**Empowering tomorrow’s leaders, today!**

# Capstone Project 1: Secure Enterprise Network Setup with Virtualisation & Monitoring

**Objective:**

Design, configure, and secure a mid-sized enterprise network including servers, storage, and virtual environments with basic automation and monitoring.

**Learning Outcomes**

By completing this project, you will be able to:

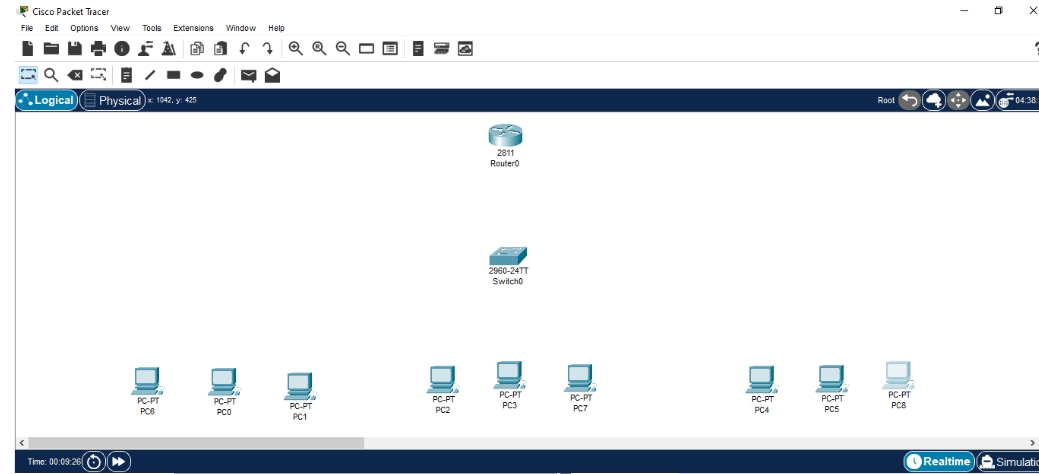
* Design network architecture using VLANs and subnetting.
* Install and configure Windows/Linux servers and storage arrays.
* Apply basic security principles and auditing tools.
* Create and manage VMs and Docker containers.
* Implement basic automation and monitoring.

