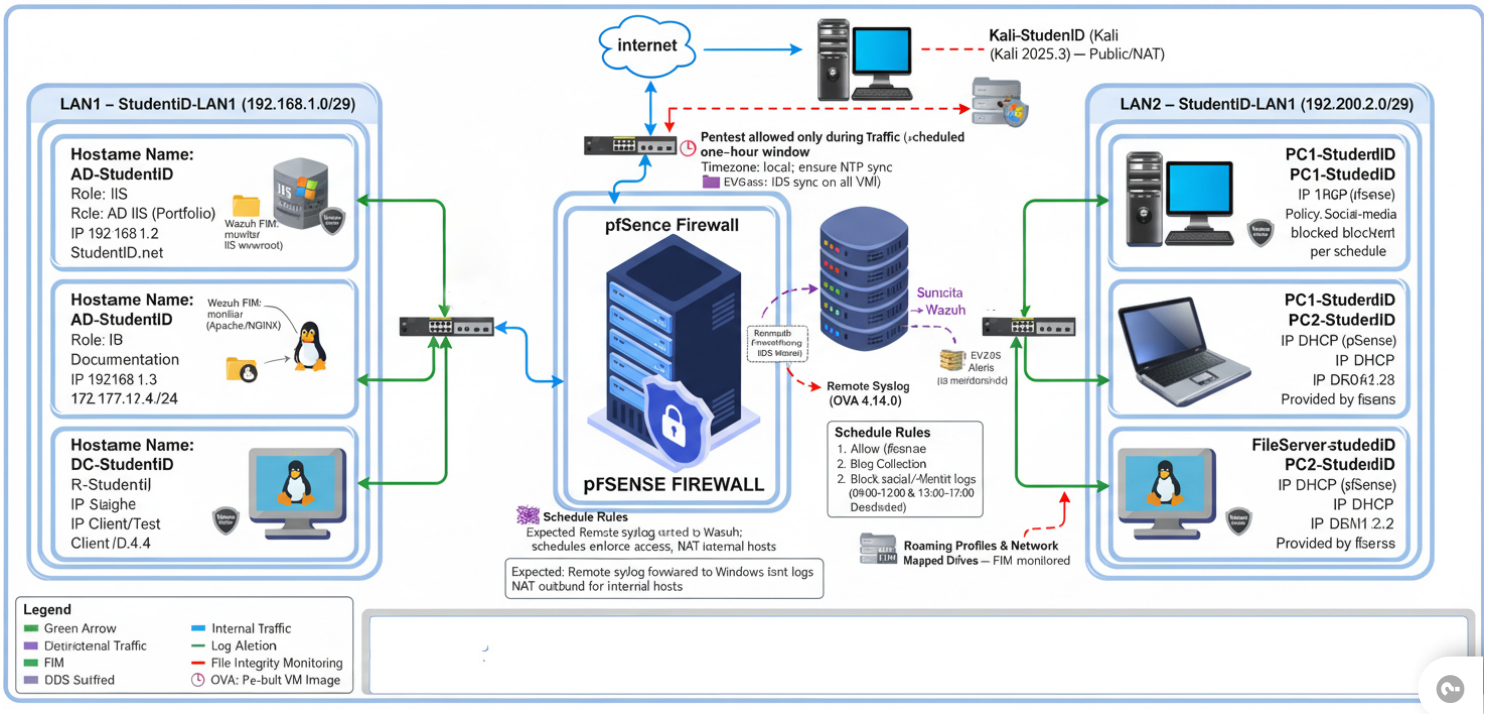
Phase 2: Network/System Configurations

- Due Nov 23 by 11:59pm
- Points 100
- Available Nov 2 at 12am - Nov 24 at 11:59pm



INTRODUCTION:

In today's IT-driven world, IT workers should become proficient in network and system setups. This phase of the project helps you in setting up, managing, and testing an integrated, secure network environment while simulating real-world enterprise difficulties. You will also set up centralized services, including Active Directory, sophisticated group policy implementation, monitoring of networks, and setup of a specialized firewall with backup and restore capabilities, in addition to working with Linux and Windows computers. Please confirm only if you are in compliance.

Executive Summary:

You will design, deploy, secure, monitor and test a segmented virtual lab that simulates an enterprise environment. The lab shall demonstrate real-world capability in centralized directory services, web hosting, logging & detection, firewall policy and scheduling, IDS integration, and controlled offensive testing. The pfSense captive portal must be removed/disabled. Public network access will be via NAT. DHCP responsibility is split: pfSense provides DHCP only to LAN2; Linux server provides DHCP to LAN1.

