security

- confidentiality
- integrity
- authentication / authorization

⇓

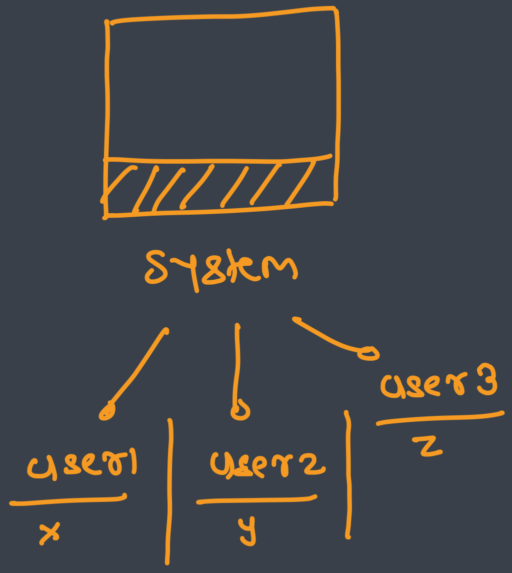
checking user is legitmade / valided user

Users

Linux Users

- A user account is used to provide security boundaries between different people and programs that can run commands
- User always have name to get identified to the human users and make them easier to work with
- Internally the OS identifies every user uniquely by using user ID or UID (integer / number)
- If a user account is used by a human user, then it will generally be assigned a password

user - sunbeam → pass
name password



Linux Users

- Superuser – root
  - → manage users / groups
  - → manage services / servers
  - → manage backup / restore
  - It is used for administration of the system
  - The superuser name is root and user id will always be 0
  - The superuser has full access to the system
- System users – hidden → used by programs ↱ processes
  - Used by the processes that provide supporting services
  - These users generally do not log in the system interactively
  - Generally they are assigned non-privileged accounts ↳

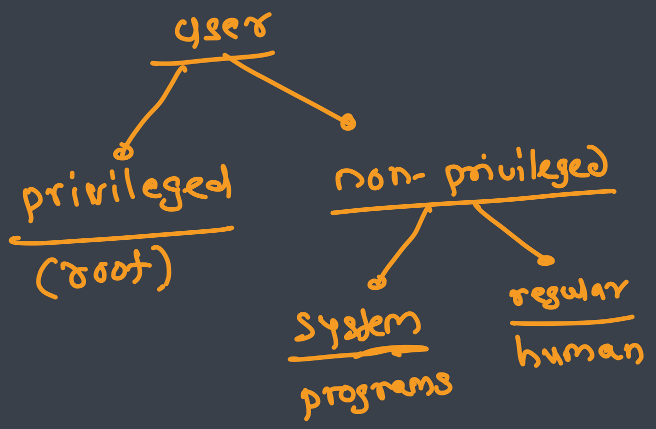
mysql → mysql user → db administrator

apache → apache user → website hosting

→ generally system users have uid between 1 to 999

- Regular users – human users
  - These accounts are generally used by human users for their day-to-day work
  - Like system users, regular users also have limited access to the system

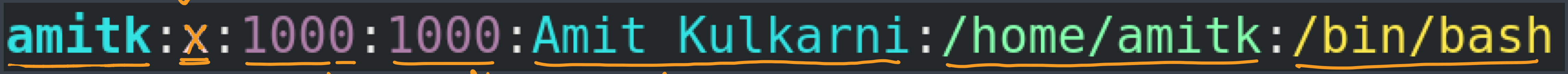
• generally uid of regular users starts from 1000



