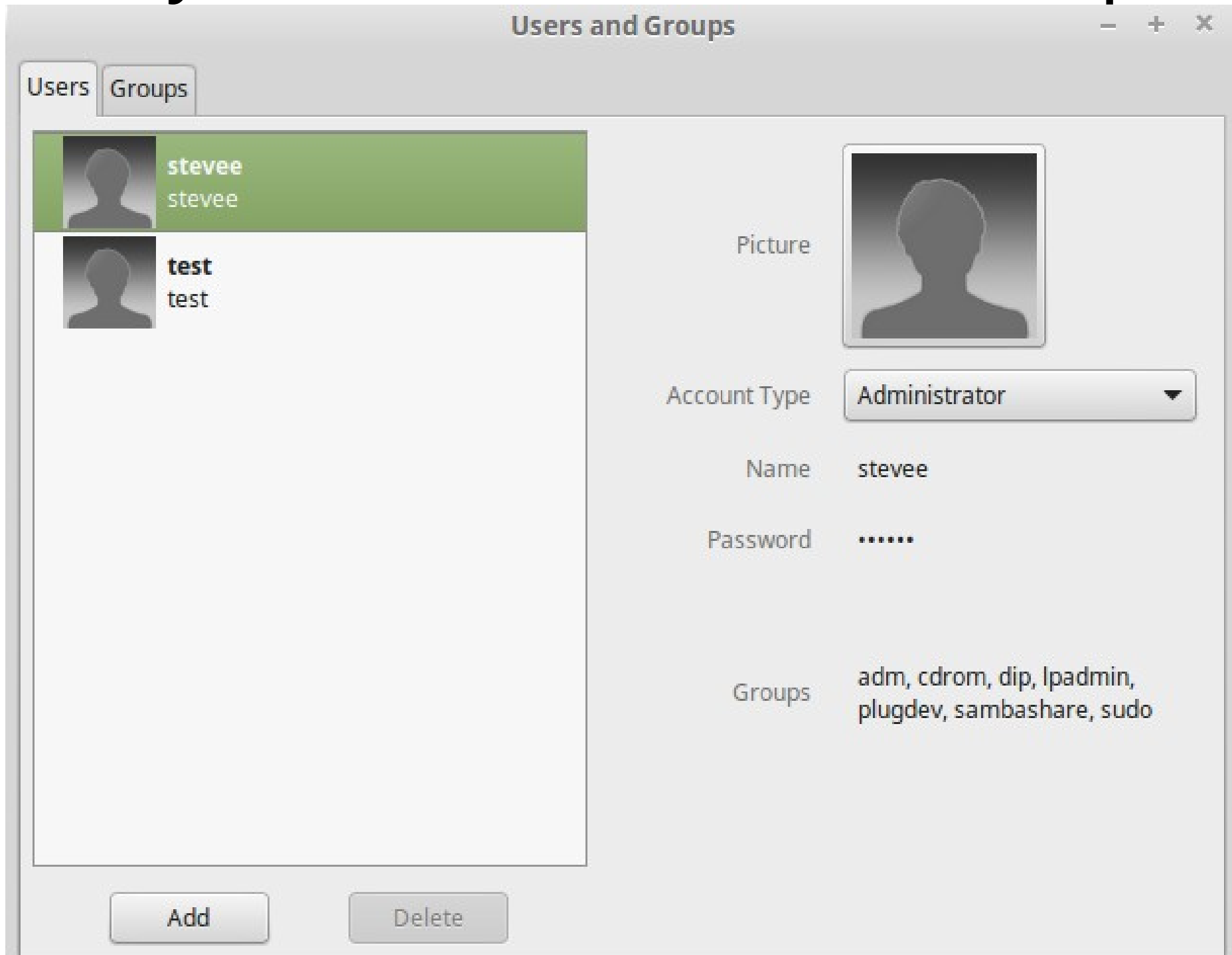


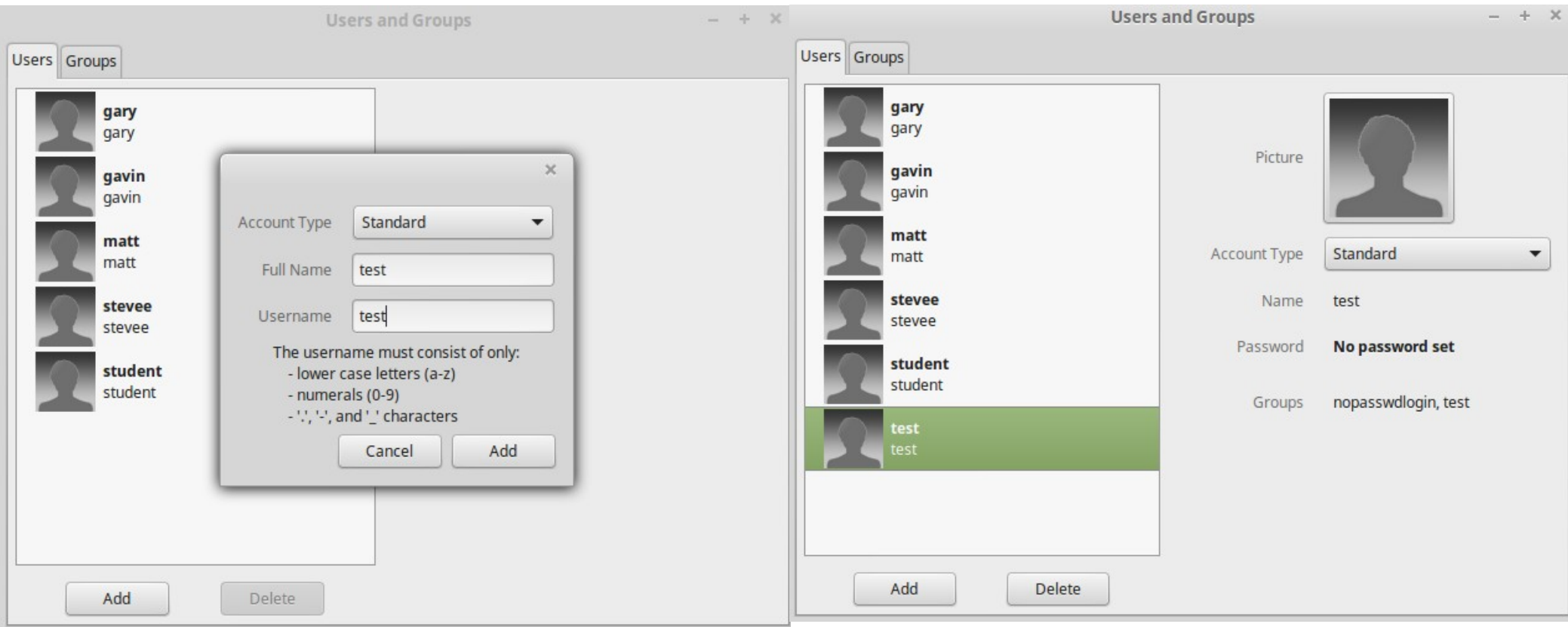
Day 2 Admin: Users and Groups



Basic Admin on any OS includes:

- System Security – access: physical, login account, network availability, malware protection: access intended or not – system design flaws, bugs?
- Data protection – backups, redundancy, hardware/software monitoring
- User account maintenance – access privilege: sudo/other groups, passwords, network etc.
- Security policies, system user contracts, legality (Data Protection Act 1998 etc.), legal obligations e.g. privacy, child porn, terrorism
- <https://www.gov.uk/data-protection/the-data-protection-act>

Add a test user named “test”



