HONEYPOT MONITORING SYSTEM

Name : Ena Luhadia

Enrollment Number : 0827CS221089

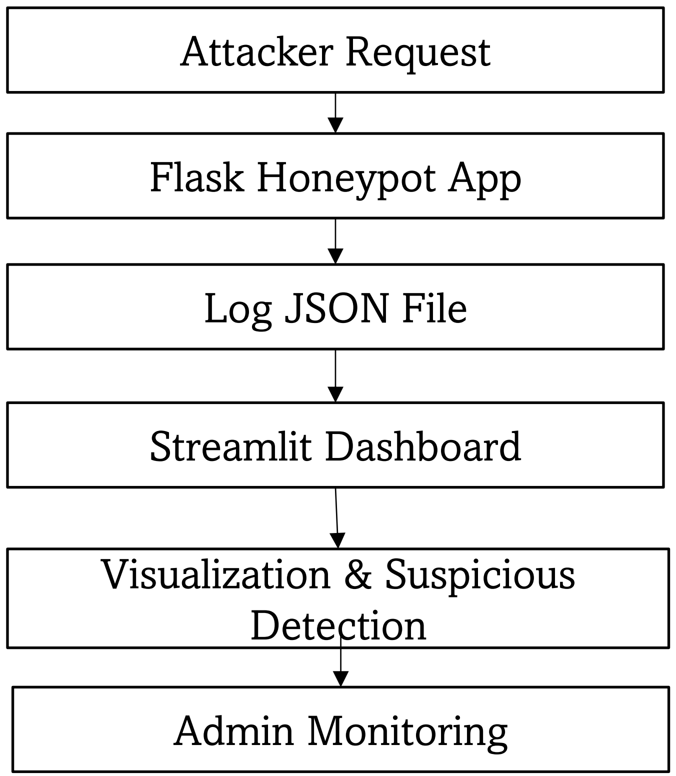
OBJECTIVE

- Capture and analyze suspicious traffic
- Detect potential attacks and intrusions early
- Provide real-time monitoring of requests
- Help understand attacker behavior and techniques
- Build a foundation for cybersecurity awareness

WORKFLOW

1. Attacker/User sends request to Honeypot
2. Flask app logs the request into JSON log file
3. Logs are continuously stored with timestamp, IP, method, and request details
4. Streamlit dashboard reads and visualizes the logs
5. Suspicious activity is flagged and highlighted
6. Admin monitors traffic patterns & suspicious requests in dashboard

FLOWCHART



Attacker Request

Flask Honeypot App

Log JSON File

Streamlit Dashboard

Visualization & Suspicious Detection

Admin Monitoring

DASHBOARD FEATURES

- Total Requests & Unique IPs
- Suspicious vs Normal Traffic (Pie Chart)
- Requests by Method (Bar Chart)
- Top Attacking IPs (Bar Chart)
- Expandable Raw Logs

CONCLUSION

- Successfully implemented a Honeypot Monitoring System
- Learned how to integrate Flask for logging & Streamlit for visualization
- Dashboard provides real-time insights into suspicious activity
- Can be extended with:
  - Alert notifications (Email/SMS)
  - Advanced attack classification (ML/NLP)
- Useful for cybersecurity training, research, and threat detection