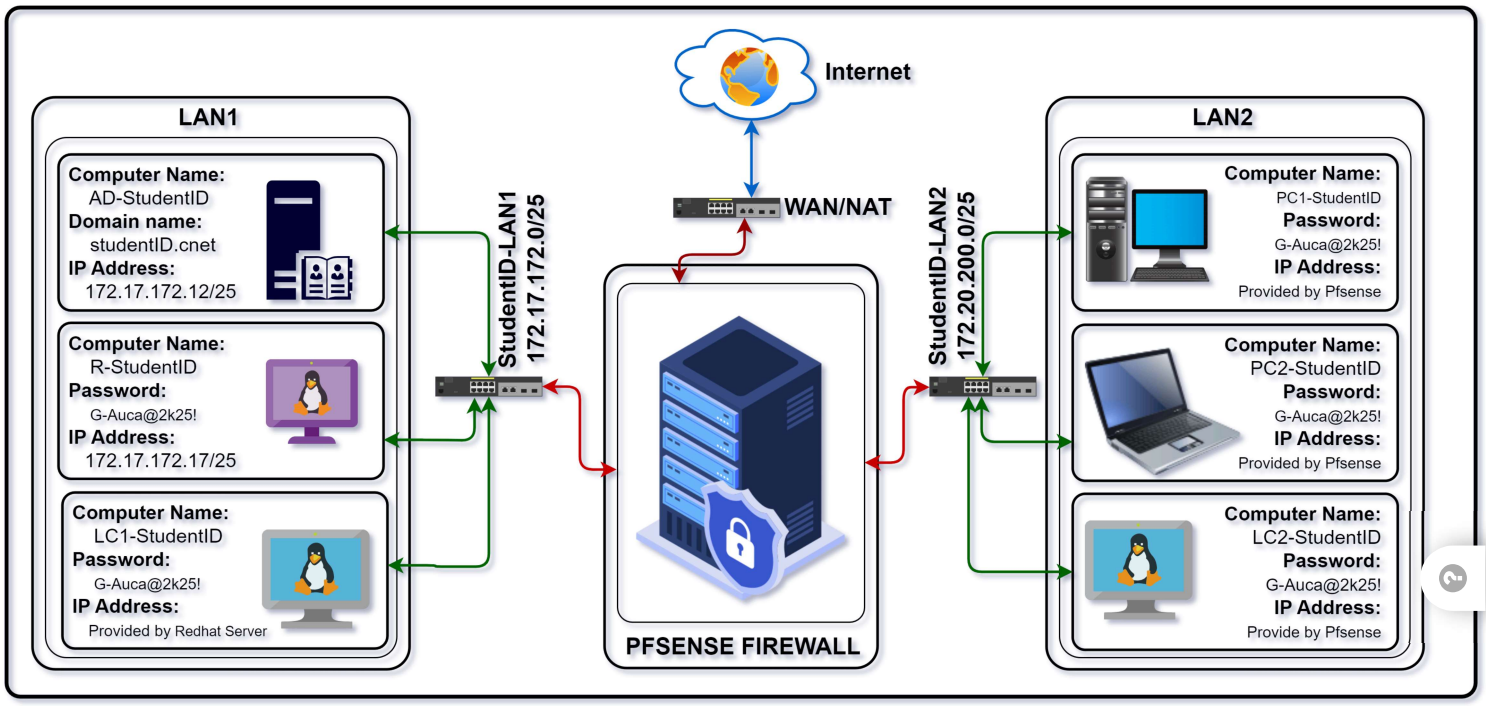
Phase 2: Network/System Configurations

Start Assignment

- Due Apr 28 by 5am
- Points 100
- Submitting a website url
- Available Mar 30 at 12am - Apr 28 at 6am



1. Introduction

In today's IT-driven world, mastering network and system configurations is essential for IT professionals. This phase of the project simulates real-world enterprise challenges and guides you through setting up, managing, and testing a secure and integrated network environment. You will work with both Windows and Linux systems, configure centralized services like Active Directory, implement advanced group policies, set up a captive portal with personalized student information, perform network monitoring, and configure a dedicated firewall with backup and restore functionality. All required images and tools are available at **CompNetworkFinalProjectTools (https://drive.google.com/drive/folders/14mMntbJKF9hiscuxeHVkSyagkyMGfvqu?usp=sharing)**

