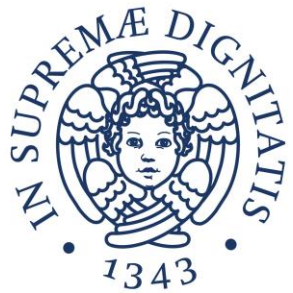


LABORATORIO DI SISTEMI OPERATIVI

Corso di Laurea in Ingegneria Informatica

A.A. 2023/2024

Ing. Maurizio Palmieri


maurizio.palmieri@unipi.it

ESERCITAZIONE 3

Utenti e gruppi (seconda parte)

File di configurazione utenti

- File con informazioni pubbliche sugli utenti
  - `/etc/passwd`
- File con informazioni sensibili (password)
  - `/etc/shadow`

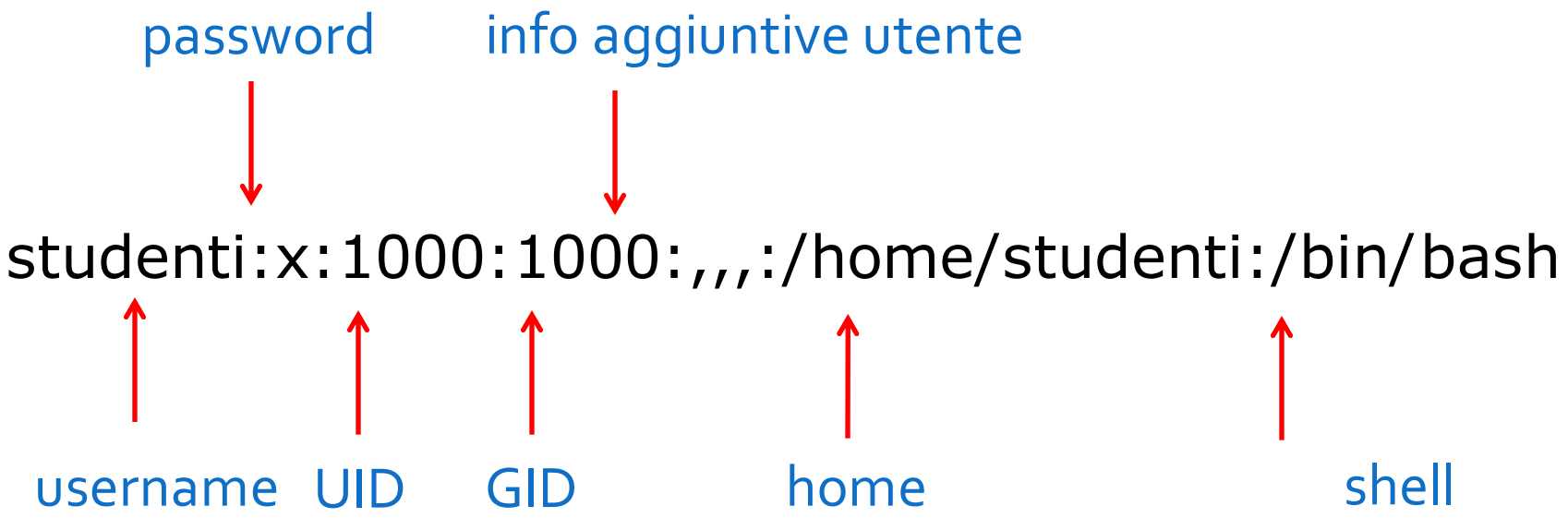
File /etc/passwd

- Informazioni del manuale:
  - `man 5 passwd`
- Si può aprire in editing con il comando
  - `vipw`

```
 GNU nano 2.2.6                                File: /etc/passwd.edit

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:Mailing 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
systemd-timesync:x:100:103:systemd Time Synchronization,,,:/run/systemd:/bin/false
systemd-network:x:101:104:systemd Network Management,,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:105:systemd Resolver,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:106:systemd Bus Proxy,,,:/run/systemd:/bin/false
messagebus:x:104:109::/var/run/dbus:/bin/false
avahi:x:105:110:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/bin/false
Debian-exim:x:106:112::/var/spool/exim4:/bin/false
statd:x:107:65534::/var/lib/nfs:/bin/false
avahi-autoipd:x:108:115:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/bin/false
colord:x:109:117:colord colour management daemon,,,:/var/lib/colord:/bin/false
geoclue:x:111:118::/var/lib/geoclue:/bin/false
pulse:x:112:120:PulseAudio daemon,,,:/var/run/pulse:/bin/false
speech-dispatcher:x:113:29:Speech Dispatcher,,,:/var/run/speech-dispatcher:/bin/sh
rtkit:x:114:122:RealtimeKit,,,:/proc:/bin/false
saned:x:115:123::/var/lib/saned:/bin/false
usbmux:x:116:46:usbmux daemon,,,:/var/lib/usbmux:/bin/false
Debian-gdm:x:117:125:Gnome Display Manager:/var/lib/gdm3:/bin/false
studenti:x:1000:1000:,,,:/home/studenti:/bin/bash
vboxadd:x:999:1::/var/run/vboxadd:/bin/false
```

