Honeypot Server to Detect Attack Patterns

Introduction

Cybersecurity threats are increasing day by day, with attackers frequently targeting servers and networks using brute-force techniques. To analyse and defend against such threats, security researchers use honeypots, which act as decoy systems to attract attackers and study their activities. A honeypot records malicious attempts without putting real systems at risk. Among them, Cowrie SSH Honeypot is a widely used medium-interaction honeypot that simulates SSH services. It captures login attempts, executed commands, and attacker behaviour in detail, providing valuable insights. This data helps in identifying attack patterns, techniques, and malicious intentions. Through this project, Cowrie demonstrates how honeypots can enhance cybersecurity by offering. real-time threat intelligence and strengthening defence strategies.

Abstract

- This project implements the **Cowrie SSH Honeypot** to study malicious login attempts.
- Cowrie simulates an SSH environment to attract attackers and log their activities.
- It captures brute-force logins, executed commands, and attacker IP addresses.
- The collected data provides insights into attack patterns and hacker behaviour.
- These insights help improve cybersecurity defence strategies with real-time intelligence.

Tools Used

- Kali Linux
- Cowrie SSH Honeypot
- Python (for email & geo-location)
- GeoLite2 Database
- Gmail SMTP

Steps Involved in Building the Project

- **Setup Environment** – Prepare Kali Linux as the base system.
- **Install Dependencies** – Install Python and required packages.
- **Download & Install Cowrie** – Clone and configure the Cowrie honeypot.
- **Configure Cowrie** – Set up SSH simulation, ports, and logging.
- **Start the Honeypot** – Run Cowrie to emulate a fake SSH server.
- **Capture Attacks** – Record brute-force attempts, executed commands, and attacker IPs.
- **GeoIP2 Integration** – Use GeoIP2 database to identify attacker location from IP addresses.
- **Email Alert Integration** – Use a Python script to send attack details through email.
- **Analyse Logs** – Review log files for attack behaviour and patterns.

Conclusion

The **Cowrie SSH Honeypot** project successfully demonstrated how attackers attempt brute-force logins and execute malicious commands. By integrating **GeoIP2**. the project tracked attacker locations and provided valuable insights into global attack sources. The addition of **email alerts** ensured real-time monitoring of malicious activities. Overall, this project highlights the importance of honeypots in understanding attacker behaviour and strengthening cybersecurity defence strategies.