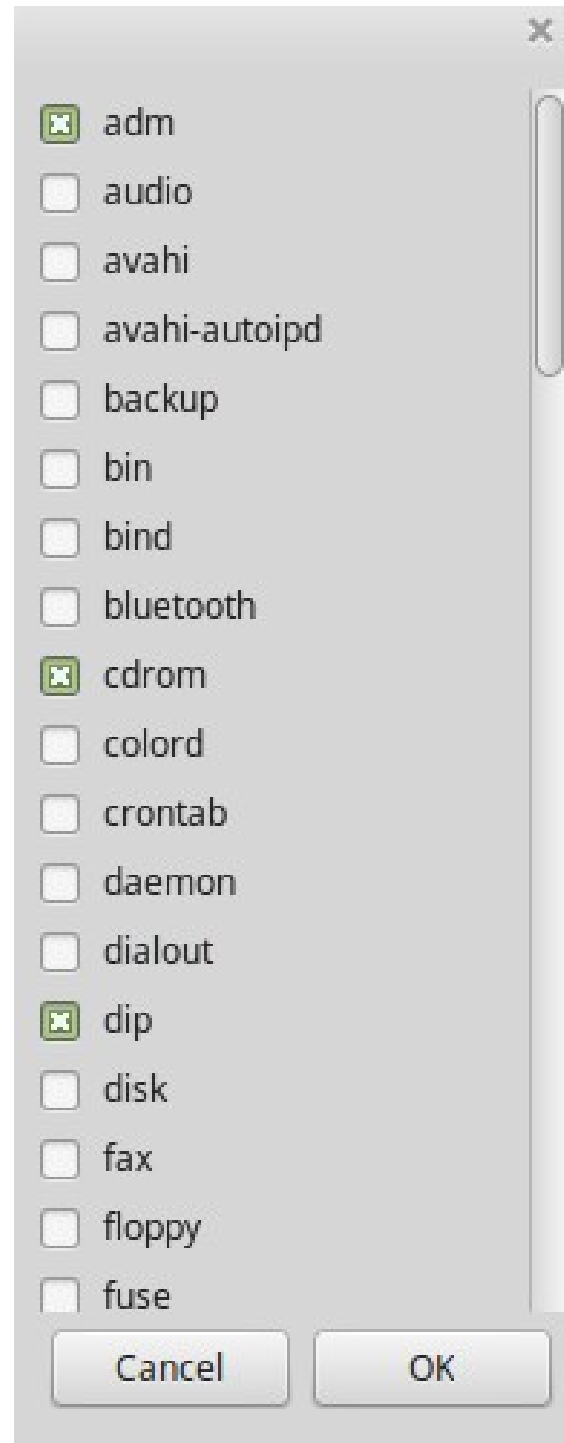
Click the different user's attributes

- **Picture:** browse to add one
- **Account type:** Administrator or Standard
- **Name:** = account user name, NOT real name info
- **Password:** set or null?
- **Group membership:** own group and/or other groups?

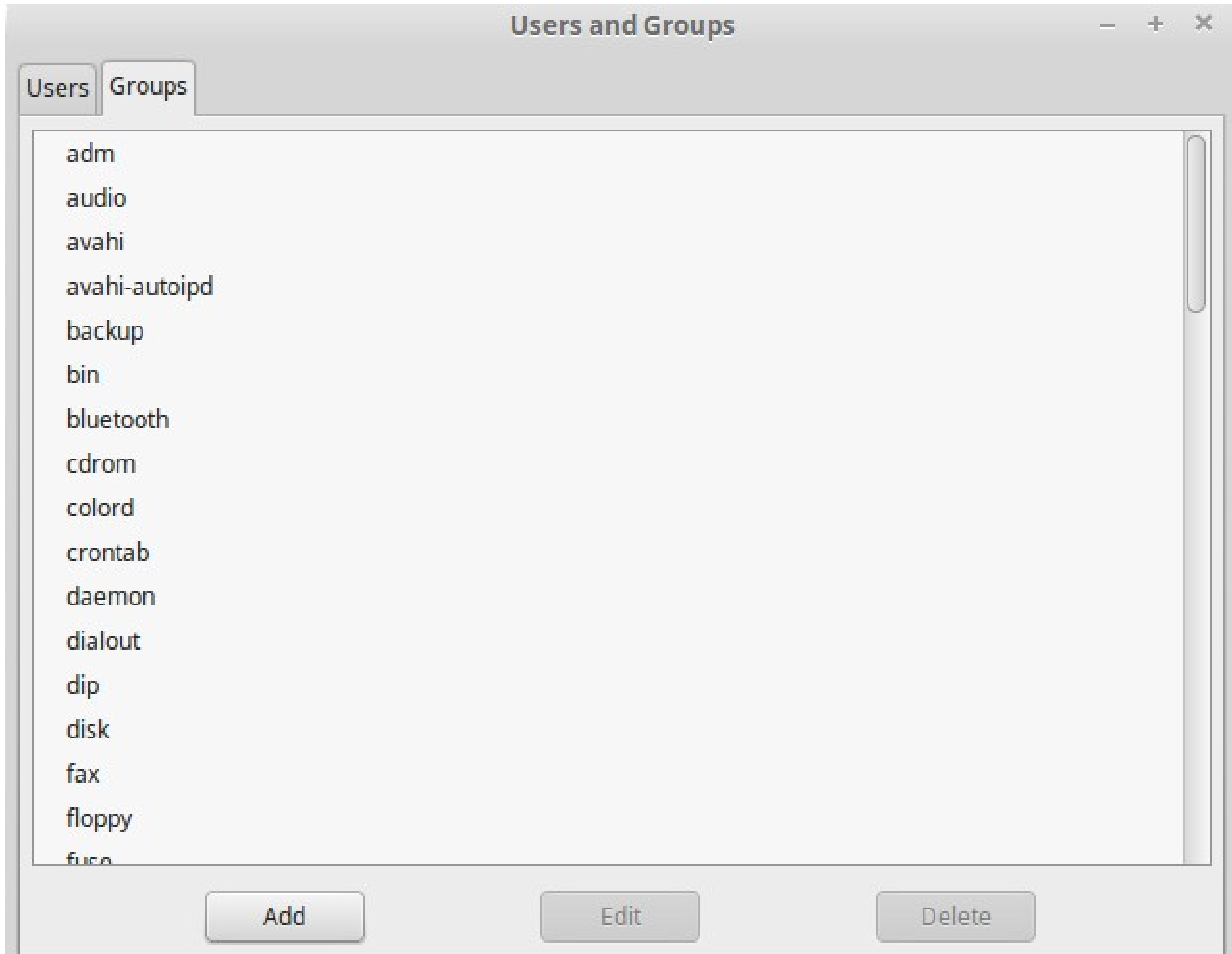
What are the Installer's/Administrator's group memberships compared to a Standard User's memberships?

