Kaya Nelson

CST – 221

Micheal Landreth

06/16/2024

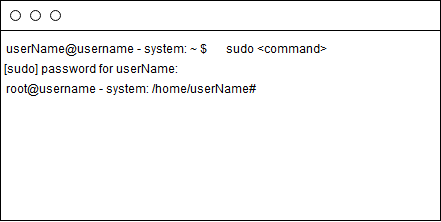
GitHub Link: [Kdeshun/CST-221-WEEK-7 (github.com)](https://github.com/Kdeshun/CST-221-WEEK-7)

**User Interface and Security**

Single-Factor Authentication for Elevated Privileges  
Accessing Superuser Capabilities through the Command Line

The superuser authentication process is carried out within the terminal environment, seamlessly integrating the user interface. The authentication factor in this case is the password associated with the superuser account. Key security measures that must be implemented include, but are not limited to, password validation, password anonymity, password entry timeout, and unique character processing.

* The password must be entered directly in the terminal
* The password characters will not be visually displayed to the user
* Inputs exceeding the maximum allowed length will be rejected and an error will be generated
* Non-alphanumeric characters will not be accepted as valid input
* The password will be encrypted and compared against the stored password
* The password will be stored in an encrypted format
* The system will check for proper input, and blank fields will be rejected
* A failsafe mechanism will be triggered after a certain number of incorrect password attempts
* The superuser access attempt will be discarded after a predefined period of user inactivity
* Password requirements will include a minimum of 8 characters and the inclusion of at least one special character



A diagram of a software process

Description automatically generated

Two-Factor Authentication: Secure Login through Username and Password

The username and password authentication process is typically employed for login purposes, with a dedicated screen for user verification. The two factors in this authentication scheme are the username and password associated with the user's account. Security measures that must be implemented include, but are not limited to, username validation, password validation, password encryption, password anonymity, unique character processing, and length verification.

* The username and password are bound to a specific host within the system
* The username is limited to a maximum length of 50 characters
* Both the username and password can include non-alphanumeric characters
* The password is limited to a maximum length of 25 characters
* Password requirements include a minimum of 8 characters and the inclusion of at least one special character
* Password encryption is supported, but only for the password field
* The password will be displayed as bullets instead of the actual character representation
* A password reminder will be triggered after a failed login attempt
* The password will be locked for 1 minute after 3 failed attempts, and the lockout duration will double for each additional failure

A screenshot of a computer login box

Description automatically generated

A diagram of a system

Description automatically generated

Secure Database Access: A Multi-Factor Authentication Approach

Database connections are typically established within the functional context of a program, although an interface can be utilized to input and manage the various authentication factors. In this multi-factor authentication scheme, the key factors include the database port, database name, root username, and root password. Security measures that must be implemented include, but are not limited to, port authentication, username authentication, password authentication, database authentication, and connectivity monitoring.

* The input for the database port will be checked for length and numerical data
* The username will be authenticated by comparing it to the entry stored in the database
* The username length will be restricted to a maximum of 50 characters
* The password requirements will include a minimum of 8 characters, with at least one special character
* The password will be encrypted
* The password length will be restricted to a maximum of 25 characters
* The password will be authenticated by comparing it to the entry stored in the database
* The target database will be authenticated
* The database name length will be restricted to a maximum of 50 characters

A screenshot of a computer

Description automatically generated

A diagram of a program

Description automatically generated