---

2. Executive Summary

In this phase you will:

- **Deploy a Virtual Network Environment:**
  Create a virtual environment integrating Windows and Linux servers and clients across multiple LAN segments.
- **Centralize Management & Security:**
  Configure a domain controller with multiple Organizational Units (OUs), create user accounts, and enforce policies using Group Policy Objects (GPOs).
- **Implement a Personalized Captive Portal:**
  Use a Pfsense firewall to set up a captive portal that requires users to log in. The portal must display your profile (including profile picture, full name, and StudentID) when connecting via LAN1 or LAN2 or switching between networks.
- **Enable Network Monitoring:**
  Deploy NTOPng to monitor real-time network traffic, bandwidth usage, and anomalies.
- **Configure Advanced Firewall Features:**
  Use Pfsense to create firewall rules, configure port forwarding, enable traffic inspection, set up ARP monitoring, deploy web filtering (using SquidGuard), and implement an automated backup & restore procedure (with email notifications).
- **Demonstrate and Document:**
  Record a detailed video demonstration covering all configuration steps and test results. Your video must clearly show all features as per the rubric and include your full name, StudentID, and class group.

---

3. Objectives

By completing this phase, you will:

- **Deploy and Manage Infrastructure:**
  Install and configure Windows and Linux systems in a virtualized environment.
- **Configure Centralized Directory and Policies:**
  Set up Active Directory, create multiple OUs, implement GPOs for software deployment, drive mappings, login restrictions, roaming profiles, and strong password policies.
- **Set Up a Captive Portal:**
  Build a custom captive portal using Pfsense. The login page should capture and display user information (profile picture, full name, StudentID) and control access to selected websites.
- **Monitor Network Traffic:**
  Install NTOPng on your Pfsense appliance to observe traffic across LAN segments, generate usage reports, and detect anomalies.

- **Secure and Control Network Access:**
  Configure advanced firewall features including port forwarding, traffic inspection, ARP monitoring, and web filtering with SquidGuard.
- **Automate Backup & Restore:**
  Schedule regular Pfsense configuration backups that are automatically emailed to a designated address and verify the restoration process.
- **Record and Report:**
  Produce a video demonstration (15–20 minutes) that walks through every implemented feature, along with a detailed written report documenting the setup, testing, and results.

---

4. Expected Outcomes

At the end of this phase, your environment should be able to:

1. **Centralized Domain Services:**
   - Run a Windows Server as a Domain Controller with OUs (e.g., IT, HR, Students, Finance) and user accounts configured.
2. **Group Policy Enforcement:**
   - Automatically deploy software, map network drives (both centralized and department-specific), enforce login restrictions, implement roaming profiles, and enforce robust password policies.
3. **Linux-Based Services:**
   - Run DHCP, Samba, FTP, and SSH services accessible from Windows clients.
4. **Email & Web Services:**
   - Host an Exchange server for internal email communication and deploy a personal portfolio website using IIS.
5. **Captive Portal with Personalization:**
   - Deploy a Pfsense captive portal that prompts users (from LAN1 or LAN2) to log in using a custom page that displays their student information.
6. **Real-Time Network Monitoring:**
   - Utilize NTOPng to continuously monitor network performance and detect anomalies.
7. **Advanced Firewall & Security:**

- Configure Pfsense with firewall rules, port forwarding, traffic inspection, ARP monitoring, web filtering, and an automated backup system.

8. **Video Demonstration:**
   - Record a comprehensive video that shows each configuration step, testing procedures, and evidence of successful implementation.
9. **Detailed Documentation:**
   - Produce a final report that includes configuration screenshots, testing procedures, explanations, and conclusions.

---

5. Detailed Step-by-Step Instructions

5.1 Hardware & Network Setup

- **Memory Allocation:**
  - Clients: 256 MB RAM
  - Servers: 512 MB RAM
- **Network Adapters:**
  - **WAN:** Use a Bridged Adapter.
  - **LAN Segments:** Use NAT Adapters for internal networks.
- **IP Addressing:**
  - **LAN1:** 172.17.172.0/25
  - **LAN2:** 172.20.200.0/25
  - **Domain Naming:** Use a convention such as **studentID.cnet**

5.2 Windows Server – Active Directory & Group Policy

A. Domain Controller Setup

1. **Installation and Promotion:**
   - Install Windows Server 2003.
   - Run `dcpromo` to promote the server to a Domain Controller.
   - Set the domain name to **studentID.cnet**.