Special note on academic honesty: If you check a box for a task on the submission form that is not completed and that task is not shown in your demonstration video, you will lose the points assigned to that task (i.e., instead of +5, claimed but not demonstrated will be−5). This is academic dishonesty.

Video submission should comprehensively cover:

- Clear recording of the screen of each task banner/segment, face-in-picture webcam, and clearly spoken explanation of what is being shown.
- Sound quality has to be clear - record in a quiet room. Your voiceover must explain why each step is done, not just what you click.
- Every segment should demonstrate before/after or evidence (Evidences and logs) as stated in the rubric.

Topology, Naming & Addressing:

Domain: StudentID.f25
Wazuh hostname: StudentID (the Wazuh OVA VM must use this hostname)
Examples of hostnames (use your StudentID prefix):

Virtual Machines Configuration & IP Address Allocation Table:

No.	VM Role / Operating System	VM Name (Hostname)	Primary Function / Description	Network Segment	IP Address Assignment	Additional Notes
1	**Windows Server (Active Directory + DNS + NTP)**	**AD-StudentID**	Acts as Domain Controller, DNS Server, NTP Server, and manages centralized authentication & GPOs	**LAN1**	**Static: 192.168.1.2/29**	**Domain name:** `StudentID.f5` Promoted using **dcpromo**.
2	**Linux Server (DHCP + Samba + FTP + SSH, IDS Services)**	**LS-StudentID**	Provides DHCP for LAN1 clients, file sharing (Samba), FTP services, remote access via SSH, and IDS (**Suricata/Snort**).	**LAN1**	**Static: 192.168.1.3/29**	Acts as **DHCP provider** for LAN1; ensure proper DHCP range configured.
3	**Wazuh Server (SIEM + File Integrity Monitoring)**	**WS-StudentID**	Monitors network endpoints, firewall logs, and mapped/roaming folders for file integrity and threats	**LAN1**	**Static: 192.168.1.4/29**	Integrated with Windows and Linux clients; include monitored folder paths in Wazuh config.

No.	VM Role / Operating System	VM Name (Hostname)	Primary Function / Description	Network Segment	IP Address Assignment	Additional Notes
4	**Windows Client (Domain Member)**	**PC1-StudentID**	Joins `StudentID.f25` domain; used for Group Policy testing, drive mapping, and AD login verification	**LAN2**	**Dynamic (from pfSense DHCP)**	DHCP provided by **pfSense** for LAN2; test roaming profiles and folder redirection.
5	**Windows Client (Domain Member)**	**PC2-StudentID**	Used to test GPOs, software deployment, and mapped drives	**LAN2**	**Dynamic (from pfSense DHCP)**	Test domain login & access to both LAN1 and LAN2 hosted web services.
6	**Linux Client (Workstation)**	**LC-StudentID**	Accesses Samba shares, tests DHCP from both servers, and SSH connections	**LAN1/LAN2 (Switchable)**	**Dynamic (from DHCP Server depending on VLAN)**	Switch adapter between **LAN1** (Linux DHCP) and **LAN2** (pfSense DHCP) to validate configuration.
7	**pfSense Firewall / Gateway**	**PF-StudentID**	Acts as the main security gateway handling routing, firewalling, VPN, NAT, and monitoring	**LAN1, LAN2, WAN/NAT**	**LAN1:** 192.168.1.1/29 **LAN2:** 192.168.2.1/29 **WAN/NAT:** DHCP (Public)	Enable **OpenVPN Remote Access** for IT OU users, configure inter-LAN rules and NAT access to both LANs.
8	**Kali Linux (Penetration Testing)**	**Kali-StudentID**	Used for penetration testing, network scanning, and firewall rule validation	**NAT Network (Internet Segment)**	**Dynamic (from NAT network)**	Used to simulate external attack or VPN connection test.
9	**Windows Client (VPN**	**VPNClient-StudentID**	Used to test **OpenVPN Remote**	**NAT Network**	**Dynamic (from NAT network)**	After VPN connection,

No.	VM Role / Operating System	VM Name (Hostname)	Primary Function / Description	Network Segment	IP Address Assignment	Additional Notes
	Access Testing)		**Access** connection to **LAN1** from NAT Network			should access LAN1 resources (e.g., `AD-StudentID`, shared folders).

