LAB_5

1. Identify Assets in the Online Banking System

ANS: Key assets in an online banking system include:

- **Customer Accounts**: Bank account numbers, balances, personal data.
- **Authentication System**: Login credentials, session tokens, OTPs.
- **Transaction Processing System**: Handles fund transfers, bill payments.
- **Banking APIs**: Facilitates interactions with third-party services.
- **Core Banking System**: Stores financial transactions, user records.
- **Communication Channels**: Web interfaces, mobile apps, SMS, email.

2. Identify Threats Using STRIDE

ANS:

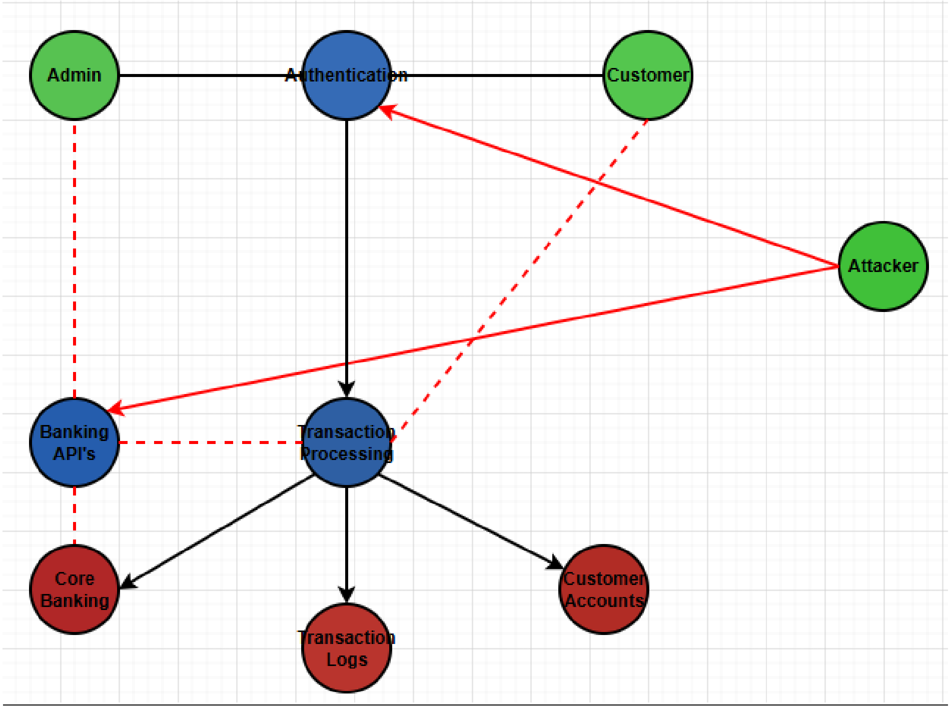
STRIDE Category	Threat Description	Affected Asset
Spoofing	Attackers impersonate legitimate users using stolen credentials (phishing, credential stuffing).	Authentication System
Tampering	Unauthorized modification of transactions (e.g., altering transfer amounts, modifying payee details).	Transaction Processi System
Elevation of Privilege	A regular user exploits vulnerabilities to gain admin access.	Authentication System, Core Banking System
Information Disclosure	Leakage of sensitive data (e.g., account balances, personal info) due to weak encryption or insider threats.	Customer Accounts, APIs

Repudiation	Users deny perform certain transactions, causing disputes.	Transaction Logs, Core Banking System
Denial of Service (DoS)	Attackers flood the banking server with fake requests, making it unavailable.	Web & Mobile Banking Services

3. Attack Vectors & Mitigation Strategies
   ANS:

Attack Vector	Possible Threats (STRIDE)	Mitigation Strategies
Privilege Escalation via API Misuse	Elevation of Privilege	Implement Role-Based Access Control (RBAC), monitor API logs.
SQL Injection	Tampering, Information Disclosure	Use parameterized queries, validate inputs
DDoS Attack on Banking APIs	Denial of Service	Deploy rate-limiting, Web Application Firewalls (WAF).
Session Hijacking	Elevation of Privilege, Spoofing	Implement secure cookie attributes, session expiration policies.
Phishing Attacks	Spoofing	Implement MFA, educate users on phishing awareness.
Man-in-the-Middle (MITM)	Information Disclosure	Enforce HTTPS, use TLS encryption

4. Threat Model Diagram



- Blue - Processes
- Red - Data Stores
- Red Arrow – Threat Paths (STRIDE)
- Green – Entites