Intro to Linux

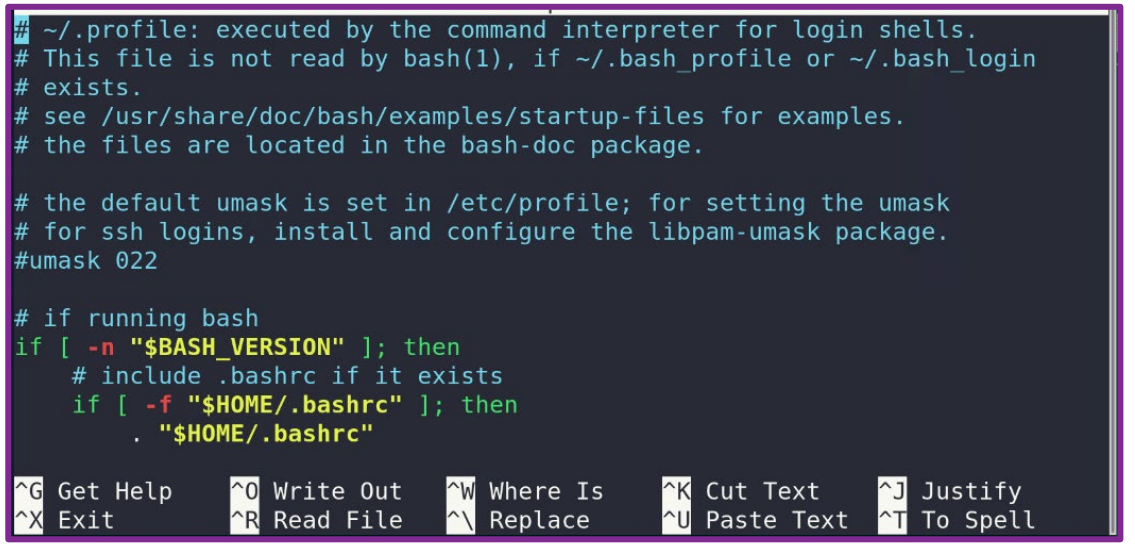
2.2.2 - Account Configuration and Management

CYBER.ORG
THE ACADEMIC INITIATIVE OF THE CYBER INNOVATION CENTER

Account Creation and Configuration

Creation of a user leads to several actions and configurations to create a secure environment tailored to the user's needs.

- Typically, a Linux system will run a series of shell commands in Bash upon startup.
- The system's shell acts as an interpreter between the user and the operating system, reading startup configs and inputs.



Account Authentication

Prior to Bash running setup and configuration commands a user must be authenticated on the system

- The **`passwd`** command is used when adding a user and setting up their password
- The command can also be used to view password statues, set expirations, and more

```
OPTIONS
       The options which apply to the passwd command are:

       -a, --all
           This option can be used only with -S and causes show status for
           all users.

       -d, --delete
           Delete a user's password (make it empty). This is a quick way
           to disable a password for an account. It will set the named
           account passwordless.

       -e, --expire
           Immediately expire an account's password. This in effect can
           force a user to change their password at the user's next login.

       -h, --help
```

```
ubuntu@ip-10-15-88-93:~$ sudo useradd Linda
ubuntu@ip-10-15-88-93:~$ sudo passwd Linda
New password:
Retype new password:
passwd: password updated successfully
ubuntu@ip-10-15-88-93:~$ ls -al
```

Password Directives

- Along with the **`passwd`** command, the **`chage`** command can be used to change the expiration details of a user such as the age , expiration warning parameters, and the account expiration date
- The /etc/login.defs file is associated with an account when created and sets password directives

```
ubuntu@ip-10-15-88-93:~$ sudo chage Linda
Changing the aging information for Linda
Enter the new value, or press ENTER for the default

        Minimum Password Age [0]: 30
        Maximum Password Age [99999]: 365
        Last Password Change (YYYY-MM-DD) [2024-04-10]:
        Password Expiration Warning [7]:
        Password Inactive [-1]:
        Account Expiration Date (YYYY-MM-DD) [-1]: 2025-4-10
ubuntu@ip-10-15-88-93:~$
```