File /etc/passwd



File /etc/passwd

Campo	Significato
username	Nome utente utilizzato per il login
password	Campo (un tempo) dedicato a password (cifrata). 'x' indica che la password cifrata si trova in `/etc/shadow`
UID (user id)	Identificatore numerico univoco dell'utente
GID (group id)	Identificatore numerico univoco del gruppo primario (numero)
dati personali	Nome completo dell'utente e altre informazioni
cartella home	Percorso assoluto della cartella personale (home). Viene utilizzato per impostare la variabile d'ambiente $HOME
shell	Interprete dei comandi da utilizzare per l'utente

- La shell può essere impostata a `/sbin/nologin` o `/bin/false` per indicare che non è possibile fare login con tali utenti

File /etc/shadow

- Informazioni del manuale:
  - `man shadow`
- Si può aprire in editing con il comando
  - `vipw -s`

File /etc/shadow

Campo	Significato
username	Deve essere un nome valido (esistente)
password	La password cifrata dell'utente (vedere **crypt**)
Ultima modifica	Data di modifica della password (giorni dal 1970)
Età min	Durata minima della password
Età max	Durata massima della password
Periodo di avviso	Giorni prima della scadenza in cui l'utente viene avvisato
Periodo inattività	Giorni dopo la scadenza della password in cui questa è ancora accettata
Scadenza	Data scadenza account
Campo riservato	Riservato per utilizzo futuro

Comandi per la gestione dei gruppi

- `addgroup`
- `delgroup`
- `gpasswd`
- `newgrp`

Creazione e rimozione gruppi

- Creazione di un gruppo:
  - `addgroup gruppo`
- Rimozione di un gruppo:
  - `delgroup gruppo`
- La creazione/rimozione di gruppi richiede i privilegi di root

gpasswd

- Aggiungere un utente a un gruppo
  - `gpasswd -a utente gruppo`
- Rimuovere un utente da un gruppo
  - `gpasswd -d utente gruppo`
- Definire i membri di un gruppo
  - `gpasswd -M utente1,utente2,… gruppo`
- Definire gli amministratori di un gruppo
  - `gpasswd -A utente1,utente2,… gruppo`

- Solo gli amministratori di un gruppo (oltre a root) possono aggiungere/rimuovere utenti a/da un gruppo
- Solo root può aggiungere/rimuovere gli amministratori

gpasswd

- Impostare/cambiare la password di un gruppo
  - `gpasswd gruppo`
- Rimuovere la password di un gruppo
  - `gpasswd -r gruppo`
- Se la password non è impostata, solo i membri del gruppo possono averne i privilegi

gpasswd

- Se la password è impostata
  - Gli altri utenti (non membri del gruppo) possono acquisire temporaneamente i privilegi del gruppo mediante il comando newgrp
  - I membri del gruppo non hanno bisogno di utilizzare la password

- Le password di gruppo sono intrinsecamente poco sicure, in quanto conosciute da più utenti