2. **Organizational Units (OUs):**
    - Create OUs for IT, HR, Students, and Finance.
3. **User Accounts:**
    - Create user accounts in each OU following a naming convention (e.g., IT1–IT4, HR1–HR4, Student1–Student4, Fin1–Fin4).
    - Use a default password such as **G-Auca@2k25!**

B. Group Policy Configuration

1. **Software Deployment:**
    - Deploy applications (e.g., vlc.msi, mozilla.msi) via the Group Policy Management Console (GPMC) under Computer Configuration > Software Settings.
    - Link the GPO to the appropriate OU.
2. **Mapped Network Drives:**
    - **Centralized Drive:**
        - Create a shared folder on the Domain Controller (e.g., *DomainName-Centralized-Drive*).
        - Map this drive for all domain users via a GPO.
        - Set permissions so that only file owners and IT have modify rights.
    - **Department-Specific Drives:**
        - Create shared folders for IT, HR, and Finance.
        - Use separate GPOs to map these drives only for users in the respective OUs.
        - Exclude the Students OU from these department-specific mappings.
3. **Login Restrictions & Roaming Profiles:**
    - Configure GPO and login scripts to restrict specific users to certain PCs or time windows (e.g., Student1 may only log in on PC1 during the morning).
    - Set account expiration dates (e.g., Student1 expires on April 6, 2025).
    - Enable roaming profiles for all users (excluding Students) to maintain consistency across different workstations.
4. **Password Policies:**
    - Set a minimum password length of 12 characters.
    - Enforce password complexity (a mix of uppercase, lowercase, digits, and special characters).

- Configure passwords to expire every 24 hours (or as per your policy).
- Maintain a password history of 5 entries.
- Lock accounts after 3 failed login attempts (lockout duration of 15 minutes, with a reset counter after 10 minutes).
- Require a password change on first login.

5. **Logging and Monitoring on Windows Server:**
   - Configure Event Viewer to monitor Security (e.g., Event IDs 4624 for successful logins and 4625 for failures), System, and Application logs.
   - Retain logs for at least 7 days.
   - Use filtering to capture key events and schedule alerts using Task Scheduler.

5.3 Linux Server Setup (Red Hat)

1. **Services to Configure:**
   - **DHCP:**
     - Configure the DHCP service to assign IP addresses dynamically on LAN1 and LAN2.
     - Ensure that servers have reserved static IPs.
   - **Samba:**
     - Set up Samba to provide file sharing between Linux and Windows clients.
     - Test share access from a Windows client.
   - **FTP:**
     - Configure an FTP service (e.g., vsftpd) to allow file transfers.
   - **SSH:**
     - Enable and secure SSH for remote management.
     - Test using tools like PuTTY (from Windows) or OpenSSH.

