Lezione 8
Autenticazione

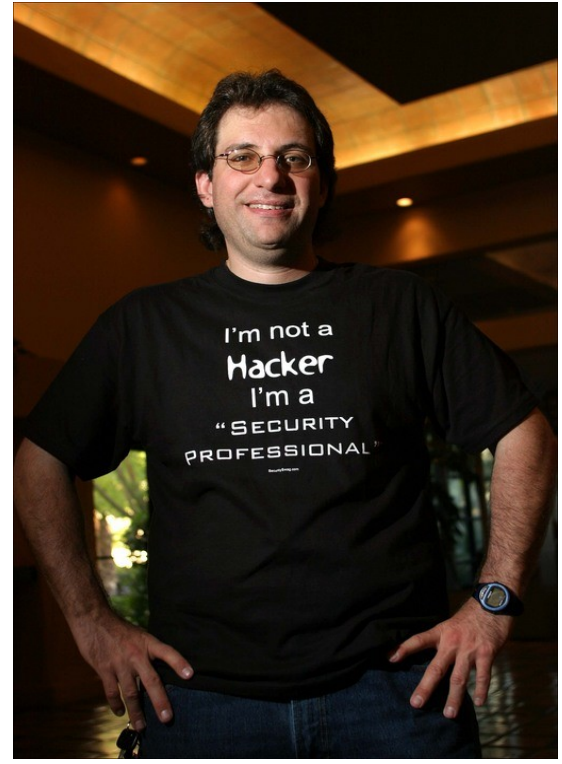
Sistemi Operativi (9 CFU), CdL Informatica, A. A. 2021/2022
Dipartimento di Scienze Fisiche, Informatiche e Matematiche
Università di Modena e Reggio Emilia
http://weblab.ing.unimo.it/people/andreolini/didattica/sistemi-operativi

Quote of the day

(Meditate, gente, meditate...)

“Companies spend millions of dollars on firewalls, encryption and secure access devices, and it’s money wasted, because none of these measures address the weakest link in the security chain.”

Kevin Mitnick (1963-)
Esperto di sicurezza informatica

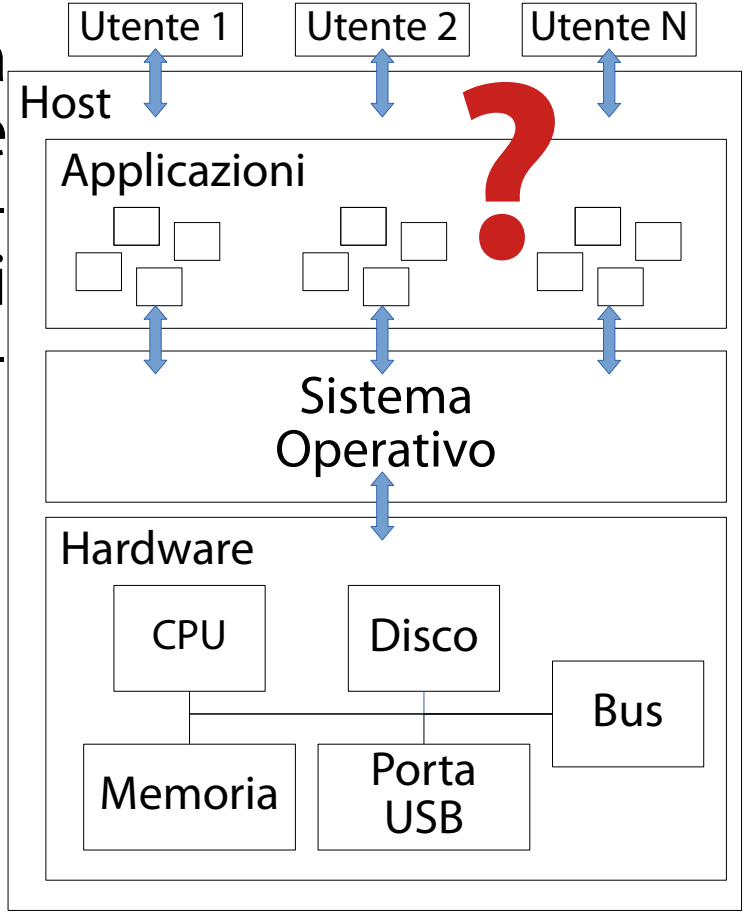


INTRODUZIONE

Lo scenario

(Uno studente vuole capire cosa è e come funziona l'autenticazione in UNIX)

