Chapter 3
Rootly Powers

The Root

- Root
  - Root is God, also called super-user.
  - UID is 0
- UNIX permits the superuser to perform any valid operation on any file or process, such as:
  - Changing the root directory of a process with **chroot**
  - Creating device files (**mknod**)
  - Setting the system clock
  - Raising anyone's resource usage limits and process priorities (**renice, edquota**)
  - Setting the system's hostname (**hostname** command)
  - Configuring network interfaces (**ifconfig** command)
  - Shutting down the system (**shutdown** command)

Becoming root (1)

- Login as root
  - Console login
    - Allow root login on console but not cross network.
    - If you don't want to permit root login in the console

      ttyv1 "/usr/libexec/getty Pc" cons25 on secure

      ➔ttyv1 "/usr/libexec/getty Pc" cons25 on *insecure*
  - Remote login (login cross network)
    - sshd:

      /etc/ssh/sshd_config

      #PermitRootLogin yes

Becoming root (2)

- su : substitute user identity
  - su, su -, su *username*
  - ※ Environment is unmodified with the exception of USER, HOME, SHELL which will be changed to target user.
  - ※ “su -” will simulate as a full login.
- sudo : a limited su
  - Subdivide superuser’s power
    - **Who** can execute **what command** on **which host**.
  - Each command executed through sudo will be logged

```
Sep 22 23:24:19 chbsd sudo:   chwong : TTY=ttyp4 ; PWD=/usr/ports ;
                    USER=root ; COMMAND=/usr/bin/make update fetchindex
```

  - Install sudo
    - /usr/ports/security/sudo
  - Edit /usr/local/etc/sudoers using **visudo** command
    - **visudo can check mutual exclusive access of sudoers file**

Becoming root (3)

- sudoers format
  - **Who** can execute **what command** on **which host**
    - **The user to whom the line applies**
    - **The hosts on which the line should be noted**
    - **The commands that the specified users may run**
    - **The users as whom they may be executed**
  - Use absolute path

```
Host_Alias      BSD=bsd1,bsd2,alumni
Host_Alias      LINUX=linux1,linux2

Cmnd_Alias      DUMP=/usr/sbin/dump, /usr/sbin/restore
Cmnd_Alias      PRINT=/usr/bin/lpc, /usr/bin/lprm
Cmnd_Alias      SHELLS=/bin/sh, /bin/tcsh, /bin/csh
```

Becoming root (4)

```
Host_Alias      BSD=bsd1,bsd2,alumni
Host_Alias      LINUX=linux1,linux2

Cmnd_Alias      DUMP=/usr/sbin/dump, /usr/sbin/restore
Cmnd_Alias      PRINT=/usr/bin/lpc, /usr/bin/lprm
Cmnd_Alias      SHELLS=/bin/sh, /bin/tcsh, /bin/csh
Cmnd_Alias      SU=/usr/bin/su

User_Alias      wwwTA=jnlin, ystseng
User_Alias      printTA=thchen, jnlin

chwong          ALL=ALL
chiahung        ALL=(ALL)ALL,!SHELL,!SU
printTA         csduty=PRINT
wwwTA           BSD=(nobody)/usr/bin/more
%wheel          ALL=NOPASSWD:/sbin/shutdown
```

Becoming root (5)

- % sudo –u nobody more /usr/local/etc/apache/httpd.conf
- % cp –p /bin/csh /tmp/csh; sudo /tmp/csh

Advantage of sudo

- Accountability is much improved because of command logging
- Operators can do chores without unlimited root privileges
- The real root password can be known to only one or two people
- It's faster to use sudo than to run su or login as root
- Privileges can be revoked without the need to change the root password
- A canonical list of all users with root privileges is maintained
- There is less chance of a root shell being left unattended
- A single file can be used to control access for an entire network