Project 3: "Red Team Operations and Simulated Attack"

Objective: Conduct a simulated attack on a network environment using red team methodologies to test incident response capabilities.

Week 1: Planning and Reconnaissance

- **Task**: Develop a red team engagement plan, define attack scenarios, and gather intelligence on the target environment.
- **Deliverables**: Engagement plan, reconnaissance report, defined attack scenarios.

Week 2: Initial Compromise and Pivoting

- **Task**: Exploit initial vulnerabilities to gain access, escalate privileges, and pivot within the network.
- **Deliverables**: Screenshots and documentation of successful exploitation, privilege escalation, and lateral movement.

Week 3: Maintaining Access and Persistence

- **Task**: Deploy backdoors, schedule tasks, and maintain access without detection.
- **Deliverables**: List of persistence mechanisms, evidence of undetected presence.

Week 4: Reporting, Security Posture Improvement, and Presentation

- **Task**: Provide a detailed report of findings, including simulated attacker behavior and recommendations for improving the security posture. Prepare a presentation to summarize the engagement.
- **Deliverables**: Red team engagement report, improvement plan for incident response and defense strategies. **Final presentation** summarizing the attack scenarios, findings, and recommendations.