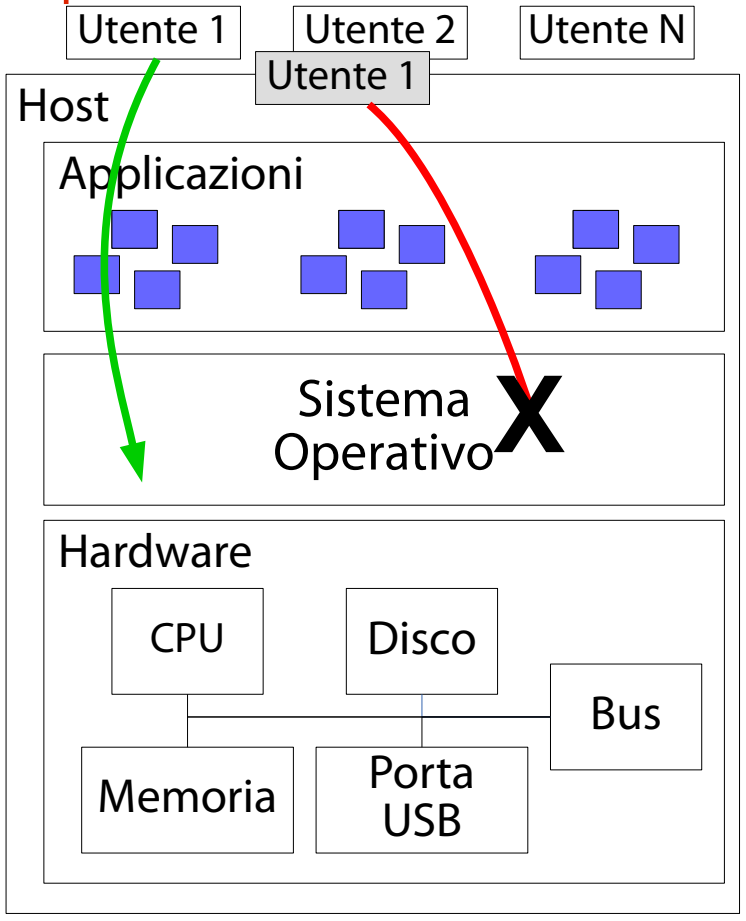
Uno studente in grado di usare la linea di comando vuole capire cosa è e come funziona la procedura di autenticazione nei sistemi UNIX-like (GNU/Linux, nello specifico).



Interrogativi 1/2

(Come fa il SO ad identificare l'utente per chi è veramente?)