5.4 Exchange Server Setup (Email Communication)

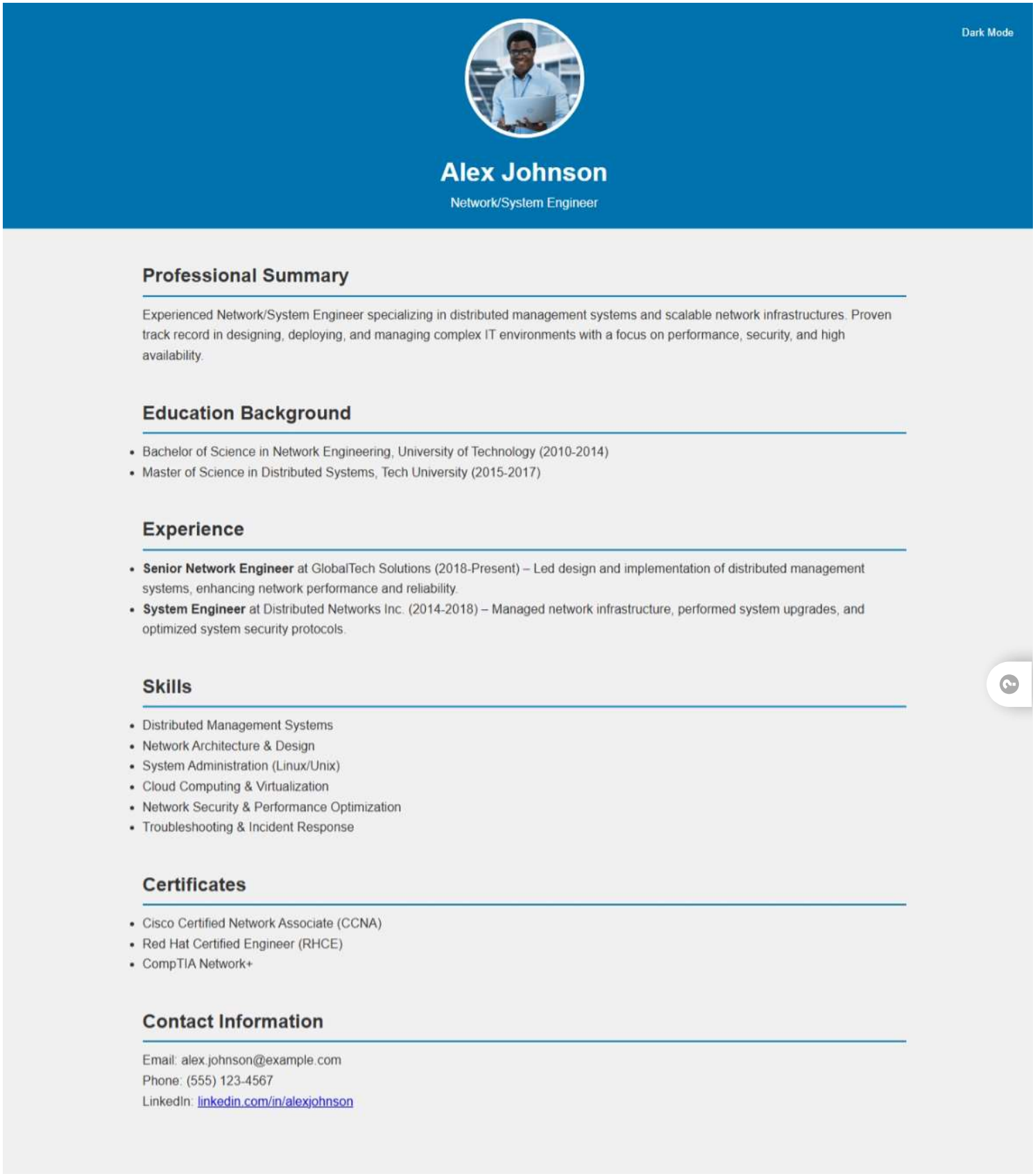
1. **Installation and Mailbox Setup:**

- Install the Exchange Server on the Domain Controller.
- Create mailboxes for all Active Directory users.
- Configure an email client (e.g., Outlook on a Windows XP client) to send and receive emails within the domain.

