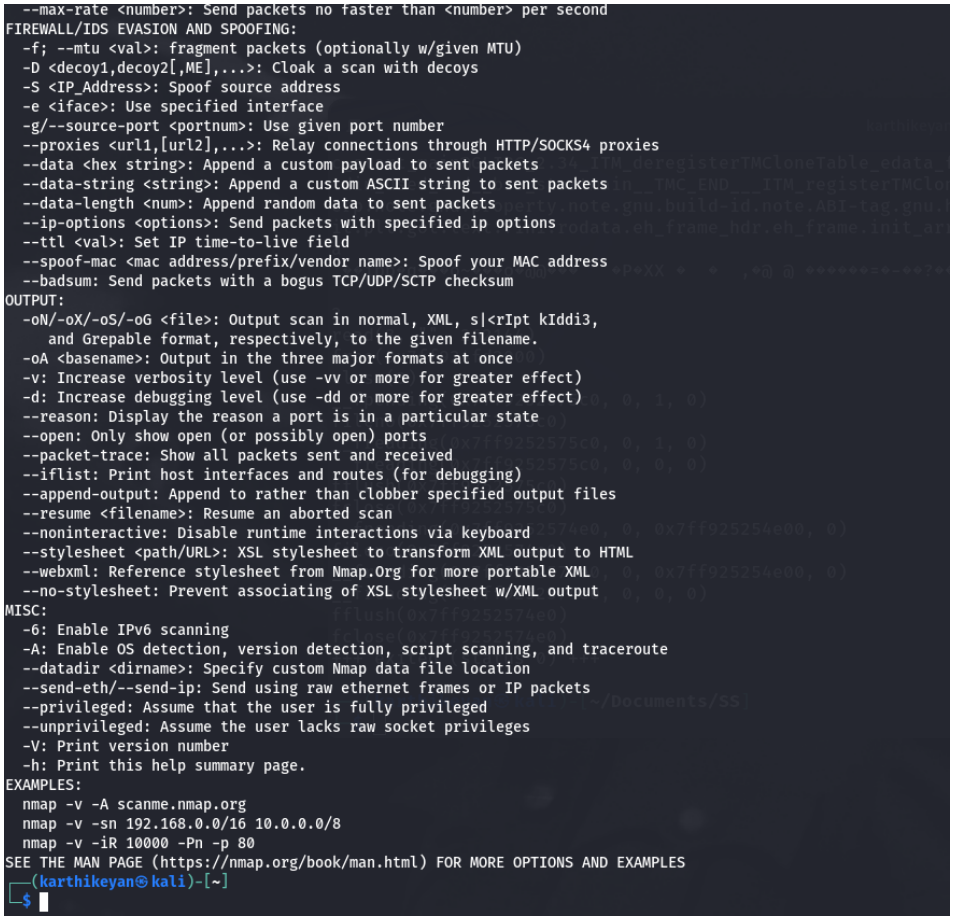
Amrita Vishwa Vidyapeetham
Name: karthikeyan G
Roll No: cb.sc.p2cys24008

24CYS682 – Cyber Security Lab
Assignment 1: Exploring Tools in Kali Linux

Contents

1 Information Gathering

1. **Nmap**:
   - Nmap is used to scan networks and find active hosts, open ports, and services running on those ports.
   - It helps analyze system vulnerabilities by mapping the network's structure.
   - Security analysts rely on it for reconnaissance before deeper penetration testing.



2. **Recon-ng**:
   - Recon-ng automates data gathering about domains, IPs, or emails using open-source intelligence.
   - It provides modules for seamless API integrations, like Shodan and VirusTotal.
   - Its lightweight framework is perfect for organizing and reporting findings.

3. **Maltego**:

   - Maltego is a visualization tool that links data points like domains, IPs, and email addresses.
   - It's great for mapping relationships during investigations, particularly in OSINT.
   - Investigators use it to uncover connections that aren't immediately visible.