Password file

- When you create a user, Linux adds the user properties in a file /etc/passwd
- Every user is represented by a row having 7 columns

password is now stored in /etc/ shadow



```
amitk:x:1000:1000:Amit Kulkarni:/home/amitk:/bin/bash
```

user name

user id

group id

gener /display name

description

home directory

login shell

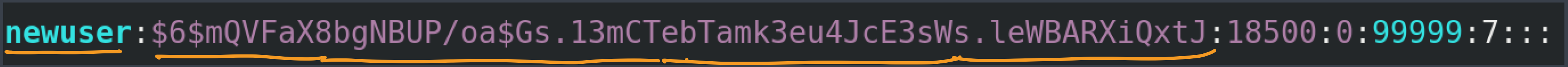
- Column 1: User name
- Column 2: Earlier it was used to store the user password. Now password is stored in /etc/shadow
- Column 3: User Id
- Column 4: Group Id
- Column 5: GECOS [General Electric Common Object Subscription] Field (Comment for a user)
- Column 6: User’s home directory
- Column 7: User’s login shell

Shadow File

- In modern Linux, user's password is stored in another file /etc/shadow

test → abcd234
↑
test → abcd234

rainbow table
⇓
brutforce



```
newuser:$6$mQVFaX8bgNBUP/oa$Gs.13mCTebTamk3eu4JcE3sWs.leWBARXiQxtJ:18500:0:99999:7:::
```

username

encrypted password → YESCRIPT algorithm

SALT (key)

- Column 1: User name
- Column 2: Encrypted Password
- Column 3: Date of last password change
- Column 4: Minimum password age
- Column 5: Maximum password age
- Column 6: Password warning period
- Column 7: Password inactivity period
- Column 8: Account expiration date
- Column 9: Reserved field

decryption is not possible
one way
YESCRIPT
MD5, SHA

decryption is possible
two way
AES, DES

plain text → encryption → cypher text
readable ← decryption ← unreable

Commands

Command	Meaning
id	Used to get id information of a user
useradd	Used to add user with different configuration
adduser	Used to add user with different configuration interactively
usermod	Used to modify user configuration
passwd	Used to configure password related settings
su	Used to switch to a user account
su -	Used to switch to root user account
sudo	Temporarily get root privileges and perform the task
userdel	Used to delete a user

System and User Profiles

- As a sysadmin, you can use a few different files to set the system up the way your institution prefers
- Use /etc/profile to set system-wide environment variables and startup programs for new user shells
- Use /etc/bashrc to establish system-wide functions and aliases for new user shells
- The ~/.bash_profile sets user-specific environment variables for new Bash shells, and ~/.bashrc runs when noninteractive shells are launched
- The tilde character (~) represents the current user's home directory
- The system-wide files process first, and then the user-specific files are executed
- The user-specific configuration files take precedence over system files, allowing users to customize their environments to suit their needs

Setting User Defaults

- useradd: used to get the default settings for new user
- /etc/login.defs is used as the default configuration file
  - Change it to make sure the passwords are valid less than 99999 days
- /etc/skel contents are copied to the user home directory upon their creation
- Linux does not offer an easy solution to apply the new default to previously created users

Managing Passwords

- Password complexity can be set using file /etc/security/pwquality.conf
- passwd:
  - Users can change their passwords using passwd command
  - As the root user, you can change a password for any account.
    - > sudo passwd <username>
  - It works with following parameters
    - -d: Delete a password and disable the account
    - -e: Immediately expire a password, forcing a password change by the user
    - -l: Lock the account (for example, during a leave of absence)
    - -u: Unlock a locked account
- chage:
  - Password requirements are also configured by using the chage command
  - It works with following parameters
    - –l: shows the current values configured for the user
    - -M: sets maximum number of days between password change
    - -m: sets minimum number of days between password change
    - -W: sets number of warning days before password expires
    - -E: lock an account after specified date