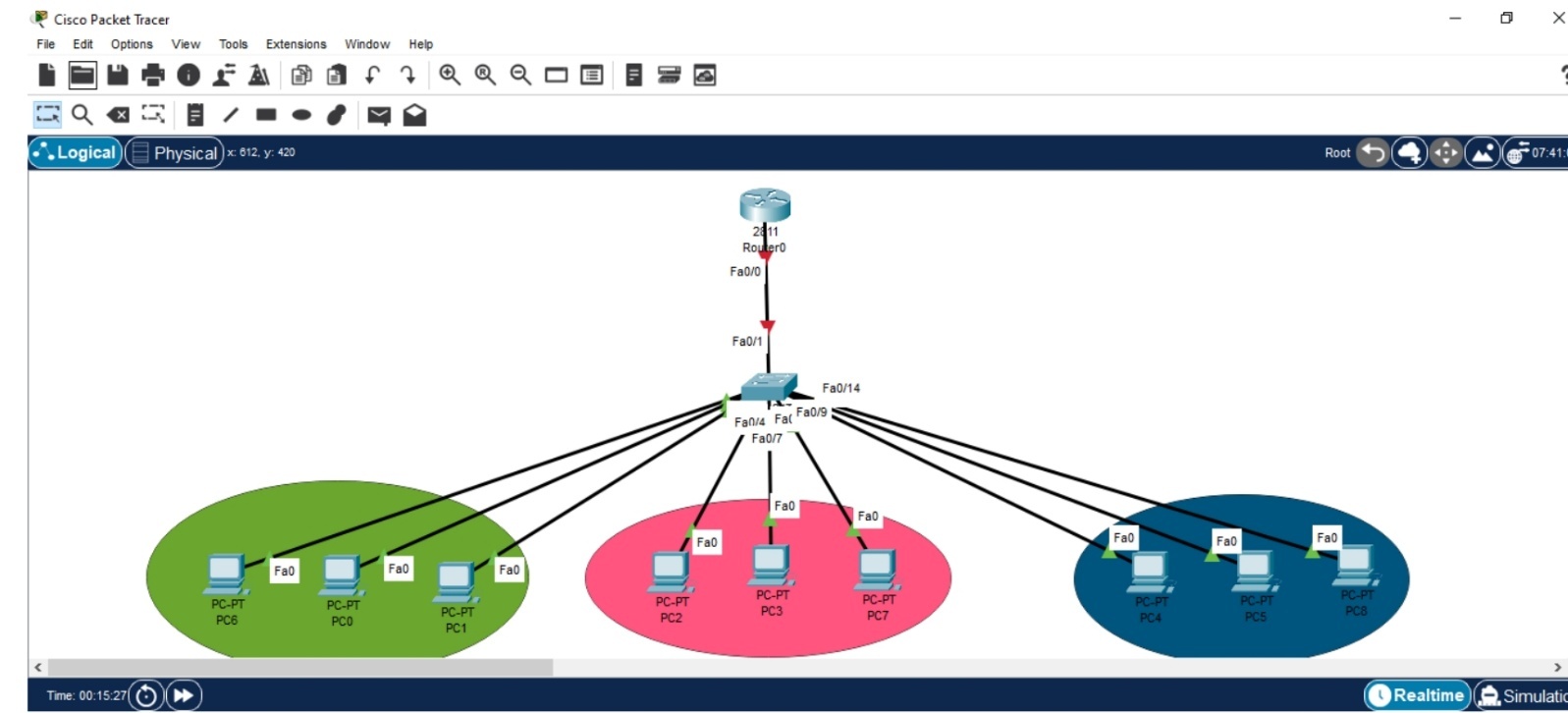
# Tasks

## 1. Network Design & Configuration

* 1. **Design a 3-segment VLAN network: Admin, Sales, and IT.**

1. Cisco 2811 Router (1)
2. Cisco 2960 switch (1)
3. End Device - PC (9)



STEP 1: Add Network Device

