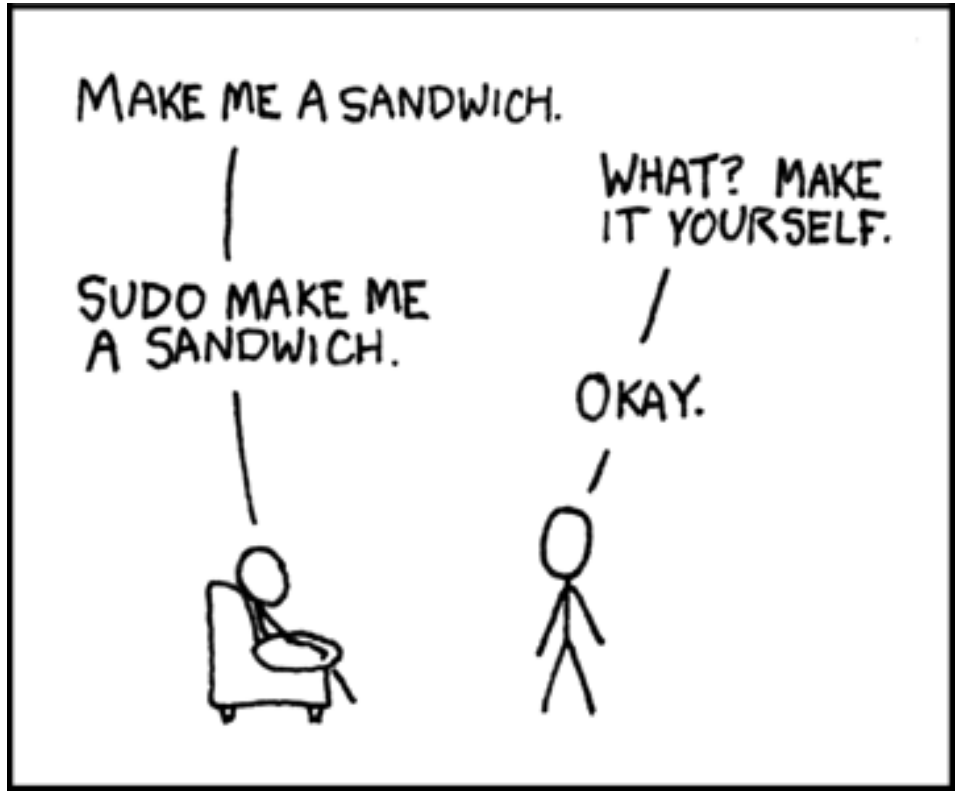
Lezione 12
Elevazione privilegi

Sistemi Operativi (9 CFU), CdL Informatica, A. A. 2022/2023
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

(https://xkcd.com/149/)



SOLUZIONI DEGLI ESERCIZI

Esercizio 1 (1 min.)

Stampate tutti gli identificatori:

dell'utente attivo sul vostro terminale;

dell'utente **`root`**.

Stampa identificatori con **`id`**

Per stampare tutti gli identificatori (utente, gruppo primario, gruppi secondari) dell'utente attualmente in uso, si esegue il comando **`id`** senza argomenti:

```
id
```

Per stampare tutti gli identificatori (utente, gruppo primario, gruppi secondari) dell'utente **`root`**, si esegue il comando id con argomento **`root`**:

```
id root
```

Esercizio 2 (1 min.)

Diventate l'utente **`root`**. Stampate le variabili di ambiente con il comando interno **`export`**.

Notate qualcosa di strano?

Elevazione dei privilegi con **`su`**

Il modo più semplice di diventare **`root`** è quello di usare il comando **`su`**:

```
su
```

Ora si dovrebbe essere **`root`**.

Stampa ambiente con **`export`**

Si stampa l'ambiente con il comando interno **`export`**:

```
export
```

Alcune variabili di ambiente (ad esempio, **`USER`**) non sono state aggiornate.

```
USER="studente"
```

Esercizio 3 (2 min.)

Diventate **`root`**, caricando in memoria il suo ambiente. Stampate le variabili di ambiente con il comando **`export`**. Confrontate l'output attuale con quello dell'esercizio precedente.