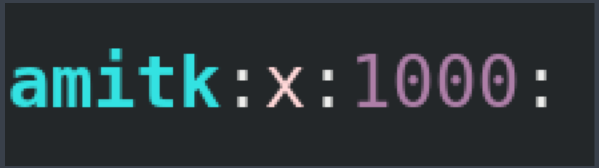
Groups

Group

- A group is a collection of users that need to share access to files and other system resources
- Groups can be used to grant access to files to a set of users instead of just a single user
- Like users, groups have group names to make them easier to work with
- Internally, the system identifies groups by the unique identification number knows as group ID or GID
- Types
  - Primary Group
    - Every user has exactly one primary group
    - By default this is the group that will own new files created by the user
    - Normally, when you create a new user, Linux adds a new group with the same name
  - Supplementary Groups
    - User may be a member of one ore more supplementary groups
    - Membership is determined by /etc/group
    - Users are granted access based on whether any of their groups have access

Group File

- Every group is represented by a line in /etc/group file



```
amitk:x:1000:
```

- Every line has 4 columns
  - Column 1: Group name
  - Column 2: Group password (this is empty as no group password is needed)
  - Column 3: Group Id
  - Column 4: A list of usernames that are the members of this group separated by commas

Commands

Command	Description
groupadd	Used to add a new group
groupdel	Used to delete a group
lid	Used to show the list of users

Understanding Session Management

- who and w show who is currently logged in
- loginctl allows for current session management
    - loginctl list-sessions
    - loginctl show-session <id>
    - loginctl show-user <username>
    - loginctl terminate-session <session-id>

Exercise

- Make sure that new users require a password with a minimum length of 6 characters and maximum validity of 90 days
- Ensure that while creating users, a file with newfile is created in their home directory with contents:
    - “this is a test file”
- Create user anna, elsa, kristoff and olaf
- Set password for anna and elsa to password and disable the password for olaf
- Create groups girls and boys
- Make users anna and elsa part of girls and kristoff and olaf part of boys

Managing Permissions

Managing Permissions

- File permissions control access to files
- Linux file permissions are simple but flexible, easy to understand and apply, yet still able to handle most normal permission cases easily
- Files have three user categories to which permissions apply
  - The file is owned by a user, normally the one who created the file
  - The file is also owned by a single group, usually the primary group of the user who created the file, but this can be changed
  - Different permissions can be set for the owning user, the owning group, and for all other users on the system that are not the user or a member of the owning group