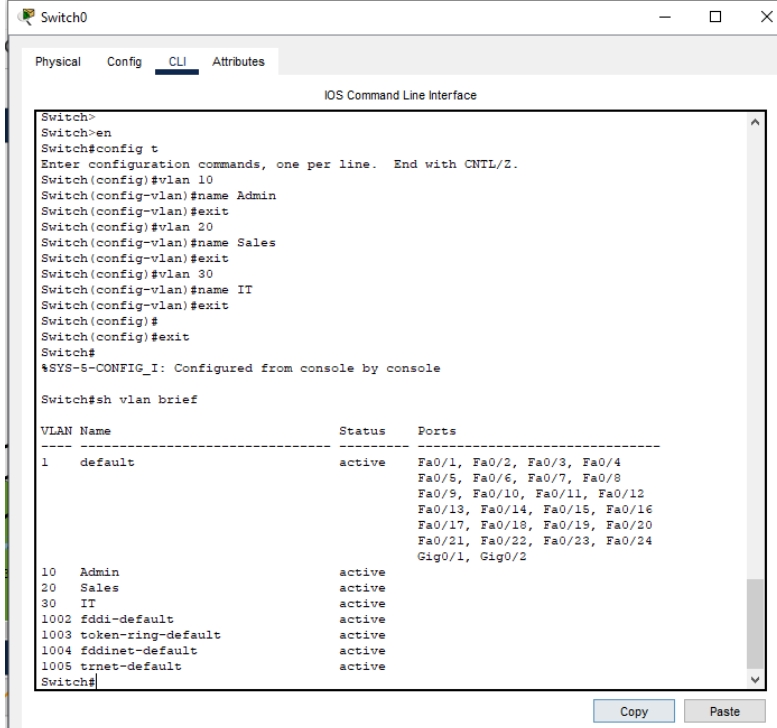
STEP 2: Connections Made

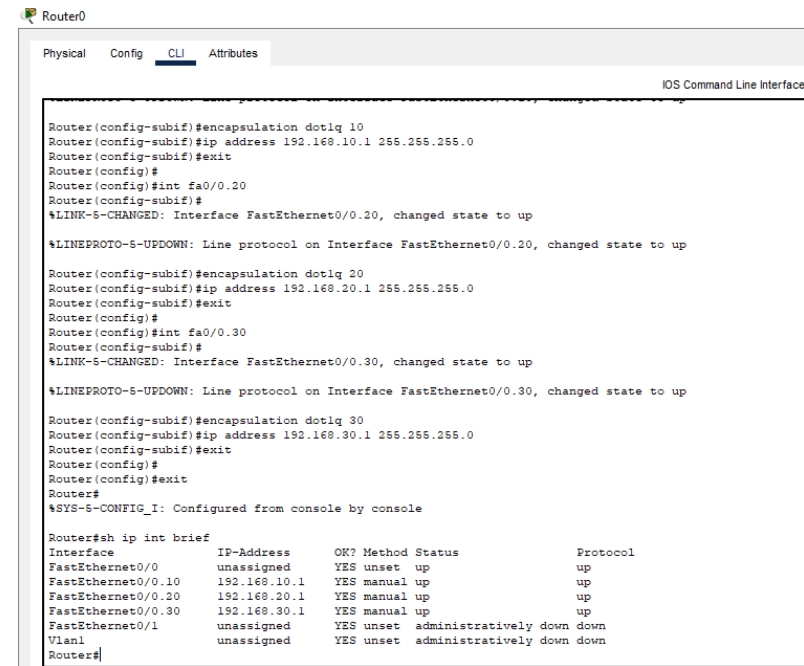
* 1. **Subnet each segment with CIDR.**
* Assign IP Addresses and Default gateways
* Determine IP Address Class and Subnetting