newgrp

- Utilizzo del comando newgrp:
  - `newgrp gruppo`

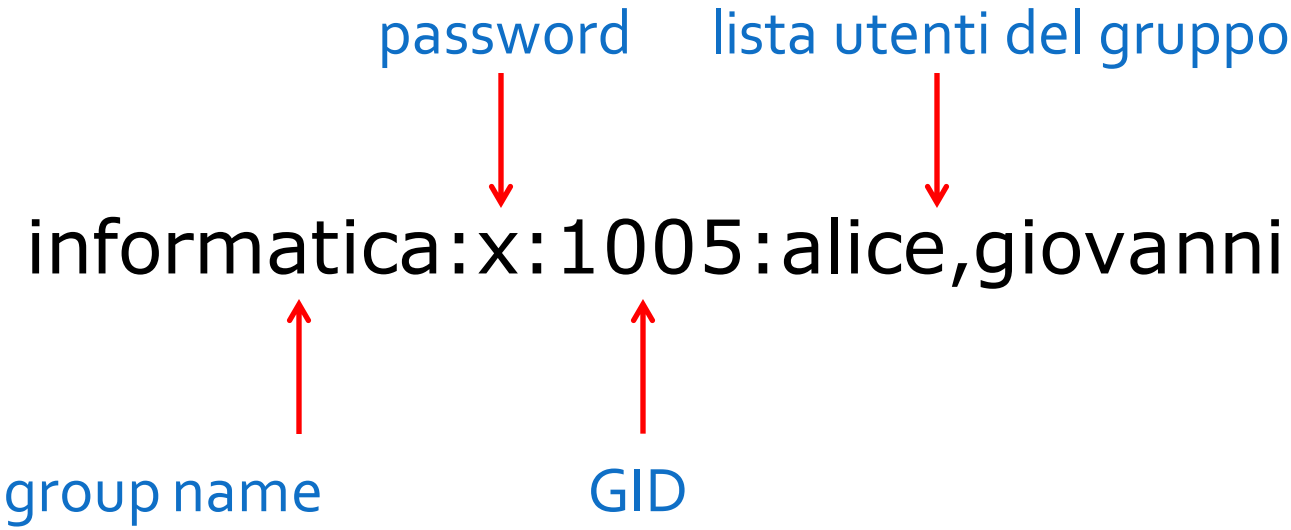
- Con il comando `newgrp`, il gruppo specificato diventa il nuovo gruppo primario dell'utente per la sessione di login corrente

File di configurazione gruppi

- File con informazioni pubbliche sui gruppi
  - `/etc/group`
- File con informazioni sensibili (password e amministratori)
  - `/etc/gshadow`