Failed Login Attempts

- The pam_tally2 and faillock utilities allow viewing and managing failed login attempts such as locking an account after so many attempts

Data Associated with Authentication

- System users and accounts created by applications are stored in the /etc/passwd file
- Information includes
  - Username
  - User and group ID
  - Home directories
  - Default shell used
- The /etc/group file will store similar data, but with groups instead

```
ubuntu@ip-10-15-88-93:~$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
```

Data Associated with Authentication cont'd

- In the past, passwords were also stored in the /etc/passwd file; however, that has changed to now being stored in the /etc/shadow file, or the /etc/gshadow for group information
- The password will not appear in plaintext, but is instead shown in a salted, hashed format

```
student:!:19823:0:99999:7:::
Tom:$6$r7nQLhkDqhe2ADiz$xuY8M04R.qEnD2GxWHVMZHCf6jb4VgYtuZWPDO7bA4/WTY
HFQGT6YJaOmsFQikcNCfnF4Y3VgGhTxa/hfGyJs/:19823:0:99999:7:::
Linda:$6$pHc1xeO.9Kwtml9.$DxqkEhMJOwEE4D0aDhlIsvPA0f9MR0CxBii9uRuLiFof
dY5eT37hu30Y3ExB3cyTzepqMcH6vTrbJL8.Fm3Z90:19823:30:365:7::20188:
```

Environment Configuration

- The /etc/profile file is read when a user logs in and sets up the initial environment, such as system paths, shell prompts, aliases, and other functions

```
ubuntu@ip-10-15-88-93:~$ cat /etc/profile
# /etc/profile: system-wide .profile file for the Bourne shell (sh(1))
# and Bourne compatible shells (bash(1), ksh(1), ash(1), ...).

if [ "${PS1-}" ]; then
  if [ "${BASH-}" ] && [ "$BASH" != "/bin/sh" ]; then
    # The file bash.bashrc already sets the default PS1.
    # PS1='\h:\w\$ '
    if [ -f /etc/bash.bashrc ]; then
      . /etc/bash.bashrc
    fi
  else
    if [ "`id -u`" -eq 0 ]; then
      PS1='# '
    else
      PS1='$ '
```

Environment Configuration cont'd

- /etc/skel is a directory that contains files and directories that are copied when an account is created
- When the account is created, these provide the user with a pre-configured, or default, environment

```
ubuntu@ip-10-15-88-93:/etc/skel$ ls -la
total 28
drwxr-xr-x   2 root root  4096 Oct 25 21:51 .
drwxr-xr-x 154 root root 12288 Apr 10 16:39 ..
-rw-r--r--   1 root root   220 Feb 25  2020 .bash_logout
-rw-r--r--   1 root root  3771 Feb 25  2020 .bashrc
-rw-r--r--   1 root root   807 Feb 25  2020 .profile
ubuntu@ip-10-15-88-93:/etc/skel$
```

Bash Configuration

- .bash_profile is initially executed upon logging in to setup the behavior and environment for the Bash shell
- The .bashrc file has the same purpose but is applied immediately and only requires relaunching the terminal

```
 GNU nano 4.8                          .bashrc
else
    PS1='${debian_chroot:+($debian_chroot)}\u@\h:\w\$ '
fi
unset color_prompt force_color_prompt

# If this is an xterm set the title to user@host:dir
case "$TERM" in
xterm*|rxvt*)
    PS1="\[\e]0;${debian_chroot:+($debian_chroot)}\u@\h: \w\a\]$PS1"
    ;;
*)
    ;;
esac

# enable color support of ls and also add handy aliases
if [ -x /usr/bin/dircolors ]; then
    test -r ~/.dircolors && eval "$(dircolors -b ~/.dircolors)" || eval
    alias ls='ls --color=auto'
```