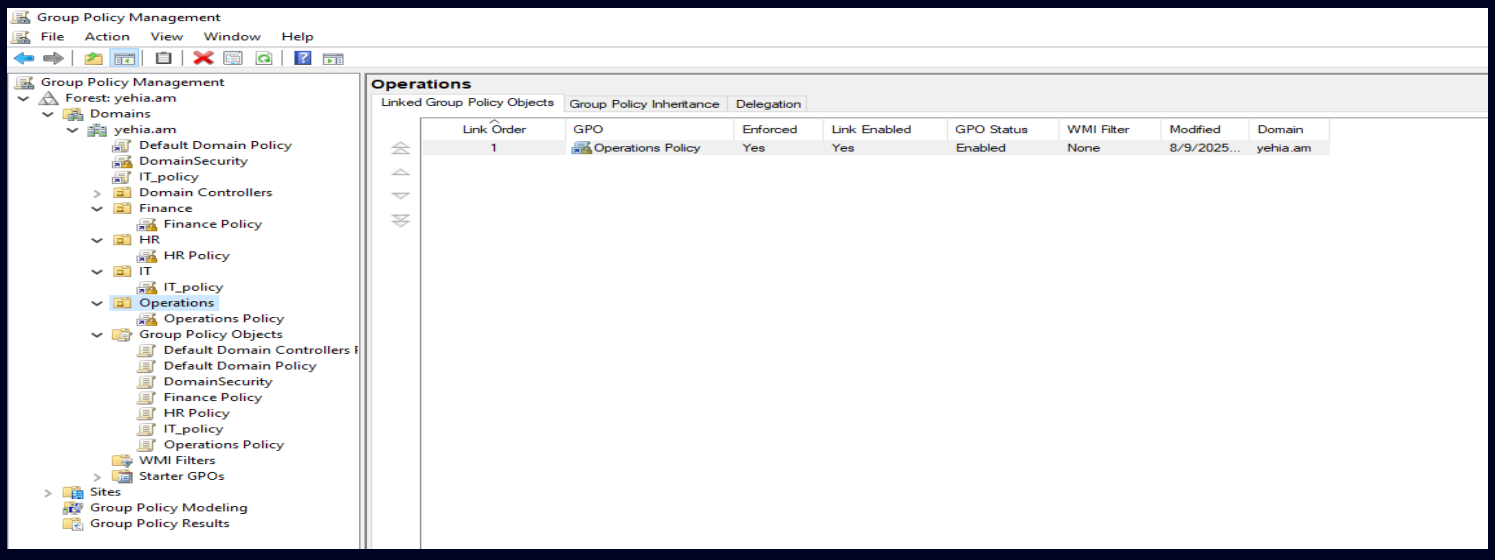
zero$ploit

WINDOWS ENVIRONMENT DESIGN AND SECURITY HARDENING FOR HORIZON TECHNOLOGY

A Mid-sized tech company's environment using Active Directory for centralized identity and policy control.

WE INNOVATE BOOTCAMP – 2025

- **Yehia A. Mostafa**
  - *Documentation, Windows Server, & 2 Departments (3 VMs)*
- **Zeyad T. Ghoneim**
  - *2 Departments (2 VMs), & github*



zero$ploit

PROJECT OVERVIEW

Design and implement a secure Windows environment for Horizon Technology (mid-sized tech company). The environment uses Active Directory (AD) for centralized identity and policy control.

DESIGN GOALS

- Centralized identity, least privilege, and auditability
- Departmental isolation via OUs + scoped GPOs
- Domain-wide security baseline (passwords, lockout, Defender, auditing)
- Per-department hardening tailored to risk profile (IT, HR, Finance, Operations)
- Secure remote/admin access and encrypted remote connectivity for branch/remote VMs (Tailscale)

zero$ploit

OU HIERARCHY

- yehia.am
  - OU=IT
    - IT_Computer
    - IT_Admin
  - OU=HR
    - HR_Computer
    - HR_Admin
  - OU=Finance
    - Finance_Computer
    - Finance_Admin
  - OU=Operations
    - Operations_Computer
    - Operations_Admin

zero$ploit

Policies Applied

DOMAIN-LEVEL POLICIES

1. **Password Policy**: Minimum 12-character passwords, complexity enabled, 90-day expiration, and 24-password history.
2. **Account Lockout Policy**: Lockout after 5 failed attempts for 15 minutes.
3. **Windows Defender Configuration**: Real-time protection, daily scans, and cloud-based protection enabled.
4. **Audit Policy**: Audit logon events, account management, and policy changes (Success and Failure).
5. **Network Firewall Configuration**: Enable firewall for all profiles, block inbound connections except allowed ones, and log blocked outbound traffic.

