

Here's an overview of how to set up system and software security configurations on MySQL securely on Ubuntu in accordance with the CIS benchmarks:

1. Package Management:

- **Keep Updated:** Regularly update the operating system and MySQL packages to address security vulnerabilities. Utilize tools like apt update and apt upgrade to keep your system patched.
- **Unnecessary Packages:** Identify and remove any unnecessary packages from your system to minimize your attack surface.

2. User and Group Management:

- **Disable Root Login:** Consider disabling remote root login to the MySQL server. This reduces the risk associated with compromised root credentials.
- **Least Privilege:** Apply the principle of least privilege to system users and groups. Grant only the minimum permissions required for their tasks.

3. Service Management:

- **Disable Unnecessary Services:** Identify and disable any unnecessary system services that could be exploited by attackers.

4. Logging and Monitoring:

- **Enable Logging:** Enable appropriate logging for MySQL server activity and system events. This helps with security analysis and incident detection.
- **Review Logs Regularly:** Regularly review logs to identify suspicious activity or potential security issues.

5. Network Security:

- **Firewall Configuration:** Configure your firewall to restrict access to the MySQL server port (default: 3306) only from authorized IP addresses.
- **Deny All:** Consider a "deny all" approach on the firewall, explicitly allowing only the necessary traffic.

6. Secure Configuration Files:

- **Review Configuration:** Review the MySQL configuration file (/etc/mysql/my.cnf) for security-sensitive settings. The CIS benchmarks will likely recommend specific configurations for options like bind-address to restrict access and disable unnecessary features.
- **Permissions:** Ensure the configuration files have appropriate permissions to prevent unauthorized modification.

Additional Resources:

- CIS MySQL Security Benchmarks (reference security guides that mention these

benchmarks): While not directly available online, security guides referencing CIS benchmarks can offer details. Search for "CIS MySQL Security Benchmarks Ubuntu".

- Ubuntu documentation on security: <https://ubuntu.com/security>
- MySQL documentation on security: <https://dev.mysql.com/doc/refman/8.0/en/security.html>

Remember:

- This is a general overview based on common CIS recommendations. The specific controls and configurations will vary depending on your Ubuntu version and the CIS benchmark revision you're following.
- Consult the official CIS MySQL benchmarks for your Ubuntu version for the most up-to-date and detailed security recommendations.
- Regularly review and update your system and software security configurations to maintain a secure environment.