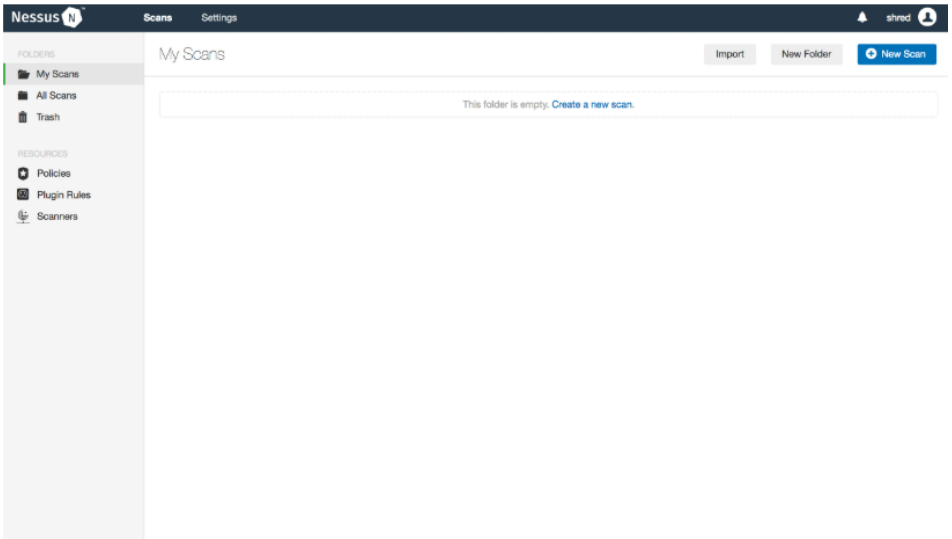
2 Vulnerability Analysis

4. **Nikto**:

   - Nikto scans web servers to find outdated software, insecure configurations, or vulnerabilities.
   - It provides detailed information about headers, subdomains, and security missteps.
   - It's a fast and effective way to identify low-hanging security risks.

5. **Nessus**:

   - Nessus is a powerful vulnerability scanning tool designed to identify weaknesses in systems, applications, and networks.
   - It provides in-depth reports with recommendations for mitigating identified risks and prioritizes vulnerabilities based on criticality.
   - Security professionals frequently use Nessus to perform comprehensive assessments and ensure compliance with industry standards.
   - It supports scanning for misconfigurations, outdated software, and known vulnerabilities across various platforms.
   - Nessus is widely regarded for its extensive plugin library, which allows it to detect over 50,000 vulnerabilities, including zero-day threats.

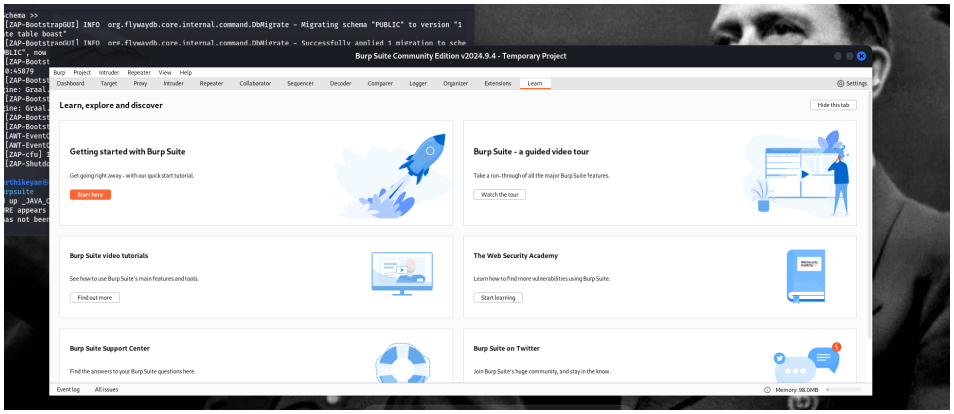


6. **Lynis**:

