Honey Pot

Abstract

The purpose of this project was to design, implement, and execute a honeypot to enhance understanding of cybersecurity threats and defensive measures. A honeypot, a decoy system intended to attract and analyze potential cyber-attacks, was created using Pentbox. The objective was to simulate a vulnerable environment to study malicious activities and gather data on attackers' tactics, techniques, and procedures (TTPs).

The project aimed to achieve two key outcomes:

1. Threat Intelligence: Collecting actionable data on real-world attack methods, including IP addresses, timestamps, and attack vectors.
2. Skill Development: Enhancing practical knowledge of network security, logging, and forensic analysis.

The findings contribute to improving defensive strategies and raising awareness about the importance of proactive security measures. This project demonstrates the potential of honeypots in educational contexts and as tools for real-time monitoring in cybersecurity infrastructures.

What is a HoneyPot

A honeypot is a cybersecurity tool designed to attract, detect, and analyze malicious activity by simulating a vulnerable system or network. It serves as a decoy that mimics real systems, making it an attractive target for cyber attackers. The idea is to engage with attackers in a controlled environment to study their tactics, techniques, and procedures (TTPs) without risking actual assets or data.

Objectives of the Honeypot Project:

1. **Simulate a Vulnerable Environment:**
   To create a controlled, decoy system that mimics a real network or service, designed to attract and engage attackers.
2. **Collect Threat Intelligence:**
   To gather data on malicious activities, including attack methods, tools, IP addresses, and techniques used by potential attackers.

3. **Study Attacker Behavior:**
   To analyze how attackers interact with the honeypot, identifying patterns and understanding their tactics, techniques, and procedures (TTPs).

4. **Enhance Defensive Strategies:**
   To use the data collected from the honeypot to improve detection systems, hone security measures, and develop stronger proactive defense mechanisms.

5. **Skill Development and Practical Experience:**
   To gain hands-on experience with cybersecurity tools and techniques, such as honeypot deployment, network traffic analysis, and forensic investigation.

6. **Raise Awareness:**
   To highlight the importance of honeypots in real-time cybersecurity monitoring and threat intelligence gathering.