What “key” Admin membership allows power?

Add user to groups button window



Group Graphic User Interface



Command Line: adduser and addgrp

stevee@AMDA8 ~ \$ **adduser joe**

adduser: Only root may add a user or group to the system.

Why the complaint? You could add “test” user in the GUI?

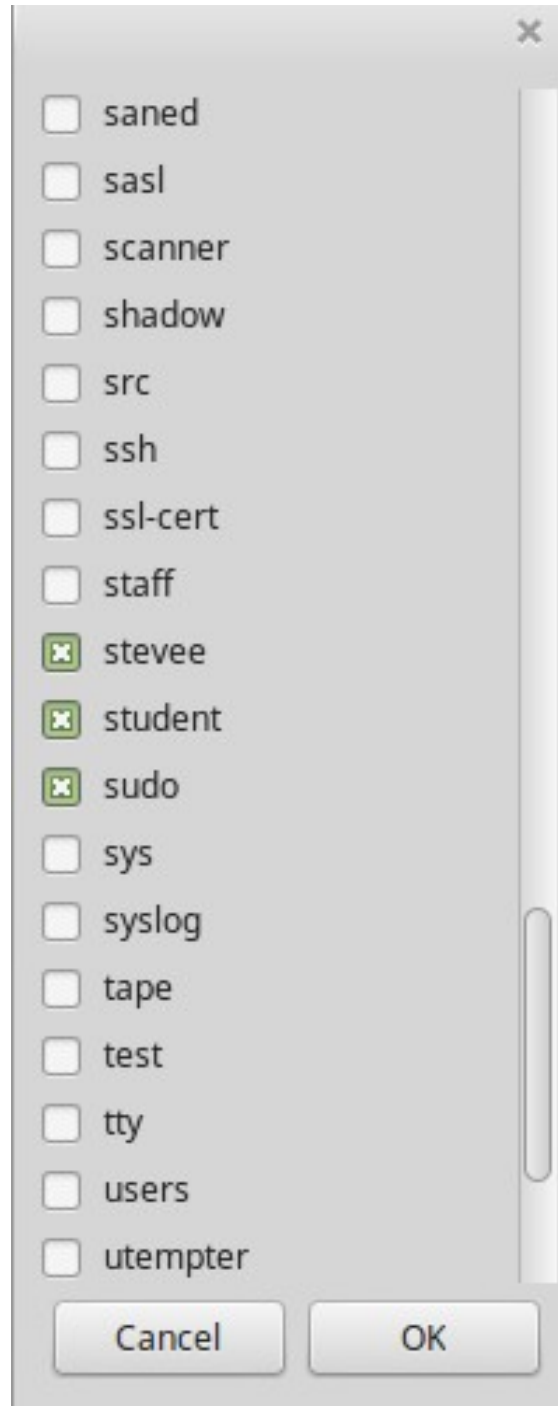
Did you have to login to the GUI?

What did that login act as on the command line? - “sudo su”.

You become “root” temporarily, but you have to be in the “sudo” group, and your own group – which you are as the OS Installer.

