Copilot

Certainly! Setting up **MySQL accounts and authentication securely on Ubuntu** in accordance with the **CIS (Center for Internet Security) benchmarks** is essential for safeguarding your database. Let's walk through the steps:

1. **Understanding CIS Benchmarks**:
   - **CIS Benchmarks** provide best practices and guidelines for securing systems.
   - They offer specific configuration recommendations to minimize security risks.
   - The **CIS MySQL Benchmark** focuses on securing MySQL Enterprise Edition 8.0.
2. **Install MySQL**:
   - If you haven't already, install MySQL on Ubuntu using:

     ```
     sudo apt install mysql-server
     ```
3. **Create MySQL Users**:
   - Create separate users for different purposes (e.g., application, administration).
   - Avoid using the root account for regular tasks.
   - Use strong passwords for each user.
4. **Grant Permissions**:
   - Grant minimal privileges to each user based on their role.
   - For example, use the following command to grant permissions to a user named `myuser`:

     ```
     GRANT SELECT, INSERT, UPDATE, DELETE ON mydb.* TO 'myuser'@'localhost' IDENTIFIED BY 'mypassword';
     ```
5. **Secure Authentication**:
   - Use **strong authentication mechanisms**:
     - **SHA-256 password hashing** (default in MySQL 8.0)
     - **Authentication plugins** (e.g., `caching_sha2_password`)
   - Disable **old authentication methods** (e.g., `mysql_native_password`).
6. **Audit User Accounts**:
   - Regularly review user accounts and their privileges.
   - Remove unnecessary accounts.
   - Ensure each account has the least privilege necessary.
7. **Network Access Control**:
   - Bind MySQL to specific IP addresses (avoid binding to all interfaces).
   - Modify the `bind-address` directive in `/etc/mysql/mysql.conf.d/mysqld.cnf`.
8. **TLS Encryption**:
   - Enable **SSL/TLS** for secure communication.
   - Generate SSL certificates and configure MySQL to use them.
9. **Logging and Auditing**:
   - Enable MySQL **audit logging**.
   - Log failed login attempts, privilege changes, and other critical events.
10. **Regularly Review CIS Benchmarks**:
    - Stay informed about updates to the benchmarks.
    - Continuously assess and adjust your MySQL configuration.

Remember that these steps are a starting point. Always adapt them to your specific environment and business needs. By following these guidelines, you'll enhance the security of your MySQL installation on Ubuntu. 🛡️🔒

For more detailed instructions, refer to the CIS Benchmark for MySQL Enterprise Edition and the Ubuntu Security Guide.