Users and Groups

Linux System Administration
Fall 2022

What is a User Account?

- A user account is a set of credentials that give a person access to the machine.
- There are several attributes associated with each account on a system.

Attributes of a User Account

- Username
- Password (password placeholder)
- User ID (UID)
- Primary Group ID (GID)
- Textual Description (Gecos)
- Home Directory
- Default Shell

What is a Group

- A group is a set of users that allows permissions to be granted in a more organized way.
  - File access
  - Used directly by some programs like sudo

Group Attributes

- Group Name
- Group ID (GID)
- Group Members

Special accounts

- System processes (daemons) need accounts on the machine too and you will sometimes see accounts for specific programs
  - Limit elevated access as much as possible
- What is running on the system

```
ps -eo user|sort|uniq -c
ps -eo user,pid,comm | sort
```

In the beginning

- User information stored in files
  - /etc/passwd
  - /etc/group
- Password encrypted but vulnerable to attack
- All credentials local

Hiding secrets

- /etc/passwd
  - User name, UID, etc
- /etc/shadow
  - Encrypted password, pasword aging

/etc/passwd format

mscott:x:5001:5000:Michael Scott:/home/mscott:/bin/bash

`mscott` - user name

`x` - password is encrypted and stored in /etc/shadow

`5001` - User ID

`5000` - Group Id

`Michael Scott` - Full name (GECOS)

`/home/mscott` - home directory

`/bin/bash` - login shell

/etc/shadow format

mscott:6hyz$bx0cpZOlif0:18056:0:99999:7::

`mscott` - user name

`$6$hyz....` encrypted password

- x sets encryption algorithm
- First few digits is the salt

`18056` - Last date password changed

`0` - Minimum password age

`99999` - Maximum days password is valid

`7` - Days of warning before expiration

Inacitive and Expire is blank

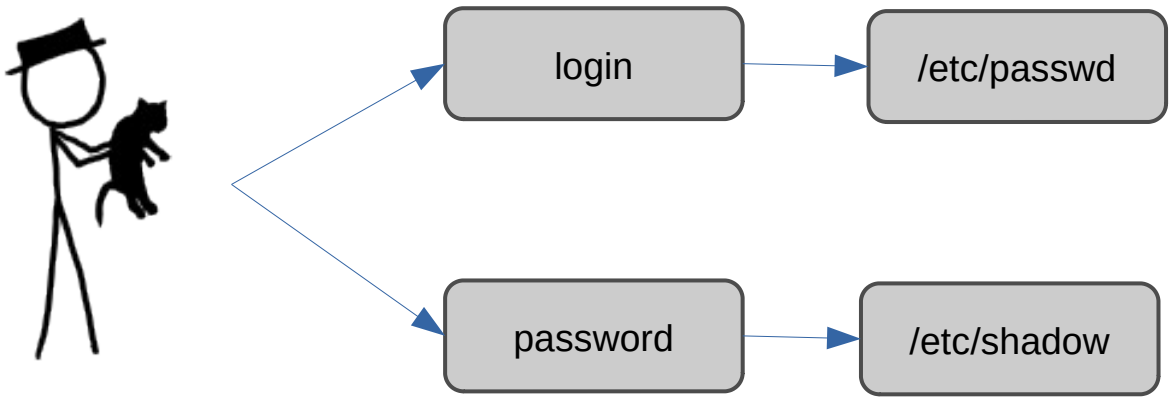
/etc/group format

managers:x:6001:mscott,jhalpert,dschrute

- `managers` - group name
- `x` - password in /etc/gshadow
- `6001` - Group ID
- `mscott,jhalpert,dschute` - members
  - Users with the GID as their primary group will also be members of this group