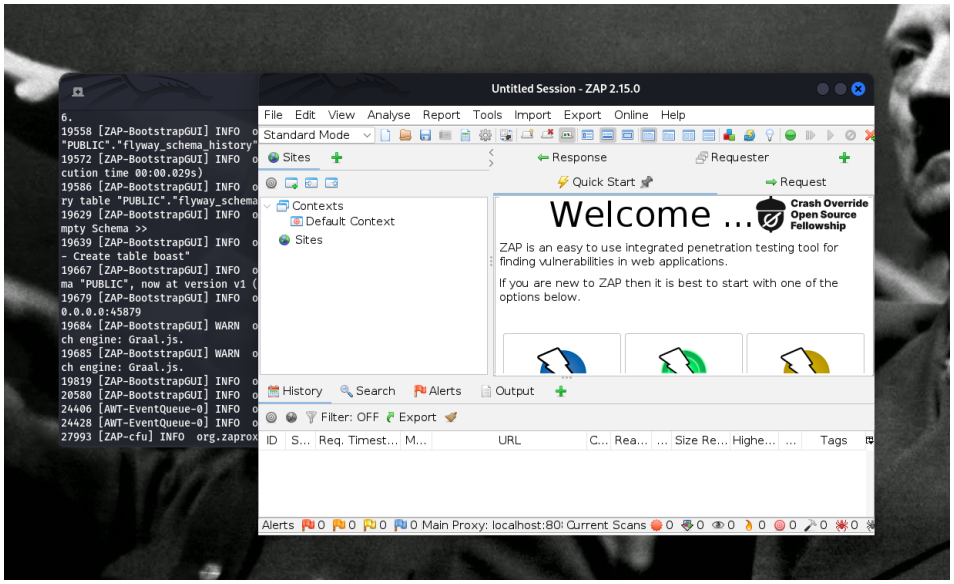
   - Lynis performs security audits on Linux systems, scanning for misconfigurations and weak points.
   - It generates suggestions for improving hardening and reducing risk.
   - Its command-line interface makes it ideal for advanced system assessments.

3 Web Application Analysis

7. **Burp Suite**:
   - Burp Suite intercepts and manipulates web traffic to identify vulnerabilities in web applications.
   - Testers use it to simulate attacks like injection or authentication bypasses.
   - It also allows for automated scans alongside manual testing.



8. **OWASP ZAP**:
   - OWASP ZAP is an open-source tool for finding vulnerabilities in web applications.
   - It simulates attacks to expose issues like XSS or SQL injection.
   - Its automated spider feature helps map the entire application structure.



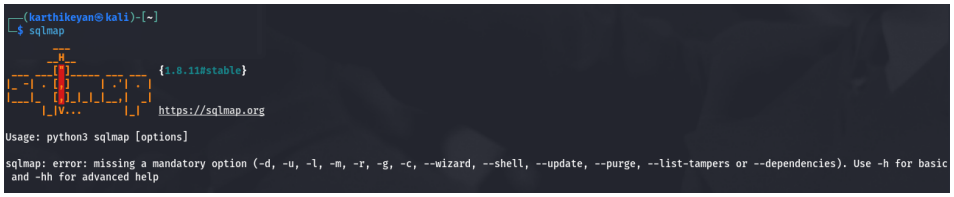
9. **Wapiti**:

   - Wapiti scans web applications for vulnerabilities like file inclusion, XSS, and CRLF injections.
   - It works by crawling the application and launching various payloads.
   - It's lightweight but still provides a thorough vulnerability report.

4 Database Assessment

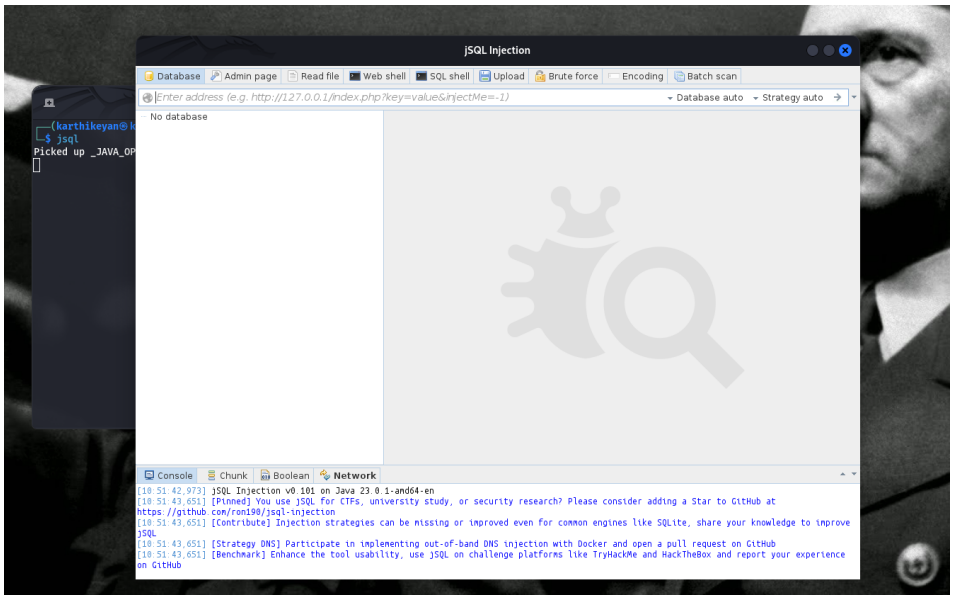
10. **sqlmap**:

    - sqlmap automates SQL injection attacks to exploit database vulnerabilities.
    - It can dump databases, test blind SQL injection, and even crack hashes.
    - It's perfect for both detection and exploitation of database flaws.