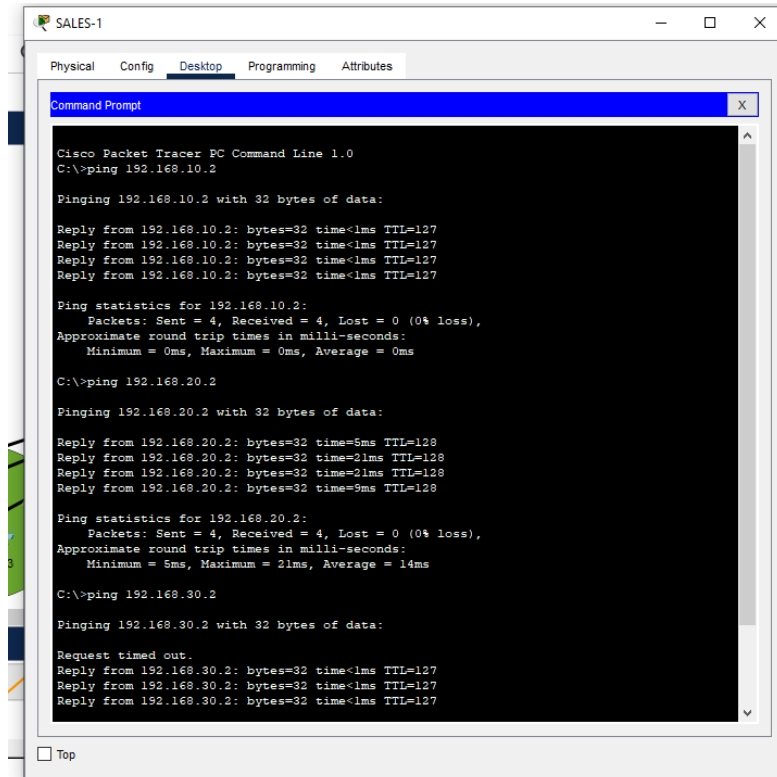
**VLAN 10 (Admin)**: 192.168.10.0/24

**VLAN 20 (Sales)**: 192.168.20.0/24

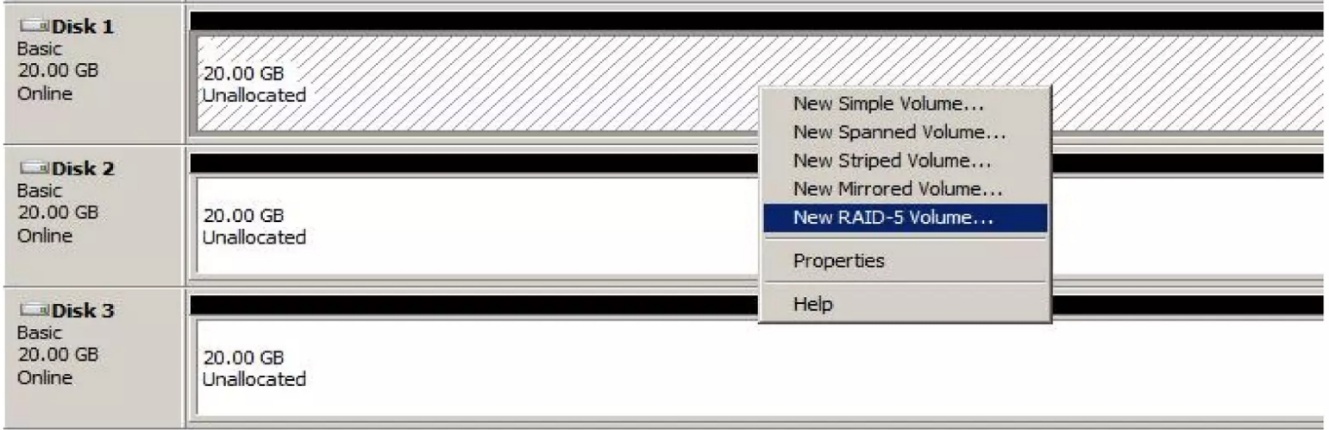
**VLAN 30 (IT)**: 192.168.30.0/24

* **VLAN 10 - Admin:** Default gateway: 192.168.10.1 Subnet Mask: 255.255.255.0
* **VLAN 20 - Marketing:** Default gateway: 192.168.20.1 Subnet Mask: 255.255.255.0
* **VLAN 30 - IT:** Default gateway: 192.168.10.1 Subnet Mask: 255.255.255.0
* Configure VLANs on switch
  1. **Implement basic routing between VLANs.**





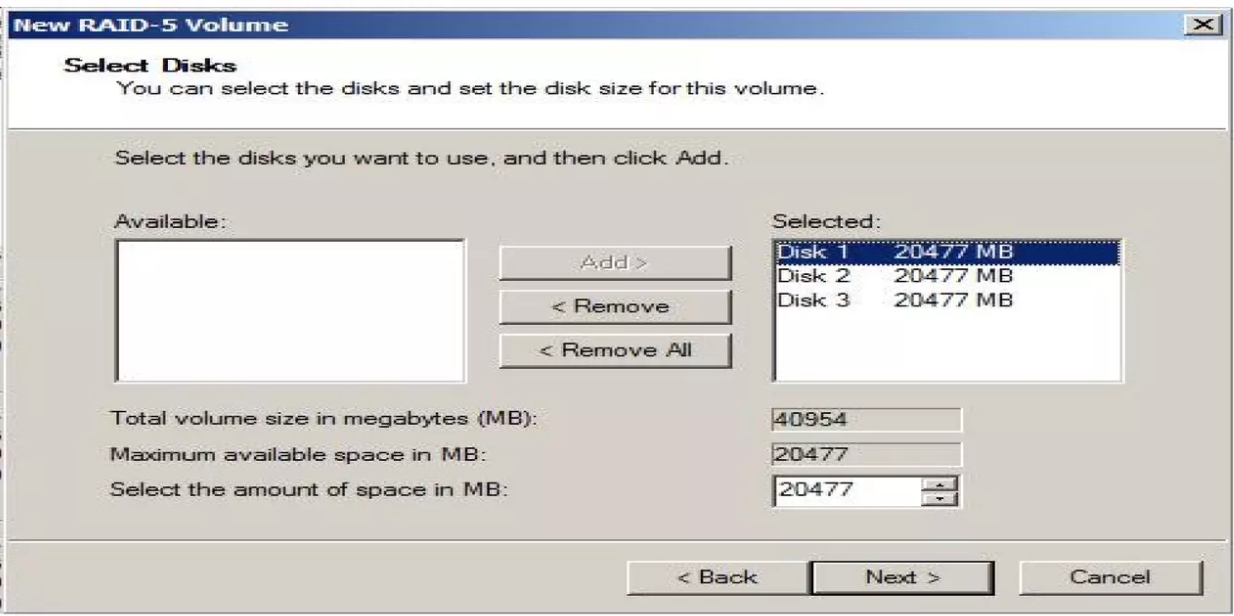
## 2. Server & Storage Setup

* Install a Linux (Ubuntu) and a Windows Server VM.
* Configure RAID 5 using virtual disks.
* To create a RAID 5 array open disk management. Right click the Disk 1 in the unallocated space and click New RAID 5 Volume option as shown below.