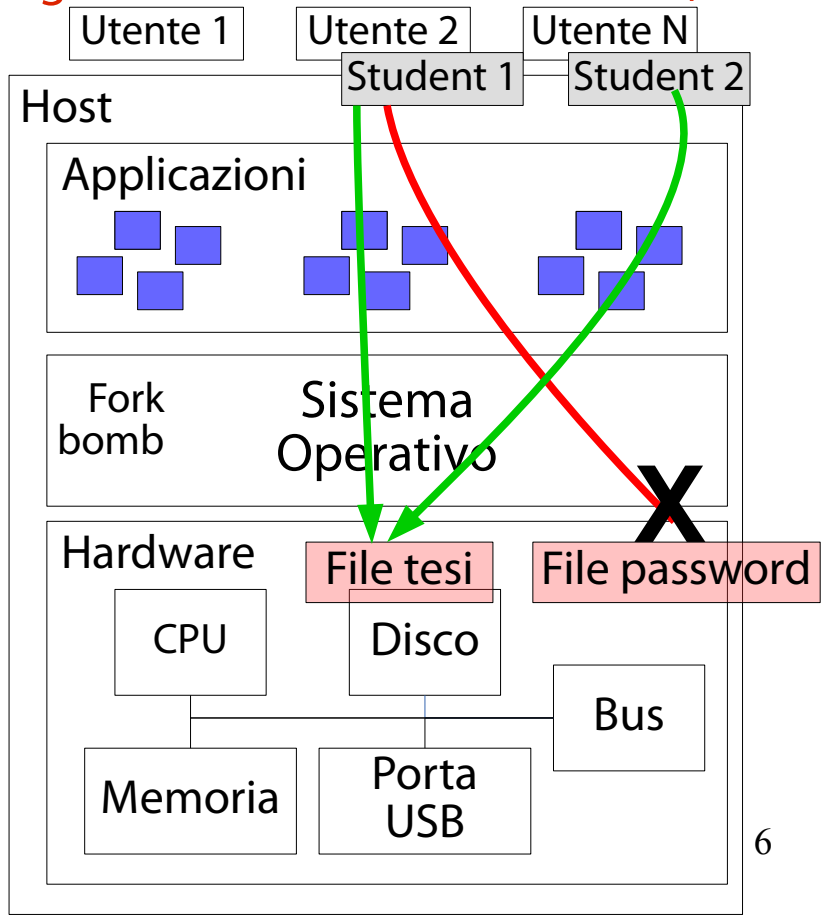
Un utente legittimo si identifica onestamente presso il SO, senza spacciarsi per qualcun altro.
Un utente malizioso potrebbe invece presentarsi al SO nelle vesti di un altro utente e fare danni, addossando la colpa ad un altro.
Il SO è in grado di impedire la "sostituzione di persona"?



Interrogativi 2/2

(Quali strumenti esistono per la gestione degli utenti? Come funzionano?)

Il SO mette a disposizione gli strumenti per la gestione degli utenti?
Come funzionano tali strumenti?



Autenticazione

(Permette di verificare l'identità di un utente)

I SO moderni forniscono astrazioni software per l'autenticazione.

Autenticazione (login): è la procedura con cui il SO conferma la veridicità di una informazione data per vera da una entità.

L'autenticazione si svolge in due operazioni.

- **Identificazione.** Nel momento in cui una entità si presenta, Il SO prova ad associarla ad un nome di login a lui noto.
- **Verifica delle credenziali di accesso.** Il SO chiede all'utente una informazione che solo lui può dare.

Fattori di autenticazione

(Le tipologie di informazioni fornite dall'utente)

Le informazioni fornite da un utente per verificare la propria identità prendono il nome di **fattori di autenticazione** (**authentication factor**).

I fattori di autenticazione si riferiscono ad informazioni
- che solo l'utente è supposto conoscere (password);
- che solo l'utente è supposto avere (dati memorizzati in un badge personale);
- che solo l'utente è supposto saper fare o fornire geneticamente (firma, impronta digitale).

Una avvertenza

(Non si può spiegare tutto in 36 lezioni/72 ore)

In questo corso introduttivo si considererà esclusivamente la password come fattore di autenticazione. In realtà, ne esistono altri:

- chiave pubblica GPG.
- codice numerico OTP a 6 cifre (One Time Pad).
- impronta del pollice.

I sistemi moderni possono prevedere una forma di **autenticazione a fattori multipli** (solitamente, due).

- Google, Facebook: **two factor authentication** con verifica delle credenziali tramite password ed un codice di 6 lettere inviato al proprio smartphone.

L'astrazione software “utente”

(Rappresenta un utente del sistema, umano o non)

Il SO fornisce una astrazione software dal nome **utente** (**user**). L'utente rappresenta una entità qualunque (umana o non) abilitata ad usufruire dei servizi dell'host.

Non tutti i servizi.

Solo quelli per cui è autorizzata.

Informazioni associate all'utente

(Le più importanti)

Identificatore utente (user id): un numero intero non negativo univoco per un utente. È usato dal nucleo del SO per distinguere utenti diversi.

Nome di login (username, login name): stringa alfanumerica di lunghezza non nulla. È una rappresentazione ad alto livello dell'identificatore utente (per l'utente umano).

Password: una sequenza alfanumerica per la verifica delle credenziali.

Shell di login: il percorso dell'interprete dei comandi.

