Project Breakdown

The project consists of three main parts:

1- Hardening Ubuntu (Host System) → Securing your main OS
2- Setting up a Windows VM → Simulating an enterprise endpoint for security monitoring
3- Monitoring & Logging Security Events → Using auditd Sysmon, and network monitoring tools

---

🔴 Part 1: Hardening Ubuntu (Host)

The first part of the project focuses on securing your Linux machine against common cyber threats.

✅ Steps in Ubuntu Hardening

🔹 Disable Root SSH Login & Secure Remote Access

- Prevent brute force attacks on SSH by disabling root login
- Set up fail2ban to block repeated failed login attempts

🔹 Configure UFW (Uncomplicated Firewall) to Control Network Traffic

- Set strict rules for inbound and outbound connections

🔹 Enable AppArmor for Process Isolation

- Restrict system processes from performing unauthorized actions

🔹 Implement System Logging with auditd

- Monitor and log system changes, failed login attempts, and file modifications

🔹 Disable Unused Services & Secure File Permissions

- Reduce attack surface by disabling unnecessary background services

🔹 Check for Open Ports & Remove Unused Software

- Identify exposed services that could be exploited by attackers

✅ **Outcome:** Your Ubuntu system will be hardened and protected against unauthorized access.

🟡 Part 2: Setting Up a Windows VM

The second part of the project involves installing a Windows 11 virtual machine on Ubuntu using KVM (Kernel-based Virtual Machine). This VM will be used to simulate a Windows system in an enterprise environment, where we will apply security controls and monitoring tools. Or you can also use your computer if you have windows systems on it.

✅ Steps in Windows VM Security Hardening

🔹 Disable SMBv1 (Protection Against Ransomware Attacks)

- SMBv1 is an outdated protocol exploited by threats like WannaCry

🔹 Enable Windows Defender & Controlled Folder Access

- Prevent unauthorized modification of important files

🔹 Set Up Windows Firewall Rules

- Block all unnecessary inbound traffic except for required services

🔹 Install & Configure Sysmon (System Monitor)

- Capture detailed logs of process creation, network connections, and file changes

🔹 Use Wireshark to Capture Network Traffic

- Analyze network activity and detect suspicious traffic

✅ **Outcome:** Your Windows VM will be secured, and you will collect logs for security analysis.

🟢 Part 3: Security Monitoring & Analysis

This part of the project involves collecting and analyzing security logs from Ubuntu and Windows.

✅ Steps in Security Monitoring

🔹 Monitor Linux System Logs with auditd

- Detect unauthorized file modifications and failed login attempts

🔹 Monitor Windows Logs with Sysmon

- Track process execution, network connections, and registry changes

🔹 Use Wireshark to Capture & Analyze Traffic

- Identify potential attacks by analyzing network packets

🔹 **Simulate a Cyber Attack (Ethical Testing)**

- Run a **brute-force attack on SSH (using Hydra) or simulate malware execution on Windows**
- Capture and analyze logs to understand the attack pattern

✅ **Outcome:** You will have **real-world security logs and forensic data**, which you can analyze and document.

📌 Final Deliverable: Security Report & Resume Project

After completing this project, you will compile a detailed security report that can be added to your resume, GitHub, or portfolio.

🚀 How to Present This on Your Resume

💡 Example Resume Entry:

Windows & Linux Security Hardening & Monitoring Project

- Implemented security hardening techniques on an Ubuntu host and Windows VM

- Configured firewall rules (UFW & Windows Defender Firewall) to restrict network access

- Deployed Sysmon & auditd for real-time security monitoring & logging

- Captured and analyzed network traffic using Wireshark for intrusion detection

- Simulated cyber-attacks to test and improve system defenses.