Notate qualcosa di strano?

Elevazione dei privilegi con **`su`**

Per diventare **`root`** ed importare l'intero ambiente si può eseguire il comando **`su`** con l'opzione **`--login`**, **`-l`** o **`-`**:

```
su -
```

Stampa ambiente con **`export`**

Si stampa l'ambiente con il comando interno **`export`**:

```
export
```

Il valore della variabile di ambiente **`USER`** ora è corretto:

```
USER="root"
```

→ Le variabili di ambiente sono state aggiornate ai valori giusti per l'utente **`root`**.

Esercizio 4 (1 min.)

Create un utente **`docente`**, se già non esiste.
Lanciate una shell da utente **`docente`**.

Creazione utente con **adduser**

Si crei l'utente **docente** (ad esempio con il comando adduser), se non esiste già:

```
adduser docente
```

Elevazione dei privilegi con **`su`**

Per elevare i privilegi al nuovo utente si esegue il comando **`su`** con l'opzione **`-`** e argomento pari al suo username:

```
su - docente
```

Esercizio 5 (1 min.)

Lanciate da utente **`prova`** un comando che mostri solo file e directory nascosti nella sua home directory.

Elevazione ed esecuzione con **`su`**

Si usa il comando **`su`** nello stesso modo dell'esercizio precedente, aggiungendo l'opzione **`-c`** per eseguire un comando specifico:

```
su -c COMANDO - prova
```

Il comando da eseguire è:

```
ls -ad .*
```

In definitiva, il comando richiesto è il seguente:

```
su -c "ls -ad .*" - prova
```

Esercizio 6 (2 min.)

Aprite un terminale e lanciate il comando **`env`**.
Aprite un altro terminale e lanciate il comando **`env`** come il vostro utente:

Notate delle differenze nell'output dei due comandi?

Esecuzione comando **`env`**

Si apre un nuovo terminale e si esegue il comando **`env`**:

```
env
```

Esecuzione comando **`env`** con **`sudo`**

Si apre un altro terminale e si esegue **`env`** con i privilegi dello stesso utente, usando **`sudo`**:

```
sudo -u studente env
```

Esercizio 7 (2 min.)

Eseguite come utente **`prova`** e gruppo primario **`disk`** il comando che legge il primo disco rigido SATA.

Cambio di privilegio con **sudo**

Si esegue **sudo** con le opzioni **-u** e **-g** per cambiare utente e gruppo:

-u prova: utente → **docente**
-g disk: gruppo primario → **disk**

In definitiva, il comando richiesto è il seguente:

```
sudo -u prova -g disk cat /dev/sda
```

Esercizio 8 (2 min.)

Modificate il file **`/etc/sudoers`** in modo tale da permettere al vostro utente l'esecuzione come **`root`** e senza password dei seguenti comandi:

```
slabtop
cat /dev/mem
```

Specifica dei privilegi

Il formato della specifica dei privilegi è:

<who> <where> = <as whom> <what>

In questo esercizio:

who	→	**studente**
where	→	**ALL** (tutti gli host)
as whom	→	**root**
what	→	**/usr/bin/slabtop**
		/bin/cat /dev/mem

Si scriva questa riga nel file **/etc/sudoers**:

```
studente ALL=(root:root) /usr/bin/slabtop,/bin/cat /dev/mem
```

Verifica della configurazione con **`sudo`**

Si provano i comandi con le credenziali di **`root`** tramite **`sudo`**:

```
sudo slabtop
sudo cat /dev/mem
```

Esercizio 9 (5 min.)

Il binario eseguibile **`top`** permette di monitorare i processi in maniera interattiva.
Copiate il file dell'eseguibile **`top`** nella vostra home directory, dandogli il nome **`newtop`**.
Cambiate utente creatore del file nel modo seguente:

utente creatore → **`root`**.

Impostate il bit SETUID e eseguite **`newtop`**.
Con quali diritti esegue **`newtop`**?