Home directory: la directory in cui si trova l'utente subito dopo aver fatto il login.

Account utente

(Account = insieme di informazioni riguardanti l'utente)

Un **account utente** (**user account**, **account**) è l'insieme di tutte le informazioni riguardanti un dato utente.

- Nome di login.
- Password.
- Home directory.
- Shell di login.
- …

Classificazione degli utenti: normali

(Utente normale → identificatore utente in [1000, 2^{64}-1))

Alcuni utenti rappresentano umani.

- Identificatore utente: nell'intervallo [1000, 2^{64}-1].
- Nome utente: una stringa alfanumerica che ricorda un nome di persona.

Questi utenti possono eseguire una shell interattiva al loro login.

- **`/bin/bash`** (ma può essere cambiata).

Questi utenti hanno una home directory.

- **`/home/username`** (può essere cambiata).

Questi utenti non possono configurare o alterare direttamente le risorse hw/sw.

- Devono elevare i loro privilegi in qualche modo.

Classificazione degli utenti: superutente

(Superutente → identificatore utente = 0)

Nei sistemi UNIX (GNU/Linux non fa eccezione), uno degli utenti può fare tutto.

L'utente **amministratore** (o **superutente**).

Identificatore utente: 0.

Nome utente: **`root`**.

L'utente amministratore può eseguire una shell interattiva al login.

Tipicamente, **`/bin/bash`** (ma può essere cambiata).

L'utente amministratore ha una home directory.

`/root` (può essere cambiata).

L'utente **`root`** può configurare o alterare direttamente le risorse hw/sw.

Dischi, schede di rete, file delle password…

Classificazione degli utenti: di sistema

(Utente di sistema → identificatore utente in [1, 1000))

Infine, alcuni sistemi non rappresentano umani, bensì impersonificazioni di servizi in esecuzione.

- Identificatore utente: >0 (tipicamente, anche < 1000).
- Nome utente: una stringa alfanumerica che ricorda un nome di servizio.

Tali utenti non usano mai una shell interattiva al login, che viene pertanto disabilitata.

Tali utenti possono non avere una home directory.

Tali utenti possono accedere a risorse specifiche dei servizi (per il resto, non possono fare altro).

- File di configurazione, file di log.

Il file `/etc/passwd`

(Per l'identificazione degli utenti)

Il file **`/etc/passwd`** contiene l'elenco degli utenti noti al SO.

- È una base di dati primordiale.
- Elenco di record (uno per riga).
- I campi di un record sono separati dal carattere `:`.

Questo file è:

- leggibile da tutti gli utenti.
- Modificabile solo dall'utente **`root`**.

I campi di `/etc/passwd`

(Informazioni associate agli utenti; `man 5 passwd` per tutti i dettagli)

Nome di login.
Password cifrata (nelle distribuzioni GNU/Linux attuali è conservata in un altro file, per motivi di sicurezza).
Identificatore utente.
Identificatore del gruppo di lavoro del file (usato per il controllo degli accessi).
Nome e cognome veri.
Home directory.
Interprete dei comandi usato.

Il file `/etc/shadow`

(Per la verifica delle credenziali dell'utente con password)

Il file **`/etc/shadow`** contiene informazioni sulle password associate a ciascun nome di login.

- È una base di dati primordiale.
- Elenco di record (uno per riga).
- I campi di un record sono separati dal carattere `:`.

Questo file è leggibile e modificabile dal solo utente **`root`**.

- Notate la separazione in un file separato (e ben protetto) delle informazioni riguardanti le password.
- → Il principio del minimo privilegio è in azione!

I campi di `/etc/shadow`

(Informazioni associate alla password utente; **`man 5 shadow`** per i dettagli)

Nome di login.
Password cifrata.
Data ultimo cambio password.
Età minima e massima della password.
Periodo di avviso password.
Periodo di inattività password.
Data scadenza account.

Una considerazione di efficienza

(È doveroso ribadirla)

Per motivi legati all'efficienza, il nucleo del SO mantiene nelle sue strutture di controllo una sola informazione fra tutte quelle ora viste: l'identificatore dell'utente.

Il nucleo preferisce lavorare con numeri interi al posto delle stringhe (è più efficiente).

