Access Control

Lorenzo Colombi e Lucia Ferrari

Dipartimento di Ingegneria Università di Ferrara

28 febbraio 2025

Indice

1 Utenti e gruppi

2 File

3 Processi

Indice

1 Utenti e gruppi

2 File

3 Process

Lista degli utenti nel file /etc/passwd

```
$ cat /etc/passwd | grep fglmtt
fglmtt:x:15875:15875:Fogli Mattia:/home/fglmtt:/bin/bash
```

```
$ cat /etc/passwd | grep fglmtt
fglmtt:x:15875:15875:Fogli Mattia:/home/fglmtt:/bin/bash
/ata/passwd pap à l'unica pasta in qui vangana definiti gli utanti. Par avera una lis
```

/etc/passwd non è l'unico posto in cui vengono definiti gli utenti. Per avere una lista completa di tutti gli utenti conosciuti da un certo host

\$ getent passwd

```
$ cat /etc/passwd | grep fglmtt
fglmtt:x:15875:15875:Fogli Mattia:/home/fglmtt:/bin/bash
```

- username
- password
- user id
- group id
- comment field
- working directory (home)
- initial shell

La "x" indica che la password si trova nel file /etc/shadow. Altrimenti la password criptata sarebbe visibile.

CyberChallenge 2024/2025

```
$ cat /etc/passwd | grep fglmtt
fglmtt:x:15875:15875:Fogli Mattia:/home/fglmtt:/bin/bash
```

I sistemi operativi moderni (UNIX-like) hanno spostato le password cifrate in /etc/shadow per evitare che chiunque possa vedere l'hash delle password degli utenti. Nota che

```
$ ls -l /etc/passwd
-rw-r--r-- 1 root root 2250 Dec 19 21:44 /etc/passwd
```

```
$ cat /etc/passwd | grep fglmtt
fglmtt:x:15875:15875:Fogli Mattia:/home/fglmtt:/bin/bash
```

Per informazione su user/group id e gruppi senza dover consultare /etc/passwd

```
$ id
uid=15875(fglmtt) gid=15875 groups=15875
```

Testo

- Eseguire in modalità interattiva un container con Ubuntu
- Verificare il proprio user/group id
- Oreare due nuovi utenti alice e bob con relativa home directory
- Assegnare una password a ciascun utente
- Passare da un utente all'altro

Suggerimenti

\$ docker run -dit --name myFirstUbuntu ubuntu bash

- \$ docker run -dit --name myFirstUbuntu ubuntu bash
- ② \$ docker attach myFirstUbuntu ubuntu

- \$ docker run -dit --name myFirstUbuntu ubuntu bash
- \$ docker attach myFirstUbuntu ubuntu
- § id

- \$ docker run -dit --name myFirstUbuntu ubuntu bash
- \$ docker attach myFirstUbuntu ubuntu
- \$ id
- \$ useradd --create-home <username>

- \$ docker run -dit --name myFirstUbuntu ubuntu bash
- \$ docker attach myFirstUbuntu ubuntu
- 3 \$ id
- \$\text{useradd} --create-home <username>
- \$ passwd <username>

- \$ docker run -dit --name myFirstUbuntu ubuntu bash
- \$ docker attach myFirstUbuntu ubuntu
- 3 \$ id
- \$\text{useradd} --create-home <username>
- \$ passwd <username>
- \$ su <username>

```
$ cat /etc/passwd | grep -e alice -e bob
alice:x:1000:1000::/home/alice:/bin/sh
bob:x:1001:1001::/home/bob:/bin/sh
```

```
$ cat /etc/shadow | grep -e alice -e bob
alice:$y$j9T$yevkBsuUAIfxFHZ7oQF8G1$HJmqWKjivjzy8Q7/otlCF6ccuzd7tCPtLICyyYd9Rj3:19111:0:99999:7:::
bob:$y$j9T$3hGSsU9QYXrx.3IgsKN7S/$TZLP01mvSvdKM79UC7w6Bz4Mow4Ab.Je/xjLF7awDc2:19111:0:99999:7:::
```

12 / 25

```
$ cat /etc/group | grep -e alice -e bob
alice:x:1000:
bob:x:1001:
```

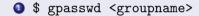
13 / 25

```
$ 1s -1 /home
drwxr-x--- 2 alice alice 4096 Apr 29 07:38 alice
drwxr-x--- 2 bob bob 4096 Apr 29 07:38 bob

$ su - alice
$ cd /home/bob
-sh: 2: cd: can't cd to /home/bob
```

Testo

- Impostare una password per il gruppo bob
- Impersonare l'utente alice
- Impostare bob come group id
- Verificare il proprio user/group id
- Entrare nella home directory dell'utente bob (/home/bob)



- \$ gpasswd <groupname>
- 2 \$ su <username>

- \$ gpasswd <groupname>
- 2 \$ su <username>
- \$ sg <groupname>

- \$ gpasswd <groupname>
- 2 \$ su <username>
- \$ sg <groupname>
- 4 \$ id

- \$ gpasswd <groupname>
- 2 \$ su <username>
- \$ sg <groupname>
- 4 \$ id
- \$ cd <path/to/dir>

