K. J. SOMAIYA COLLEGE OF ENGINEERING, MUMBAI – 400 077
(A CONSTITUENT COLLEGE OF SOMAIYA VIDYAVIHAR UNIVERSITY)
DEPT. OF COMPUTER ENGINEERING
T.Y. B. TECH. SEMESTER –VI (2024-25)
INFORMATION SECURITY
INTERNAL ASSESMENT I

IMPLEMENTATION OF HONEYPOT USING PEN T BOX

1. YASH SHETH (16010122310)
2. SHRUSTI VORA (16010122233)
3. MINIT SHAH (16010122315)
4. MUKUL CHAUDHARI (16010122311)

INTRODUCTION

1. Kali Linux is a Debian-based distribution designed for penetration testing and digital forensics. It is developed and maintained by Offensive Security.
2. The operating system includes 600+ penetration testing tools, such as:

- Armitage – A cyber attack management tool
- Nmap – A network scanner
- Wireshark – A network traffic analyzer
- John the Ripper – A password-cracking tool
- sqlmap – An SQL injection testing tool
- Aircrack-ng – A wireless security auditing suite
- Burp Suite – A web security testing tool
- OWASP ZAP – A web application security scanner

3. Kali Linux was developed by Mati Aharoni and Devon Kearns, employees of Offensive Security, by rewriting BackTrack, a previous security-focused Linux distribution based on Knoppix. The name "Kali" is inspired by the Hindu goddess Kali.

HONEYPOT

What Are Honeypot ?

A honeypot is a decoy system or network trap designed to attract attackers, detect cyber threats, and analyze malicious activity. It appears as a legitimate system but is intentionally vulnerable to lure hackers, allowing cybersecurity professionals to monitor attack techniques and improve defenses.

Types of Honeypots ?

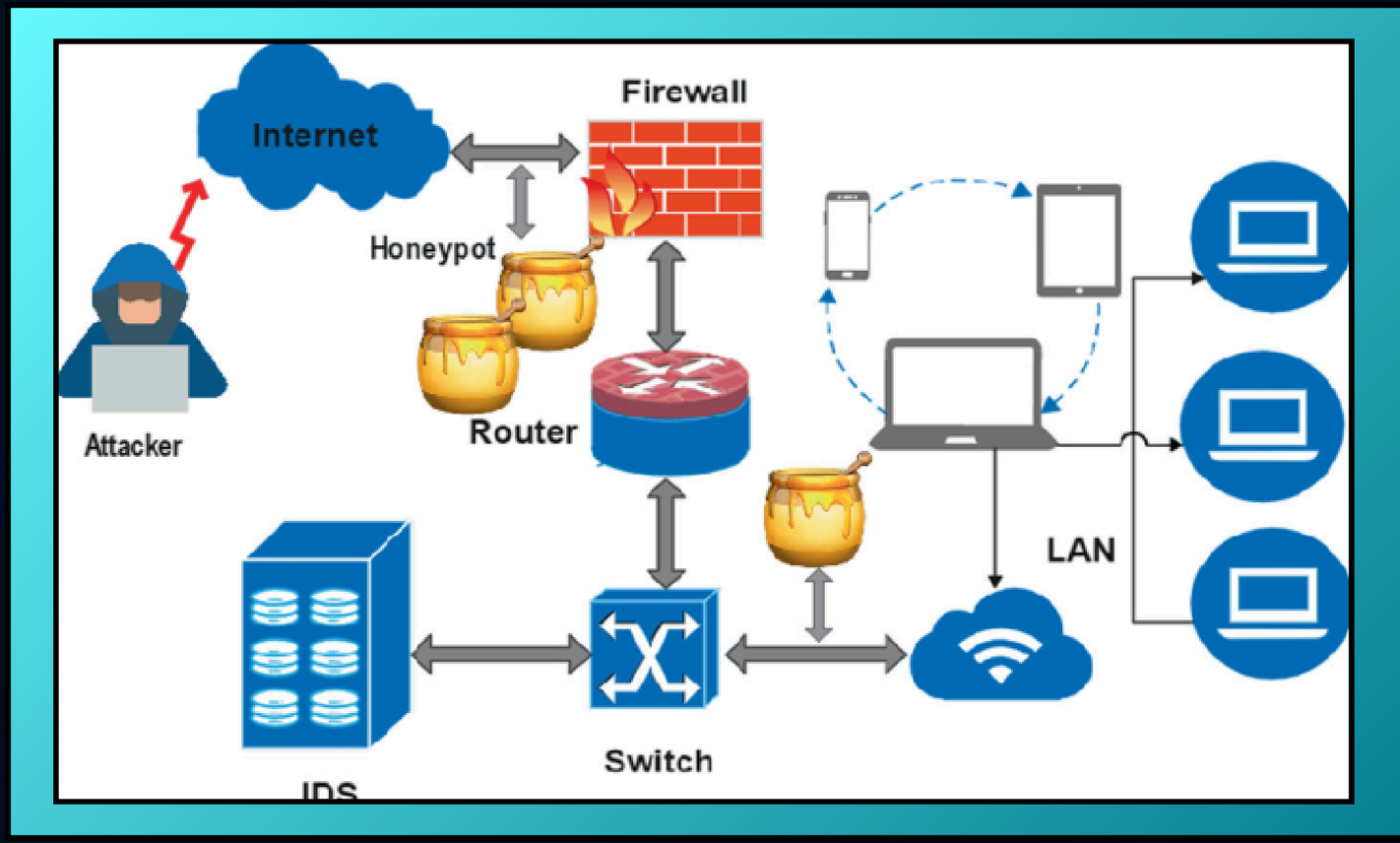
1. Low-Interaction – Simulates basic services (e.g., Honeyd, Kippo).
2. Medium-Interaction – Allows limited attacker interaction (Cowrie).
3. High-Interaction – Fully functional system for deep analysis (Dionaea, Glastopf).

