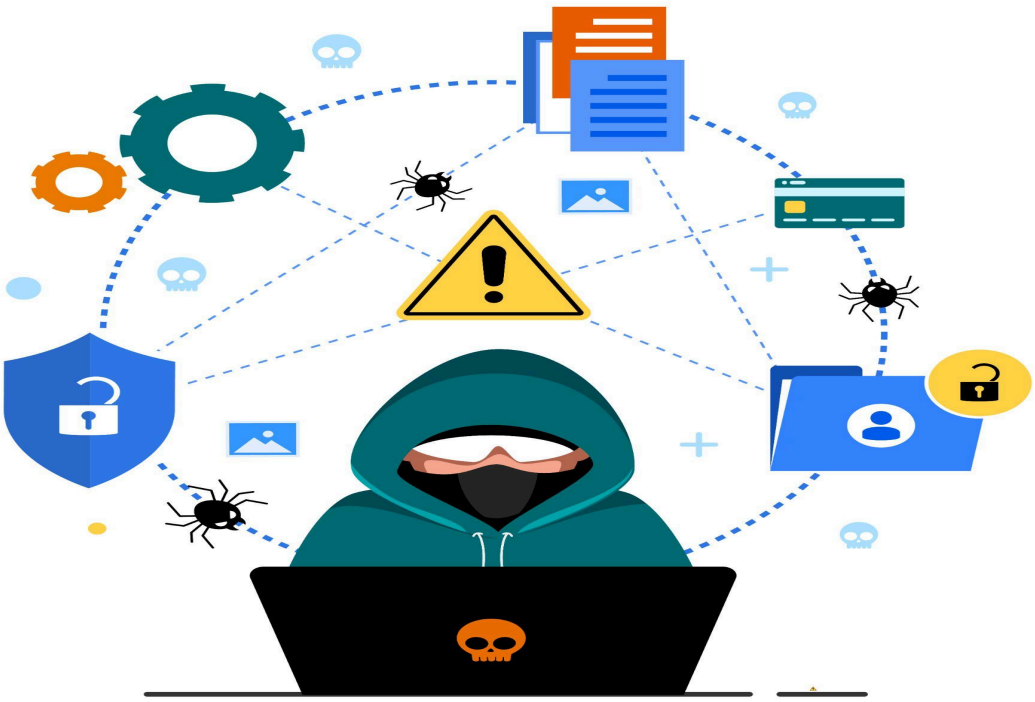
📄 PROJECT REPORT TITLE :

HONEYPOT SERVER TO DETECT ATTACT PATTERNS

🔐 **Cyber Security Mini Project**
📅 **Date: 15/07/2025**
👤 **Submitted By: Saurabh Rajendra Chavanke**
🏫 **Institute: Elevated LabS**



1🧭Introduction

🛡️A Honeypot is a security mechanism that simulates vulnerable services to lure attaker and study their behavior.
🎯The goal is to collect intelligence on attack patterns without compromising real system.Goal of high-interaction honeypot is to gain root–or administrator level– access to the server and then monitor the attacker'S activity.

2🎯 Objective

📎Simulate fake SSH/FTP services
📩 Log attacker attempt and commands
🔍 Analays repeated intrusion patterns
🚫 Block threats using fail2ban
🌏Visualize attacker IP geolocation

3🧰 Tools & Technologies Used

🔧 **Tool**	🔍 **Purpose**
🐍 Python	Scripting & automation
🐮Cowrie	SSH/FTP honeypot emulation
🚫fail2ban	Auto IP blocking
🌐MaxMind GeoIIP	IP Geolocation

4️⃣🧩 System Architecture

🌐Internet
↓
🚨Attacker IPs
↓
🗃️Log files + fail2ban Bans
↓
📈GeoIP + Data Analysis

5️⃣⚙️ Implemantation Steps

A) 🖥️ Deploy Honeypot on VM

— Installed Ubuntu on VirtualBox
— Set up Cowrie or custom python SSH server
— Enabled ports (22/21) for emulated services

B) 📩 Log Connection

—🌐IP Address
—💠Username tried
— 💻Command attempted

C) 🔍 Analyze Log Files

— Parsed logs with python script
— Detected brute-force patterns
— Counted top attacking IPs

D) 🚫 Block with fail2ban

— fail2ban setup to read logs
— Regex filters for Cowrie
— Auto ban via iptables

E) 🌍Visualize IP Geolocation

— Used GeoIP2 with IP logs
— created maps with folium

6️⃣📂 Sample Logs & Analysis

📊 Top 5 Attacking IPs:

🌐IP Address	🔁Attempts
102.22.34.55	48
185.234.123.10	33
182.75.65.20	25
196.52.20.18	19
203.0.113.77	17

7️⃣🗺️ IP Geolocation Map

🌍 Using folium, attacker IPs were plotted
🧭 Red markers = High threat
🟡 Yellow = Medium
🟢 Green = Low

🚀🔗 References

— 🐮 Cowrie: https://github.com/cowrie/cowrie
— 🔐 fail2ban: https://www.fail2ban.org
— 🌍 MaxMind: https://www.maxmind.com
— 📘 Python Docs: https://docs.python.org