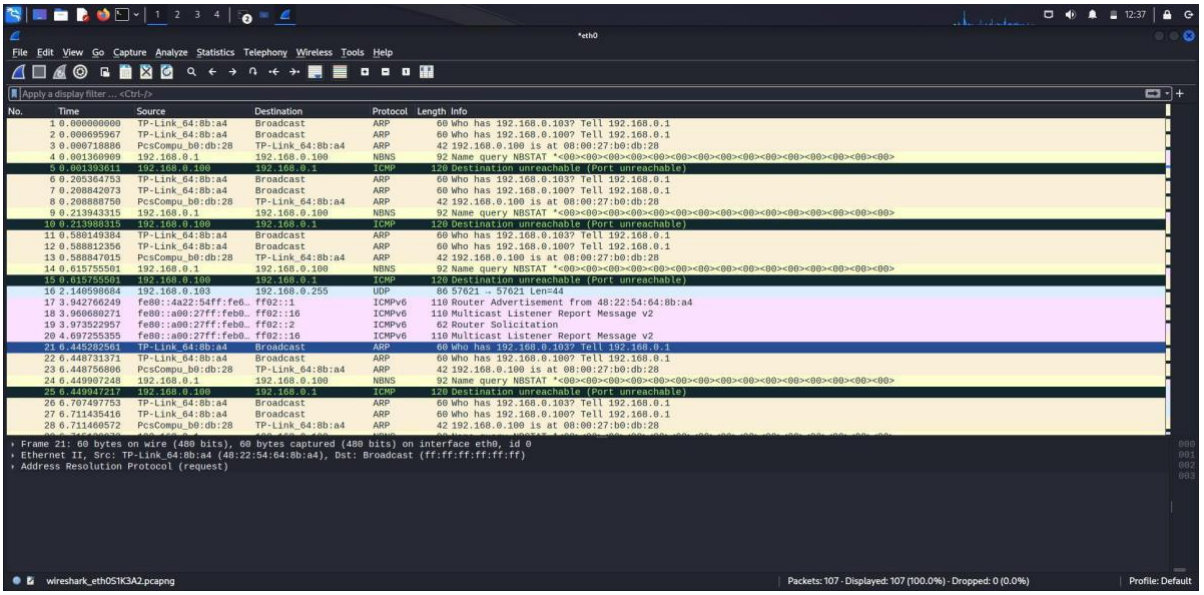
For exploiting ip address, Metasploit Framework tool is used. The Metasploit Framework is a widely used open-source penetration testing and exploitation tool that provides a
comprehensive set of tools for identifying vulnerabilities, creating, and deploying exploits, and conducting security assessments. Metasploit is used by security professionals, penetration testers, and ethical hackers to test and assess the security of systems and
applications.





9. Sniffing and Spoofing:

For exploring sniffing and spoofing, Wireshark tool is used. Wireshark is a widely used open-source network protocol analyzer. While it is primarily designed for network traffic analysis, it can be used for network sniffing. However, it is important to note that Wireshark is a legitimate tool for network troubleshooting and security analysis when used responsibly and within legal and ethical boundaries. Network administrators, security professionals, and ethical hackers commonly use Wireshark for legitimate purposes, such as monitoring network traffic, diagnosing network issues, and assessing network security.



10. Post Exploitation:

For exploring Post exploitation, Mimikatz tool is used. Mimikatz is a powerful post-exploitation tool that is widely known for its capability to extract plaintext passwords, hashes, and other authentication credentials from memory, as well as performing other post-exploitation tasks on Windows systems. It is used by security professionals, penetration testers, and sometimes malicious actors for legitimate and malicious purposes.