Purpose Based Honeypots

1. Research Honeypots – Study attacker behavior (Dionaea).
2. Production Honeypots – Detect real-world threats (T-Pot).
3. Malware Honeypots – Capture malware (Ghost USB).
4. Spam Honeypots – Trap email spammers (Spamtrap).

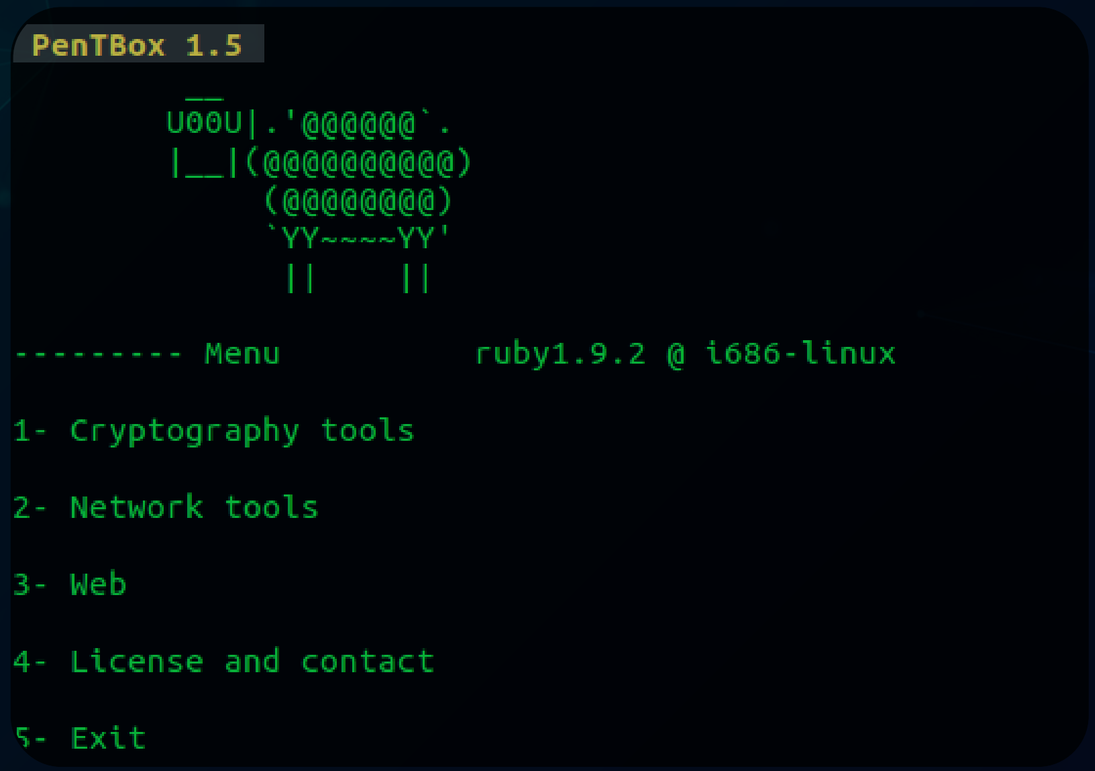
It has Several Pros & Cons

1. Detects threats early
2. Improves security policies
3. Cost-effective monitoring
4. Can be exploited by hackers
5. Requires continuous updates
6. Only captures direct interactions



PEN T BOX

PenTBox is a security suite that can be used in penetration testing engagements to perform a variety of activities.Specifically these activities include from cracking hashes,DNS enumeration and stress testing to HTTP directory brute force.