5.5 Web Server Setup (IIS)

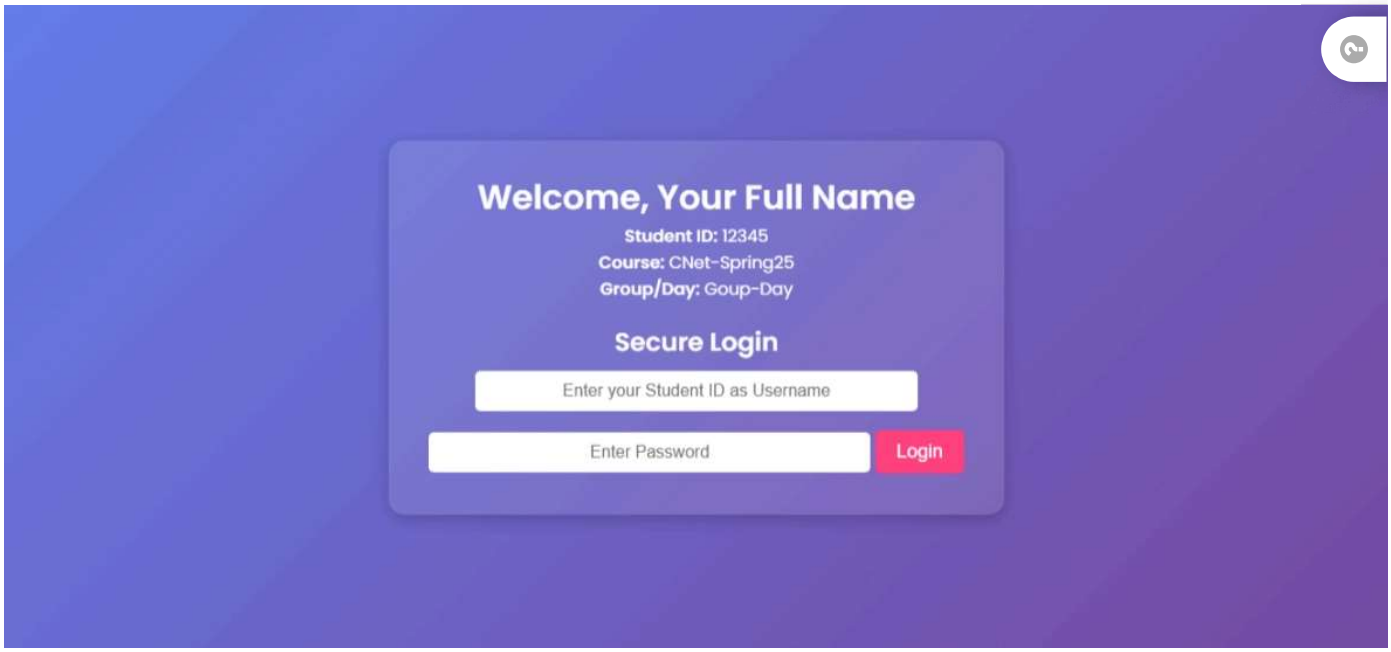
1. **IIS Installation:**
   - Install Internet Information Services (IIS) on Windows Server 2003.
2. **Portfolio Website Development:**
   - Design a personal portfolio website including:
     - **Personal Information:** Full name, profile picture, and StudentID (this is critical to match the captive portal personalization).
     - **Professional Summary:** A brief overview of your expertise.
     - **Educational & Experience Background:** Your academic and professional history.
     - **Skills & Certificates:** List of relevant skills and any certifications.
     - **Contact Information:** How to reach you.
   - Develop the website using HTML and CSS. Ensure that the design is professional, user-friendly, and accessible to all network clients.
   - Document the configuration and test the accessibility of the website.

For Example:



5.6 Pfsense Firewall Configuration

A. Core Firewall and Captive Portal Tasks

1. **Pfsense Basic Setup:**
   - Install and configure the Pfsense firewall appliance with multiple LAN interfaces (for LAN1 and LAN2).
2. **Captive Portal Configuration:**
   - **Objective:** Enforce a captive portal that requires students to log in and display their personal information.
   - **Steps:**
     - Enable the Captive Portal service in Pfsense.
     - Create a custom login page using HTML (and optionally a server-side script such as PHP) that includes fields for full name, StudentID.
     - Configure captive portal rules so that users on LAN1 or LAN2, or those switching networks, are required to authenticate.
     - On successful login, allow access to specified websites (e.g., allow access to auca.ac.rw, google.com, and youtube.com).
   - **For example:**
   - 

3. **Web Filtering with Squid & SquidGuard:**
   - Install Squid and SquidGuard via the Pfsense package manager.
   - **For LAN1:** Configure ACLs to block certain websites (e.g., social media or sites with keywords such as “kill,” “bet,” “ball”).
   - **For LAN2:** Configure ACLs to allow access only to approved websites (e.g., auca.ac.rw, google.com, youtube.com).

4. **Network Monitoring with NTOPng:**
    - Install NTOPng on the Pfsense appliance.
    - Configure NTOPng to monitor real-time traffic on LAN1 and LAN2.
    - Set up dashboards and logging to track bandwidth usage and flag unusual activities.
5. **Backup & Restore Configuration:**
    - Set up Pfsense to perform regular backups of its configuration.
    - Configure an automated process (using Pfsense's built-in backup scheduler or custom scripting) to email the backup file to a designated email address.
    - Test the restore process by simulating a configuration loss and re-importing the backup.