Network subnets:

Network	Name	Subnet	Usable hosts	Suggested gateway
Internal Network Adapter	StudentID-LAN1	192.168.1.0/29	192.168.1.1 → 192.168.1.6	pfSense (e.g., `192.168.1.1`)
Internal Network Adapter	StudentID-LAN2	`192.168.2.0/29`	192.168.2.1 → 192.168.2.6	pfSense (e.g., 192.168.2.1)
NAT/Public	`NAT`	NAT as provided by VirtualBox	Windows Host + Kali on NAT	pfSense WAN

VM resource guidance (minimum & recommended):

VM	Minimum (to avoid crashes)	Recommended
Windows Server (DC + IIS) (**version**: 2008 and Above)	1–2 vCPU, 1~**2 GB** RAM	4 vCPU, **2–4 GB** RAM, 50–100 GB disk
Windows Clients (each) (**Version:** Window 7 and Above)	512 MB – **1 GB** RAM	1–2 vCPU, 1–2 GB RAM, 20–50GB disk
Linux Server (Apache/NGINX + DHCP for LAN1) (**Version**: Ubuntu or Redhat/CentOS)	1 vCPU, **1–2 GB** RAM	2 vCPU, **4 GB** RAM, 40 GB disk
Wazuh OVA (4.14.0)	2 vCPU, **2 GB** RAM (may fail under load)	4 vCPU, **2–4GB** RAM, 100 GB disk
Kali (2025.3)	1 vCPU, 1–**2 GB** RAM	2 vCPU, **2 GB** RAM
pfSense	1 vCPU, **512 MB** RAM	1–2 vCPU, **1 GB** RAM

Deliverables (what you must submit)

1. Documentation site (hosted on the Linux documentation server) — multi-tab web pages (this replaces a PDF): every tab documents one major area: topology, pfSense, AD/GPO, Wazuh, IDS, Kali tests, backups. Each step must include Evidences, commands, explanations and timestamps.
2. Portfolio site (hosted on Windows IIS) — personal portfolio with your full name, profile picture and StudentID; link to documentation site.
3. Wazuh evidence package - Evidences of manager UI showing StudentID hostname, agent list, FIM alerts, IDS alerts and exported JSON snippets for at least 3 alerts pfSense config backup (config.xml) plus Evidence proving captive portal disabled.
4. Video demonstration uploaded to Google Drive - include share link in the documentation site submission (see below for video requirements)
5. Topology diagram & IP allocation table below (image included in documentation site).
    1. **Optional:** VM snapshots/OVAs (if instructor requests), labeled with StudentID.

Expected Outcomes (what the environment must demonstrate)

At the end of the project your environment should be able to:

1. **Centralized Domain Services:** Configure and implement a Windows Server as Domain Controller for StudentID.f25, organizing OUs (IT, HR, Students, Finance) and user accounts.
2. **Group Policy Enforcement:** Deploy software via GPO, map centralized & department drives, enforce login restrictions and roaming profiles, and apply strong password policies.
3. **Linux-Based Services:** Provide DHCP (LAN1), Samba, FTP, SSH reachable from Windows clie
4. **E-mail & Web Services:** Setup an Exchange server on the domain (optional) and set up a personal portfolio web site on IIS.
5. **Real-Time Network Monitoring:** Run NTOPng on pfSense to see the traffic per LAN and find out anomalies.
6. **Advanced Firewall & Security:** pfSense configured with firewall rules, port forwarding, traffic inspection via IDS/Suricata, ARP monitoring, and web filtering. Automated backups of pfSense configuration are set up and tested.
7. **Logging & Detection:** Wazuh OVA 4.14.0 deployed w/agents on Windows, Linux and syslog forwarding from pfSense; FIM includes network mapped & roaming profile folders; IDS logs (Suricata or Snort) integrated in Wazuh.
8. **Controlled Pentesting & Detection:** Kali 2025.3 performs defined tests during a one-hour scheduled window; IDS/Wazuh detect and correlate events. Reporting & **Evidence:** Multitab documentation site with Evidences, commands, and logs; a 15–20 minute recorded demonstration video.

Full Task Breakdown — Requirements, How-to & Expected Output

Each major task below must have an associated documentation tab on the Linux site with Evidences for *every* numbered step. Caption each Evidence with step number, short description, and timestamp.

Task 1 — pfSense (Firewall, NAT, Schedules, NTOPng, Logging & Backup)

Requirements:

- Configure WAN (NAT), OPT1 (LAN1), OPT2 (LAN2) interfaces.
- **DHCP:** pfSense provides DHCP for LAN2 ONLY. Linux will provide DHCP for LAN1.
- Configure NAT outbound so internal hosts access internet.
- Setup firewall rules (names must include `StudentID`):
  - **ALLOW_StudentID_LAN1_TO_LAN2** — allow bi-directional traffic between LAN1 and LAN2.
  - **ALLOW_StudentID_ALL_TO_WEBPAGES** — allow LAN1, LAN2, and NAT to access both hosted web pages (IIS and Linux doc server).
  - **KaliPentest_StudentID** — allow Kali (Public/NAT) to internal networks for **one hour** only (use a schedule).
  - **LAN2_NoSocial_StudentID** — block social media on LAN2 during 09:00–12:00 and 13:00–17:00 (local time).
- Install NTOPng package on pfSense and configure dashboards for both LAN segments.
- Forward pfSense logs to Wazuh (remote syslog — RFC3164/RFC5424).
- Configure automated backups of pfSense config and verify restore (AutoConfigBackup or scheduled export+email).
- Enable ARP monitoring (pfSense packages or built-in) and enable traffic inspection features available (e.g., IDS integration).