Il nucleo preferisce lasciare alle applicazioni di sistema la conduzione della procedura di autenticazione e dedicarsi ad altre faccende più urgenti (gestione I/O, processi, memoria, …).

GESTIONE DEGLI UTENTI

Scenario e interrogativi

(Come sono gestiti gli utenti? È possibile visionare le proprietà di un utente?)

Scenario: in un SO moderno (time sharing, multi-utente), un amministratore vuole creare, modificare, rimuovere utenti.

Interrogativi:

Esistono strumenti per creare, modificare, rimuovere utenti?

Esistono strumenti per prendere visione delle caratteristiche di un utente?

Creazione di un utente in Debian

(Si usa il comando **`adduser`**)

Debian GNU/Linux e derivate semplificano molto la procedura di creazione di un nuovo utente.
È sufficiente eseguire il comando seguente da amministratore:

`adduser` ***`nome_di_login`***

Ad esempio:

`adduser` ***`prova`***

Il comando **`adduser`** è interattivo; il SO chiede informazioni all'utente, che le deve immettere.

Immissione dei campi

(Pochi e immediati: password, nome completo, stanza, numeri di telefono)

I campi da immettere sono pochi e di immediata comprensione.

La password (da immettere due volte per sicurezza).
Il nome completo (nome e cognome dell'utente).
Il nome/numero dell'ufficio in cui si lavora.
I numeri di telefono di lavoro e di casa.
Una stringa di testo (immessa dall'amministratore) di compendio alle informazioni precedenti.

Il risultato del comando **adduser**

(Un utente nuovo di zecca con la sua home directory ed il suo gruppo primario)

Il risultato del comando **adduser** è un utente nuovo di zecca (nel caso in questione, l'utente di nome **prova**).

L'utente **prova** ha le seguenti risorse.

- Una home directory **/home/prova**.
- Un gruppo primario di lavoro **prova** (e, per il momento, nessun altro gruppo secondario).
- Un interprete di default (**/bin/bash**) con una configurazione iniziale copiata pari pari dalla directory **/etc/skel** ("skel" → "skeleton" → "scheletro").

Esercizio 1 (1 min.)

Create un nuovo utente con nome di login **`studente2`**.

Analisi dell'utente

(Visione del file **`/etc/passwd`**)

Si apra il file **`/etc/passwd`** e si cerchi il record relativo all'utente di nome **`prova`**:

```
grep prova /etc/passwd
```

Si dovrebbe ottenere il record seguente:

```
prova:x:1001:1001:Prova,10,0123,4567,testo:/home/prova:/bin/bash
```

Analisi dell'utente

(Visione del file **`/etc/passwd`**)

Si apra il file **`/etc/passwd`** e si cerchi il record relativo all'utente di nome **`prova`**:

```
grep prova /etc/passwd
```

Si dovrebbe ottenere il record seguente:

```
prova x:1001:1001:Prova,10,0123,4567,testo:/home/prova:/bin/bash
```

Nome di login dell'utente

Analisi dell'utente

(Visione del file **`/etc/passwd`**)

Si apra il file **`/etc/passwd`** e si cerchi il record relativo all'utente di nome **`prova`**:

```
grep prova /etc/passwd
```

Si dovrebbe ottenere il record seguente:

```
prova x:1001:1001:Prova,10,0123,4567,testo:/home/prova:/bin/bash
```

Password
(celata all'utente)

Analisi dell'utente

(Visione del file **`/etc/passwd`**)

Si apra il file **`/etc/passwd`** e si cerchi il record relativo all'utente di nome **`prova`**:

```
grep prova /etc/passwd
```

Si dovrebbe ottenere il record seguente:

```
prova:x:1001:1001:Prova,10,0123,4567,testo:/home/prova:/bin/bash
```

Identificatore utente
(partono da 1000)

Analisi dell'utente

(Visione del file **`/etc/passwd`**)

Si apra il file **`/etc/passwd`** e si cerchi il record relativo all'utente di nome **`prova`**:

```
grep prova /etc/passwd
```

Si dovrebbe ottenere il record seguente:

```
prova:x:1001:1001:Prova,10,0123,4567,testo:/home/prova:/bin/bash
```