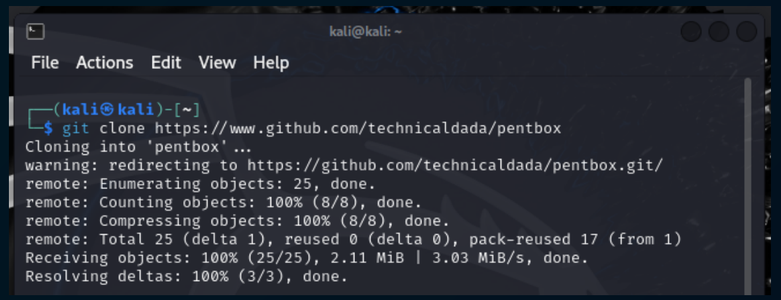
FEATURES

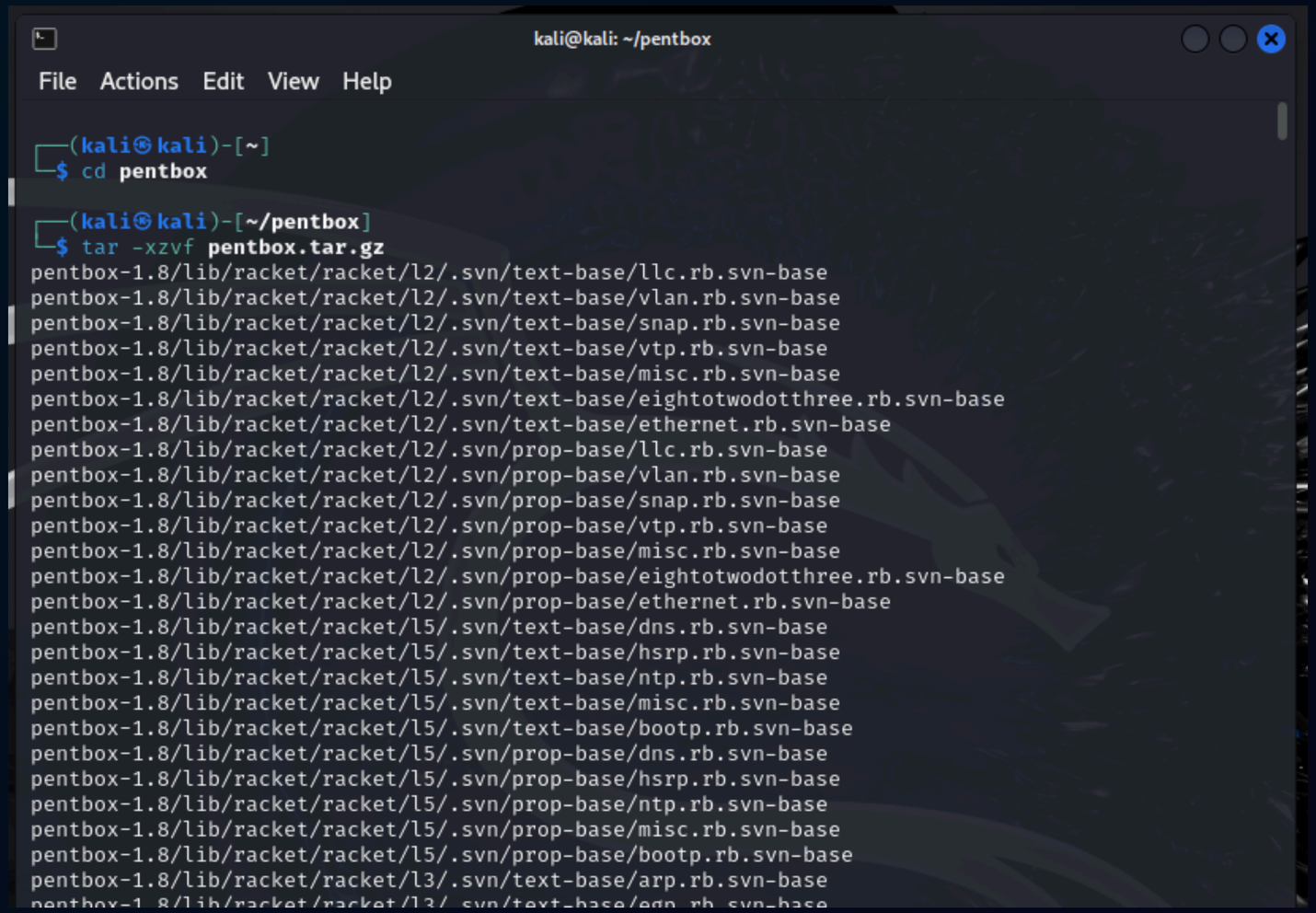
Pentbox is a security tool used for penetration testing, and it includes a honeypot module to detect unauthorized access attempts. The key features of implementing a honeypot using Pentbox include:

1. Intrusion Detection – Logs unauthorized access attempts and helps identify potential threats.
2. Port Scanning Detection – Alerts users when someone is scanning the system for open ports.
3. Emulated Services – Simulates various services (e.g., HTTP, FTP) to attract attackers.