How-to (high level)

- **Interfaces:** `Interfaces → Assignments` → set WAN, OPT1 (192.168.1.1/29), OPT2 (192.168.2.1/29). Evidence.
- **DHCP:** `Services → DHCP Server → OPT2 (LAN2)` — configure pool & reservations. Document Linux DHCP settings for LAN1 on Linux tab.
- **NTOPng:** `System → Package Manager → Available Packages → ntopng` → install → configure interfaces and dashboards.

- **Schedules:** `Firewall → Schedules` — create `KaliPentest_StudentID` and `LAN2_NoSocial_StudentID`.
- **Firewall rules:** create rules on appropriate interface and assign Schedule where needed. Name rules exactly as requested.
- **Logging:** `System → Settings → Logging/Targets` → add Wazuh manager IP: port (syslog) and select format. Verify in Wazuh.
- **Backup:** install `AutoConfigBackup` or schedule a script to export `config.xml` and send email; capture Evidence of backup job & restore test.

Expected evidence (attach to pfSense tab)

- Evidence: Interfaces page showing IPs.
- Evidence: DHCP page for LAN2.
- Evidence: Firewall rules list with `StudentID` naming and schedules visible.
- Evidence: NTOPng dashboard showing traffic per LAN.
- Evidence: `config.xml` backup and restore test Evidence.
- Evidence: Wazuh manager showing incoming pfSense syslog entries.

Task 2 — Active Directory & Group Policy (Windows Server)

Requirements

- Install Windows Server (From 2008 to 2022 recommended). Promote to Domain Controller for `StudentID.f25`.
- **Create OUs:** `IT`, `HR`, `Students`, `Finance`.
- Create example user accounts in each OU (e.g., `IT1`, `HR1`, `Student1`, `Fin1`) and describe naming convention.
- Install IIS and host your portfolio site (HTTP) with StudentID, full name, profile picture, and short CV or Resume (Professional Profile).
    - **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.
  - □

- Configure **NTP** on the DC and push NTP client settings via GPO to all domain systems.
- Configure **Roaming Profiles** and **Mapped Drives** via GPO. Use `StudentID` in folder/share names (e.g., `\\fileserver\roaming\StudentID\%username%`).
- Implement **Login Restrictions** via GPO (time-based login restrictions), account expiration, and account lockout policies.
- Implement **Password Policy**:
  - **Minimum password length:** 12 characters
  - Complexity required
  - Password expire policy (document intended policy; recommended not less than 30 days in real world — instructor may require 24 hours for lab)
  - Password history: 5
  - Lockout after 3 failed attempts; 15-minute duration; reset counter after 10 minutes
  - Require password change at first login
- Deploy software via GPO (MSI packages) for sample apps (e.g., Mozilla.mis, VLC.msi, and).
- Configure Wazuh agent on Windows and forward Security, System, Application logs. Configure Windows FIM paths to include roaming and mapped folders.

How-to (high level)

- **Promote to DC:** `Server Manager → Add Roles & Features → Active Directory Domain Services → Promote this server to a domain controller` → set domain `StudentID.f25`.
- **Create OUs & users:** `ADUC (Active Directory Users and Computers)` → New OU → create users with passwords (evidence Evidence).
- **GPOs:** `Group Policy Management` → New GPO `GPO_StudentID_Roaming` etc. Configure:

  - `Computer Configuration → Policies → Windows Settings → Scripts` or `Preferences → Drive Maps` for mapped drives.
  - `Computer Configuration → Policies → Administrative Templates → System → Logon` (roaming profile paths)
  - `Computer Configuration → Policies → Administrative Templates → System → Group Policy → Configure Password Policy` via domain controller security policy or GPO for fine-grained.
- **Software deployment:** `Computer Configuration → Policies → Software Settings → Software Installation` — assign `.msi` to OU.
- **NTP:** `Group Policy: Computer Configuration → Policies → Administrative Templates → System → Windows Time Service` or set registry via GPO.
- **Wazuh agent:** install Windows agent, register with Wazuh manager, configure to report Security, System, Application events and FIM for:
  - `C:\inetpub\wwwroot\StudentID_portfolio\*`
  - `\\fileserver\roaming\StudentID\*`
  - any mapped drive `Z:\Shared_StudentID\*`

Expected evidence (attach to AD/GPO tab)

- Evidence: ADUC with OUs and users.
- Evidence: GPOs list with `StudentID` in names and key settings pages.
- Evidence: Mapped drives active for test user (explorer showing Z: mapped).
- Evidence: IIS portfolio page (browser) showing StudentID, name, picture.
- Evidence: Wazuh manager showing Windows agent online and example EventID alerts (4624/4625).
- FIM alert Evidence showing a test modification in roaming/mapped folder.