DEPARTMENT-LEVEL POLICIES

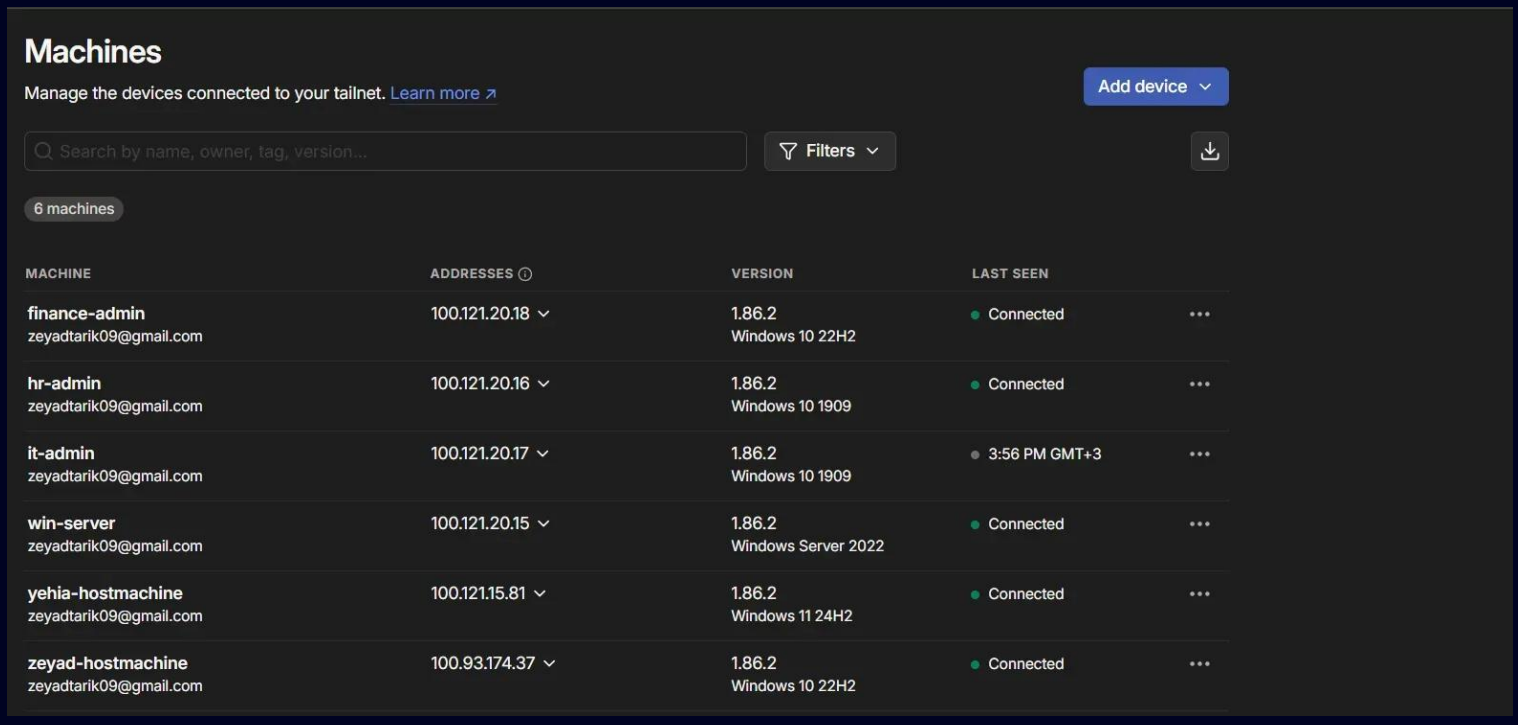
- **IT**: Administrative privileges, flexible software installation, and enhanced logging.
- **HR**: BitLocker encryption, AppLocker restrictions, and file access auditing.
- **Finance**: MFA, USB restrictions, and rapid screen locks.
- **Operations**: Device control, internet access restrictions, and audit logging for operational data.

zero$ploit

CONFIGURATION STEPS & JUSTIFICATIONS

1. SETTING UP TAILSCALE FOR REMOTE CONNECTIONS

Added all VMs to the Tailscale admin portal where we could configure networking settings. We also used the WinServer machine as the DNS of the network on both (the admin console and statically on the etho adapters). All VMs were configured to obtain ips automatically.



After configuring all networking settings, we started testing the connectivity and that every device is visible to other devices.

zero$ploit

2. GROUP POLICY OBJECTS (GPOs)

HR DEPARTMENT GPOs

- Required BitLocker encryption with recovery keys stored in AD.
- Configured AppLocker to allow only signed applications and block executables in user-writable directories.
- Enabled auditing for file access (Success and Failure) on HR shared folders.
- **Justification**: Encryption protects sensitive employee data, AppLocker prevents malware, and file access auditing ensures compliance with GDPR by tracking access to HR data.

FINANCE DEPARTMENT GPOs

- Enforced MFA for Finance users via Windows Hello or smart cards.
- Restricted USB devices to read-only and blocked unauthorized storage devices.
- Set screen lock after 5 minutes of inactivity with password required.
- **Justification**: MFA reduces account compromise risks for financial transactions, USB restrictions prevent data exfiltration, and rapid screen locks secure unattended workstations, aligning with PCI DSS.

zero$ploit

OPERATIONS DEPARTMENT GPOs

- Restricted device installation to authorized hardware (e.g., approved scanners and printers).
- Limited internet access to business-critical sites via proxy settings.
- Enabled auditing for operational data access (Success and Failure).
- **Justification**: Device restrictions prevent unauthorized hardware from compromising operational systems, internet restrictions reduce exposure to web-based threats, and auditing ensures tracking of access to operational data (e.g., production schedules), supporting operational integrity.

IT DEPARTMENT GPOs

- Allowed IT users in the local Administrators group and enabled Remote Desktop.
- Disabled AppLocker restrictions to allow software installation.
- Enabled auditing for privilege use and process tracking (Success and Failure).
- **Justification**: IT staff require administrative access and Remote Desktop for system management. Flexible software installation supports their role, while enhanced logging monitors privileged actions to prevent misuse.

zero$ploit

3. CUSTOM SECURITY SETTINGS

- Verified domain and department GPO settings via Group Policy Management Console (GPMC) using each admin's user (shown in the github repo) and applied additional configurations
    - Ensured Windows Defender real-time protection is active across all systems.
    - Configured AppLocker rules for HR and Operations using GPMC.
- **Justification**: These settings reinforce domain and department policies, mitigating malware, unauthorized device usage, and data breaches while ensuring scalability

GITHUB REPOSITORY

All configuration files, scripts, and exported GPO reports are available in the GitHub repository