Scope

1. **Target System**
   - **Public-Facing Systems:** Bank's customer portal, mobile application, public website, and associated APIs.
   - **Internal Systems:** Employee email systems, intranet portals, and sensitive databases (e.g., customer records, transaction logs).
   - **Physical Security:** Simulated attempts to access restricted areas such as server rooms or employee workstations (if included in scope).
2. **Objective**
   - Simulate a real-world cyberattack to assess:
     - Vulnerabilities in digital infrastructure.
     - Security gaps in employee awareness and internal controls.
     - The effectiveness of the Blue Team's detection and response capabilities.
   - Ensure the operation remains ethical and adheres to defined rules of engagement, avoiding disruption to live systems or customer data.

Engagement Phases

1. **Planning Phase**
   - **Objective:** Define the approach, rules, and expected outcomes.
   - **Key Actions:**
     - Obtain management approval and clarify the scope, ensuring all exclusions are documented (e.g., live transaction systems).
     - Establish a communication plan to avoid conflicts during the operation.
     - Develop attack scenarios aligned with the bank's infrastructure and threat model (e.g., insider threats, external cyberattacks).
2. **Execution Phase**
   - **Objective:** Conduct simulated attacks while adhering to the agreed scope.
   - **Key Actions:**
     - **Reconnaissance:**
       - Collect information about the bank's systems, network architecture, and employees.

            - Identify publicly exposed endpoints, subdomains, and third-party integrations.
        - **Initial Access:**
            - Simulate phishing campaigns targeting employees or clients.
            - Exploit misconfigured systems or publicly known vulnerabilities (if approved).
        - **Privilege Escalation:**
            - Explore ways to gain higher access (e.g., admin accounts, sensitive databases).
            - Test weak permissions or poorly secured internal resources.
        - **Lateral Movement:**
            - Move through the network to access high-value systems (e.g., transaction databases).
            - Simulate accessing sensitive data or systems without triggering detection mechanisms.
        - **Exfiltration Simulation:**
            - Identify potential data exfiltration paths and document findings without actual data transfer.

3. **Reporting Phase**
    - **Objective:** Provide detailed insights into vulnerabilities, attack pathways, and defensive recommendations.
    - **Key Deliverables:**
        - **Executive Summary:** High-level overview of findings and their business impact.
        - **Technical Report:** Detailed breakdown of each phase, vulnerabilities exploited, and the impact of attacks.
        - **Recommendations:** Actionable steps for remediation, such as patching vulnerabilities, improving detection systems, and employee training.

Identifying Potential Attack Vectors (No Tools)

1. **Reconnaissance:**
    - Review the bank's public website for exposed data or misconfigurations.

   - Examine API documentation and look for endpoints that may allow unauthorized actions.
   - Analyze employee habits (e.g., weak email practices) through social media or professional networking platforms.

2. **Initial Access:**
   - Email phishing targeting employees with financial privileges or administrative access.
   - Exploit insecure login portals (e.g., password reuse, weak authentication policies).
3. **Privilege Escalation:**
   - Identify shared credentials or weak password policies for privileged accounts.
   - Exploit system misconfigurations, such as overly permissive file shares or admin tools left exposed.
4. **Lateral Movement:**
   - Use compromised accounts to move to sensitive systems, such as transaction databases or internal communications platforms.
5. **Data Exfiltration:**
   - Identify potential exfiltration paths, such as unsecured email attachments or cloud storage misconfigurations.