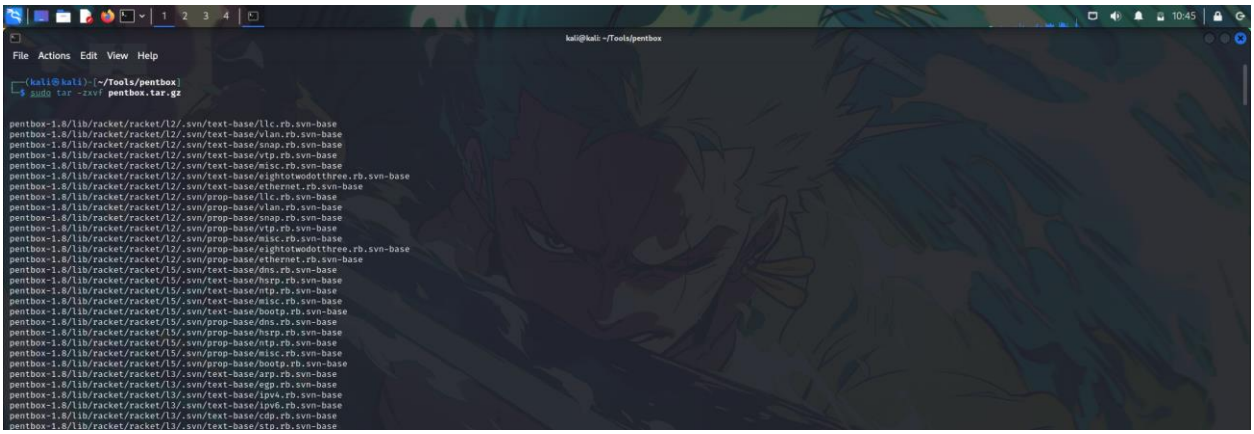
Steps to Deploy a Honey Pot

Step 1 :- Download a tool from github called **Pentbox**

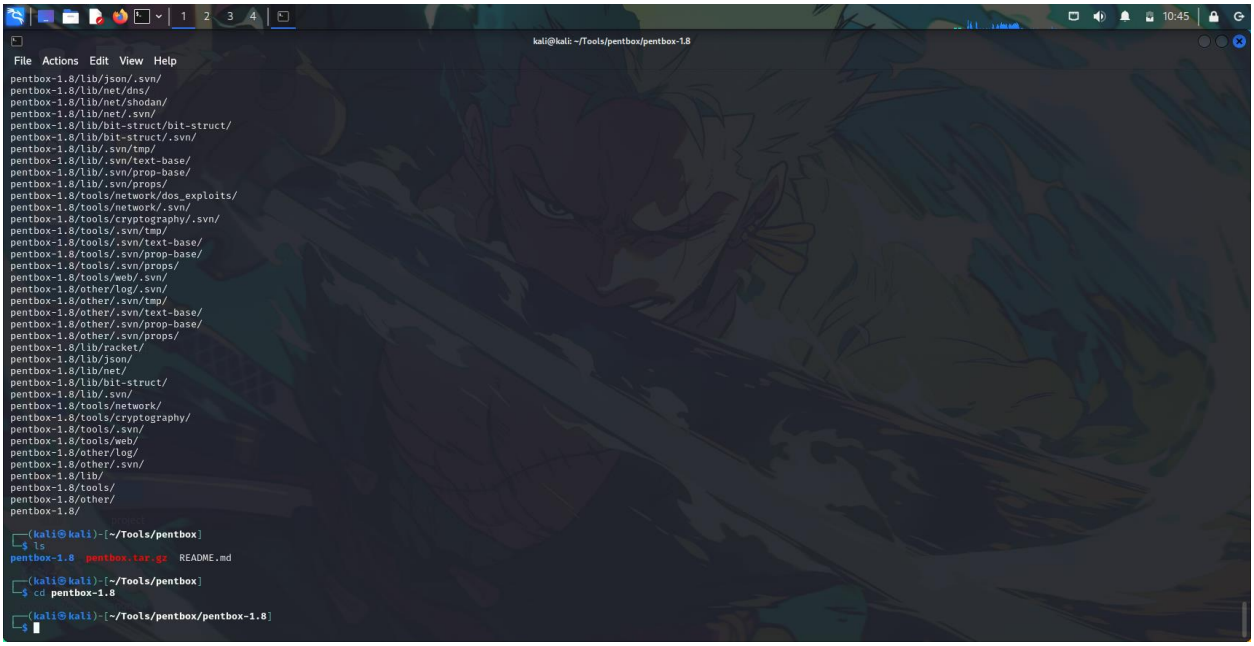
Step 2 :- Change into the Pentbox Directory