Click on the group button – see below:

Add user to groups button window



Default adduser group creation: user “joe” in group “joe” by default

```
Terminal
stevee@MintServer ~ $ sudo adduser joe
[sudo] password for stevee:
Adding user `joe' ...
Adding new group `joe' (1006) ...
Adding new user `joe' (1005) with group `joe' ...
Creating home directory `/home/joe' ...
Copying files from `/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for joe
Enter the new value, or press ENTER for the default
  Full Name []:
  Room Number []:
  Work Phone []:
  Home Phone []:
  Other []:
Is the information correct? [Y/n]
stevee@MintServer ~ $
```

Sudo – or “superuser do”

`man sudo`

`sudo, sudoedit` — **execute a command as another user**

DESCRIPTION

`sudo` allows a permitted user to execute a command as the superuser or another user, **as specified by the security policy.**

`sudo` supports a plugin architecture **for security policies and input/output logging.**

So, `sudo` “logs” the `sudo` user's activity, so Admin staff know who did what, when.

Remember at install, you added a passwd for root by becoming “su” using `sudo`?
Run your command history list and grep for “su”

```
stevee@AMDA8 ~ $ history | grep su
```

```
1 sudo su
```

The first command I got you to run after install – you had to be able to become “su” or “root”, as the installer, so you could add a passwd for root and secure that user and group! Similar to the Administrator in Windows, but that does NOT have total system control of all “Windows” files without much knowledge, at least. Root DOES, so is the Holy Grail of the Hacker. “...I got Root at blah.com!” **UNIX expects responsible, *thinking* users!**

Become root and add a package

stevee@AMDA8 ~ \$ `su root`

Password:

`apt-get install nemo-terminal`

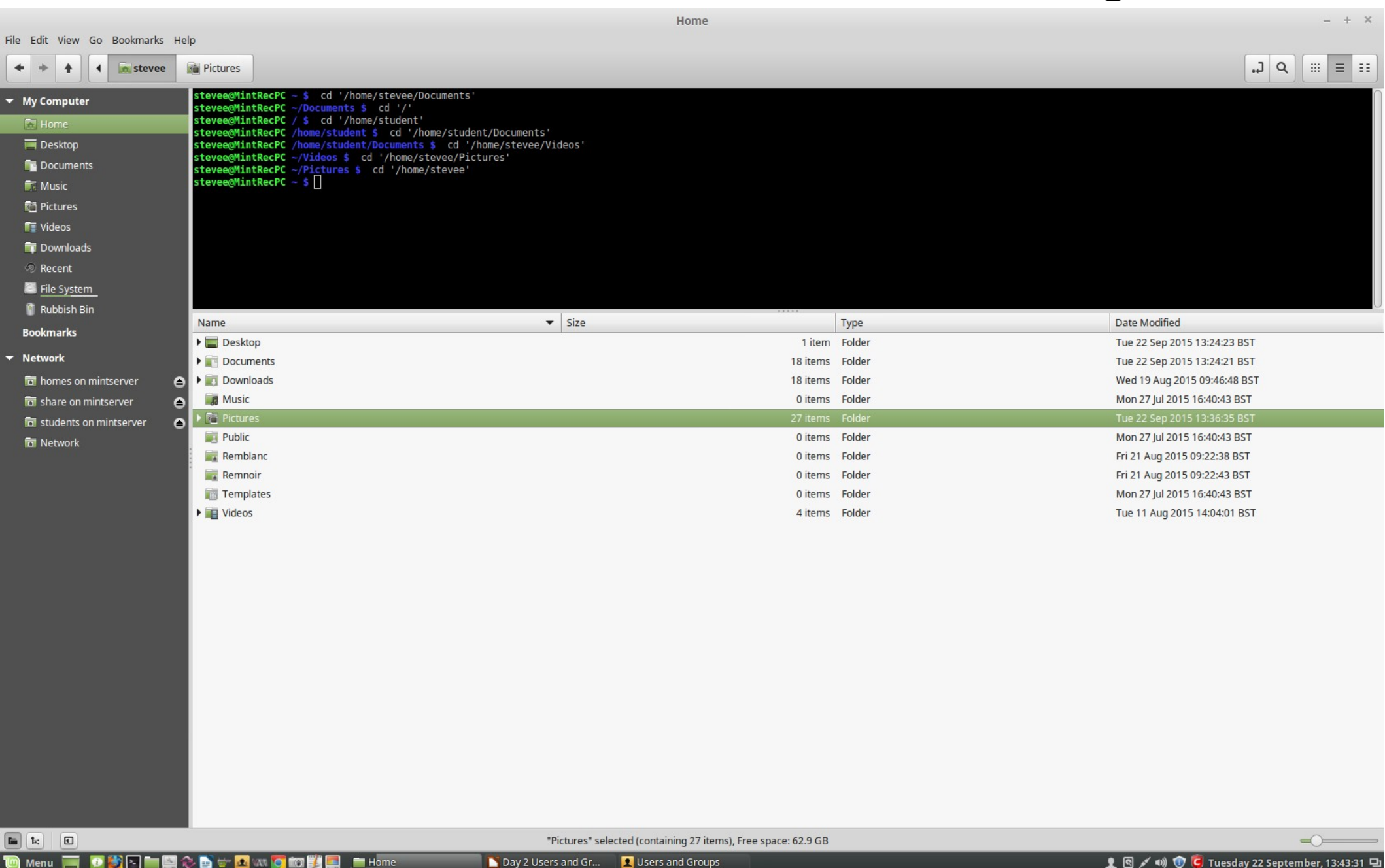
Remember [TAB] to help you auto-complete the command line

