Adding New users

- This is a routine chore on most systems
  - Automate the process
  - Example:
    - Lab access accounts in CS Labs
      - Get info from MTU NID database
      - Big Update Every semester
      - All automated using scripts
- The /etc/passwd file
  - A list of users
  - Consults at login time to determine a user's UID and to verify the users' password

1

/etc/passwd File

- Example:
  nagios:x:667:667:Nagios Monitor:/usr/host/nagios:/bin/ksh
  amanda:x:33:6:Amanda user:/var/lib/amanda:/bin/ksh
- Each line contains seven fields separated by :
  - Login name
  - Encrypted Password
  - UID number
  - Default GID number
  - user information: full name, office, phone, …
  - Home directory
  - Login shell
- Login name
  - Usually no more than 8 characters long
  - Unique
  - Case sensitive, do use all lower case if possible

2

/etc/passwd File

- Encrypted password
  - Encrypted password is set by
    - Command passwd
      - yppasswd if NIS is used
    - Manual manipulation
      - Copy a encrypted string
      - Empty means no password
      - Use fake passwd * to prevent unauthorized use of the account
  - Default algorithm is DES
    - Encrypt the first 8 chars with 2 character "salts"
    - The encrypted passwd will be 13 character long
    - Does not take too long to decode it using faster hardware
  - Algorithm MD5
    - Passwords can be any length
    - Encrypted password starts with 1, 31character long
    - Third party software may not accept it.

/etc/passwd File

- UID number
  - 32-bit integers
  - Limit to 32,767 if possible
  - By definition, root is UID 0
  - Fake logins at the beginning of /etc/passwd: bin, daemon, …
  - Start at 100 for assigning uids.
- Discuss:
  - Reuse uid?
  - Recycling uid?
  - Uid across different machines?

/etc/passwd File

- Default GID number
  - 16 or 32bit integer (signed or unsigned)
  - GID 0 is for group root or wheel
  - Groups are defined in /etc/group
  - GID in /etc/passwd provides the effective GID at login time.
    - The effective GID is not used to determine access
    - The effective GID is used during creation of new files and directives.
      - Use setgid bit (2000)
      - Use newgrp command
  - UNIX allows a user to be in upto 16 groups

5

/etc/passwd File

- GECOS field
  - Record personal information about each user
- Home directory
  - Users are placed in their home dirs when they log in.
  - If home dir is missing
    - Some system will put the user in the root dir /
    - Some system will reject the user
- Login shell
  - Typically a command interpreter (/etc/shells)
  - Can be any program
  - The default is sh if nothing specified
  - Use chsh/password –e to change the default shell
    - Be careful to change root's default shell

6

Shadow Password

- To prevent the dictionary password cracking -hide the encrypted password
  - Make /etc/passwd from world readable to root readable only?
    - Lots of applications depend on /etc/passwd to get information about user
  - Use shadow password mechanism
    - Move encrypted password to another file which readonly by root
    - Besides password, shadow has the password aging info.
    - Mandatory in Solaris
    - Available Shadow utility in Linux distributions

7

Shadow Password

- The /etc/shadow file
  - Readonly by superuser

    -r-------- 1 root root 1039 Nov 7 09:58 /etc/shadow
  - Provides account information that's not available from /etc/passwd –
    - password aging info
      - Forcing user to change password
  - One line for each user, including nine fields separated by colons:

8

Shadow Password

username:password:lastchg: min:max:warn: inactive:expire:flag

1. Login name
2. Encrypted password
3. Date of last password change
4. Minimum number of days between password changes
5. Maximum number of days between password changes
6. Number of days in advance to warn users for password expiration
7. Number of inactive days before account expiration
8. Account expiration date
9. Flags

Shadow Password

- Example: On fc4

```
[root@icu0 ~]# tail -n 1 /etc/shadow
millert:kE7WRAQ5jLoKY:13194::180:14::18627:

[root@icu0 ~]# chage -l millert
Last password change                                    : Feb 15, 2006
Password expires                                        : Aug 14, 2006
Password inactive                                       : never
Account expires                                         : Dec 31, 2020
Minimum number of days between password change          : -1
Maximum number of days between password change          : 180
Number of days of warning before password expires       : 14
```

Shadow Password

- Set password aging
  - Use password command
    - Example, On system V, some options of password command:
      - -n: minimum
      - -m: maximum
      - -f: force the change at next login
      - -S: list
      - -l: lock the account
      - -u: unlock
  - User default characteristics
    - Solaris: /etc/default/passwd, /etc/default/login
    - Linux: /etc/login.defs

11

On Solaris 8

```
$more /etc/default/passwd
#ident  "@(#)passwd.dfl 1.3     92/07/14 SMI"
MAXWEEKS=
MINWEEKS=
PASSLENGTH=6
```

12

FC1

```
$grep PASS 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_MIN_LEN    Minimum acceptable password length.
#       PASS_WARN_AGE   Number of days warning given before a password expires.
PASS_MAX_DAYS   99999
PASS_MIN_DAYS   0
PASS_MIN_LEN    5
PASS_WARN_AGE   7
```

13

Group file

- /etc/group file
  - Contains names of UNIX groups and member list
  - Example:

```
s3141.1:#$cs3141.1:3411:cs3141gr,jpwoods,ljinsok,mguclu,rcvanden,jrfreibe
cs3141.2:#$cs3141.2:3412:cs3141gr,ajnowick,dmhardzi,drdeverr,joelarso
```

  - Each line has 4 fields:

    groupname:password: gid:user-list
  - Group password is rarely used
    - For changing to another group using newgrp which the user does not belong
  - Start gid with a large number, such as 100.
    - Avoid collisions with vendor-supplied GIDs.