File /etc/group

- Manuale:
  - `man group`
- Si può aprire con il comando
  - `vigr`

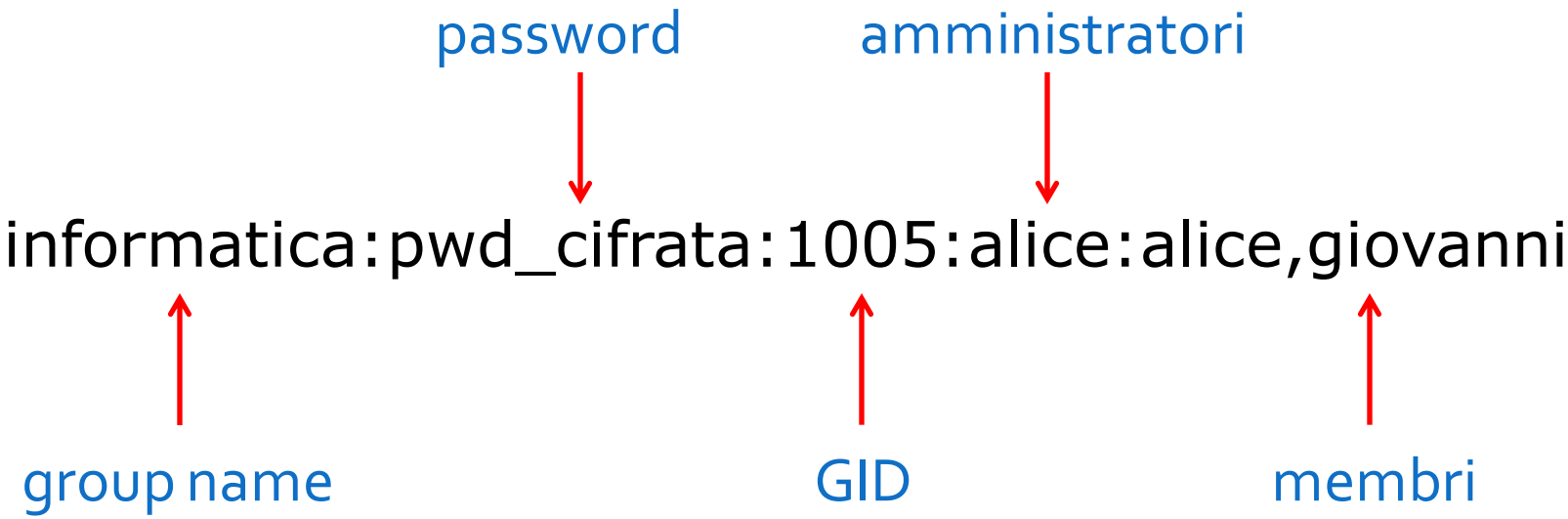


File /etc/group

Campo	Significato
gruppo	Nome del gruppo
password	Password cifrata del gruppo. 'x' indica che la password cifrata si trova in `/etc/gshadow`
GID (group id)	Identificatore univoco del gruppo (numero)
Lista utenti	Utenti appartenenti al gruppo (separati da virgole). Non contiene l'utente per il quale il gruppo è il «primary group», in quanto questa informazione è già in /etc/passwd

File /etc/gshadow

- Manuale:
  - `man gshadow`
- Si può aprire con il comando
  - `vigr -s`



File /etc/gshadow

Campo	Significato
gruppo	Nome del gruppo
password	Password cifrata del gruppo. Un campo vuoto oppure i caratteri '*' o '!' indicano che la password non è impostata. In tal caso solo i membri del gruppo possono avere i privilegi del gruppo.
GID (group id)	Identificatore univoco del gruppo (numero)
Amministratori	Lista degli utenti amministratori del gruppo (separati da virgole). Gli amministratori possono cambiare la password e aggiungere/rimuovere utenti al/dal gruppo.
Lista utenti	Altri utenti del gruppo (separati da virgole)

ESERCIZI

Preparazione Esercizio

- Eliminare eventuali utenti creati per gli esercizi precedenti:
  - Visualizzare solo gli utenti che hanno la home in `/home` con il comando `cat /etc/passwd | grep home`
  - Eliminare gli utenti mostrati, lasciando solo studenti (non eliminare gli utenti di sistema!)
    - Cercare sul manuale l'opzione di `deluser` per rimuovere la home dell'utente
    - Se necessario rimuovere manualmente la home di utenti già rimossi

Esercizio

- Aggiungere tre nuovi utenti con username *alice*, *giovanni*, *simone*
  - Verificare le nuove informazioni contenute nei file di configurazione (`/etc/passwd` e `/etc/shadow`)
- Fare login come alice
- Spostarsi nella home di alice
- Creare un file documento dentro una cartella docs
- Scrivere la stringa «messaggio importante» dentro documento
- Fare login come giovanni o simone
  - giovanni e simone possono leggere documento?
- Modificare i permessi di documento in modo che non possa essere letto dagli altri
  - Verificare che gli altri non possono leggere

Esercizio

- Fare login come root
  - Creare un gruppo informatica e aggiungere alice ai membri del gruppo
    - Usare il comando `exit` (se necessario più volte) per tornare alla shell di alice.
  - Se si utilizza il comando `groups`, si vede il gruppo informatica nei gruppi di alice?
    - Provare a fare logout e login nuovamente (utilizzando i comandi `exit` e `su`), e poi lanciare di nuovo `groups`.
- Dal terminale di alice
  - Cambiare il group owner di documento, in modo che sia il nuovo gruppo informatica
  - Verificare con `ls -l` che il nuovo group owner è informatica e che gli appartenenti al gruppo hanno accesso in lettura (mentre gli altri utenti non possono accedere)
  - Provare ad aggiungere giovanni al gruppo «informatica», è possibile per alice?
    - In caso negativo fare in modo che alice possa amministrare il gruppo e aggiungere giovanni
- Accedere al terminale di giovanni e verificare la possibilità di accedere al file
- Controllare se simone può leggerlo

Esercizio

- Dal terminale di alice
  - Impostare una password per il gruppo informatica
  - giovanni e alice hanno bisogno della password per accedere a documento?
- Accedere al terminale di simone
  - Leggere il contenuto di documento sfruttando la password del gruppo
  - Spostarsi nella home di Simone e creare un file prova
  - Qual è il group owner di prova?
- Accedere al terminale di root ed eliminare il gruppo informatica
- Tornare al terminale di alice e spostarsi nella home
  - Visualizzare le informazioni di documento con `ls -l`, cosa viene visualizzato al posto del group owner?
  - Impostare alice come group owner del file.