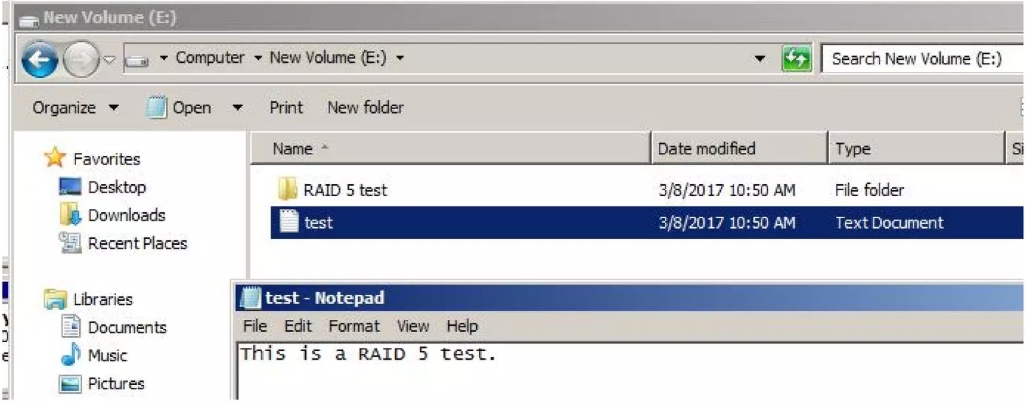
- On the next screen that is displayed, select Disk 2 and click Add.

- The Next button will not be enabled as RAID 5 requires minimum 3 hard disks.

- Thus select Disk 3 and click Add. The final view should be as shown below. Then click Next



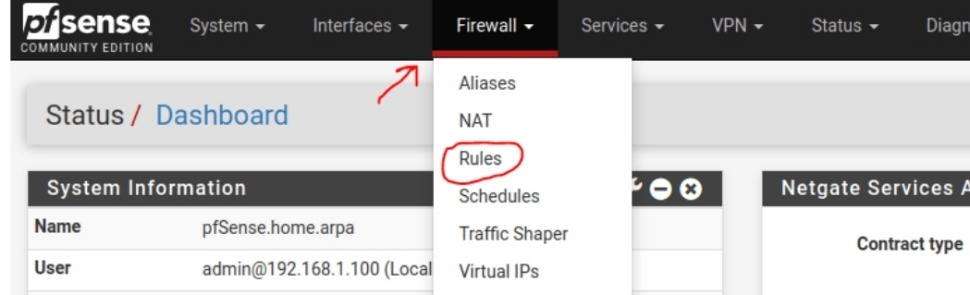
* Demonstrate file sharing between servers.