11. **jSQL Injection**:

    - jSQL is a lightweight tool for detecting and exploiting SQL injection vulnerabilities.
    - It supports different attack types, like blind, time-based, and error-based.
    - It's beginner-friendly while still being effective for testing.



5 Password Attacks

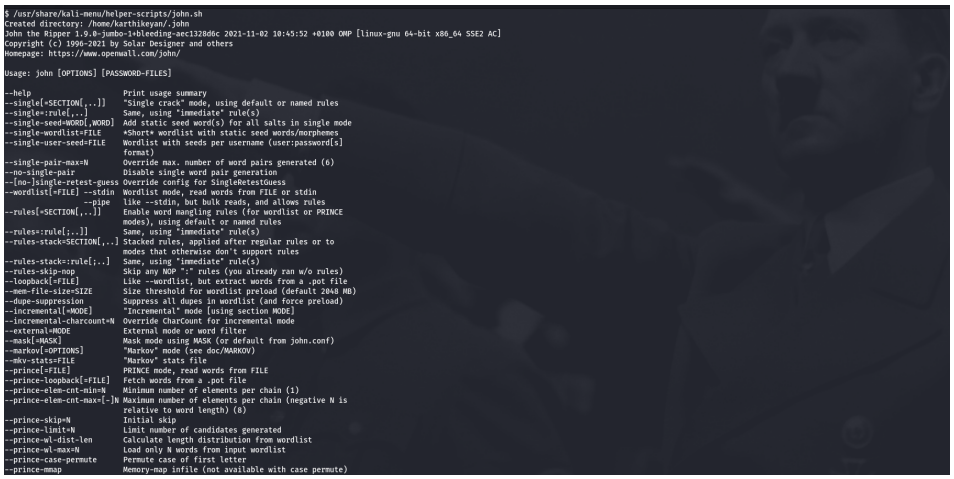
12. **Hydra**:

    - Hydra performs brute-force attacks on network protocols like SSH, FTP, or Telnet.
    - It's highly configurable with options to test usernames, passwords, or both.
    - It's a go-to tool for testing weak or default credential setups.

13. **John the Ripper**:

    - John the Ripper cracks hashed passwords using brute-force or dictionary attacks.

- It supports a variety of password formats, including MD5 and SHA.
- Security testers use it to ensure proper password policies are enforced.



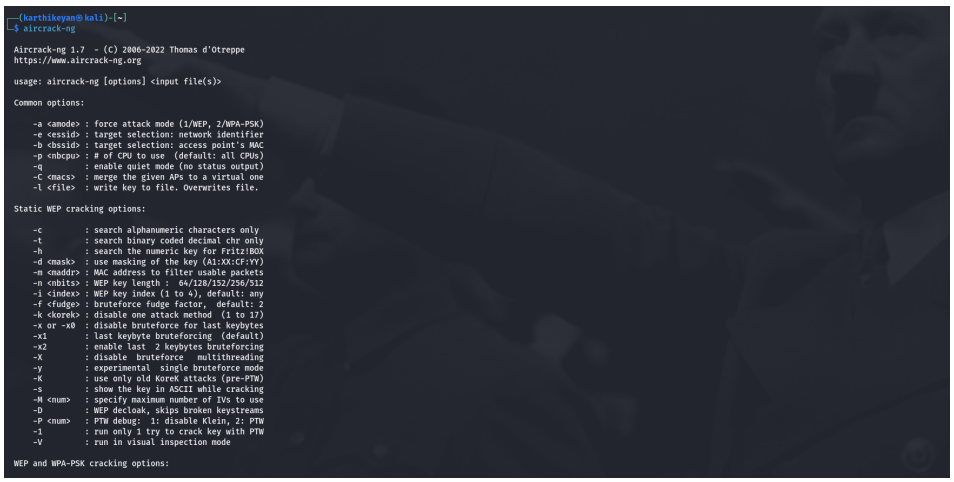
14. **Hashcat**:

- Hashcat is used to crack password hashes via brute-force, hybrid, or rule-based attacks.
- It supports GPU acceleration, making it extremely fast for cracking tasks.
- It's widely used in practical password recovery or policy testing.