Understanding ownership

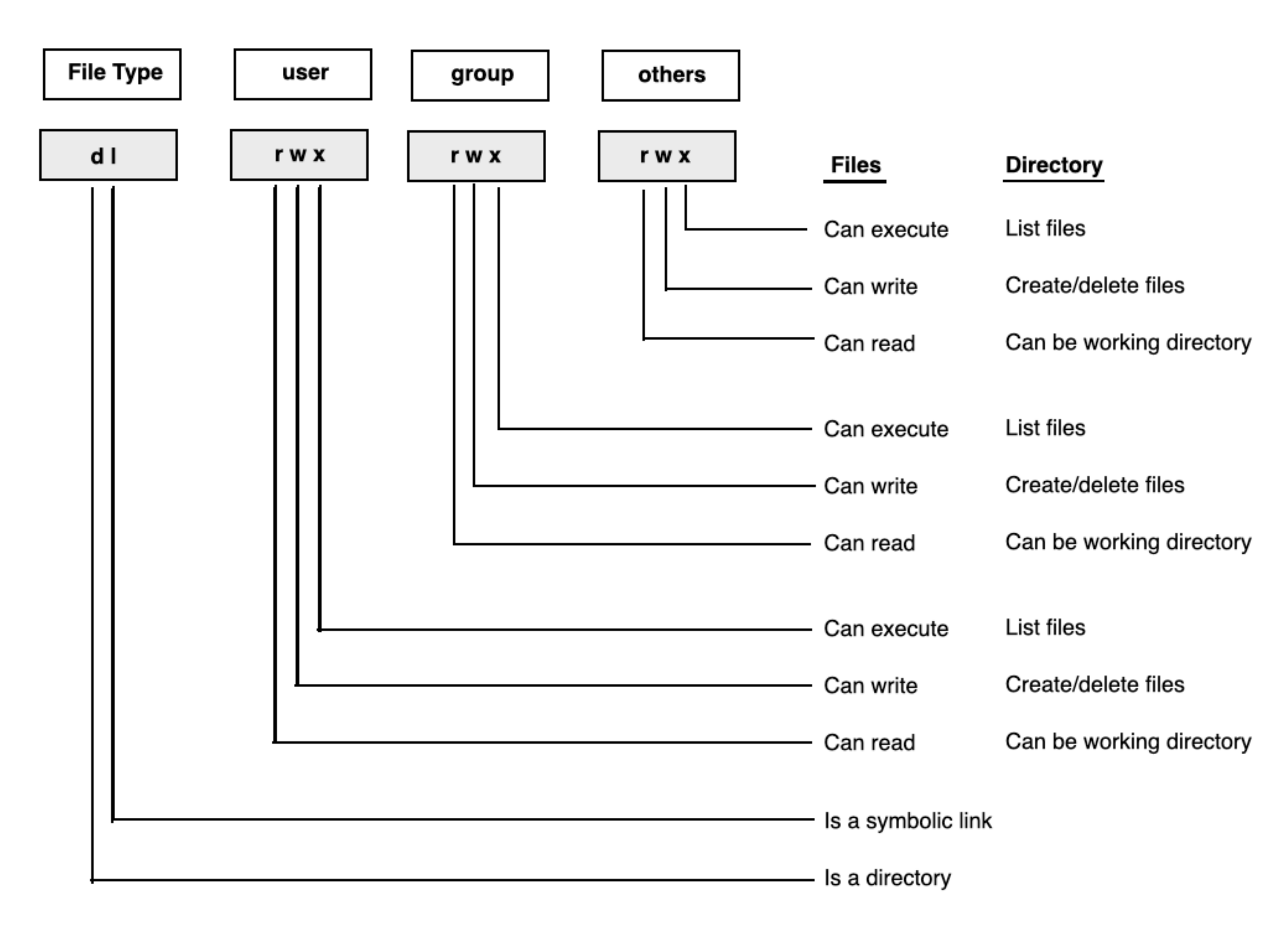
- To determine which permissions a user has, Linux uses ownership
- Every file has a user (owner), a group owner and the others entity that is also granted permissions
- Linux permissions are not additive i.e. if you are the owner, the permissions are applied and that’s all
- To be more specific, Linux tries to see who you are and applies the permissions appropriately
- Use ls –l to display current ownership and associated permissions

Understanding Permissions

- Linux uses Read, Write and Execute permissions to control the file access

Permission	Effect on files	Effect on directory
read (r or 4)	File contents can be read	Contents of directory can be listed
write (w or 2)	File contents can be changed	Any file in the directory can be created or deleted
execute (x or 1)	File can be executed as a command	Directory can become a working directory

Permissions summary



File Type

user

group

others

d l

r w x

r w x

r w x

Files	Directory
Can execute	List files
Can write	Create/delete files
Can read	Can be working directory
Can execute	List files
Can write	Create/delete files
Can read	Can be working directory
Can execute	List files
Can write	Create/delete files
Can read	Can be working directory
Is a symbolic link	
Is a directory	

Changing File Ownership

- Use **chown user[:group] file** to set the user ownership
- User **chgrp group file** to set the group ownership

Manage basic permissions

- chmod is used to manage the file permissions
- It can be used in two ways
  - Absolute
    - Uses permission int representation
    - Read (4), Write (2), Execute (1)
    - E.g.
      - chmod 750 file
  - Relative
    - Uses r, w and x instead of integer numbers
    - Uses + or – to add or remove permissions
    - E.g
      - chmod +x file

Understanding umask

- The umask is a shell settings that subtracts the umask from the default permissions
- Default permissions for a file are 666
- Default permissions for a directory are 777
- You can change the default umask