4. Logging & Reporting – Records attacker activities for analysis.
5. Easy Deployment – A simple command-line interface for quick setup.
6. Customizability – Configurable options to suit different security needs.
7. Decoy System – Acts as a trap to deceive hackers and study their behavior.

METHODOLOGY/DEMONSTRATION

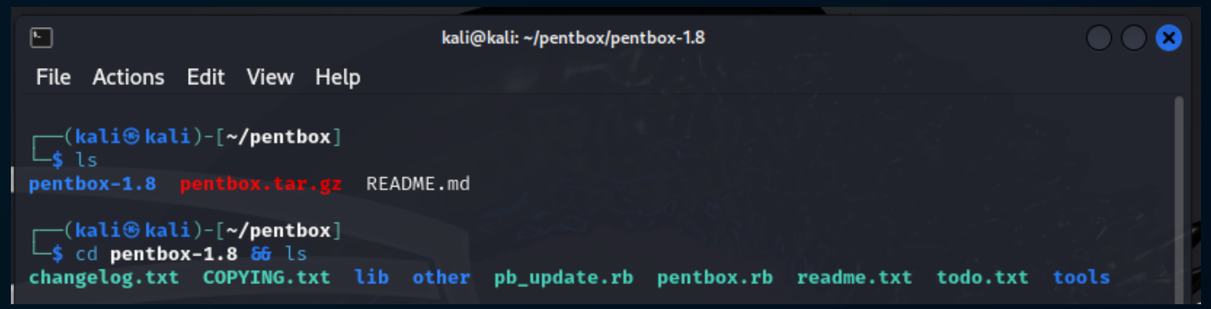
To set up a honeypot in our Kali Linux system we need to download a tool from GitHub it called Pentbox. This tool is written in ruby language. To download this we use the following command:

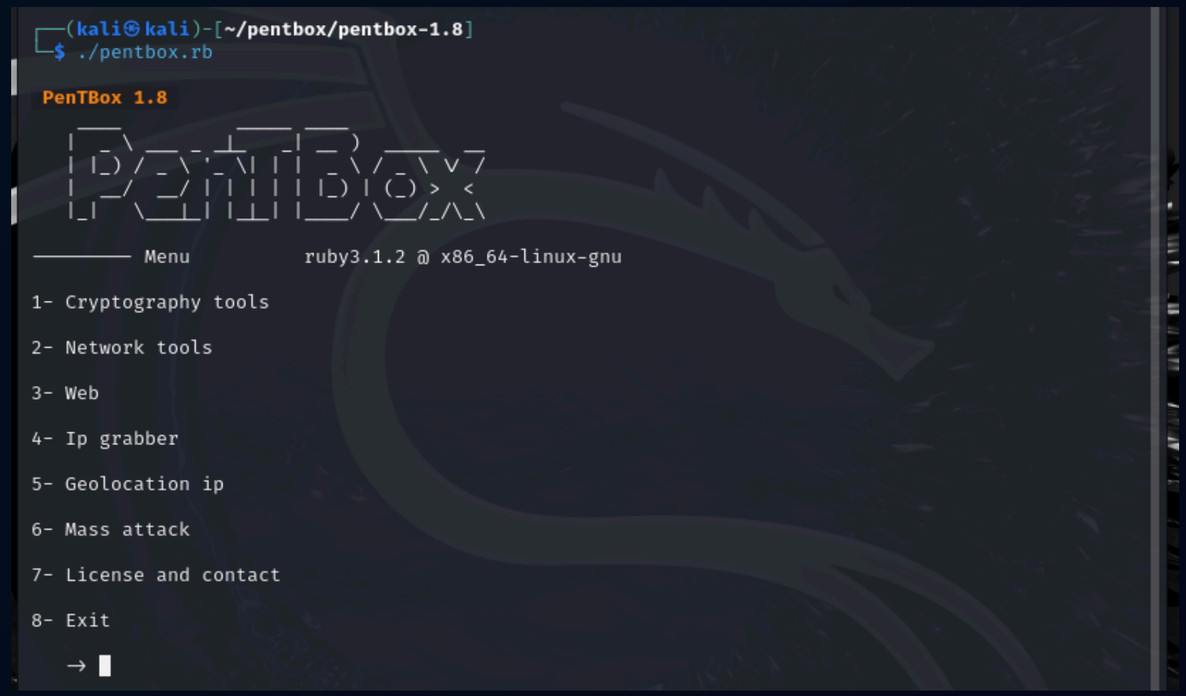




METHODOLOGY/DEMONSTRATION

Then we need to go into the pentbox folder by using cd command. Here we have a compressed file named pentbox.tar.gz and to extract it. Then we run this ruby tool by using simple command as following: ./pentbox.rb



