UEEN 3113 / 3413

SERVER CONFIGURATION AND MANAGEMENT

Users Management

- 2 options to add user: **useradd** and **adduser**
  - useradd

    useradd –d /home/user2 –m user2
    - -d: specify the home directory for new user, however, the directory will not be created (have to create it manually)
    - -m: specify that the new user's home directory should be created during the process

  - Use the **passwd** command to set a password for new user

    sudo passwd user2

Users Management

- 2 options to add user: **useradd** and **adduser**
  - adduser: a Perl script that helps to add new user
    - Creates a new group (usually named as user name) and adds the new user into the group
    - New user's home directory will be created automatically
    - Copy files from /etc/skel
    - Setup password
    - Prompt for other information: Full Name, Room Number, Work Phone, Home Phone and Other
  - adduser uses useradd to perform the operation

Users Management

- 2 options to add user: **useradd** and **adduser**
  - adduser adds user according to the options and configuration in /etc/adduser.conf
  - The same configuration file is also used by **addgroup**, **deluser** and **delgroup**
  - For more information about adduser, refer to the manual page (man adduser)

Manual Page

- Generally, organised into 8 sections

Section	Description
1	General / user commands
2	System calls
3	Library call / functions, particularly C standard library
4	Special files (usually devices found in /dev) and drivers
5	File formats and convention, configuration files
6	Games and funny little programs available on the system
7	Overviews of various topics, conventions and protocols, character set standards, the standard filesystem layout, and miscellaneous other things.

Manual Page

- Location: /usr/share/man
- Each manual section has an introduction which can be accessed with man command. Examples:
  - man intro
  - man 3 intro

Users Management

- A newly added user will be assigned the next available **UID**
- A newly added group will be assigned the next available **GID**
- Both UID and GID can be overwritten

Users Management

- To remove user from system: userdel
- By default, userdel will not remove user's home directory.
  - This is useful as the user's home directory might contain important files. Some company might retain user's home directory for certain period.
- To remove user's home directory at the same time we remove an account, add the –r option
  - userdel –r user_name

Users Management

- User account information is stored in special text files
  - /etc/passwd
  - /etc/shadow (accessed by root only)
- Sam

```
sshd:x:115:65534::/var/run/sshd:/usr/sbin/nologin
user:x:1000:1000:user,,,:/home/user:/bin/bash
```

- Each line contains information for each user account, divided into columns, separated by colon.

Users Management

```
user:x:1000:1000:user,,,:/home/user:/bin/bash
```

Column	Description
1	User name
2	Refer to encrypted user's password stored in /etc/shadow
3	UID
4	GID
5	User's information, commonly first and last name, might be empty
6	User's home directory

Users Management

- Sample output from sudo cat /etc/shadow

```
user:$6$9MCDX0pI$0HJoqQ8WgxAJHz5rXQsUN9I5Y1KU95kjx7Uan8vLsj/DSV9UeUtfdo9L0LovjGA54KGLKJWiG8WnJ3BU9fbiL.:17583:0:99999:7:::
```

- 1st column is the user name
- The most important part of the file is the 2nd column of each line, which is the hash for user's password.
- 3rd column is the number of days that the password last changed since 1 Jan 1970 (UNIX Epoch).
  - A better way to get the actual date: chage -l user_name

Users Management

```
user:$6$9MCDX0pI$0HJoqQ8WgxAJHz5rXQsUN9I5Y1KU95kjx7Uan8vLsj/DSV9UeUtfdo9L0LovjGA54KGLKJWiG8WnJ3BU9fbiL.:17583:0:99999:7:::
```

- 4th column is minimum password age: number of days the user has to wait password can be changed. In the sample output, it is set to 0, that means user can change password anytime.
- 5th column is maximum password age: number of days after which user will have to change the password.
- 6th column is password warning period: number of days before a password going to expire.