Step 3 :- Extract the Zip file of the Pentbox

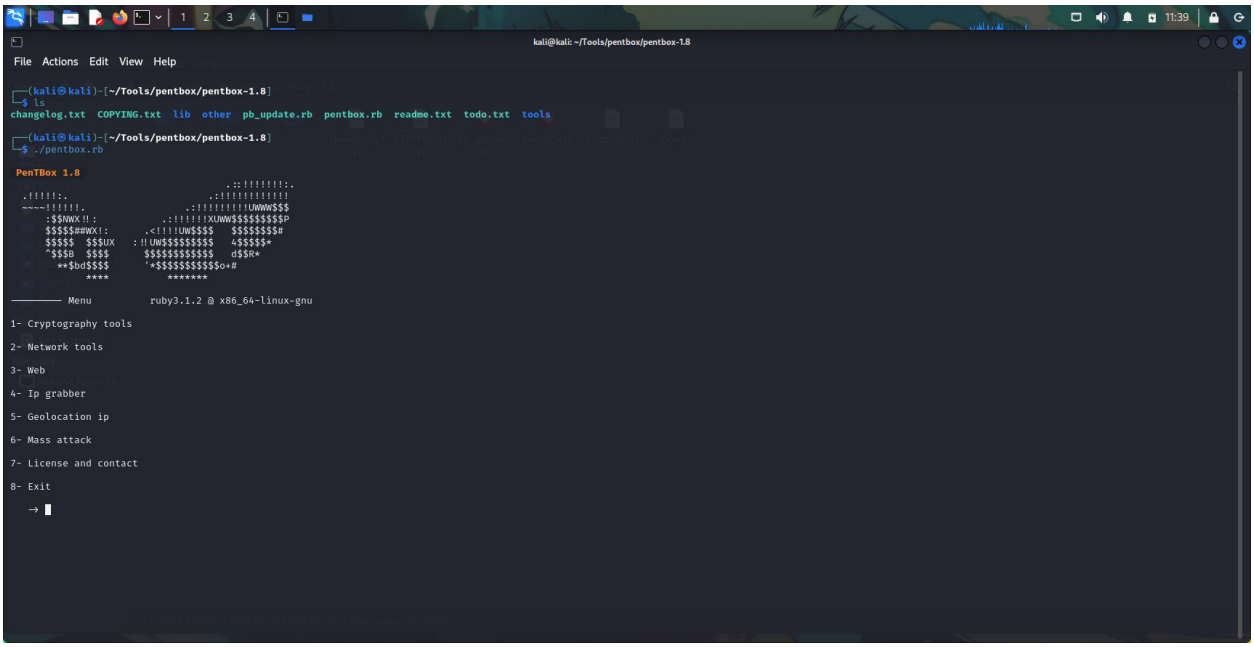
sudo tar -zxvf pentbox.tar.gz



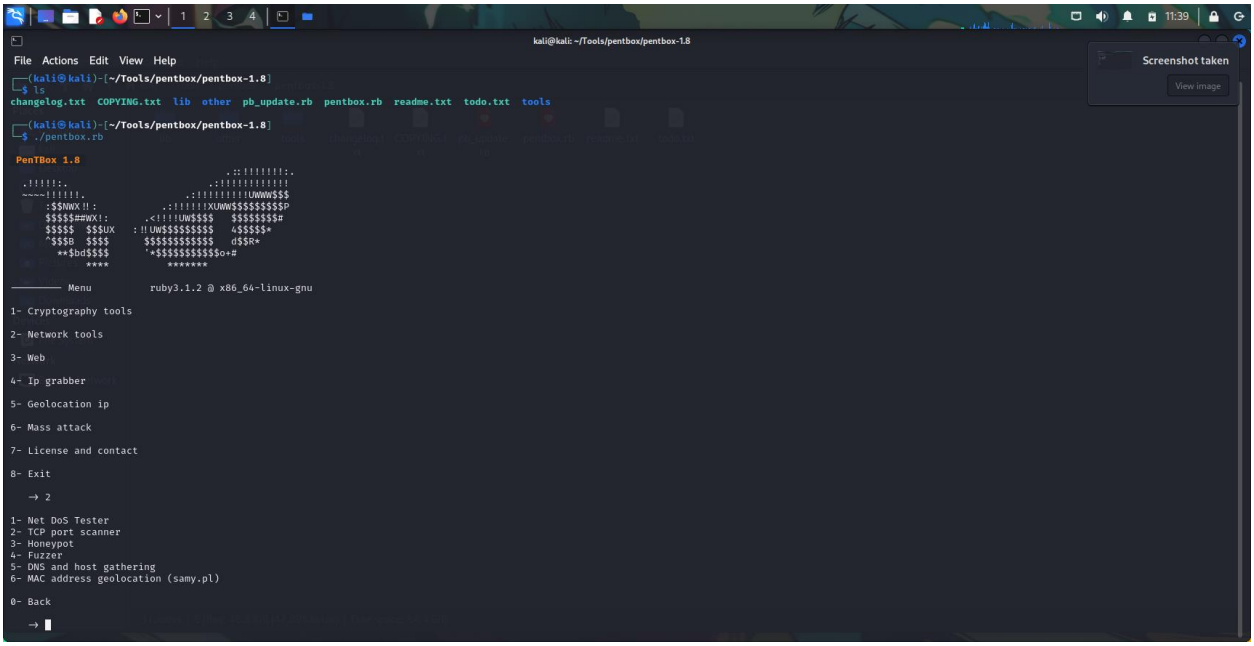
Step 4 :- Change the Directory to the Pentbox-1.8