6 Wireless Attacks

15. **Aircrack-ng**:

- Aircrack-ng is used to capture and analyze Wi-Fi packets for cracking WEP/WPA keys.
- It relies on techniques like dictionary or statistical attacks for key recovery.
- It's a go-to tool for assessing Wi-Fi network security weaknesses.



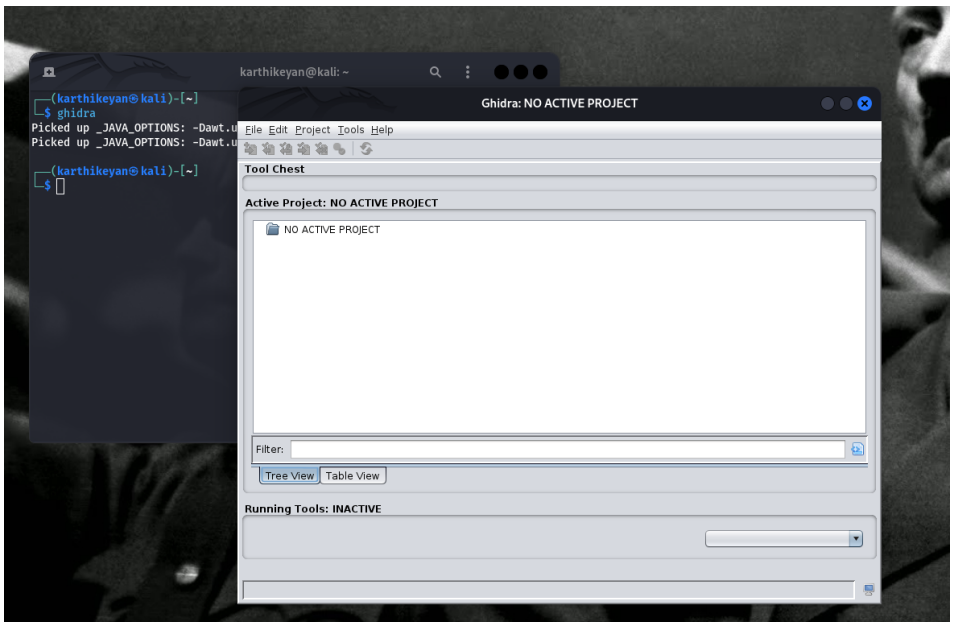
16. **Wifite**:

- Wifite automates Wi-Fi network attacks, focusing on WEP, WPA, and WPS.
- It's a simple solution for launching deauthentication or handshake-capture attacks.
- Security testers use it to quickly assess multiple networks.

7 Reverse Engineering

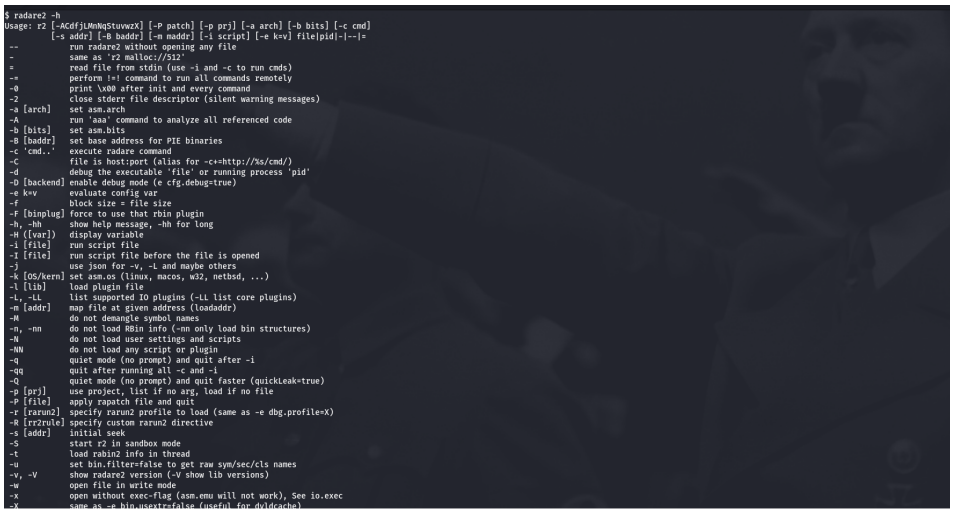
17. **Ghidra**:

- Ghidra is a reverse engineering tool that decompiles binaries into human-readable code.
- Analysts use it to study malware behavior or analyze software.
- It's highly modular, allowing for plugin development.