Identificatore gruppo primario
(partono da 1000)

Analisi dell'utente

(Visione del file **`/etc/passwd`**)

Si apra il file **`/etc/passwd`** e si cerchi il record relativo all'utente di nome **`prova`**:

```
grep prova /etc/passwd
```

Si dovrebbe ottenere il record seguente:

```
prova:x:1001:1001:Prova,10,0123,4567,testo:/home/prova:/bin/bash
```

Nome completo dell'utente
(nome e cognome)

Analisi dell'utente

(Visione del file **`/etc/passwd`**)

Si apra il file **`/etc/passwd`** e si cerchi il record relativo all'utente di nome **`prova`**:

```
grep prova /etc/passwd
```

Si dovrebbe ottenere il record seguente:

```
prova:x:1001:1001:Prova,10,0123,4567,testo:/home/prova:/bin/bash
```

Numero di stanza

Analisi dell'utente

(Visione del file **`/etc/passwd`**)

Si apra il file **`/etc/passwd`** e si cerchi il record relativo all'utente di nome **`prova`**:

```
grep prova /etc/passwd
```

Si dovrebbe ottenere il record seguente:

```
prova:x:1001:1001:Prova,10,0123 4567,testo:/home/prova:/bin/bash
```

Numero di telefono
di lavoro

Analisi dell'utente

(Visione del file **`/etc/passwd`**)

Si apra il file **`/etc/passwd`** e si cerchi il record relativo all'utente di nome **`prova`**:

```
grep prova /etc/passwd
```

Si dovrebbe ottenere il record seguente:

```
prova:x:1001:1001:Prova,10,0123,4567,testo:/home/prova:/bin/bash
```

Numero di telefono
di casa

Analisi dell'utente

(Visione del file **`/etc/passwd`**)

Si apra il file **`/etc/passwd`** e si cerchi il record relativo all'utente di nome **`prova`**:

```
grep prova /etc/passwd
```

Si dovrebbe ottenere il record seguente:

```
prova:x:1001:1001:Prova,10,0123,4567,testo:/home/prova:/bin/bash
```

Informazioni suppletive

Analisi dell'utente

(Visione del file **`/etc/passwd`**)

Si apra il file **`/etc/passwd`** e si cerchi il record relativo all'utente di nome **`prova`**:

```
grep prova /etc/passwd
```

Si dovrebbe ottenere il record seguente:

```
prova:x:1001:1001:Prova,10,0123,4567,testo:/home/prova /bin/bash
```

Home directory dell'utente

Analisi dell'utente

(Visione del file **`/etc/passwd`**)

Si apra il file **`/etc/passwd`** e si cerchi il record relativo all'utente di nome **`prova`**:

```
grep prova /etc/passwd
```

Si dovrebbe ottenere il record seguente:

```
prova:x:1001:1001:Prova,10,0123,4567,testo:/home/prova:/bin/bash
```

Percorso assoluto dell'interprete dei comandi dell'utente

Esercizio 2 (1 min.)

Identificate la home directory e l'interprete dei comandi dell'utente **`studente2`**.

Rimozione di un utente in Debian

(Si usa il comando **`deluser`**)

Debian GNU/Linux e derivate semplificano molto la procedura di rimozione di un utente esistente.
È sufficiente eseguire il comando seguente da amministratore:

```
deluser nome_di_login
```