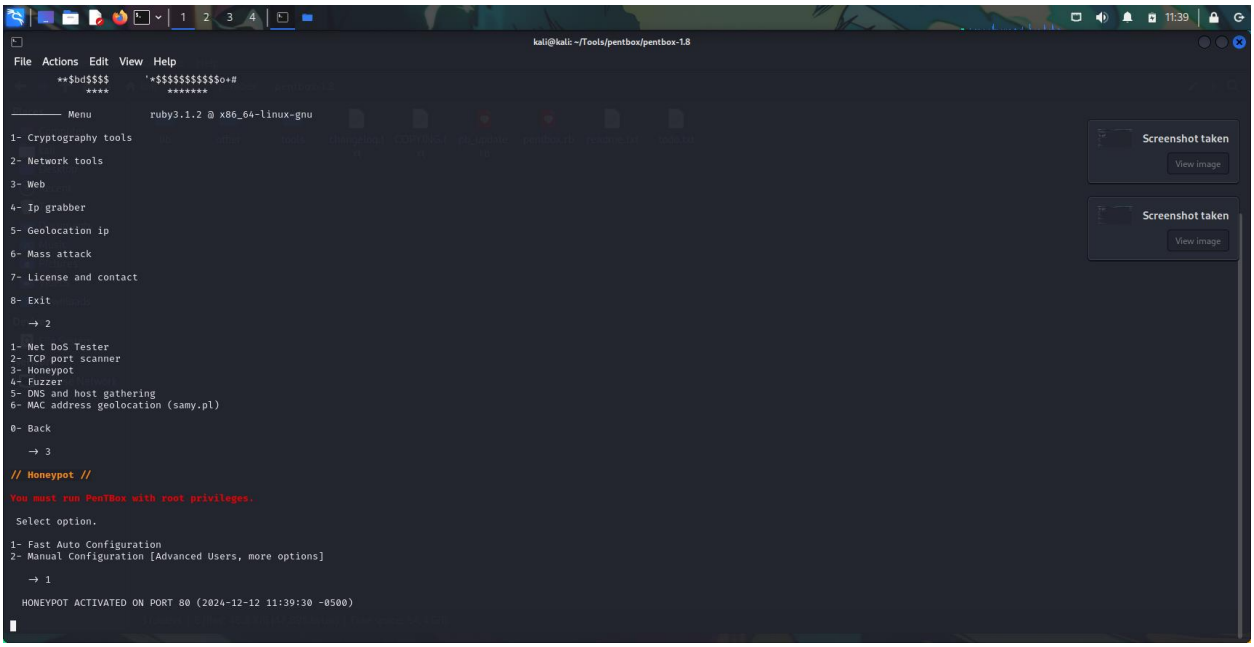
Step 5 :- Executing the Honey Pot



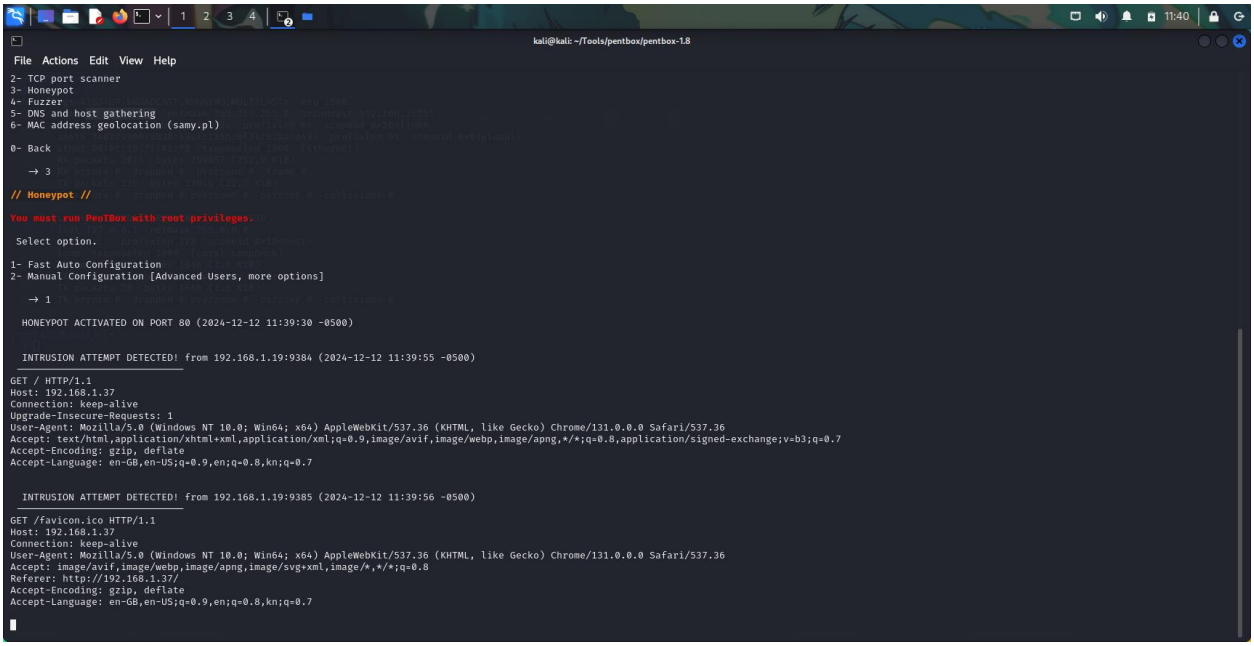
Step 6 :- Select the option 2 Network Tools



Step 7 :- Now Select the option 3 HoneyPot



Step 8 :- Wait for the attacker to attack and eventually we can get his information



Conclusion

The successful implementation and execution of a honeypot using Pentbox provided valuable insights into the nature of modern cybersecurity threats and attacker behavior. By simulating a vulnerable environment, the project effectively attracted and recorded malicious activity, enabling the collection of critical data such as IP addresses, attack methods, and interaction patterns.

The findings demonstrate the effectiveness of honeypots as tools for threat intelligence gathering and proactive defense. Additionally, the project highlighted the importance of monitoring and analyzing attacker behavior to strengthen overall cybersecurity measures.