# 🔐 Exam Simulation Plan — SSI Lab

## 1. Linux Permissions (Basic and ACLs):

📄 **Exam Task:**

**Scenario:**

Company *TechCorp* has 7 users. Each user belongs to one of two departments:

- Group **G1**: alice, bob, charlie
- Group **G2**: dave, eve, frank

All users should have **read & execute** access to a shared directory “Common”.

Each group has its own folder:

- G1_Data: Full access for G1 members, no access for others.
- G2_Data: Read-only for G2 members, no access for others.

Specific ACL rules:

- User admin (not part of G1 or G2) should have **read+write** access to both group folders.
- User eve should have **execute-only** access to G1_Data.

Set ownerships and permissions accordingly.

## 2. Documentative Firewall Table:

📄 **Exam Task:**

1. Block all HTTP access from host 192.168.0.3 to host 192.168.0.7.
2. Allow **only** Telnet traffic (TCP port 23) from LAN1 (192.168.1.0/24) to LAN3 (192.168.3.0/24). Drop everything else between those subnets.
3. Block all DNS requests from 192.168.2.100 to **any** server.
4. Allow HTTPS (port 443) from any LAN device to external IP 10.10.10.10.

## 3. OpenSSL Encryption/Decryption Tasks:

📄 **Exam Task:**

1. Encrypt a file named secret.txt using AES-256 and password CyberLab2025.
2. Decrypt the encrypted file.
3. Generate SHA256 checksum of report.pdf.
4. Create a public/private RSA key pair.
5. Encrypt report.txt with the **public key**.
6. Decrypt the encrypted file with the **private key**.
7. Digitally sign report.txt using your **private key**.
8. Verify the signature using your **public key**.

## 4. OpenVPN Infrastructure:

📄 **Exam Task:**

1. Set up a VPN infrastructure using OpenVPN solution.
2. Use certificate-based authentication.
3. Use one Root CA, one Server and one Client.
4. Generate small keys in order to improve generation time.
5. Implement appropriate configurations for both Server and Client.
6. Start the VPN service and connect the VPN Client to the VPN Server.
7. Test that the PING operation is functioning in the VPN environment.

## 5. Python & Scapy — Packet Sniffing Scenario:

📄 **Exam Task:**

1. Intercept all incoming SYN packets to your host that target port 80 (HTTP) or 443 (HTTPS).
2. Display the source IP and destination port of each matching packet.
3. Implement this solution in Python with Scapy.