Operating System –CMP 325

Lab – 05 (Fall 2017)

Objectives:

1. Understanding the concept of software packages and package managers
2. Installing software using binary and source packages
3. Understanding the concept of user management in Linux
4. Creating and deleting users and groups and understanding the related configuration files

Resources:

- Video Lecture 14: https://www.youtube.com/watch?v=vX2whCYjhec
- Video Lecture 15: https://www.youtube.com/watch?v=eA3YOhtWHQk

Task 1: (2 marks each)

1. What is the difference between a binary package and a source package.

   Binary Package: A binary package contains machine code of the software for the specific platform amd64, i386, ia64, asm64, mips. Binary package consist of following:
   - Exe file(s)
   - Man/info pages
   - Copy rights info
   - Config/install scripts

   Source Package: A source package is eventually converted into binary package for a specific platform
   - Source code file
   - README and INSTALL
   - Authors
   - Configuration
   - Makefile.am and makefile.in

2. What is the role of a package manger, what all package managers are available to you for installing Debian packages.

Package manager is a program used to install, remove, upgrade and manage packages on UNIX based system. Three main binary package formats. Xxx.deb this format is used by Debain and distribution drive from Debian Such as Ubuntu, Mint, Kali Linux, Arch Linux and etc.

For installing Debian packages, package managers available are:

1. Apt
2. Dpkg
3. Aptitude
4. Synaptic

3. Which Tool is used to convert the package format and also tell where installed packages are placed (Full Path).
   i. Alien
   ii. /var/cache/apt/archives/

4. Differentiate the following commands.
   - apt -get remove packageName

Only binary files will be removed.

- apt -get remove --purge packageName
  binary files, configuration files and man pages will be removed.

5. Write set of commands to install the source package.
   ./configure
   make
   make install

Task 2: (2 marks each)

1. What are different types of users in linux and write their default Id's?
   - Root user ID = 0
   - Regular user ID starts from 1000
   - System/ No login users

- What is the difference between **`su`** and **`sudo`** command
  - Su: (root)
    ➔ switch user to root. Root user by default disabled.
  - Sudo:(user become root)
    > regular user encourages to use command that is known as sudo which carry out system administrative tasks. So instead of switching to root we use this command to perform administrative tasks.

- What is the difference between switching user using **`su`** command and **`su –`** command
  - su: this command doesn't give environment of target user.
  - su -: - gives environment of target user. We find ourselves in target user's home directory and its default login shell

- Difference between primary and secondary groups.
  Primary: Every user is mandatory member of group which is primary group
  Secondary: It can also member of any other group which is secondary group
- Why the root is default member of all groups?
  Because its ID =0
  Uid=0 gid=0 groups=0
- Check the contents of home directory of newly created user. What all hidden files you see, from where they come, what are their contents, for what all purposes they are used.
  Ls –a
  This show hidden files bashrc, profile and bashlogout. These files copied from the location /etc/skel files copied in every user home directory.

  .bash_logout (Script file executed on logout normally responsive for clear screen)
  .bshrc (contain different environment veriables)
  .profile (You can set path of env. Veriable and umask in this file)

- View the contents of the file **`/etc/default/useradd`**, and try to understand its impact on user creation and his password expiration.

  less /etc/default/useradd

- "/etc/default/useradd" this file contain settings for skel,home,password expiration and shell
- To get basic snapshot of fileinfo of this file use command: "**useradd -D**"

- View the contents of the file **/etc/login.defs**, and make a note of its contents and its usage.

less /etc/login.defs

=> **"/etc/login.defs"** contain some default configurations (for shadow password suite and others)