Indice

Utenti e gruppi

2 File

3 Process

Testo

- Impersonare l'utente bob
- ② Creare la directory mydir in /home/bob/
- Oreare il file only-bob-can-delete-this.txt in /home/bob/mydir
- Togliere tutti i permessi al gruppo per only-bob-can-delete-this.txt
- Impersonare l'utente alice
- Impostare bob come group id
- alice può cancellare /home/bob/mydir/only-bob-can-delete-this.txt?
- se si, limitare i permessi del gruppo bob di conseguenza

Suggerimenti

① \$ su - <username>

19 / 25

- ① \$ su <username>
- ② \$ mkdir <path/to/dir>

- ① \$ su <username>
- ② \$ mkdir <path/to/dir>
- \$ touch <path/to/file>

- \$ su <username>
- ② \$ mkdir <path/to/dir>
- \$ touch <path/to/file>
- \$ chmod g-rwx <path/to/file>

- \$ su <username>
- ② \$ mkdir <path/to/dir>
- \$ touch <path/to/file>
- \$ chmod g-rwx <path/to/file>
- \$ su <username>

- ① \$ su <username>
- ② \$ mkdir <path/to/dir>
- \$ touch <path/to/file>
- \$ chmod g-rwx <path/to/file>
- \$ su <username>
- \$ sg <group>
- \$ rm <path/to/file>

- \$ su <username>
- ② \$ mkdir <path/to/dir>
- \$ touch <path/to/file>
- \$ chmod g-rwx <path/to/file>
- \$ su <username>
- \$ sg <group>
- \$ rm <path/to/file>
- O Per cancellare un file c'è bisogno dei permessi di scrittura ed esecuzione per la directory che contiene quel file, ma non c'è bisogno dei permessi di lettura e scrittura per il file stesso

- \$ su <username>
- ② \$ mkdir <path/to/dir>
- \$ touch <path/to/file>
- \$ chmod g-rwx <path/to/file>
- \$ su <username>
- \$ sg <group>
- \$ rm <path/to/file>
- O Per cancellare un file c'è bisogno dei permessi di scrittura ed esecuzione per la directory che contiene quel file, ma non c'è bisogno dei permessi di lettura e scrittura per il file stesso
- 9 \$ chmod g-wx <path/to/dir>

Testo

- Impersonare l'utente bob
- Verificare i permessi di /var/tmp
- Creare il file bob.log in /var/tmp
- Impersonare l'utente alice
- Sometime of the state of the
- Perchè alice non può cancellare /var/tmp/bob.log nonostante other abbia sia i permessi di scrittura che di esecuzione per /var/tmp?

Suggerimenti

\$ su - <username>

CyberChallenge 2024/2025

- \$ su <username>
- ② \$ ls -l <path/to/dir>

- 1 \$ su <username>
- ② \$ ls -l <path/to/dir>
- \$ touch <path/to/file>

- 1 \$ su <username>
- ② \$ ls -l <path/to/dir>
- \$ touch <path/to/file>
- 4 \$ su <username>

- 1 \$ su <username>
- \$ ls -l <path/to/dir>
- \$ touch <path/to/file>
- \$ su <username>
- \$ rm <path/to/file>

- 1 \$ su <username>
- 4 \$ ls -l <path/to/dir>
- \$ touch <path/to/file>
- \$ su <username>
- \$ rm <path/to/file>
- Perchè è impostato lo sticky bit. Quando lo sticky bit è impostato per una directory i file in quella directory possono essere rimossi o rinominati solo se lo user ha i permessi di scrittura e o possiede il file o possiede la directory o è superuser

Indice

Utenti e gruppi

2 File

3 Processi

CyberChallenge 2024/2025

Testo

- Impersonare l'utente alice
- ② Creare il file /home/alice/i-am-good.sh come segue

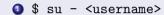
```
#!/bin/sh
/usr/bin/env echo "I'am good"
```

Oreare il file /home/alice/echo come segue

```
#!/bin/sh
/usr/bin/echo "I'm malicious!"
```

Fare in modo che /home/alice/i-am-good.sh esegua /home/alice/echo anziché la versione "vera" di echo

Suggerimenti



ATTENZIONE

Potrebbe essere necessario installare Vim o Nano!

Suggerimenti

- 1 \$ su <username>
- vim/nano AND \$ chmod +x <filename>

ATTENZIONE

Potrebbe essere necessario installare Vim o Nano!

Suggerimenti

- \$ su <username>
- vim/nano AND \$ chmod +x <filename>
- oum/nano AND \$ chmod +x <filename>

ATTENZIONE

Potrebbe essere necessario installare Vim o Nano!

24 / 25

Suggerimenti

- ① \$ su <username>
- vim/nano AND \$ chmod +x <filename>
- oum/nano AND \$ chmod +x <filename>
- \$ \$ export PATH=<path/to/malicious-echo>:\$PATH

ATTENZIONE

Potrebbe essere necessario installare Vim o Nano!

Esercizio 6 + challenge sulla piattaforma

Testo

Le ultime 3 challenge sono gentilmente prese in prestito dalla Ca' Foscari: https://secgroup.dais.unive.it/teaching/system-security/lab-unix-linux-access-control/