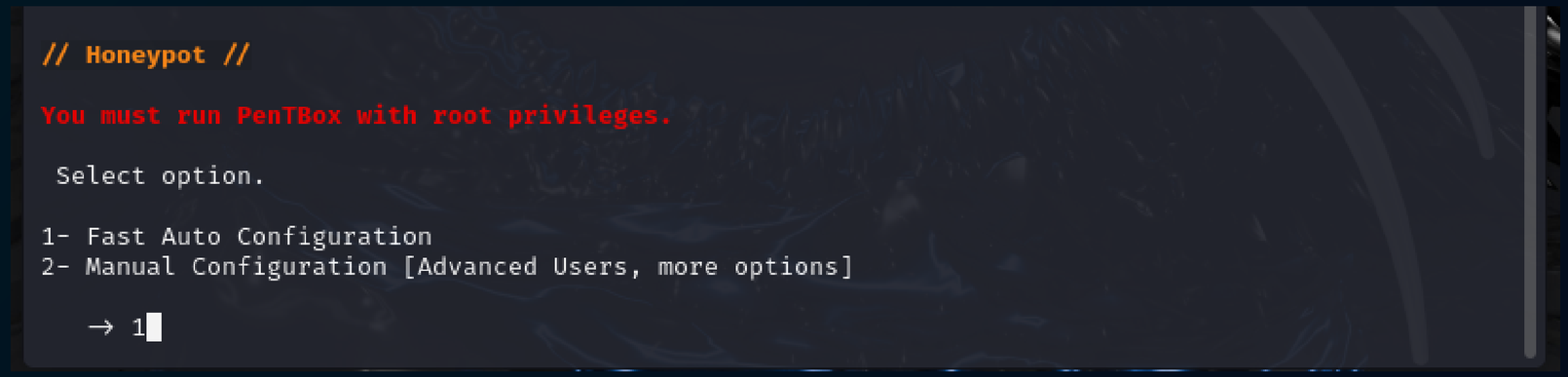


METHODOLOGY/DEMONSTRATION

Then this tool will open. Here we need to go to the Network tools option. Then we can see the Honeypot option.

METHODOLOGY/DEMONSTRATION

