**Initial Report**

Project 1: Conducting a Man-in-the-Middle (MITM) Attack and Privilege Escalation

Name: Elif Öztoprak ID: 6715930083

**Definition:**

To perform a Man-in-the-Middle (MITM) attack to intercept sensitive data like Session IDs, cookies or login credientials. With the sensitive captured credentials ecalate priviliges of the root in the system, extract password files and crack with pasword cracking tool. The project will provide insights into network vulnerabilities, techniques for exploitation, and mitigation strategies.

**Tools to be used:**

* Wireshark: For packet capturing and analysis.
* Metasploit: To exploit system vulnerabilities.
* John The Ripper (or Jumbo-John): To crack password hashes.
* Ettercap: To conduct MITM attack.
* Kali Linux: Platform to penetration testing tools.

**Steps:**  
 **Preparation Phase:**

1. Metasploit settings:
   1. Set up Metasploit as the target machine.
   2. Configure a safe network environment
2. Setup of Kali Linux
   1. Use Kali as the attacker’s machine.
   2. Install the necessary tools as Wireshark, John the Ripper, Ettercap.
3. Check communication:
   1. Check if both the machines can communicate via ping.

**Phase 1:**

1. Start capturing the network traffic via Wireshark:
   1. Select the corresponding network interface and start capturing
2. Apply filters:
   1. Use Wireshark filters to isolate HTTP traffic or any other protocol needed.
3. Analyze traffic:
   1. Look for sensitive information like login credentials or session cookies.

**Phase 2:**

1. Initiation of MITM
   1. Run Ettercap in graphical mode.
   2. Select target machines.
   3. Perform ARP spoofing to intercept traffic.
2. Intercept and analyze**:**
   1. Monitor and manipulate captured traffic via Ettercap.

**Phase 3:**

1. Leverage Captured Credentials:
   1. Use accessed credentials to log in to Metasploitable.
2. Privilege Escalation:
   1. Identify the vulnerabilities on the system to gain privilege escalation.
3. Extract Password Files:
   1. Locate and copy /etc/shadow and /etc/passwd files.
4. Crack located passwords:
   1. Use John the Ripper to crack the hashed passwords.