Copia locale di **top** con **cp**

In quale directory si trova l'eseguibile **top**?

```
which top
/usr/bin/top
```

Si copia **top** nella propria home, con nome **newtop**:

```
cp /usr/bin/top ~/newtop
```

Impostazione proprietario con **chown**

Si imposta il proprietario di **newtop** a **root** tramite il comando **chown** (che deve essere eseguito con le credenziali di **root**):

```
chown root ~/newtop
```

Impostazione SETUID con **chmod**

Si imposta il bit SETUID di **newtop** tramite il comando **chmod** (che deve essere eseguito con le credenziali di **root**):

```
chmod u+s ~/newtop
```

Esecuzione **`newtop`**

Si esegua il comando **`newtop`**:

```
~/newtop
```

Osservando l'output di newtop, si scopre che newtop esegue con i privilegi effettivi di **`root`**.

Esercizio 10 (1 min.)

Per quale motivo non siete riusciti ad eseguire il comando **`getcap`**?
Che cosa dovete fare per eseguire il comando **`getcap`**?

Stampa PATH con **`echo`**

Si stampi il valore della variabile di ambiente **`PATH`** (che contiene l'elenco delle directory scandite alla ricerca di comandi da eseguire):

```
echo $PATH
```

Analisi PATH

Nel PATH mancano le directory **`/usr/sbin`** e **`/sbin`**, in cui sono memorizzati i comandi per l'amministrazione del SO.
Tali comandi possono essere eseguiti da utente normale, ma offrono piena funzionalità quando sono eseguiti dall'utente **`root`**.

Locazione di **`getcap`**

Ipotesi: **`getcap`** si trova in **`/sbin`** oppure in **`/usr/sbin`**. Si verifica tale ipotesi elencando **`getcap`** nelle due directory **`/usr/sbin`** e **`/sbin`**:

```
ls /usr/sbin/getcap
ls /sbin/getcap
```

→ **`getcap`** si trova in **`/sbin`** e in **`/usr/sbin`**. L'utente normale può eseguire **`getcap`** scrivendo:

```
/sbin/getcap
/usr/sbin/getcap
```

Esercizio 11 (5 min.)

Usando il comando **`cp`**, copiate il comando **`ping`** nella vostra home directory, dandogli il nome **`newping`**.
Annullate le capability del file **`newping`**.
Eseguite **`newping 8.8.8.8`**. Funziona?
Assegnate le capability **`cap_net_raw`** agli insiemi permitted ed effective sul file **`newping`**.
Eseguite **`newping 8.8.8.8`**. Funziona?

Copia locale di **`ping`** con **`cp`**

In quale directory si trova l'eseguibile **`ping`**?

```
which ping
/usr/bin/ping
```

Si copia **`ping`** nella propria home, con nome **`newping`**:

```
cp /usr/bin/ping ~/newping
```

Verifica capability **`ping`** con **`getcap`**

Si stampano le capability di **`newping`** con il comando **`getcap`**:

```
/sbin/getcap ~/newping
```

L'output di **`getcap`** è vuoto; pertanto, la copia ha cancellato le capability.

E ci mancherebbe altro!

Esecuzione **`newping`**

Si esegue **`newping`**:

```
./newping 8.8.8.8
```

Si dovrebbe ottenere il messaggio di errore seguente:

```
ping: socket: Operazione non permessa
```

Una osservazione importante

ATTENZIONE! Non è detto che ciò si verifichi!
Le distribuzioni GNU/Linux più aggiornate permettono la creazione e l'invio di pacchetti di rete da utente normale.

Per maggiori dettagli (assolutamente non richiesti all'esame):

https://lwn.net/Articles/420800/

Ripristino capability con **setcap**

Si ripristinano le capability di **newping** con il comando **setcap** (eseguito con le credenziali di **root**):

```
setcap cap_net_raw+ep ~studente/newping
```

Si verifica l'impostazione delle capability (si possono usare anche le credenziali di **studente**):

```
/sbin/getcap $HOME/newping
```

Si dovrebbe ottenere la capability CAP_NET_RAW impostata sugli insiemi permitted ed effective:

```
cap_net_raw+ep
```

Verifica funzionamento **`newping`**

Si esegue **`newping`**:

```
./newping 8.8.8.8
```

Dopo la riassegnazione delle capability **`newping`** torna a funzionare correttamente.