Logout and back in again.

Check if terminal is in nemo GUI?

Click on your Home Dir:

Nemo terminal in file manager



Users are listed in /etc/passwd
cat /etc/passwd
awk '{print \$0}' /etc/passwd

The screenshot shows a Linux desktop environment. On the left is a sidebar with navigation options: My Computer, Network, and Bookmarks. The main window is titled 'Pictures' and displays a terminal window. The terminal shows the command 'cat /etc/passwd' being executed, displaying the contents of the /etc/passwd file. Below the terminal, a file manager window shows a list of files in the 'Pictures' directory.

Terminal Output:

```
stevee@MintRecPC ~/Pictures $ 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:Mail List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin)/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
libuuid:x:100:101:/var/lib/libuuid:
syslog:x:101:104:/home/syslog:/bin/false
messagebus:x:102:106:/var/run/dbus:/bin/false
usbmux:x:103:46:usbmux daemon,,,:/home/usbmux:/bin/false
dnsmasq:x:104:65534:dnsmasq,,,:/var/lib/misc:/bin/false
avahi-autoipd:x:105:114:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/bin/false
kernoops:x:106:65534:Kernel Oops Tracking Daemon,,,:/bin/false
avahi:x:107:115:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/bin/false
colord:x:108:117:colord colour management daemon,,,:/var/lib/colord:/bin/false
pulse:x:109:118:PulseAudio daemon,,,:/var/run/pulse:/bin/false
hplip:x:110:7:HPLIP system user,,,:/var/run/hplip:/bin/false
mdm:x:111:120:MDM Display Manager:/var/lib/mdm:/bin/false
rtkit:x:112:122:RealtimeKit,,,:/proc:/bin/false
saned:x:113:123:/home/saned:/bin/false
speech-dispatcher:x:114:29:Speech Dispatcher,,,:/var/run/speech-dispatcher:/bin/sh
stevee:x:1000:1000:stevee,,,:/home/stevee:/bin/bash
sshd:x:115:65534:/var/run/sshd:/usr/sbin/nologin
libvirt-qemu:x:116:125:Libvirt Qemu,,,:/var/lib/libvirt:/bin/false
libvirt-dnsmasq:x:117:126:Libvirt Dnsmasq,,,:/var/lib/libvirt/dnsmasq:/bin/false
gary:x:1002:1002:gary,,,:/home/gary:/bin/bash
gavin:x:1003:1003:gavin,,,:/home/gavin:/bin/bash
motion:x:118:127:/home/motion:/bin/false
mysql:x:119:128:MySQL Server,,,:/nonexistent:/bin/false
ntp:x:120:129:/home/ntp:/bin/false
bind:x:121:130:/var/cache/bind:/bin/false
mythtv:x:122:132:/home/mythtv:/bin/sh
student:x:1004:1004,,,:/home/student:/bin/bash
matt:x:1005:1005,,,:/home/matt:/bin/bash
test:x:1001:1001:test,,,:/home/test:/bin/bash
stevee@MintRecPC ~/Pictures $
```

File Manager Table:

Name	Date Modified	Size	Type
nemoterm.png	Tue 22 Sep 2015 13:43:32 BST	188.2 kB	Image
testuser2.png	Tue 22 Sep 2015 13:36:35 BST	44.4 kB	Image
testuser.png	Tue 22 Sep 2015 13:35:32 BST	44.6 kB	Image
Screenshot from 2015-08-21 13:42:16.png	Fri 21 Aug 2015 13:42:19 BST	551.2 kB	Image