Ad esempio:

```
deluser prova
```

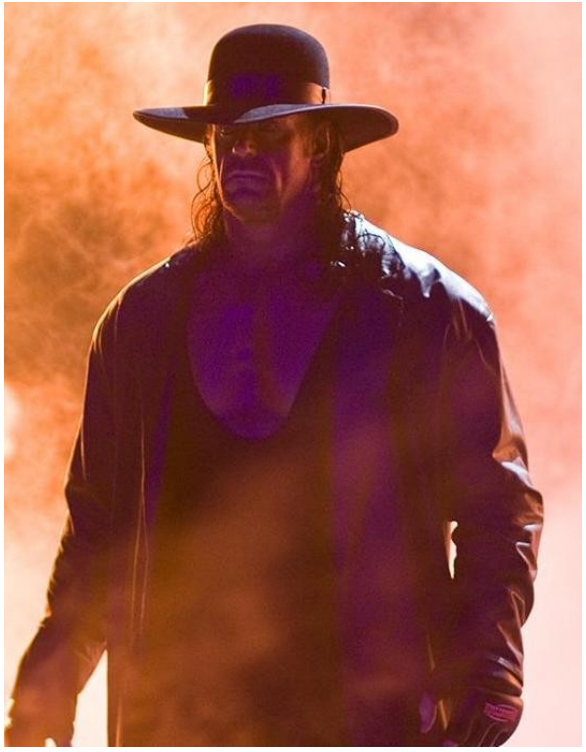
Il comando **`deluser`** non è interattivo (non ha bisogno di esserlo).

Il risultato del comando **`deluser`**

(User has been buried, just like Mark would)

Il risultato del comando **`deluser`** è la rimozione completa dell'utente.

- Cancellazione del nome di login dalle liste di utenti e gruppi.
- Cancellazione del gruppo primario dalla lista dei gruppi.
- Rimozione della home directory (tramite l' opzione **`--remove-home`**).



Esercizio 3 (1 min.)

Cancellate l'utente **`studente2`**.

Una osservazione ed una domanda

(Potreste non trovare **`adduser`** e **`deluser`** in altre distribuzioni GNU/Linux)

I due comandi **`adduser`** e **`deluser`** sono tipici delle distribuzioni Debian GNU/Linux e derivate.
Con tutta probabilità non li troverete nelle altre distribuzioni GNU/Linux non basate su Debian.

La diaspora dei sistemi UNIX colpisce ancora…

La domanda nasce spontanea: quali comandi usano, allora, le altre distribuzioni GNU/Linux?

I comandi **useradd** e **userdel**

(Questi li trovate in tutte le distribuzioni GNU/Linux)

Le altre distribuzioni GNU/Linux usano i comandi **useradd** e **userdel**, analoghi dal punto di vista concettuale.

man useradd e **man userdel** per tutti i dettagli.

A differenza dei comandi precedenti, questi comandi presentano una maggiore difficoltà di uso legata alla loro non interattività.

Non interattività dei comandi

(Il SO non chiede nulla; è l'amministratore a dover specificare tutto)

I due comandi **`useradd`** e **`userdel`** non sono interattivi.

Il SO non pone domande all'amministratore.

È l'amministratore a dover specificare le proprietà dell'utente tramite opportune opzioni.

Se l'amministratore si dimentica di impostarle, l'utente creato non avrà tali proprietà.

Le proprietà si possono sempre impostare in seguito.

Esercizio 4 (2 min.)

Cancellate la directory **`/home/studente2`**. Provate a creare nuovamente l'utente **`studente2`**, questa volta usando il comando **`useradd`**.
Cercate di capire se sia stata creata una home directory per l'utente **`studente2`**.

Creazione della home directory

(Si usa l'opzione **-m** del comando **useradd**)

Per creare una home directory e configurare è sufficiente usare l'opzione **-m** di **useradd**.

```
useradd -m prova
```

Si esegua il comando seguente per sincerarsene:

```
ls -al /home/prova
```

Sono presenti persino i file di configurazione dell'interprete di default (BASH)!

Esercizio 5 (1 min.)

Provate a rimuovere nuovamente l'utente **`studente2`**, questa volta usando il comando **`userdel`**.
Cercate di capire se la home directory è stata rimossa.

Rimozione della home directory

(Si usa l'opzione **`-r`** del comando **`userdel`**)

Per rimuovere la home directory è sufficiente usare l'opzione **`-r`** di **`userdel`**.

```
userdel -r prova
```

Prima di eseguire questo comando, ci si assicuri che l'utente **`prova`** esista.

Configurazione più completa di utenti

(Possibile attraverso diverse opzioni)

I comandi **`adduser`** e **`useradd`** permettono ad un amministratore di impostare le caratteristiche di un account già al momento della creazione.

`man adduser` e **`man useradd`** per tutti i dettagli.

