# ISC2 CC Home Lab practice (Incomplete)

## Security Principles

- Create a Miro diagram of your home lab's network mapped to OSI layers to understand layered security
- Understanding and applying types of authentication on linux vm (single-factor, multi-factor, etc.)
- Simulate an unpatched Linux service and choose a response based on risk tolerance (patch, isolate, or accept)

## Incident Response, Business Continuity & Disaster Recovery

- Create and test scheduled backups of virtual machines or files
- Simulate a system failure and restore from snapshot or backup
- Set up two VMs (Apache/Nginx) and simulate a failover scenario
- Write a Business Continuity or Disaster Recovery Plan
- Create an Incident Response Template covering detection, containment, eradication, recovery, and lessons learned
- Simulate a phishing attack using a dummy/local mail server and respond using an incident response plan

## Access Control Concepts

- Create IAM policies in a cloud environment (AWS Free Tier or GCP)
- Set up a local SFTP server with restricted user/group access
- Change the default SSH port and disable root login on a Linux server
- Set up MFA for Linux using Google Authenticator or PAM
- Create Linux user accounts with role-specific permissions to simulate segregation of duties
- Configure least-privilege access and validate permission boundaries

## Network Security

- Capture and analyze a TCP handshake using Wireshark

- Register or use a domain and point it to a web server running on a VM
- Set up HTTPS using Let's Encrypt or a similar certificate authority
- Harden SSH by changing the default port, disabling root login, and enabling key-based authentication
- Set up pfSense and configure VLANs to segment traffic between different use cases
- Simulate network scans (rustscan /nmap) or basic attacks from Kali Linux and observe the impact via logs

## Security Operations

- Write an Acceptable Use Policy (AUP) for a fictional company
- Write a security policy that references a standard and is enforced via a documented procedure (e.g., strong passphrase policy)
- Deploy Wazuh a SIEM
- Forward logs from Linux and Windows systems to your SIEM
- Create detection rules for failed logins, suspicious PowerShell usage, and reverse shell attempts
- Test alerting and log forwarding configuration
- Simulate a basic attack, detect it via SIEM, and document your findings in a report

**Note:** This is not a comprehensive list. These are selected hands-on tasks designed to help reinforce and apply key concepts from the ISC2 CC certification. The goal is to extend theoretical knowledge into real-world, practical experience.

Reach out via https://www.linkedin.com/in/alicha/ if you have any questions