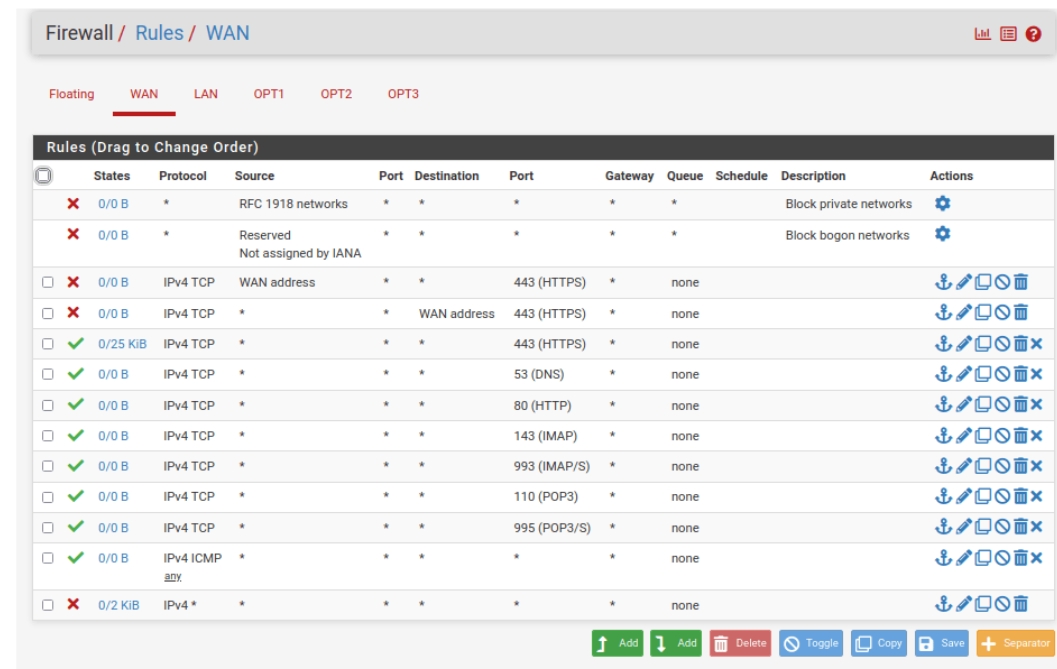


## 3. Security Implementation

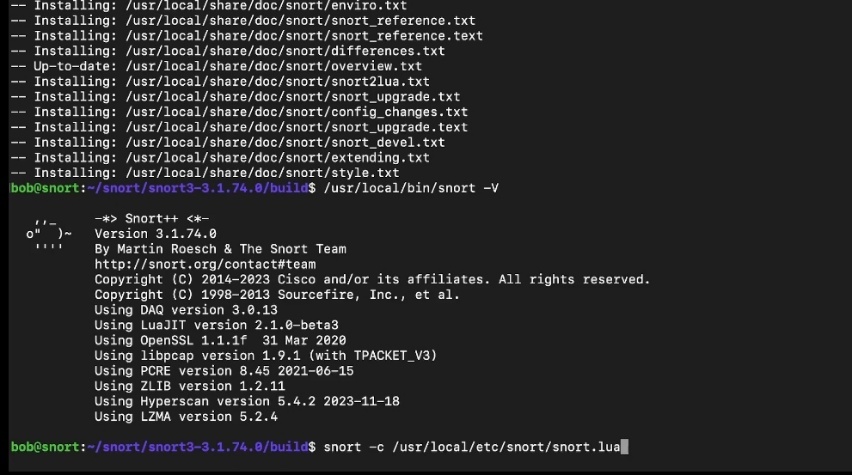
* Set up a firewall (pfSense).

- Firewall rules

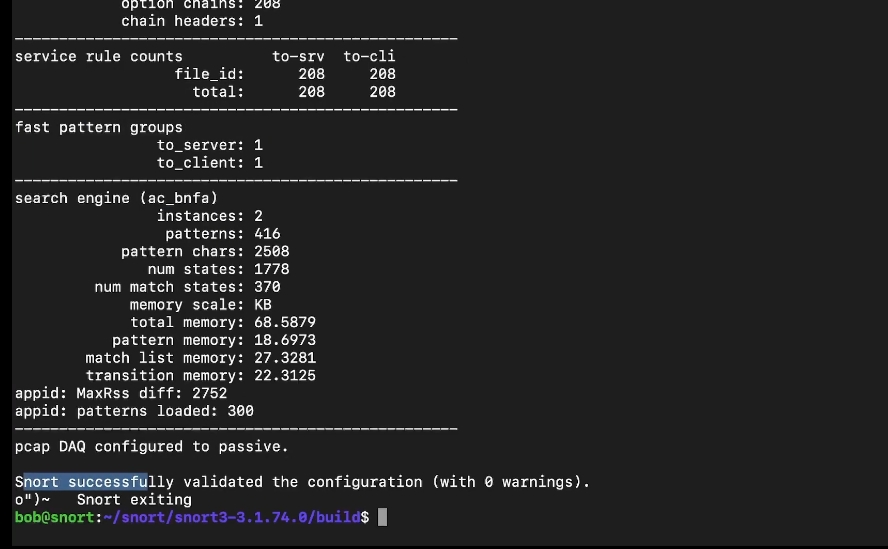




* Install and configure an IDS
* Downloading and Installing Snort



* Configuring IDS (Snort)



* Perform a basic vulnerability scan using Nmap or Nessus.
* Submit a 1-page audit report.

## 4. Virtualisation and Containers

* Create at least 2 Virtual Machines using VirtualBox or VMware.
* Install Docker and containerise a sample Python or Node.js web app.

## 5. Automation & Monitoring

* Use Ansible to automate file copy or service restart.
* Set up Nagios or Zabbix for monitoring CPU, RAM, and service health.

# Deliverables

* Network diagram
* Screenshots or screen recordings
* Docker container files and Ansible playbook
* Security audit report ● Final report with reflections