"nemoterm.png" selected (188.2 kB), Free space: 62.9 GB

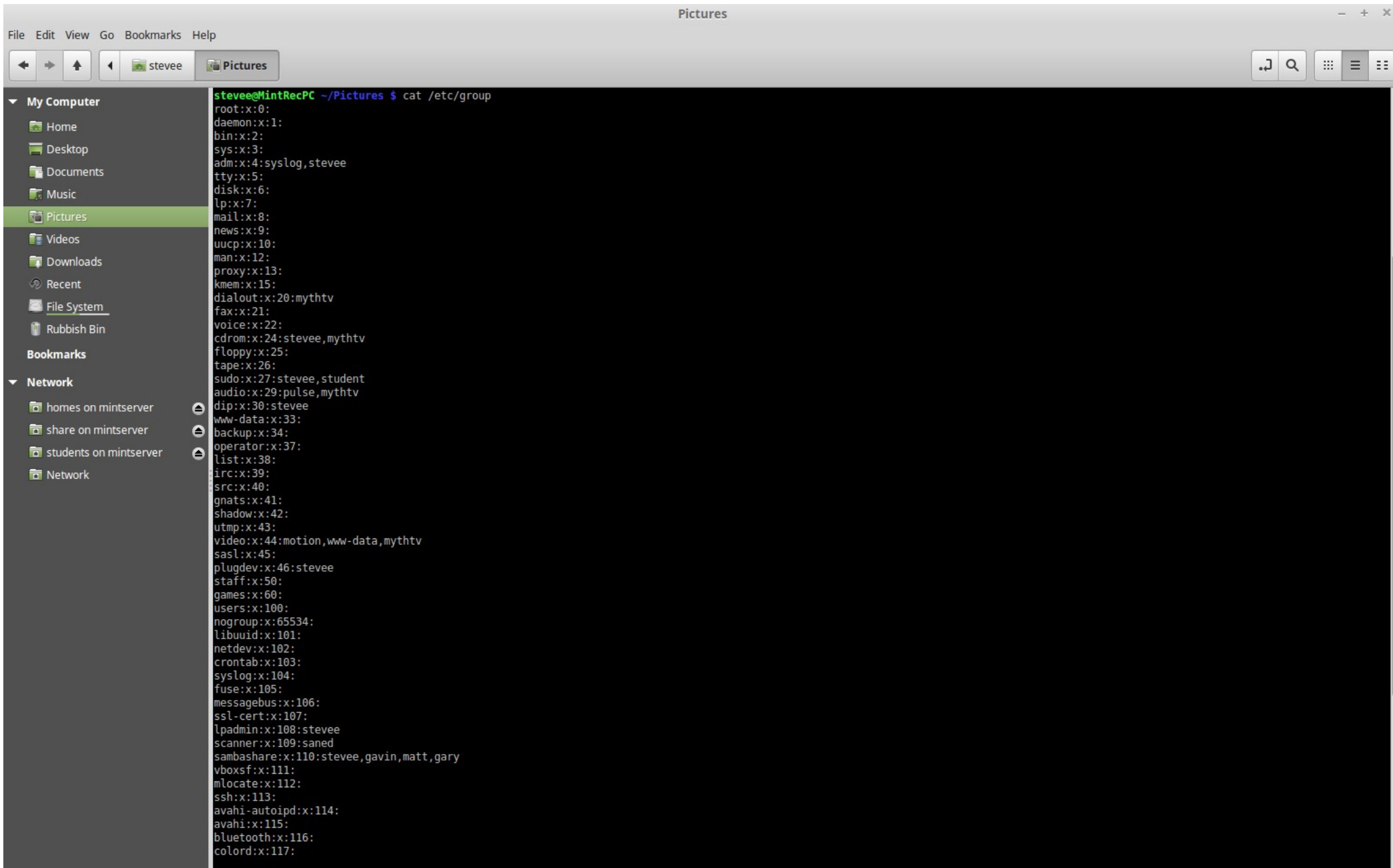
No passwords there, there's an “x” in field :2: – so look in /etc/shadow

Passwords are encrypted!