"grep PASS /etc/login.defs" this will display password configs
"grep ID /etc/login.defs" shows MIN\MAX UID and GID and other ID values

```
anas510@ubuntu:/tmp$ grep PASS /etc/login.defs
#       PASS_MAX_DAYS   Maximum number of days a password may be used.
#       PASS_MIN_DAYS   Minimum number of days allowed between password changes.
#       PASS_WARN_AGE   Number of days warning given before a password expires.
PASS_MAX_DAYS   99999
PASS_MIN_DAYS   0
PASS_WARN_AGE   7
#PASS_CHANGE_TRIES
#PASS_ALWAYS_WARN
#PASS_MIN_LEN
#PASS_MAX_LEN
# NO_PASSWORD_CONSOLE
anas510@ubuntu:/tmp$ grep ID /etc/login.defs
UID_MIN                  1000
UID_MAX                 60000
#SYS_UID_MIN              100
#SYS_UID_MAX              999
GID_MIN                  1000
GID_MAX                 60000
#SYS_GID_MIN              100
#SYS_GID_MAX              999
anas510@ubuntu:/tmp$
```

- What command is used to change password expiry info of user and in which file this command make changes.

Sudo chage username
It make changes in /etc/shadow

Task 3: (2 marks each)

1. Install binary package **cmatrix** on your machine using **apt-get** command

sudo apt-get install cmatrix

2. Download source package **hello-2.10.tar.gz** using **apt-get** as well as using **wget** command. Install it on your machine, see its manual page, use it and finally uninstall it. Note down all your observations

sudo apt-get source hello
or
wget http://ftp.gnu.org/gnu/hello/hello-2.10.tar.gz
tar xzf hello-2.10.tar.gz
for running

./configure
make
make install
For removing
sudo apt-get remove - - purge hello

Task 4: (2 marks each)

1. Add a new user named **bcsf15mXXX.** After Adding user,View the contents of **/etc/passwd, /etc/shadow,** and **/etc/group** and try understanding the new entries in those files.

   su – root

   - adduser bcsf15mXXX
   - grep bcsf15mXXX /etc/passwd
   - grep bcsf15mXXX /etc/shadow
   - grep bcsf15mXXX /etc/group

2. Try logging in as **bcsf15mXXX**, what happened? As root, assign password to **bcsf15mXXX** and try again logging in as **bcsf15mXXX**.

   - su – bcsf15mXXX
   - su – root
   - passwd bcsf15mXXX
   - tail -1 /etc/shadow

3. Change personal information of **bcsf15mXXX** using **chfn** command. Do it as **root** and then note the difference. Understand What all files have been changed?

   - su – root
   - chfn –f rootuser root
   - grep root /etc/passwd
   - usermod –G sudo kakamanna
   - chfn kakamanna

4. Login as root and lock **bcsf15mXXX**.Try logging in as **bcsf15mXXX**, what happened. View the contents of /etc/passwd file, what difference you observed.

   - su – root
   - usermod –L kakamanna

   for kakamana authentication failure

5. Login as root and unlock **bcsf15mXXX**. View the contents of /etc/passwd file, what difference you observed.

   - usermod –U kakamanna

6. Login as root, and delete user **bcsf15mXXX**. Also see if the home directory of the user is **deleted** or not?

- userdel kakamanna
- userdel –r kakamanna (It also delete associated files and home directory)

Task 5: (2 marks each)

1. Login as root, and create three users and assign them passwords.

   - adduser user1
   - adduser user2
   - adduser user3

2. Use **`su-`** command to switch user and login as these three users one after another, create files within their respective home directories. Try entering the home directories of other users and see what happens. Keep a note of your observations.
3. Delete all these three users and observe the contents of the related configuration files again.

   - userdel –r user1
   - userdel –r user2
   - userdel –r user3

Task 6: (2 marks each)

1. Login as root, and create **two** groups with the name of **faculty** and **students**.

   - su –
   - groupadd faculty
   - groupadd students

2. Create three users and made them member of **faculty** group.
   - adduser user1
   - adduser user2
   - adduser user3
   - usermod –a –G faculty user1
   - usermod –a –G faculty user2
   - usermod –a –G faculty user3
3. Create three users and made them members of **students** group.

   - adduser user4
   - adduser user5
   - adduser user5
   - usermod –a –G students user4
   - usermod –a –G students user5
   - usermod –a –G students user6

4. Give sudo privileges to the users of faculty group by adding them in the **sudo** group.

   - usermod –G sudo user1
   - usermod –G sudo user2
   - usermod –G sudo user3

5. Test what you have done, and keep a note of your observations.
   Observe what's going on in files related to users and groups.