Hardening your Ubuntu system in accordance with the CIS benchmarks involves a multi-layered approach focusing on package management, user and group management, service management, logging and monitoring, and network security. Here's an overview of key CIS recommendations:

1. Package Management:

- **Keep Updated:** Regularly update the operating system and software packages using tools like apt update and apt upgrade to address security vulnerabilities.
- **Unnecessary Packages:** Identify and remove any unnecessary packages from your system to minimize your attack surface. Tools like dpkg list and apt list can help identify unused packages.

2. User and Group Management:

- **Disable Root Login:** Consider disabling remote root login (SSH) to reduce the risk associated with compromised root credentials. Use sudo for administrative tasks when needed.
- **Least Privilege:** Enforce the principle of least privilege by creating users with restricted permissions based on their specific tasks. Avoid using privileged accounts for everyday activities.
- **Inactive Accounts:** Disable or delete inactive user accounts to minimize potential attack vectors.

3. Service Management:

- **Unnecessary Services:** Identify and disable any unnecessary system services to reduce the attack surface and improve system performance. Tools like systemctl list-unit-files can help identify services.
- **Secure Services:** For essential services, configure them securely to minimize their attack surface. This might involve adjusting configuration files and access permissions.

4. Logging and Monitoring:

- **Enable Logging:** Enable appropriate logging for system events, security-related activities, and application logs. Review logs regularly to identify suspicious activity or potential security issues.
- **Centralized Logging (Optional):** Consider setting up a centralized logging server to collect and analyze logs from multiple systems for improved visibility.

5. Network Security:

- **Firewall Configuration:** Implement a firewall to restrict incoming and outgoing network traffic. Allow only authorized connections to specific ports based on your system's purpose.
- **Deny All (Optional):** For high-security environments, consider a "deny all" approach on the firewall, explicitly allowing only the necessary traffic.

Additional Resources:

- CIS Ubuntu Linux Benchmark: While the specific document might not be publicly available, security guides referencing CIS benchmarks can offer details. Search for "CIS Ubuntu Linux Benchmark".
- Ubuntu documentation on security: https://ubuntu.com/security
- Ubuntu documentation on hardening: https://ubuntu.com/blog/18-04-end-of-standard-support

Remember:

- These are general recommendations. The specific CIS controls and configurations will vary depending on your Ubuntu version and the specific benchmark revision you're following.
- Consult the official CIS Ubuntu Linux Benchmark for your version for detailed security recommendations.
- Regularly review and update your system hardening practices to maintain a secure environment.