Users \ Groups

Folders \ Files permissions

User

```
[-= gentoo - en1 192.168.1.102 =- ao 18:34:14] ~
$ id
uid=501(ao) gid=20(staff) groups=20(staff),12(everyone),61(localaccounts),79(_appserverusr),80(admin),
95(com.apple.access_ftp),398(com.apple.access_screensharing),399(com.apple.access_ssh)
[-= gentoo - en1 192.168.1.102 =- ao 18:34:16] ~
$ ls -lah /tmp/
total 0
drwxrwxrwt  7 root  wheel   238B Oct  1 19:56 ./
drwxr-xr-x@ 6 root  wheel   204B Sep  5 14:31 ../
drwx------  3 ao    wheel   102B Sep 27 23:18 .wine-501/
drwxrwxrwx  6 ao    wheel   204B Sep 27 23:18 Wineskin/
drwx------  3 ao    wheel   102B Sep 27 12:04 com.apple.launchd.8prf7XZAjP/
drwx------  3 ao    wheel   102B Sep 27 12:04 com.apple.launchd.MrSll3sUZQ/
drwx------  3 ao    wheel   102B Sep 27 12:07 tmux-501/
[-= gentoo - en1 192.168.1.102 =- ao 18:34:19] ~
$
```

/etc/passwd file

- username:password:UID:GID:GECOS:/home/dir:shell
- root:x:0:0:root:/root:/bin/bash

/etc/shadow file

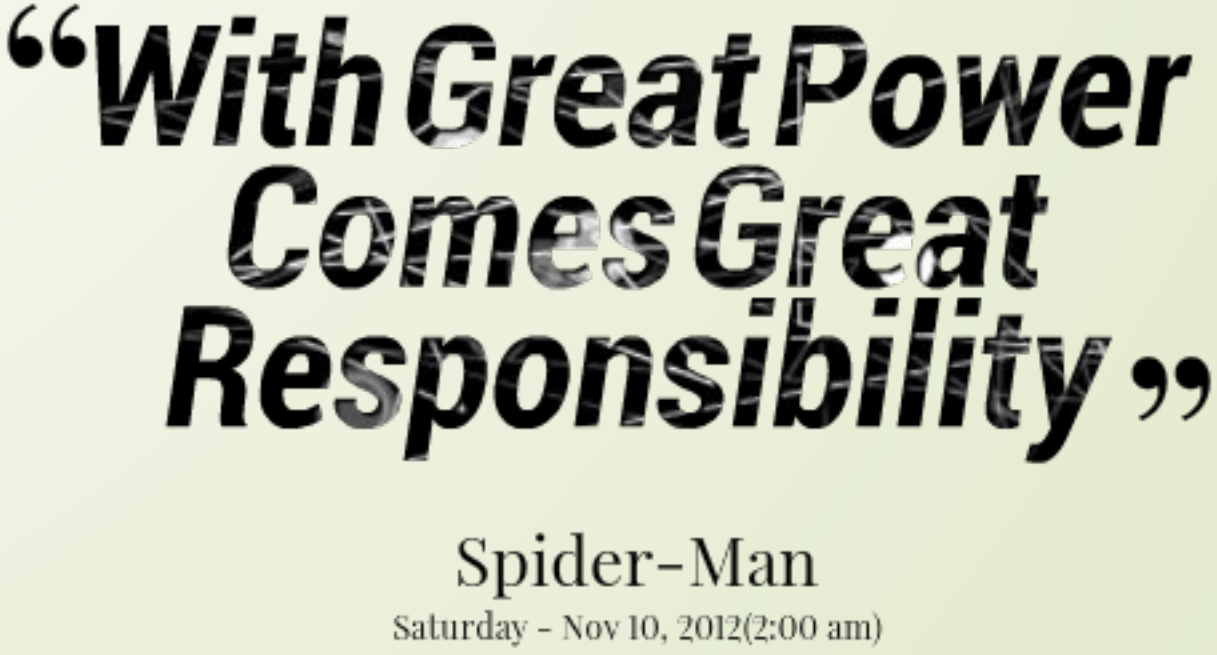
- root:6EA9I7IWI$1KXpR1dYwKe0icL0ohivqdyPdwzcxn0FuH.:16856:0:99999:7:::
- Username, up to 8 characters. Case-sensitive, usually all lowercase. A direct match to the username in the /etc/passwd file.
- Password, encrypted.
- The number of days since January 1, 1970 since the password was last changed.
- The number of days before password may be changed (0 indicates it may be changed at any time)
- The number of days after which password *must* be changed (99999 indicates user can keep his or her password unchanged for many, many years)
- The number of days to warn user of an expiring password (7 for a full week)
- The number of days after password expires, but can be used. Account will be disabled if pwd is not changed.
- The number of days since January 1, 1970 when an account will be disabled
- A reserved field for possible future use

Groups

- /etc/group file
- groupname:password:GID:list of users
- root:x:0:

Root user

- *root* is the user name or account that by default has access to all commands and files on a Linux or other Unix-like operating system. It is also referred to as the root account, root user and the superuser.
- Gain root access: su –



Sudo

- Example: sudo some command
- Note: all commands executed using sudo are logged by default to /var/log/secure
- /etc/sudoers file

Managing users

- useradd username - creates user
- usermod – modifies user (see help)
- userdel username – deletes user (with ‘-r’ deletes it’s home directory)
- passwd username – sets password

UID ranges

- UID 0 is always assigned to the superuser account, root.
- UID 1 – 200 is a range of ‘system users’ assigned statically to system.
- UID 200 - 999 is a range of ‘system users’ used by system processes that do not own files on the file system. They are typically assigned dynamically from the available pool when the software that needs them is installed. Programs run as these ‘unprivileged’ system users in order to limit their access to just the resources they need to function.
- UID 1000+ is the range available for assignment

Managing groups

- groupadd groupname - creates group (-g GID)
- groupmod – modifies group (see help)
- groupdel groupname - deletes group

Managing file system permissions

- chmod WhoWhatWhich file / directory
- Who is u, g, o, a (user, group, other, all)
- What is +, -, = (add, remove, set exactly)
- Which is r, w, x (read = 4, write = 2, executable = 1)

- chown username:groupname file / folder(-R recursive)