Task 3 — Linux Documentation Server (Apache/Nginx + DHCP for LAN1)

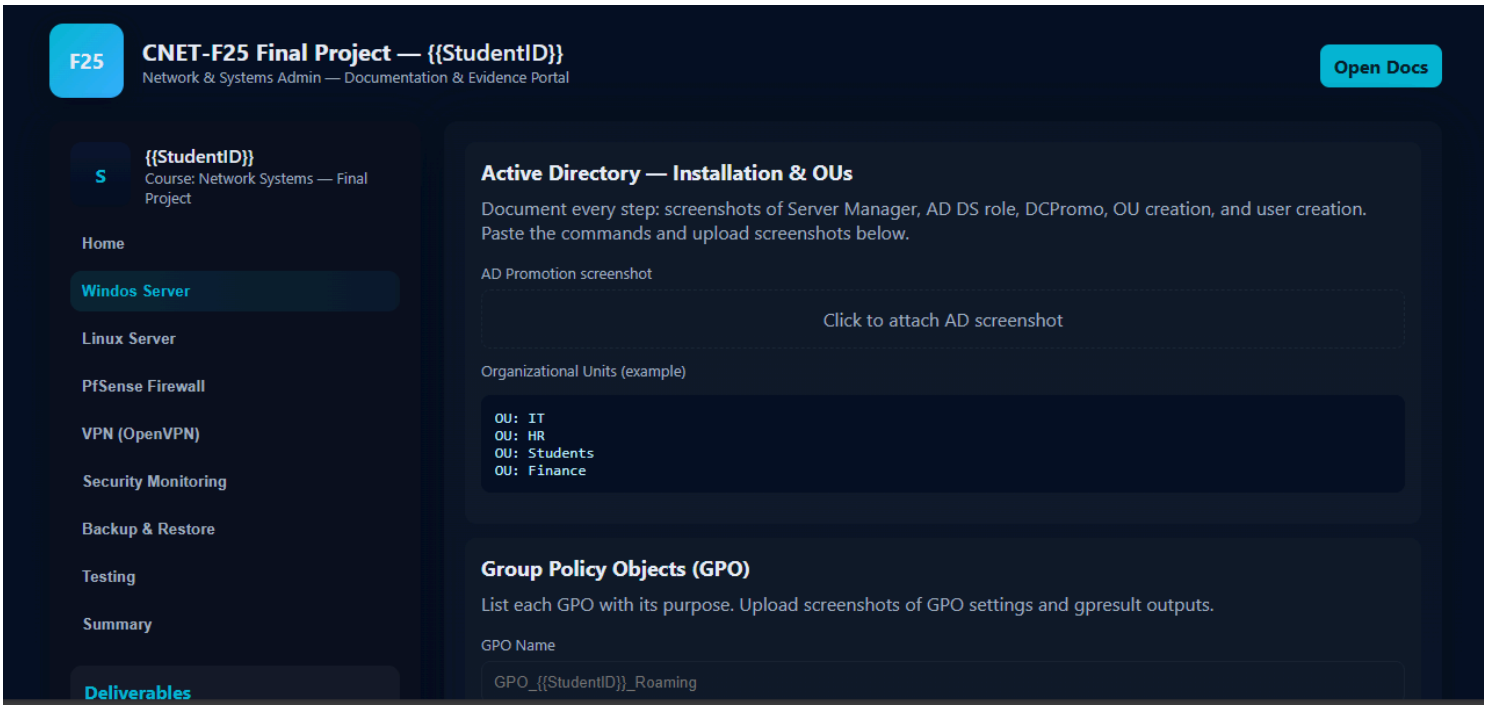
Requirements

- Install Ubuntu or Red Hat and host a **multi-tab documentation site** (each major task has its own tab). The documentation site is your final written report.
-

- Configure DHCP server to serve `StudentID-LAN2` with range and reservations.
- Install Wazuh agent and configure FIM for `/var/www/StudentID_docs/`, `/etc`, and other paths.
- Ensure the documentation site includes:
  - Topology diagram and IP allocation table
  - Step-by-step Evidences for each major task
  - Commands used and short justifications
  - Links to pdumps (logs/JSON snippets) or Evidences

How-to (high level)

- **Apache example:** install `apache2` or `nginx`, set up virtual host `studentid-docs.f25` pointing at `/var/www/StudentID_docs`.