Ad esempio, è possibile impostare i gruppi di lavoro secondari con uno dei comandi seguenti:

```
adduser --ingroup video  prova
useradd -G video -m prova
```

Modifica di un utente esistente

(Si usa il comando **`usermod`**)

Il comando **`usermod`** permette di modificare le proprietà e le risorse di un utente esistente.
La sintassi è semplice:

`usermod [opzioni]` ***`nome_di_login`***

Che cosa è possibile modificare, esattamente?

Nome di login, identificatore utente, home directory, nome e/o identificatore dei gruppi di lavoro primario e secondari, eseguibile dell'interprete, …

Un esempio concreto

(Proviamo a modificare alcune caratteristiche dell'utente **`prova`**)

Si faccia piazza pulita di un eventuale utente **`prova`** preesistente.

```
userdel -r prova
```

Si crei nuovamente un utente **`prova`**:

```
adduser prova
```

Si provi a cambiare l'utente **`prova`** nel modo che segue.

- Nome di login **`prova`** → **`prova2`**
- Identificatore utente **`1001`** → **`1100`**
- Home directory **`/home/prova`** → **`/home/prova2`**

Le opzioni di **`usermod`** richieste

(**`-l`**, **`-u`**, **`-d`** e **`-m`**)

Spulciando la pagina di manuale di **`usermod`**:

```
man usermod
```

si dovrebbero individuare le opzioni seguenti:

- **`-l`**: cambia il nome di login
- **`-u`**: cambia l'identificatore utente
- **`-d`**: specifica la nuova home in **`/etc/passwd`**
- **`-m`**: spostare il contenuto della vecchia directory nella nuova

Il comando richiesto

(Tutto sommato, abbastanza semplice da costruire)

In definitiva Il comando richiesto è il seguente:

```
usermod -l prova2 -u  1100 -d /home/prova2 -m prova
```

Lo si provi!
Non ci si preoccupi di eventuali avvertimenti riguardanti spool di posta non trovati.

Esercizio 6 (2 min.)

Assegnate l'interprete dei comandi **`/bin/zsh`** all'utente **`studente2`**.

Blocco di un account

(Si usa l'opzione **-L** del comando **usermod**)

Il comando **usermod** permette anche di disabilitare il login per uno specifico nome di login (tramite l'opzione **-L**), bloccando di fatto l'account.
Ad esempio, per bloccare l'account al (povero) utente **prova** si esegue il comando seguente:

```
usermod -L prova
```

Si provi un'autenticazione con le credenziali di **prova** tramite login manager grafico o testuale.
L'autenticazione fallisce.

Sblocco di un account

(Si usa l'opzione **-U** del comando **usermod**)

Il comando **usermod** permette anche di riabilitare il login per uno specifico nome di login (tramite l'opzione **-U**), sbloccando di fatto l'account.
Ad esempio, per sbloccare l'account al (fortunato) utente **prova** si esegue il comando seguente:

```
usermod -U prova
```

Si provi un'autenticazione con le credenziali di **prova**:

```
su - prova
```

L'autenticazione ha di nuovo successo.

Modifica di un utente esistente

(Da parte dell'utente stesso, tramite una serie di comandi)

Può l'utente cambiare da solo le preferenze del proprio account, senza scomodare ogni volta l'utente amministratore?

Certamente. Non tutte però; per l'aggiunta ai gruppi serve ancora l'amministratore!

`chfn`: cambia il nome dell'utente (se eseguito da utente **`root`**) e le altre informazioni.

`passwd`: modifica la password.

`chsh`: modifica l'interprete dei comandi.

Esercizio 7 (3 min.)

Autenticatevi come **`studente2`**.
Eseguite le operazioni seguenti:

impostazione del numero di telefono di lavoro al valore **`12345678`**;
cambio della password al valore **`strongpassword`**;
cambio di shell a **`/bin/rbash`**.

Verificate l'applicazione delle modifiche.

Esercizio 8 (2 min.)

Autenticatevi come **`studente2`**.
Eseguite le operazioni seguenti:

impostazione del campo “Altro” al valore **`Dirigente`**.

Verificate l'applicazione delle modifiche.
Notate qualche stranezza?