



CENG 510v: Topics

---

in

Linux Administration

Chapter 6: Adding New Users



# Bibliography

---

- Software Engineer at [Acxiom Corp.](#)
- Currently Enrolled in the Ph.D. program at the [University of Arkansas](#)
- M.S. in Computer Systems Engineering 1999, [University of Arkansas](#)
- B.S. in Computer Systems Engineering 1998, [University of Arkansas](#)
- [Publications:](#)  
J. Simonson, D. Berleant, A. Bayyari [Content Permanence Via Versioning and Fingerprinting](#) ACM Hypertext 2000, the eleventh of the ACM conference on hypertext and hypermedia, May 2000, pp. 226-227

[Click here for PDF version](#) and then click on "PDF" in the top right hand corner



# Objectives

---

- Create new accounts on Linux systems
- Set password aging policies on Linux systems
- Set up groups for delegation and shared work
- Removing users and disabling logins



# User Accounts

---

- Properties of an account
- The password file
- The shadow password file
- The group file



# Properties of an account

---

- Each user on the system gets a unique **login name and a password**
- Home directory
- Unique UID & default GID
- Login shell
- Mail and startup files (dot files)

# Dot Files

Filename	Command	Explanation
<code>~/.cshrc</code>	<code>/bin/csh</code>	Executed every time C shell started
<code>~/.login</code>	<code>/bin/csh</code>	Executed after <code>.cshrc</code> when logging in with C shell
<code>/etc/profile</code>	<code>/bin/sh</code>	Executed during the login of every user that uses Bourne shell
<code>~/.profile</code>	<code>/bin/sh</code>	User's personal profile. Executed when logging under Bourne

More: `~/.logout`, `~/.bash_logout`, `~/.bash_history`, `~/.forward`



# Skeleton Directories

---

- All new users get same startup files by default
- Located in `/etc/skel`



# Powers & Privileges

---

- Two main categories with varying amounts of power:
  - Normal Users: restrictions
  - Super Users: can do virtually anything (accidentally wipe out every file on the system)
  - Sudo users are restricted super users. Usually for a special function (backup admin, account admin, etc)

**CAUTION: Avoid using 'root' unless necessary**



# User Accounts

---

- Properties of an account
- The password file



# Password File

---

- Located at /etc/passwd (world-readable)
- Uses ":" as a delimiter and consists of the following:
  - Login name
  - Password field
  - UID number
  - GID number
  - "GECOS" info (full name, phone, office, etc.)
  - Home directory
  - Login shell



# Password File Example

---

abayyar:Igljf78DS:132:20:Ahmed Bayyari:/home/abayyar:/bin/csh

username : password : UID : GID : comment : home directory : login command



# User Accounts

---

- Properties of an account
- The password file
- The shadow password file



# Shadow Password File

- Located at `/etc/shadow` (readable only by root)
- Consists of the following:
  - Login name
  - Encrypted Password
  - Date of last password change
  - Min num of days between password changes
  - Max num of days between password changes
  - Num of days in advance to warn about password expiration
  - Num of days after password expiration that account is disabled
  - Account expiration date
  - Reserved field (currently empty)



# Shadow Password File Example

---

**abayyar:Igljf78DS:543:14:180:10:60::**

- Login name
- Encrypted Password
- Date of last password change (number of days since Jan 1, 1970)
- Min num of days between password changes
- Max num of days between password changes
- Num of days in advance to warn about password expiration
- Num of days after password expiration that account is disabled
- Account expiration date
- Reserved field (currently empty)



# User Accounts

---

- Properties of an account
- The password file
- The shadow password file
- The group file



# Groups

---

- The `/etc/group` file
- Each user must belong to a group
- Create a unique group for each user
- `/etc/passwd` default group overrides `/etc/group`



# Group File Example

---

**students:\*:15:user1,user2,user3**

**group name : password : GID : users of the group**



# Steps to Create a User

---

1. Add an entry into the `/etc/passwd` file
2. Set an initial password
3. Add an entry to the `/etc/group` file
4. Create user's home directory (set permissions)
5. Create the user's mail file or set a mail alias
6. Create any startup files required for the user
7. Test that the addition has worked



# User Setup Examples

---

- To create a user's home directory
  - `mkdir /home/staff/rdeaton`
  - `chown rdeaton.staff /home/staff/rdeaton`
  - `chmod 700 /home/staff/rdeaton`
  
- To copy default startup files
  - `cp /etc/skel/.[a-zA-Z]* ~rdeaton`
  - `chmod 644 ~rdeaton/.[a-zA-Z]*`
  - `chown rdeaton ~rdeaton/.[a-zA-Z]*`
  - `chgrp staff ~rdeaton/.[a-zA-Z]*`
  
- Do **NOT** use `chown rdeaton ~rdeaton/*`  
(will copy parent directory `..` - `/home/staff`)



# Automated Account Creation

---

- Account creation, modification and deletion
- The `useradd` command
- The `passwd` command
- The `usermod` command
- The `userdel` command
- Automated account creation using `linuxconf`



# Account Management Examples

---

- `useradd -c "John Smith" jsmith`
  - Adds entry in `/etc/passwd`, `/etc/shadow`, and `/etc/group`
  - Creates `/home/jsmith`
  - Copies skeleton files from `/etc/skel`
  - Sets the default shell
  - Creates mail file
- Use `passwd jsmith` to set the user password



# Account Management Examples

---

- `usermod -l johny joe`
  - Changes login name from joe to johny
  
- `usermod -d /home/johny johny`
  - Sets the new home directory



# Account Management Examples

---

- `userdel joe`
  - Removes user's info from `/etc/passwd`, `/etc/shadow`, and `/etc/group`
  - Does **NOT** delete user's home directory.
  
- `usermod -d /home/johny johny`
  - Sets the new home directory



# Tips

---

- UID (0-99 are reserved by some systems)
  - Start UID's and GID's at 100
- Don't recycle UID's
- **NEVER** leave the password field blank - use "\*" to disable an account
- OR
- Disable an account by changing the login shell to the program */bin/false*
- Avoid mail accumulation when deleting a user by removing the */etc/passwd* entry
- Use "**chage -d 0**" to force immediate password expiration



# Tools of the Trade

---

- Use “vipw” to edit the /etc/passwd file
- Use `usermod` with the `-e` option to expiration dates:
  - `usermod -e “January 31, 2004” abayyar`
- Use `edquota` to set quota limits for each user
- Use “yppasswd” instead of “passwd” when using NIS



# Summary

---

- ✓ Create new accounts on Linux systems
- ✓ Set password aging policies on Linux systems
- ✓ Set up groups for delegation and shared work
- ✓ Removing users and disabling logins



# Demos

---

Add User Demo

Add User Demo (Terminal)

**Questions?!**