- stevee@MintRecPC / \$ `sudo cat /etc/shadow`
- root:\$6\$DbJouJDg\$PEZod.z2yNGq5VBQX9....
- student:
\$6\$IvadAcAf\$Xb.F3YsAUeAqEfVAdkTo2iCw09wLS/B
FBB0kt3vV1Npsqp/kMV8EKLLZr4DXyb2R.FG4/j1zFfp
tMwxneRdl01:16696:0:99999:7:::
- matt:\$6\$GS.ICSnf\$X9c40UTWLR4VVFZywxK

Groups are listed in /etc/group

cat /etc/group



```
stevee@MintRecPC ~/Pictures $ cat /etc/group
root:x:0:
daemon:x:1:
bin:x:2:
sys:x:3:
adm:x:4:syslog,stevee
tty:x:5:
disk:x:6:
lp:x:7:
mail:x:8:
news:x:9:
uucp:x:10:
man:x:12:
proxy:x:13:
kmem:x:15:
dialout:x:20:mythtv
fax:x:21:
voice:x:22:
cdrom:x:24:stevee,mythtv
floppy:x:25:
tape:x:26:
sudo:x:27:stevee,student
audio:x:29:pulse,mythtv
dip:x:30:stevee
www-data:x:33:
backup:x:34:
operator:x:37:
list:x:38:
irc:x:39:
src:x:40:
gnats:x:41:
shadow:x:42:
utmp:x:43:
video:x:44:motion,www-data,mythtv
sasl:x:45:
plugdev:x:46:stevee
staff:x:50:
games:x:60:
users:x:100:
nogroup:x:65534:
libuuid:x:101:
netdev:x:102:
crontab:x:103:
syslog:x:104:
fuse:x:105:
messagebus:x:106:
ssl-cert:x:107:
lpadmin:x:108:stevee
scanner:x:109:saned
smbshare:x:110:stevee,gavin,matt,gary
vboxsf:x:111:
mlocate:x:112:
ssh:x:113:
avahi-autoipd:x:114:
avahi:x:115:
bluetooth:x:116:
colord:x:117:
```

What's the diff between GUI list and `cat /etc/group`

The command pipe example we saw in Day 1!

```
stevee@MintRecPC ~/Pictures $ cat /etc/group | sort | cut -d ":" -f1  
adm  
audio  
avahi-autoipd  
avahi  
backup  
bind  
bin  
bluetooth  
cdrom  
colord  
crontab  
daemon  
dialout  
dip  
disk  
fax  
floppy  
fuse  
games  
gary  
gavin  
gnats  
irc  
kmem
```


Skin the cat

`awk -F: '{print $1}' /etc/passwd`

Terminal

```
stevee@Mint5630 ~ $ awk -F: '{print $1}' /etc/group
```

root

daemon

bin

sys

adm

tty

disk

lp

mail

news

uucp

man

proxy

kmem

dialout

How many users and groups are there now?

- `cat /etc/passwd | wc -l`
- 47
- `awk -F: '{print $1}' /etc/group | wc -l`
- 77
- These change depending on what software, services, groups and users you add or install.

Research how passwords can be encrypted, so stored in /etc/shadow

- <https://www.youtube.com/watch?v=b4b8ktEV4Bg>

There are many 1 way encryption algorithms and methods e.g: password + salt + enc method = encrypted password string:

- `mkpasswd password BFVDA21wa2ENQ`
- `echo "password" | sha512sum`
- `9151440965cf9c5e07f81eee6241c042a7b78e9bb2d
d4f928a8f6da5e369cdffdd2b70c70663ee30d021157
31d35f1ece5aad9b362aaa9850efa99e3d197212a -`
- `echo mypassword | openssl enc -blowfish -a -salt`
- Mint uses sha512 shown by `6` in /etc/shadow

Day Summary

- Add users and groups in GUI and command line
- Sudo group membership required for temp “root” Admin tasks
- Where the files for user/grp info are – in “/etc/...”
- /etc/shadow holds the encrypted passwords
- Used `cat` and `awk` to view files
- Piped cat's/awk's output into another cmd to gain info in a different format – total groups etc.
- Terminal as a programming environment - `awk`
- Introduced concept of password encryption with a “one way” hash – easy to make, hard to break

Further Reading

- <https://www.youtube.com/watch?v=8ZtInClXe1Q>
- <https://www.youtube.com/watch?v=M7kEpw1tn50>
- <https://www.youtube.com/watch?v=HvMSRWTE2ml>
- <http://www.stevepedwards.com/DebianAdmin/basic-maths-and-ideas-behind-password-complexity/>
- `sudo apt-get install sysadmin-guide`
- ftp://94.244.139.11/lit/1.%20Manuals/O_Reilly_-_sed____awk_2nd_Edition.pdf
- Research google for linux user/group accounts, pw gen.
- <http://www.tecmint.com/manage-users-and-groups-in-linux/>
- <http://www.slashroot.in/how-are-passwords-stored-linux-understanding-hashing-shadow-utils>
- <http://www.tecmint.com/generate-encrypt-decrypt-random-passwords-in-linux/>