18. **Radare2**:

    - Radare2 disassembles binary code for analysis and debugging.
    - It supports various architectures and is highly customizable for advanced users.
    - It's ideal for analyzing complex malware or unauthorized code.

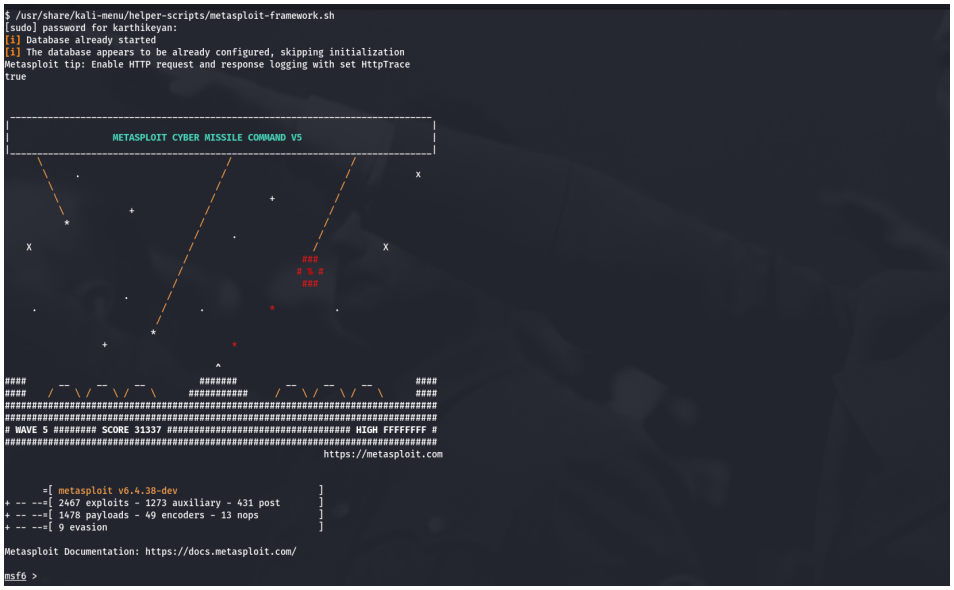


8 Exploitation Tools

19. **Metasploit Framework**:

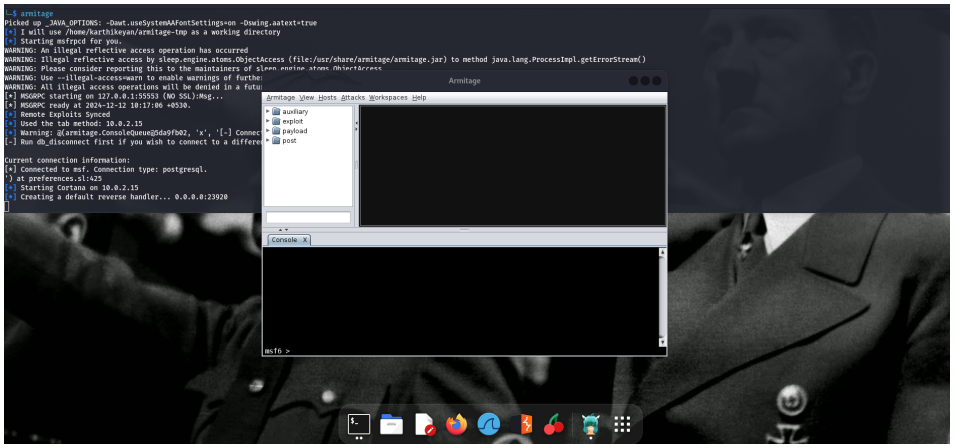
    - Metasploit is a powerful tool for discovering, exploiting, and verifying vulnerabilities.

- It includes a massive library of pre-built exploits and payloads.
- It's widely used for penetration testing and red team activities.



20. **Armitage**:

- Armitage provides a GUI interface to the Metasploit Framework for managing exploits.
- It's beginner-friendly and makes collaboration on exploitation tasks easier.
- Its interface visualizes attack paths and system weaknesses.