F25
CNET-F25 Final Project — {{StudentID}}
Network & Systems Admin — Documentation & Evidence Portal
Open Docs
S
{{StudentID}}
Course: Network Systems — Final Project
Home
Windos Server
Linux Server
PfSense Firewall
VPN (OpenVPN)
Security Monitoring
Backup & Restore
Testing
Summary
Deliverables
Active Directory — Installation & OUs
Document every step: screenshots of Server Manager, AD DS role, DCPromo, OU creation, and user creation. Paste the commands and upload screenshots below.
AD Promotion screenshot
Click to attach AD screenshot
Organizational Units (example)
OU: IT
OU: HR
OU: Students
OU: Finance
Group Policy Objects (GPO)
List each GPO with its purpose. Upload screenshots of GPO settings and gpresult outputs.
GPO Name
GPO_{{StudentID}}_Roaming


F25
CNET-F25 Final Project — {{StudentID}}
Open Docs

- **DHCP for LAN1:** configure `isc-dhcp-server` with subnet `192.168.1.0/29` and reservations.
- **Wazuh agent:** register to manager and configure FIM.

Expected evidence (attach to Linux doc tab)

- URL to documentation site.
- Evidence: DHCP server config for LAN1.
- Evidence(s): example doc tab pages showing embedded Evidences and commands.
- Evidence: Wazuh agent online for Linux.

Task 4 — Wazuh Manager & Agents (Deploy OVA 4.14.0 and configure)

Requirements

- Deploy Wazuh OVA **4.14.0** and configure hostname to exactly `StudentID` (e.g., `A0123456`).
- Configure manager, API and Kibana (if present) — create at least one administrative dashboard user.
- Enroll agents: Windows DC/IIS, Linux doc server, pfSense (via syslog forwarding), Kali (optional agent or syslog).

- Configure File Integrity Monitoring (FIM) to include network mapped and roaming profile folders.
- Configure log ingestion: Windows Event, pfSense syslog, Suricata EVE JSON.
- Create at least **three custom detection rules** (show rule text and adjust severity):
  - `StudentID_BruteForce_Windows` — grouping repeated failed login events.
  - `StudentID_Scan_Network` — correlate Suricata scan alerts with network event.
  - `StudentID_Unauthorized_FileChange` — file changes on monitored roaming/mapped shares.

How-to (high level)

- Deploy OVA, change hostname via `hostnamectl set-hostname StudentID` or the OVA interface and reboot.
- Generate registration token in manager UI or CLI. Enroll each agent and capture Evidences of successful connections.
- Configure log forwarding on pfSense to Wazuh IP and port; verify logs appear in the Wazuh dashboard.
- Add custom rules to the `rules` folder and reload manager.

Expected evidence (attach to Wazuh tab)

- Wazuh manager dashboard Evidence with hostname `StudentID`.
- Agent list Evidence showing all agents online.
- Evidences of FIM alerts triggered by controlled file changes (roaming & mapped folder changes).
- Example rule files and a Evidence showing a rule fired (alert details).

Task 5 — IDS (Suricata recommended) Integration

Requirements

- Install Suricata on pfSense or Linux Server; enable EVE JSON output for integration with Wazuh.
- Use community rules (ET) and enable categories for network scanning and brute-force detection.
- Tune rules to balance signal-to-noise; document rule IDs and justifications.
- Forward EVE JSON (or syslog) to Wazuh for correlation.

How-to (high level)

- On pfSense: Packages → Suricata → Install → Interface(s) to monitor → Enable EVE logging.
- Configure `output-eve.json` and ensure Wazuh can access that log (either via filebeat or direct reading).
- Test with `nmap` and a small brute-force simulation from Kali to confirm alerts.

Expected evidence (attach to IDS tab)

- Suricata running Evidence and EVE JSON location.
- Wazuh alert showing Suricata signature with rule id and timestamp.
- A short table describing tuned rules and the reason for tuning.

Task 6 — Kali Pentest & Controlled Detection

Requirements

- Kali Linux **2025.3** on Public/NAT.
- Use pfSense schedule `KaliPentest_StudentID` to open connectivity for one hour.
- During that hour perform:
  - Network scanning (`nmap`) — document flags used and save output.
  - Controlled brute-force attempt on a lab service you own (limit attempts and document method & intent).
- Evidence must show the same timestamp across Kali output, Suricata alert and Wazuh alert.