Basic login

- User credentials checked against files



Networked User Information

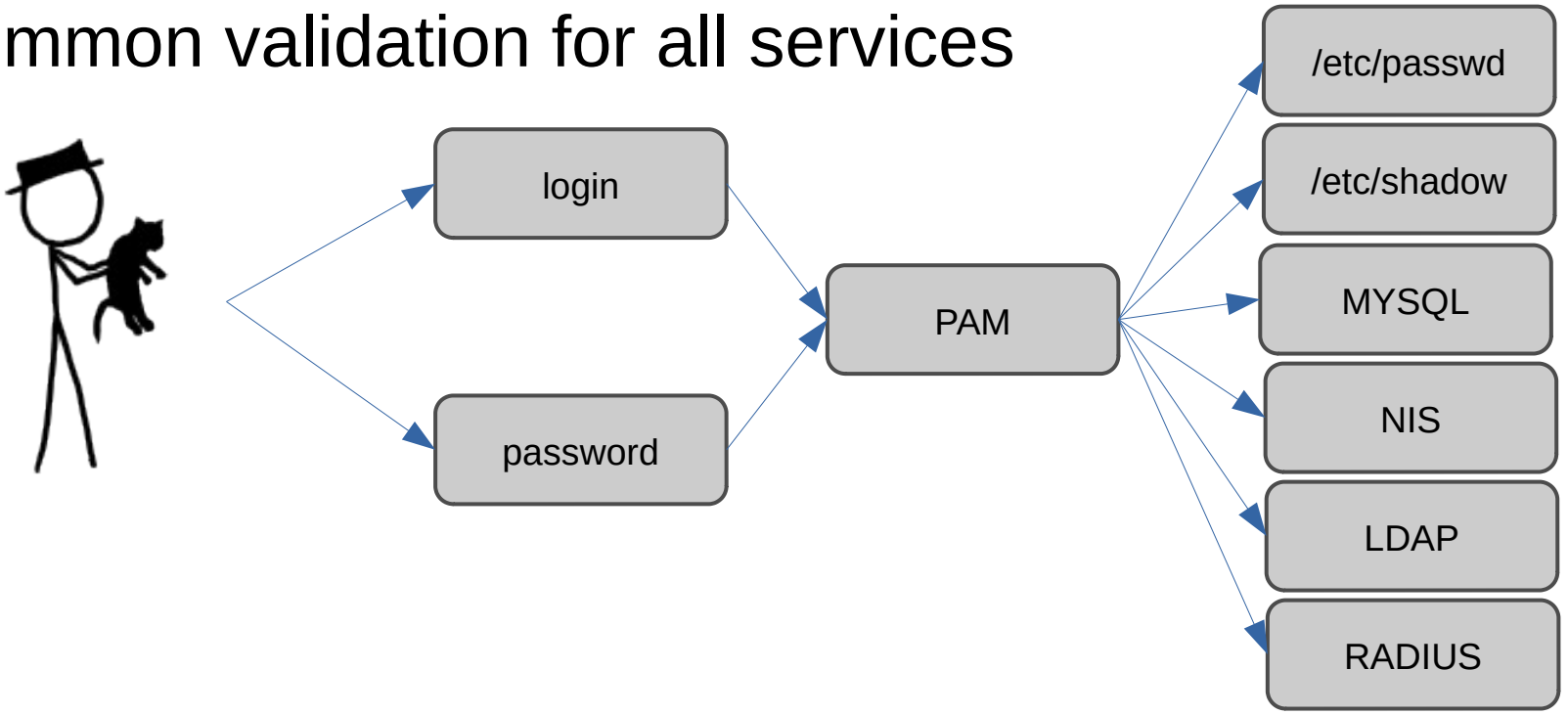
- NIS - Network Information Service
  - Originally called Yellow Pages
- LDAP - Lightweight Directory Access Protocol
- Kerberos
- many others

Which login is used?

- NSS - Name Service Switch
  - Sets order of evaluation for GNU C library
- PAM - Pluggable Authentication Module
  - Fine grained control of authenitication

PAM login

- Pluggable Authentication Modules
- Common validation for all services



Adding a user

- `vipw`
  - Trusted `vi /etc/passwd`
    - Also -p
  - -s to edit `/etc/shadow`
  - -g to edit `/etc/group`
    - Also `vigr`

- `useradd` *`login`*
  - -u - set userid
  - -U - add private group
  - -g - set GID or group
  - -G - add groups
- Must set password
- Template for files in home directory in `/etc/skel`

passwd

- Allows the user to update their own password
- `passwd` *`login`*
  - Allows root to set the password for a user

groupadd

- Creates a new group
- -g sets GID
- -p can set a group password
- `groupadd -G 6001 managers`

adduser

- debian
  - Like useradd, but also prompts for name, GECOS and password
  - `adduser` *`login group`*
    - Adds *login* to *group*
- RedHat
  - Basically just useradd
- BSD
  - Detailed prompts

Removing a user and group

- `userdel` *`login`*
  - Removes the user
  - -r also remove home directory and mail spool
- `groupdel` *`group`*
  - Removes the group

usermod *login*

- Modifies the user attributes
  - -l change login name
  - -u change UID (also modifies mailbox and files in /home)
  - -L lock (disable) login by removing password
  - -g set primary group for user
  - -G add user to this secondary group
  - -p change password
  - -s change shell

Change user info and shell. Users can also change their own

- `chfn`
  - Change “finger” data
  - Full Name
  - GECOS data
    - Office
    - Phone number
- `chsh`
  - Change login shell for user
  - -l list available shells

Special groups

- wheel - traditional users with root access
  - Redhat: users with unlimited sudo
  - debian: *wheel* group renamed to *sudo*
- dialout - users with access to serial ports
- Private groups

Gotchas

- Group membership is updated on login
  - Log out or launch new login shell