PROJECT REPORT – CHAPTER 1 (DOCX ke liye)

Chapter 1 – Introduction

1.1 Background

The growing number of cyber threats poses severe risks to organizations. Attackers exploit misconfigurations, weak passwords, and exposed services to gain unauthorized access. Traditional defenses like firewalls and antivirus are reactive and often insufficient against advanced attackers. Honeypots, by contrast, act as decoys designed to attract malicious activity, enabling defenders to observe attacker strategies in a controlled environment.

1.2 Motivation

Understanding adversary behaviour is critical for improving detection and response. SIEM systems aggregate and correlate logs but often lack direct insights into attacker tactics. By integrating honeypots with a SIEM, organizations gain real-time, high-fidelity attack intelligence that enhances situational awareness and supports proactive defense.

1.3 Aim & Objective

The aim of this project is to build a custom honeypot and integrate it with a SIEM solution for real-time monitoring and analysis. The objectives are:

- To develop a lightweight honeypot simulating vulnerable services.
- To capture and log attacker telemetry such as connection details and commands.
- To integrate logs into the ELK Stack for analysis and visualization.
- To design dashboards that highlight attacker IPs, attempted credentials, and activity patterns.

1.4 Scope of Project

The scope includes developing the honeypot, integrating it with ELK Stack, and visualizing attacker data. The system will initially cover SSH and HTTP services, with the possibility to extend to other protocols. The project will demonstrate real-world attack monitoring and can serve as a foundation for advanced threat intelligence research.

1.5 Project Deliverables

- Python honeypot source code.
- Log forwarding configuration (Filebeat/Logstash).
- Kibana dashboards for visualization.
- Documentation (synopsis, project report).