Example nmap command to document

```
nmap -sS -Pn -T4 -p 1-65535 --open -oN nmap_scan_StudentID_YYYYMMDD.txt 192.168.2.0/29
```

Explain why `-sS` (SYN scan) is used and why `-Pn` (skip host discovery) might be chosen for stealth in labs.

Expected evidence (attach to Kali tab)

- `nmap` output file Evidence and uploaded text.
- Evidence: pfSense schedule `KaliPentest_StudentID` active.
- Wazuh alert Evidence for scan detection and Suricata alert showing the signature.
- Short analysis describing correlation of events and suggested mitigations.

Task 7 — VPN (OpenVPN) for IT OU

Requirements

- Configure OpenVPN on pfSense or dedicated VPN server.
- Use certificate-based authentication. Name certificates with `StudentID` (e.g., `StudentID-IT-Cert`).
- Configure authentication so **only members of the `IT` OU** can use the VPN (if using Active Directory/RADIUS integration, document that; otherwise, document manual assignment step).
- VPN clients must be able to reach `StudentID-LAN1` when connected.
- Create and test an example client configuration and show a successful connection.

How-to (high level)

- `VPN → OpenVPN → Wizards` in pfSense to create server and CA, create `StudentID-IT-Cert`.
- Create firewall rule allowing VPN subnet → LAN1.
- Configure client export and show `ovpn` file and successful connection screen.

Expected evidence (attach to VPN tab)

- Evidence: OpenVPN server configuration including cert named with `StudentID`.
- Evidence: successful client connected and pinging an internal host in LAN1.
- Note: include instructions for binding OU membership to RADIUS if used.

Task 8 — Monitoring Network Traffic with NTOPng

Requirements

- Install NTOPng package on pfSense and configure interfaces to monitor.
- Create usage reports, alerts or thresholds (bandwidth spike, top talkers).
- Show NTOPng dashboards for both LAN1 and LAN2 during normal operation and when Kali scan runs.

How-to

- `System → Package Manager → ntopng` on pfSense.

- Configure interface selection, retention and reporting. Link to dashboards in documentation.

Expected evidence (attach to NTOPng tab)

- NTOPng dashboard Evidences showing traffic per LAN, host-based reports and any anomalies detected during tests.

Task 9 — Advanced Firewall Features & Web Filtering

Requirements

- Demonstrate port forwarding as needed (e.g., forward HTTP to IIS if required from public NAT).
- Configure traffic inspection via IDS and/or pfSense packages (Suricata).
- Enable ARP monitoring to detect ARP spoofing attempts.
- Implement web filtering for LAN2 social media blocking (Squid+SquidGuard or DNS/alias-based filtering with schedules).
- Enforce firewall rule allowing **ALL users (LAN1, LAN2, NAT)** to access both hosted web pages.

Expected evidence (attach to Firewall & Web Filtering tab)

- Port forwarding rules Evidence.
- Suricata traffic inspection active Evidence.
- ARP monitoring Evidence or logs.
- Proof that social media domains are blocked during scheduled hours (web block page Evidence and/or Wazuh/proxy logs showing blocked hits).

Task 10 — Automated Backup & Restore of pfSense

Requirements

- Schedule regular pfSense configuration backups.
- Configure automatic email delivery of backups to a designated address.
- Demonstrate a restore from a backup and document the steps.

How-to

- Use `AutoConfigBackup` or a Cron job that exports `config.xml` and emails it (use SMTP settings in pfSense).
- Test restore: backup current config, modify a setting, then restore backup and show setting restored.

Expected evidence (attach to Backups tab)

- Evidence: backup schedule job.
- Attachment: sample `config.xml` upload to documentation site.
- Evidence: restore operation and confirmation.

File Integrity Monitoring — Specifics (including roaming & mapped folders)

Wazuh must monitor **network mapped** and **roaming profile** folders. Include the exact paths you used and show a controlled test where you modify or create a file, then show the Wazuh alert.

Recommended monitored paths:

Platform	Example paths to monitor
Windows (IIS)	`C:\inetpub\wwwroot\StudentID_portfolio\*`
Windows (Roaming Profiles)	`\\fileserver\roaming\StudentID\%username%\*`
Windows (Mapped)	`Z:\Shared_StudentID\*`
Windows (System)	`C:\Windows\*`, `C:\Program Files\*`
Linux	`/var/www/StudentID_docs/`, `/etc/`, `/usr/bin/`
pfSense logs	forwarded syslog files (`/var/log/system.log`, `gateways.log`)

Expected evidence

- `ossec.conf` snippet showing directories (paste in Wazuh tab).
- Wazuh alert Evidence showing FIM triggered by a test modification (roaming or mapped path).
- Short note on tuning: exclude ephemeral/temp folders to reduce noise (e.g., Windows Update directories).