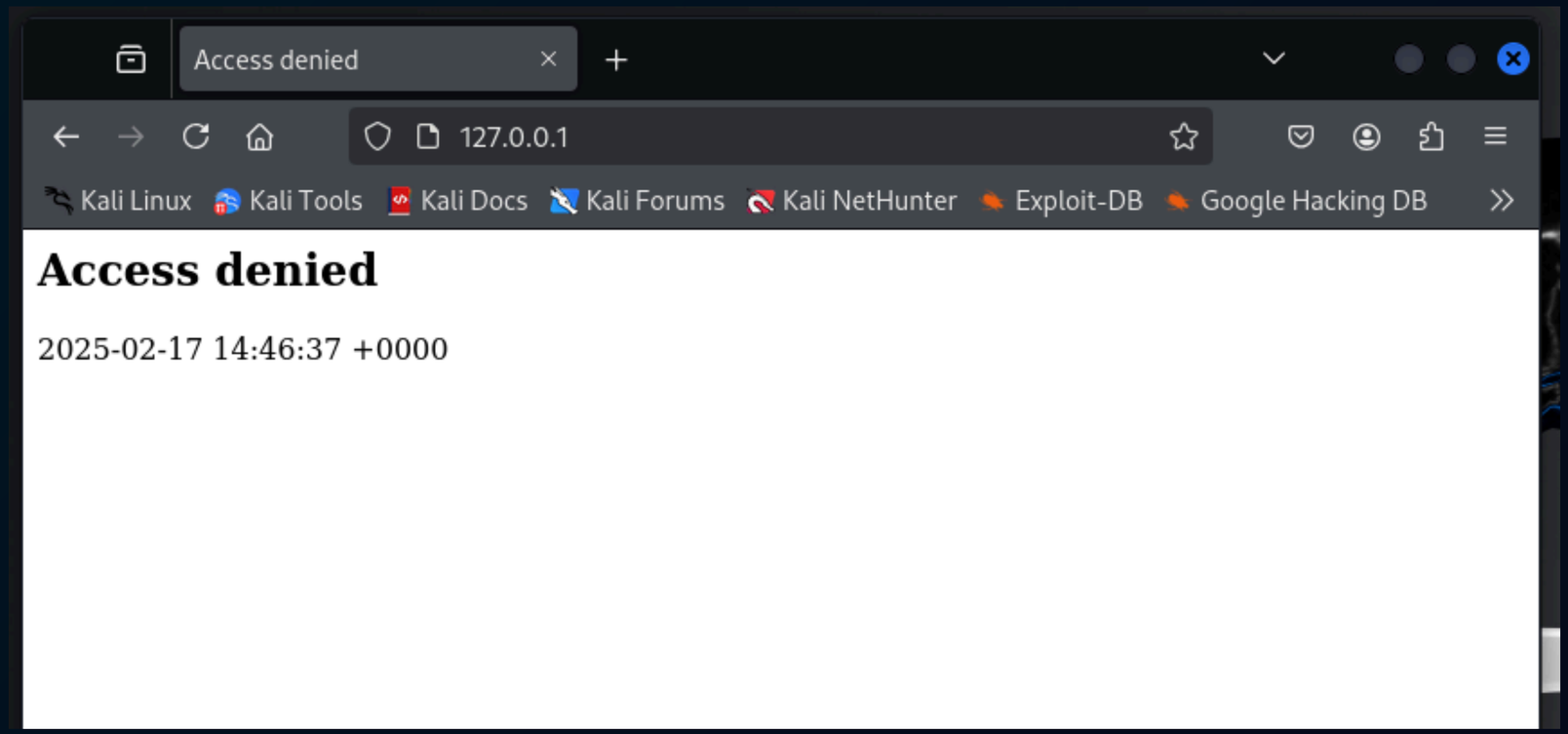
Here we can choose 1 for auto configuration this will be fast or we can choose 2 for manual configuration. Manual configuration contains more options but it is for advanced users.



