Honeypot Server to Detect Attack Patterns

Name: Aiswarya S
Date: June 2025

Objective: Deploy a honeypot to simulate vulnerable services (like SSH), log attackers, and analyze patterns.

1. Introduction

A honeypot is a cybersecurity tool designed to mimic vulnerable systems or services. Its purpose is to attract malicious attackers, allowing defenders to monitor attack methods and gather intelligence. In this project, Cowrie honeypot was deployed to simulate an SSH service, logging unauthorized connection attempts and attacker behavior.

2. Abstract

This project demonstrates how Cowrie, an SSH honeypot, can be used to detect and analyze real-world attack patterns. The honeypot was installed on a Linux machine and configured to capture attacker interactions. Logs were analyzed to identify common attack sources, attempted credentials, and malicious activity.

3. Tools Used

- Kali Linux OS
- Cowrie Honeypot v2.6.1
- Python 3.13.2
- Twisted 25.5.0
- IP lookup tools: ipinfo.io, iplocation.net
- Terminal commands: cat, less, grep

4. Steps Involved

1. Installed Linux OS
2. Cloned Cowrie repository
3. Installed dependencies in Python virtual environment

4. Configured Cowrie to run on port 2222
5. Started honeypot and allowed it to run for 48 hours
6. Collected logs from `/home/amigo/cowrie/var/log/cowrie`
7. Analyzed attacker IPs and behaviors
8. Mapped IPs to geolocation using IP lookup tools
9. Compiled findings into this report

5. Findings

(Fill this section after you collect logs — here's a sample)

- Total unique attacker IPs: **7**
- Top countries of origin:
    - China (3)
    - USA (2)
    - India (1)
    - Russia (1)
- Most common usernames: `root`, `admin`, `test`
- Common passwords tried: `123456`, `password`, `admin123`
- Example attacker command: `uname -a`, `ls`, `wget malware.sh`
- Most active attack time: 2AM - 5AM UTC

6. Conclusion

Deploying the Cowrie honeypot provided valuable insights into real-world attack trends. The project demonstrated how attackers constantly probe open SSH ports with brute-force attempts. Honeypots are an effective tool for threat intelligence and enhancing cybersecurity posture.