5.7 Testing & Verification

- **Functional Tests:**
    - **Active Directory & GPOs:**
        - Log in with different user accounts to test software deployment, drive mapping (both centralized and department-specific), and login restrictions.
    - **Linux Services:**
        - Verify that DHCP, Samba, FTP, and SSH are accessible from Windows clients.
    - **Email & Web Services:**
        - Send test emails via Exchange and access the IIS-hosted portfolio website.
    - **Captive Portal:**
        - Connect to LAN1 or LAN2 and authenticate through the custom captive portal page. Verify that the student information (profile picture, full name, StudentID) is correctly displayed.
    - **Web Filtering & NTOPng:**
        - Test web filtering by attempting to access blocked and allowed websites and verify NTOPng displays accurate network statistics.
    - **Backup & Restore:**
        - Ensure that backup emails are received and conduct a restore test.
- **Documentation:**

- Take clear screenshots of every configuration step, test results, and log outputs.
- Maintain detailed notes on the setup and testing procedures.

5.8 Reporting & Video Documentation

Final Reporting Requirements:

- **Video Demonstration (15–20 minutes):**
  - Record a video that demonstrates each configuration component, including:
    - Active Directory setup, GPOs, and drive mappings.
    - Linux server service tests (DHCP, Samba, FTP, SSH).
    - Email communication via the Exchange Server.
    - Access and testing of the IIS-hosted portfolio website.
    - Captive portal login process showing the personalized login page with student details.
    - Network monitoring using NTOPng.
    - Pfsense firewall configuration, including web filtering and backup & restore demonstration
  - **Mandatory Identification:**
    - At the start of the video, clearly state your full name, StudentID, and Class Group.
- **Written Report (With more 30 pages):**
  - Include an executive summary, objectives, methodology, and step-by-step configuration details.
  - Embed screenshots and testing evidence.
  - Provide conclusions and lessons learned.
  - Ensure the report is well-organized and logically structured.

---

6. Grading Rubric Table (Total: 100 Points)

Category	Criteria	Points
Active Directory Setup	- Successful promotion of Windows Server to Domain Controller. - Correct creation of OUs and user accounts with appropriate policies.	10

Category	Criteria	Points
Group Policy & Drive Mapping	- Effective software deployment via GPO. - Accurate configuration of centralized and department-specific network drives with proper permissions.	10
Login & Access Restrictions	- Correct implementation of login restrictions, scheduled access, account expirations, and roaming profiles.	5
Password Policies	- Enforced minimum length, complexity, expiration, history, and lockout policies through GPO.	5
Linux Server Configuration	- Proper setup and testing of DHCP, Samba, FTP, and SSH services accessible from Windows clients.	10
Exchange Server Setup	- Successful installation and configuration of an Exchange server with functional email communication.	10
Web Server Setup (IIS)	- Professional design and deployment of a personal portfolio website including all required sections and verified accessibility.	10
Captive Portal Configuration and Backup & Restore	- Custom captive portal implementation displaying student information (profile picture, full name, StudentID) on LAN1/LAN2 access with controlled web access. - Successful configuration of automated Pfsense backups with email notifications and tested restore process.	10
Network Monitoring	- Windows logs and effective deployment and configuration of NTOPng to monitor network traffic and generate usage reports.	10
Firewall & Web Filtering	- Accurate configuration of Pfsense firewall rules, port forwarding, traffic inspection, ARP monitoring, and SquidGuard web filtering rules.	10
Documentation & Video	- Comprehensive written report with detailed configuration steps, screenshots, and testing evidence. - A clear and complete video demonstration including personal identification.	10

7. Conclusion

This project phase simulates the challenges of designing and managing an enterprise-level IT environment. By carefully following these instructions and providing thorough documentation, you will develop critical hands-on skills in system administration, network security, and policy enforcement. Your ability to integrate multiple technologies cohesively will be essential for your future career in IT.

"Dream big and work hard to achieve your goals. Stay strong and keep fighting for your dreams. Do not let anything discourage you; the future looks bright."

Good luck!