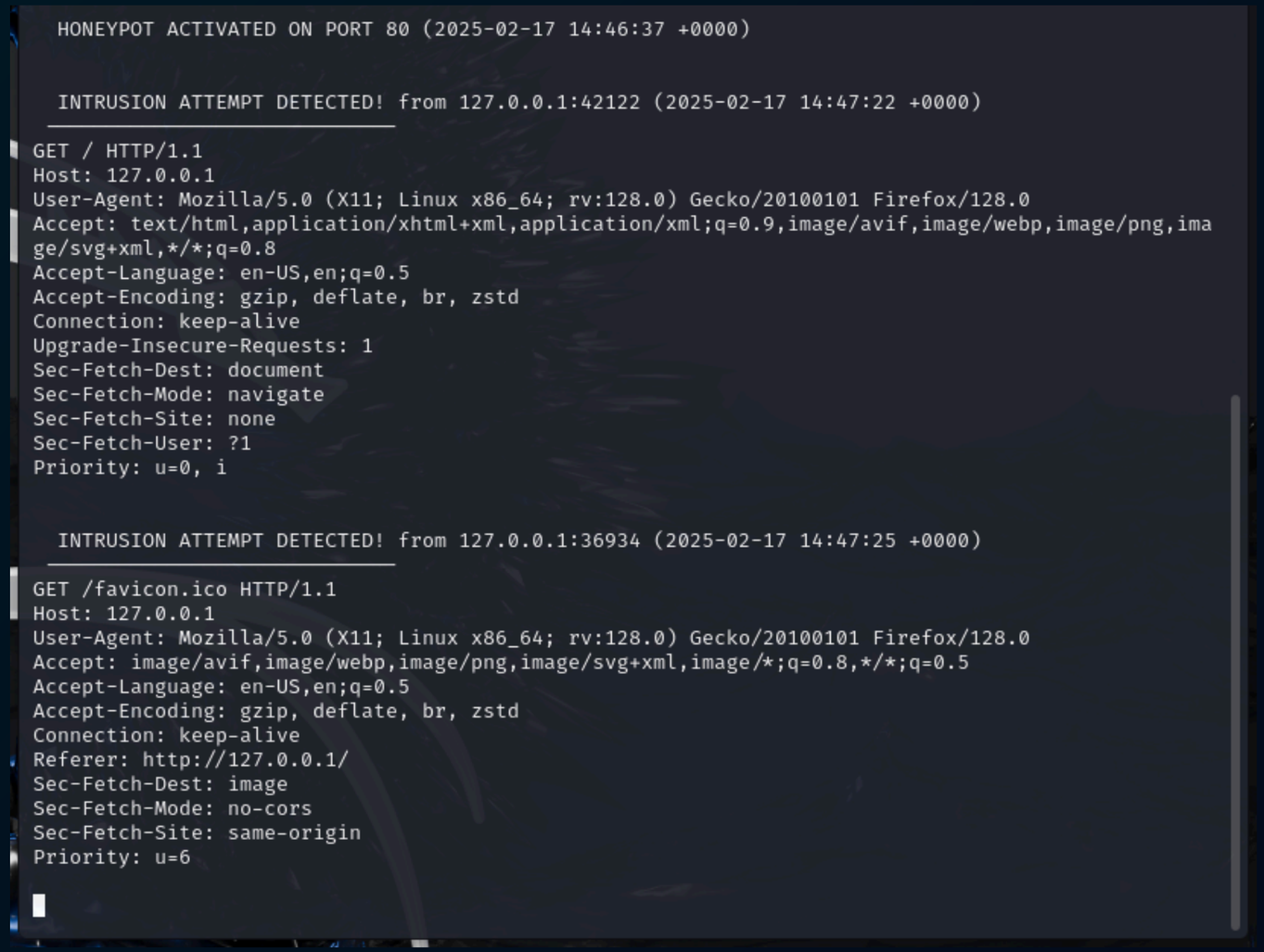
METHODOLOGY/DEMONSTRATION

Now we can see that we have successfully run honeypot in our localhost on port 80. To check how it works we can go to browser and check our localhost that is 127.0.0.1:80 and then check in the terminal where we started honeypot

```
HONEYPOT ACTIVATED ON PORT 80 (2025-02-17 15:01:37 +0000)
```



METHODOLOGY/DEMONSTRATION



RESULTS

1. PentBox Setup & Execution:
    - Successfully installed and executed PentBox 1.8 on Kali Linux.
    - Launched Honeypot on Port 80 to monitor incoming requests.
2. Intrusion Detection:
    - Multiple intrusion attempts were detected from 127.0.0.1, indicating simulated attack traffic.
    - Requests included HTTP GET for /favicon.ico and other standard HTTP headers.
3. Testing with Web Browser:
    - Successfully accessed 127.0.0.1:80 using Firefox, confirming that the honeypot was active and detecting traffic.
    - Detected User-Agent strings, signifying browser interactions.
4. File System & Execution Logs:
    - Navigated to the PentBox directory and executed the script.
    - Observed real-time logging of intrusion attempts.
5. GitHub Repository Cloning:
    - Cloned PentBox repository successfully for testing and setup.
    - Ensured that all files were intact and properly extracted.

CONCLUSION

In this project, we successfully deployed PentBox 1.8 Honeypot on Kali Linux to monitor network activity and detect potential intrusion attempts. The honeypot was activated on Port 80, and multiple unauthorized access attempts were logged, demonstrating its effectiveness in identifying suspicious activities. Through this experiment, we gained insights into network security monitoring, intrusion detection, and the importance of proactive cybersecurity measures. The results highlight how honeypots can be utilized for real-time threat analysis, helping organizations strengthen their network defenses. In the future, more advanced honeypots with AI-driven intrusion detection can be implemented to enhance security and automate threat response mechanisms.

THANK YOU