- **DAY FOUR**
- Working with Text Files
- **Local Users and Groups**
- Permissions
- Processes

CHAPTER 5: MANAGING LOCAL LINUX USERS AND GROUPS

- Users and Groups
- Gaining Superuser Access
- Managing Local User Accounts
- Managing Local Group Accounts
- Managing User Passwords

GOAL:

- To manage local Linux users and groups and administer local password policies.

OBJECTIVES:

- Explain the role of users and groups on a Linux system and how they are understood by the computer.
- Run commands as the superuser to administer a Linux system.
- Create, modify, lock, and delete locally defined user accounts.
- Create, modify, and delete locally defined group accounts.
- Lock accounts manually or by setting a password-aging policy in the shadow password file.

THE LINUX SECURITY MODEL

- Users and groups are used to control access to files and resources
- Users log in to the system by supplying their user name and password
- Every file on the system is owned by a user and associated with a group
- Every process has an owner and group affiliation, and can only access the resources its owner or group can access

USERS

- Every user of the system is assigned a unique User ID number (the uid)
- Users' names and uids are stored in /etc/passwd
- Users are assigned a home directory and a program that is run when they log in (usually a shell)
- Users cannot read, write or execute each others' files without permission

GROUPS

- **Users are assigned to groups with unique group ID numbers (the gid)**
- **gids are stored in /etc/group**
- **Each user is given their own private group**
  - They can also be added to other groups to gain additional access
- **All users in a group can share files that belong to the group**

THE ROOT USER

- **The root user: a special administrative account**
  - Sometimes called the *superuser*
  - **root** has complete control over the system
    - An unlimited capacity to damage the system!
  - You should not log in as **root** without a very good reason
    - Normal ("unprivileged") users' potential to do damage is limited

USER AND GROUP ID NUMBERS

- User names map to user ID numbers
- Group names map to group ID numbers
- Data stored on the hard disk is stored numerically

/ETC/PASSWD, /ETC/SHADOW, AND /ETC/GROUP FILES

- **Authentication information is stored in plain text files:**
  - /etc/passwd
  - /etc/shadow
  - /etc/group
  - /etc/gshadow

SYSTEM USERS AND GROUPS

- **Server programs such as web or print servers typically run as unprivileged users, not as root**
  - Examples: **daemon, mail, lp, nobody**
- **Running programs in this way limits the amount of damage any single program can do to the system**

CHANGING YOUR IDENTITY

- **To change your password, run passwd**
  - Insecure passwords are rejected
- **To start a new shell as a different user:**
  - **su**
  - **su –**
  - **su *username***
  - **su – *username***

SWITCHING ACCOUNTS

- **Syntax**
  - **su [-] [user]**
  - **su [-] [user] -c command**
- **Allows the user to temporarily become another user**
  - Default user is root
- **The "-" option makes the new shell a login shell**

SUDO

- **Users listed in /etc/sudoers execute commands with:**
  - an effective user id of 0
  - group id of root's group
- **An administrator will be contacted if a user not listed in /etc/sudoers attempts to use sudo**

ADDING A NEW USER ACCOUNT

- **Most common method is useradd:**
  - **useradd username**
- **Running useradd is equivalent to:**
  - edit **/etc/passwd**, **/etc/shadow**, **/etc/group**
  - create and populate home directory
  - set permissions and ownership
- **Set account password using passwd**
- **Accounts may be added in a batch with *newusers***

USER PRIVATE GROUPS

- **When user accounts are created, a private group is also created with the same name**
  - Users are assigned to this private group
  - User's new files affiliated with this group
- **Advantage: Prevents new files from belonging to a "public" group**
- **Disadvantage: May encourage making files "world-accessible"**

GROUP ADMINISTRATION

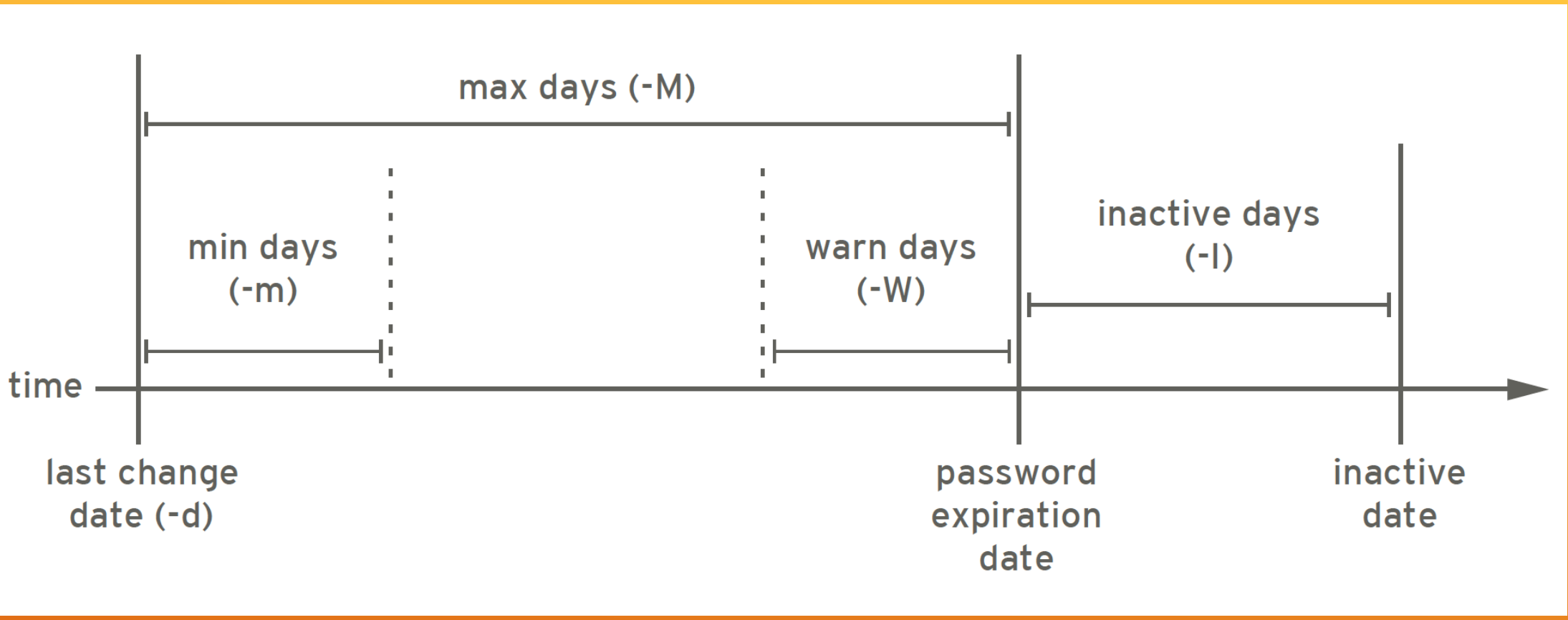
- Entries added to /etc/group
  - groupadd
  - groupmod
  - groupdel

MODIFYING / DELETING ACCOUNTS

- **To change fields in a user's /etc/passwd entry you can:**
  - Edit the file by hand
  - Use **usermod [options] username**
- **To remove a user either:**
  - Manually remove the user from **/etc/passwd**, **/etc/shadow**, **/etc/group**, **/var/spool/mail**
- **Use userdel [-r] username**

PASSWORD AGING POLICIES

- By default, passwords do not expire
- Forcing passwords to expire is part of a strong security policy
- Modify default expiration settings in /etc/login.defs
- To modify password aging for existing users, use the chage command
  - chage [options] username



PASSWORD AGING