Centralized Directory & Policies — Step-by-step checklist (must be demonstrated)

1. Install AD DS on Windows Server and promote to DC `StudentID-DC` for `StudentID.f25`.
2. Create OUs: `IT`, `HR`, `Students`, `Finance`.
3. Create sample users: `IT1`, `IT2`, `HR1`, `Student1`, `Fin1` (document default passwords and change policy).
4. Create GPO `GPO_StudentID_Roaming` — configure roaming profile path `\\fileserver\roaming\StudentID\%username%`.
5. Create GPO `GPO_StudentID_MappedDrives` — map centralized drive and department drives using Preferences → Drive Maps.
6. Create GPO `GPO_StudentID_SoftwareDeploy` — assign `vlc.msi`, `mozilla.msi` under Computer Configuration → Software Installation.
7. Create GPO `GPO_StudentID_PasswordPolicy` — set min length 12, complexity on, history 5, account lockout after 3 fails.
8. Test login restrictions: configure logon hours or computer restrictions for `Student1` (evidence Evidence).
9. Configure NTP: `Computer Configuration → Policies → Administrative Templates → System → Windows Time Service` (point clients to DC).

Expected evidence

- `Group Policy Management` Evidences with each GPO and key configured settings.
- Client Evidence showing GPO applied (gpresult /r).
- Explainer in documentation describing why each setting is used and risk mitigation.

Testing & Verification Requirements (grading evidence)

For each of these items you must include timestamped artifacts showing both action and detection:

- **Kali scan:** `nmap` output + Suricata EVE JSON alert + Wazuh alert (same timestamp).
- **FIM test:** modify a file in roaming or mapped folder → Wazuh FIM alert Evidence + file listing.

- **Schedule enforcement:** show pfSense rule active during the one-hour window, and that outside the window access is blocked (logs).
- **Social media blocking:** attempt access during blocked hours from LAN2 → blocked page Evidence + Wazuh/proxy log entry.
- **AD & GPO evidence:** OUs/users + GPOs applied to client (gpresult) + successful software installation via GPO.
- **NTOPng reports:** show baseline traffic and an anomaly resulting from Kali scan or other traffic spike.
- **Backup/restore:** `config.xml` attached and restore test Evidence.

Video Requirements (must be followed exactly)

Duration: 15–20 minutes (minimum 15). Be thorough and precise.

Sequence (required):

1. Introduce yourself: full name, StudentID and class group.
2. Show topology diagram and explain addressing.
3. PfSense: show interfaces, NAT, DHCP for LAN2, captive portal disabled, firewall rules (with `StudentID` naming), schedules for Kali and social media block, NTOPng dashboard, and backup configuration.
4. AD: show Active Directory console, OUs and users, key GPOs (roaming, mapped drives, password policy), and NTP config.
5. IIS portfolio: open the portfolio in a browser (StudentID visible).
6. Linux docs: open each tab and show evidence Evidences for each major task.
7. Wazuh: show manager dashboard, agent list, sample alerts (FIM, Windows events, IDS events), and custom rules in action.
8. IDS: show Suricata alert in EVE and correlate to Wazuh.
9. VPN: demonstrate OpenVPN certificate named with `StudentID` and successful IT OU client access to LAN1.
10. Kali: run a short `nmap` and show corresponding IDS/Wazuh detection (live or recorded with timestamps).
11. Restore demo: restore pfSense config or re-register a Wazuh agent to show recovery steps.
12. Conclusion: summarize findings and lessons learned.

Quality expectations: clear narration, face-in-picture webcam, no background noise, section banners between segments.

Scoring impact: missing steps or missing evidence in video leads to deductions as per the academic honesty rule.

Grading Rubric (total 100 points)

Category	Points	Key deliverables
pfSense & network config	15	Interfaces, NAT, DHCP (LAN2), firewall rules w/ `StudentID`, schedules, OpenVPN (Remote Access), NTOPng
Active Directory & GPOs	15	DC promotion, OUs/users, GPOs (roaming, mapped drives, software deploy), NTP
Wazuh manager & agents	20	OVA deployed & hostname `StudentID`, agents enrolled, FIM includes roaming & mapped folders, log ingestion
IDS integration & tuning	15	Suricata/Snort deployed, EVE ingestion to Wazuh, tuned rules & alerts
Kali tests & detection evidence	15	One-hour pentest window enforced & logs show detection/correlation
Documentation site (multi-tab)	10	Step-by-step docs with Evidences, timestamps and explanations
Video & presentation	10	All required segments present, face-in-picture, clear narration

> **Dishonesty policy:** claiming a task done without evidence results in negative points equal to the task weight.

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!