Users Management

```
user:$6$9MCDX0pI$0HJoqQ8WgxAJHz5rXQsUN9I5Y1KU95kjx7Uan8vLsj/DSV9UeUtfdo9L0LovjGA54KGLKJWiG8WnJ3BU9fbiL.:17583:0:99999:7:::
```

- 7th column is password inactivity period: number of days after a password expired, during which the password still be accepted and the user should update the password during next login. After this period, no login is possible.
- 8th column is account expiration date: number of days since the UNIX Epoch that will elapse before the account is disabled. In the sample output, it is not set.

Users Management

- /etc/skel
  - All the files in this directory will copied into user's home directory when it is created during the process of adding new user.
  - Any text file or configuration can be placed into this directory.

Users Management

- To switch user, use the **su** command. Examples:
  - Switch to root: sudo su
  - Switch to john: su john
- With sudo access, we can switch to any account without knowing the password.
  - Example: sudo su john

Users Management

- **groups** command will list out what groups your currently logged-in user is currently a member of.
- To know which groups that user is a member of, add the user name to the groups command.
  Example:
  groups kent
- **/etc/group** contains information regarding the groups on the system.

Users Management

- Sample output from **cat /etc/group**:

```
user:x:1000:
lpadmin:x:124:user
kent:x:1001:
dhcpd:x:125:
```

- 1st column: group name
- 2nd column: password (not used often)
- 3rd column: GID
- 4th column: list of members in the group

Users Management

- To create a group: **groupadd new_group_name**
- To delete a group: **groupdel group_name**
- To associate users with groups, use the **usermod** command (to modify user account)
  usermod option LOGIN
- To add user **kent** to groups: usermod -aG sudo,adm kent
- To change user's primary group:
  usermod -g new_group user_name
- Refer to manual page for all available options

Users Management

- To remove an user from a group:
  gpasswd -d user_name group_to_remove

- Example, remove **kent** from **sudo** group
  gpasswd -d kent sudo

Users Management

- To lock / unlock an account, we can use usermod or passwd commands with appropriate option.
- Examples
  - to lock kent's account:
    passwd -l kent
  - To unlock kent's account:
    passwd -u kent
- However, user may still login through other method such as SSH.

Users Management

- When creating new users, usually a default / preset password will be assigned. In order to force them to change the password when they first log in, we set their number of days to expiry to 0.

  chage -d 0 user_name

```
user@u-server:~$ sudo chage -d 0 kent
user@u-server:~$ sudo chage -l kent
Last password change                                    : password must be changed
Password expires                                        : password must be changed
Password inactive                                       : password must be changed
Account expires                                         : never
Minimum number of days between password change          : 0
Maximum number of days between password change          : 99999
Number of days of warning before password expires       : 7
```

Users Management

- To set an user account to require a password change after a **60** days:
  sudo chage -M **60** kent
- Based on the info in the previous slide, kent will see warning message when he logs in, 7 days before the password is to be changed.

Users Management

- Protecting the root's password is important.
- Using sudo is an alternative to using root.
  - Give administrators access to perform root tasks with sudo without actually giving them root password
- The user created during installation is automatically made a member of sudo group.
- To add other users to sudo:

  sudo usermod -aG sudo user_name

Users Management

- Sudo allows users to access everything, however we can configure sudo with visudo, which will open the /etc/sudoers file in nano text editor.
- Example of configuration line from /etc/sudoers
  root ALL=(ALL:ALL) ALL
- The 1st ALL: root is able to use sudo from any terminal
- The 2nd ALL: root can use sudo to impersonate any other user
- The 3rd ALL: root can impersonate any other group

Users Management

- Example of configuration line from /etc/sudoers

  rootALL=(ALL:ALL) ALL
- The 4th ALL: refers to what commands this user is able to do (in this case, any command)
- Examples:

  kentALL=(ALL:ALL) /usr/bin/apt,/usr/bin/apt-get
  - kent can only execute the apt and apt-get commands

  kentu-server=(john:admins) /usr/bin/shutdown
  - Kent can only shutdown u-server on behalf of john and group admins


OK,
SO WHAT'S
NEXT?