This memo outlines the server hardening measures that have been implemented across all Windows and Linux servers in our topology. The primary objective of this initiative was to reduce the attack surface and strengthen our defenses against unauthorized access by implementing a consistent, secure baseline configuration.

Our methodology is based on industry-standard best practices, primarily adhering to the principles outlined in the **CIS (Center for Internet Security) Benchmarks** for each respective operating system.

Universal Hardening Principles

The following principles were applied to all servers in the topology:

- **Principle of Least Privilege:** Users and services are only granted the absolute minimum permissions required to perform their function.
- **Default Deny:** All network traffic is blocked by default on host-based firewalls. Only explicitly allowed services are permitted.
- **Attack Surface Reduction:** All unnecessary software, services, and features have been disabled or uninstalled.

Windows Server Hardening Checklist (Applied to AD/DNS, Web, FTP, Wkst-Win11)

The following configuration changes were implemented on all Windows-based systems.

[Imaginary Screenshot 1: Local Security Policy editor showing Password Policy settings (e.g., complexity enabled, minimum length set to 12). Caption: "Figure 1: Enforcing Strong Password Policies via GPO/Local Security Policy."]

- **Password changes**
- **Security Policy Enforcement:**
    - **Password Policy:** Enforced complexity requirements, a minimum length of 12 characters, and a history of 24 passwords.
    - **Account Lockout Policy:** Configured to lock out an account after 5 invalid logon attempts.
    - **Audit Policy:** Enabled detailed logging for logon events, account management, and object access failures.
- **Windows Defender Firewall:**
    - Enabled the firewall on all network profiles (Domain, Private, Public).

    - Set the default inbound and outbound behavior to **Block**.
    - Created specific "Allow" rules only for the necessary services identified for each server's role (e.g., DNS/LDAP on the AD server, HTTPS on the Web server).
- **Services and Features:**
    - Disabled unnecessary services such as "Windows Media Player Network Sharing" and "Print Spooler" (on non-print servers).
    - Uninstalled superfluous features like the "Wireless LAN Service" and "Media Foundation."
- **Centralized Logging:**
    - Configured the system to forward all critical Security, System, and Application event logs to our central Splunk server.

[Imaginary Screenshot 2: Windows Defender Firewall advanced settings showing the inbound rule list with a "Block (default)" rule and a few specific "Allow" rules for services like DNS and RDP. Caption: "Figure 2: Host Firewall configured for Default Deny."]

Linux Server Hardening Checklist (Applied to Ecom, Webmail, Splunk, Wkst-Ubuntu)

The following configuration changes were implemented on all Linux-based systems.

[Imaginary Screenshot 3: A terminal showing the command `sudo ufw status verbose` with the output displaying "Status: active", "Default: deny (incoming), allow (outgoing)", and specific allow rules for SSH and HTTP/S. Caption: "Figure 3: UFW Host Firewall with Default Deny Policy."]

- **Password Changes**
- **System Updates:**
    - Ensured all packages are fully up-to-date using `sudo apt update && sudo apt upgrade` (for Ubuntu) and `sudo dnf upgrade` (for Fedora/Oracle).
- **Host-Based Firewall (`ufw`):**
    - The firewall was enabled and configured with a **default deny** policy for all incoming traffic.
    - Specific `allow` rules were created only for necessary services (e.g., allowing inbound HTTPS on Ecom/Webmail, allowing inbound SSH from internal admin workstations).

- **SSH Server Hardening (`/etc/ssh/sshd_config`):**
    - Disabled direct root login (`PermitRootLogin no`).
    - Disabled password-based authentication in favor of key-based authentication (`PasswordAuthentication no`).
    - Set a specific "AllowUsers" list to limit access to authorized administrators.
- **Centralized Logging (`rsyslog`):**
    - The `rsyslog` service was configured on each host to forward all `auth.log` and `syslog` events to our central Splunk server.

[Imaginary Screenshot 4: A snippet of the `/etc/ssh/sshd_config` file showing the line `PermitRootLogin no` uncommented. Caption: "Figure 4: SSH server configured to deny direct root login."]

By implementing these standardized hardening configurations, we have significantly improved the security posture of our server infrastructure.

Hardening Technique	Relevant Industry controls (primarily NIST SP 800-53)	Explanation of the Control
Attack Surface Reduction (Disabling unnecessary services/software)	**CM-7: Least Functionality**	This control requires that the information system is configured to provide only essential capabilities. It prohibits the use of functions, ports, protocols, and services that are not required for the business function of the system.
Principle of Least Privilege (Limiting user and service	**AC-6: Least Privilege**	This is a foundational control that requires an organization to enforce the most restrictive set of rights and permissions needed for users (or processes acting on behalf of users) to perform their authorized tasks.

permissions)		
Host-Based Firewall (Default Deny policy)	**AC-4: Information Flow Enforcement**	This control mandates that the system enforces approved authorizations for controlling the flow of information between different security domains (e.g., from an external network to an internal system). A "default deny" firewall is a direct implementation of this.
System Updates / Patch Management	**SI-2: Flaw Remediation**	This control requires that organizations identify, report, and correct information system flaws in a timely manner. This includes installing security-relevant software and firmware updates.
Secure SSH Configuration (Disable root login, use keys)	**AC-3: Access Enforcement** **IA-5: Authenticator Management**	AC-3 requires the system to enforce approved authorizations for logical access. Disabling root login is a form of this. IA-5 manages authenticators (like passwords or keys) and includes requirements for using strong, multi-factor, or key-based authentication.
Strong Password & Lockout Policies	**IA-5: Authenticator Management** **AC-7: Unsuccessful Logon Attempts**	IA-5 defines the minimum requirements for password complexity, length, and history. AC-7 requires the system to enforce a limit on the number of consecutive invalid logon attempts and automatically lock the account for a set period.
Malware & Virus Protection	**SI-3: Malicious Code Protection**	This control requires the use of malicious code protection mechanisms (antivirus, anti-malware) at various locations within the system. It also includes configuring these tools to be updated automatically.

Centralized & Audit Logging	**AU-2: Audit Events** **AU-4: Audit Storage Capacity**	AU-2 requires the system to generate audit records for a defined set of events. AU-4 requires allocating sufficient storage for audit records and configuring the system to prevent them from being overwritten (which centralized logging helps achieve).

Windows

Hardening Technique	Industrial Control	Implementation on Team-07 devices
Changing Default Credentials	IA-5: Change Default Passwords	
Update Device	SI-2: Flaw Remediation	
Windows Firewall Defender	AC-4: Information Flow Enforcement	
SSH Configuration (disable)	AC-3: Access Enforcement CM-7: Least Functionality	
Restrict User Access (Principle of Least Privilege)	AC-6: Least Privilege	
Disable Unnecessary services	CM-7: Least Functionality	

Linux Based Devices (Ubuntu 24, Fedora, Oracle)

Hardening Technique	Industrial Control	Implementation on Team-07 devices
Changing Default Credentials	IA-5: Change Default Passwords	
Update Device	SI-2: Flaw Remediation	
Host Based Firewall	AC-4: Information Flow Enforcement	
SSH Configuration (disable)	AC-3: Access Enforcement	
Restrict User Access (Principle of Least Privilege)	AC-6: Least Privilege	
Disable Unnecessary services	CM-7: Least Functionality	