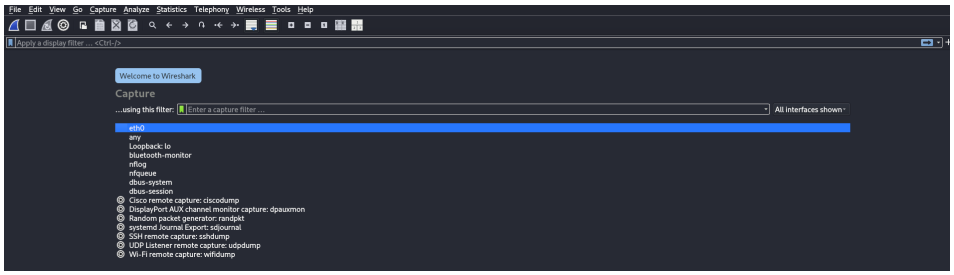


9 Sniffing & Spoofing

21. **Wireshark**:

- Wireshark captures and analyzes network traffic in real time.
- It's perfect for identifying malicious packets or debugging network issues.

- Its filtering system makes pinpointing specific data straightforward.



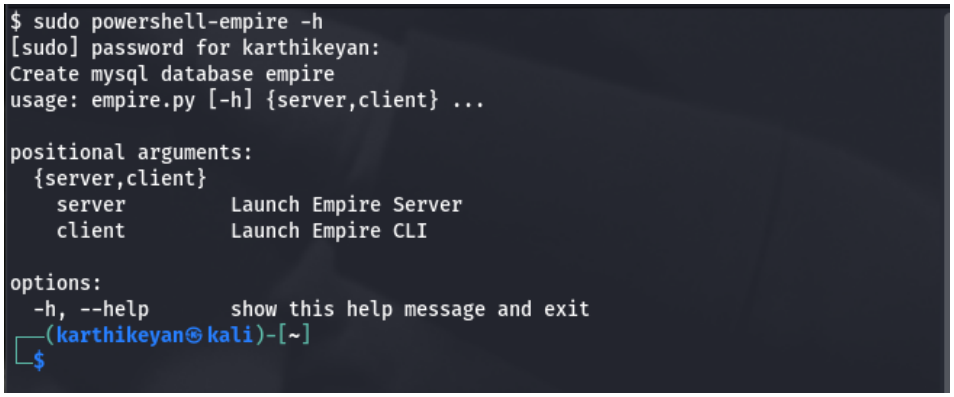
22. **Bettercap**:

- Bettercap performs network attacks like ARP spoofing and DNS poisoning.
- It also monitors traffic for credentials or other sensitive data.
- It's a versatile tool for advanced red team operations.

10 Post Exploitation

23. **Empire**:

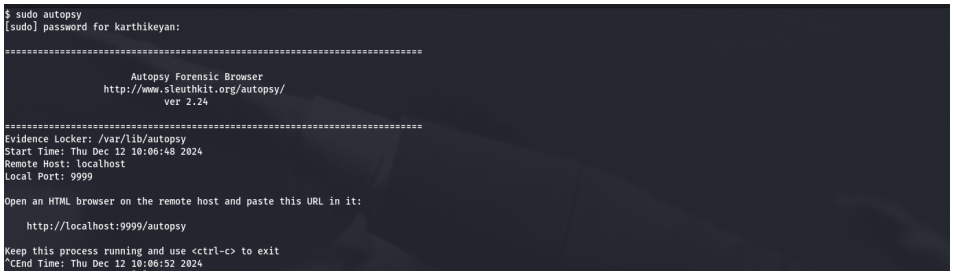
- Empire is a post-exploitation framework that helps maintain persistent access.
- It supports modules for keylogging, privilege escalation, and data exfiltration.
- Attackers use it for stealthy, long-term system compromise.



11 Forensics

24. **Autopsy**:

    - Autopsy helps recover deleted files, analyze hard drives, and extract metadata.
    - It's commonly used in digital forensic investigations for evidence collection.
    - Its user-friendly interface simplifies the forensic process.



12 Social Engineering Tools

25. **Social Engineering Toolkit (SET)**:

    - SET is a framework for creating phishing attacks, malicious payloads, and fake websites.
    - It's tailored for exploiting human vulnerabilities in security.
    - Organizations use it to test the awareness of their employees.