14

Adding New Users

- Process to add a new user
  - First, have the use sign the user agreement and policy statement
  - Required
    - Edit passwd and shadow files
    - Set an initial password
    - Create home directory
  - For the user
    - Copy default startup files to the user's home directory
    - Set the user's mail home and establish mail aliases if applicable
  - Others
    - Add the user to /etc/group file
    - Configure disk quotas
    - Verify the account

15

Adding New Users

- Editing the passwd and shadow files

  ```
  # vi
  # vipw
  ```

  - Only one person to edit the passwd at a time
  - Prompt for shadow change
- Setting an initial password

  ```
  #passwd user
  ```
- Creating the user's home directory

  ```
  # mkdir /home/joe
  # chown joe:research /home/joe
  # chmod 700 /home/joe
  ```
- Copying in the default startup files
  - Default system-wide startup files
  - User's own startup files
    - Store the typical files on a common place, such as /etc/skel
    - Copy the startup files to user's home dir

16

Common startup files

Comamnd	Filenames	Typical users
csh/tcsh	.login	Terminal type, env
csh/tcsh	.cshrc	Aliases, umask, history,path, env
csh/tcsh	.logout	Reminder, clear the screen
sh	.profile	
vi	.exrc	Editor options
emacs	.emacs_pro	
mail	.mailrc	Mail aliases, reader options
xrdb	.Xdefaults	Fonts, color, etc
startx	.xinitrc	X11 env
xdm	.xsession	X11 env

17

Adding New Users

- Example:
  - # cp /etc/skel/.[a-zA-Z]* ~joe
  - # chmod 644 ~joe/.[a-zA-Z]*
  - # chown joe:research ~joe/.[a-zA-Z]*
- Question: how about replacing the third line above with
  - # chown joe:research ~joe/.*

18

Sample .login

```
# sample .login file
if (-e ~/.hushlogin) cat /etc/motd
limit coredumpsize 0k
umask 022
setenv PATH /usr/ucb:/bin:/usr/bin:/usr/local/bin
setenv PRINTER ps
setenv EDITOR emacs
mesg y
set prompt='`hostname`-\!>> '
echo -n "Enter terminal type: "; set tt=$<
if ("$tt" != "") then
        setenv TERM $tt
        tset
endif
```

19

Sample .profile

```
# sample .profile file
 ulimit –c  0
umask 022
PATH=/usr/ucb:/bin:/usr/bin:/usr/local/bin
PRINTER=ps
EDITOR=emacs
mesg y
PS1='`hostname`-\!>> '
echo -n "Enter terminal type: "; read tt
if  [ "$tt" = "" ]; then
        tt="vt100"
fi
export TERM=$tt
```

20

Adding New Users

- Editing /etc/group file
  - Add the new user to the default group for recording purpose
  - Add the new user to root group for "su"
  - Add the new user to other groups for permission access control

21

Adding New Users

- Setting disk quotas
  - Use edquota interactively
  - Use edquota in prototype mode – copy the definition from an existing users
  - Disk is cheap, quotas may not be necessary
- Verifying the new login
  - Login in as the new user
  - Check home dir and permission
  - Check startup files and their permissions: ls –al
  - Inform the new user about their login and initial password

22

Removing Users

- When a user quits, remove the user.
  - Set disk quota to zero
  - Remove user's crontab
  - Remove temp files owned by the user in /var/tmp or /tmp
  - Remove the user from passwd and group file
  - Remove user's home dir
    - Make a copy
    - Verify there is no other space owned by the user
      - # quot /home
      - # find –x /home –nouser -print
  - Remove the user's mail spool
  - Remove the user from all other databases

Disabling Logins

- Disable a user
  - Mark the password *
  - Change the shell
    - Example:

      +@nonenrolled::::::/usr/local/shells/gone

Account Management Utilities

- Graphic utilities
  - Solaris: admintool / HPUX: sam /…
- Command utilities
  - useradd / usermod / userdel
  - groupadd / groupmod / groupdel
- Example:

  #useradd –c "David Hilbert" –d /home/csdept/hilbert –g student –G webadmin –m –s /bin/sh hilbert

  #userdel hilbert

25

Account Management Utilities

- Advantage:
  - Easy to use
- Disadvantage
  - Time consuming
  - Not flexible
  - Not all options are available

26

Standard Unix Users and Groups

- Typically predefined users
  - root
    - Superuser, uid=0
  - daemon
    - Used to execute system processes
  - bin
    - Owns the executable files for most user commands
  - sys
    - Owns system files
  - adm
    - Owns the accounting files
  - uucp
    - Unix to unix copy subsystem account, owns uucp tools and files
  - cron, mail, news, usenet, lp and lpd
    - Pseudo-users to own files and run processes needed by the corresponding subsystems
  - auth, auditor or audit
    - Pseudo-user associated with the system auditing facility
  - nobody
    - Account used by the NFS product, uid = 65534

27

Standard Unix Users and Groups

- Typically predefined groups:
  - system or root or wheel
    - Under BSD, Members of this group is allowed to su to root, gid=0
  - daemon
    - Traditional owner of the spooling directories
  - kmem or mem
    - Owns system programs needing to read kernel memory directly
  - sys:
    - Owns various system files
  - tty or terminal
    - Owns all special files connected to terminals, like write
  - cron, mail, uucp, news
    - Groups associated with various system facilities
- Note: username and group names are independent of each other.

28