



Laboration – Användare och säkerhet

OBS det kan förekomma små skillnader vad gäller sökvägar samt befintliga kommandon mellan olika distributioner. T.ex. mellan CentOS och Ubuntu,

Material: För att genomföra laborationen behöver man ha tillgång till en dator (vm) med Linux installerat. Windows Subsystem for Linux går att använda också. För vissa övningar kan lokal administratörsbehörighet behövas. I labben utgår det från att man är inloggad med en användare som heter **sysadmin**

Mål: I denna laboration kommer du att utföra följande uppgifter:

- Lär dig skillnaden mellan superanvändarkonton och vanliga användarkonton.
- Visa användarkontoinformation.

Kör kommandon som administratör

I denna uppgift lär du dig två sätt att köra kommandon som administrativ användare. Detta är ofta nödvändigt för att göra förändringar som påverkar hela systemet.

För att komma åt root-användarkontot används normalt kommandona **su** eller **sudo**.

su-kommandot används vanligtvis för att byta användare och starta ett nytt skal som en annan användare, där standarden är root-användaren. **su**-kommandot används ofta när en *serie kommandon* behöver utföras som root-användare.

sudo-kommandot används vanligtvis för att utföra ett *enda kommando* som root-användare genom att föregå kommandot med **sudo**. **sudo**-kommandot måste konfigureras av root-användaren innan en vanlig användare kan använda det. Som standard är **sudo**-kommandot i kraft i 15 minuter på Ubuntu-system där root-kontot *inte är* aktiverat som standard. Root-åtkomst kan aktiverats på den virtuella maskinen med kommandot **sudo passwd root**, för att sätta ett lösenord på root-kontot och därmed aktivera det, vilket gör att **su**-kommandot kan användas.

När kommandot **su** utförs utan argument öppnar det ett nytt skal som root-användare. Det råder viss förvirring kring vad initialerna "su" står för (substitute user, switch user och superuser refereras ofta till), men det viktigaste att notera är att det tillåter en administratör att ändra sin inloggning till vilken användare som helst på systemet.

När detta kommando matas in utan användarnamn antar systemet root-användaren. De flesta system visar den aktuella användaren i kommandoprompten, men det kan vara hjälpsamt att bekräfta vilken användare som är inloggad med **id**-kommandot som visas nedan. Detta steg säkerställer att de ändringar som krävs för specifika användare (såsom tjänstekonton) utförs korrekt.

Byt användare till root-användaren och ange root-lösenordet när du blir tillfrågad:

```
su -
```

```
sysadmin@localhost:~$ su -  
Password:
```



Bekräfta den nya användaridentiteten med kommandot `id`:

```
id
```

```
root@localhost:~# id
uid=0(root) gid=0(root) groups=0(root)
```

Efter att ha använt skalet som startades av `su`-kommandot för att utföra nödvändiga administrativa uppgifter, återgå till ditt ursprungliga skal (och ursprungliga användarkonto) genom att använda `exit`-kommandot. Bekräfta användaridentitetsändringen med kommandot `id`.

```
exit
```

```
id
```

```
root@localhost:~# exit
logout
sysadmin@localhost:~$ id
uid=1001(sysadmin) gid=1001(sysadmin) groups=1001(sysadmin),
4(adm),27(sudo)
```

Att avsluta skalet är viktigt för att undvika att utföra kommandon som root som kan skada systemet.

`sudo`-kommandot fungerar på system som som standard inte tillåter root-åtkomst. Det är att föredra för de flesta administrativa uppgifter eftersom root-åtkomst automatiskt går ut utan att man behöver avsluta det. Skriv först ett kommando som sysadmin som icke-privilegerad användare.

```
head /etc/shadow
```

Lägg märke till felmeddelandet som `head`-kommandot visar. Detta beror på att sysadmin-användaren inte har rätt att se denna fil. Root-användaren kan dock visa denna fil.

Skriv samma kommando med `sudo`. Använd ditt lösenord när du blir tillfrågad:

```
sudo head /etc/shadow
```

```
sysadmin@localhost:~$ sudo head /etc/shadow
[sudo] password for sysadmin:
root:$6$4Yga95H9$8HbxqsMEIBTZ0YoyWkYwQdK1SJyS8.:16464:0:99999:7:::
daemon:*:16463:0:99999:7:::
bin:*:16463:0:99999:7:::
sys:*:16463:0:99999:7:::
sync:*:16463:0:99999:7:::
games:*:16463:0:99999:7:::
man:*:16463:0:99999:7:::
lp:*:16463:0:99999:7:::
mail:*:16463:0:99999:7:::
news:*:16463:0:99999:7:::
```

Systemet kommer att be om den nuvarande användarens lösenord, *inte root-lösenordet*. Om den nuvarande användaren är en del av sudo-gruppen kommer kommandot att exekveras.



Som standard på många Ubuntu-system kommer `sudo`-kommandon som matas in efter det första `sudo`-kommandot att utföras som root utan att bli ombedda om lösenord under de följande 15 minuterna. Andra system kan ha andra timeouts.

Användarkonton

I denna uppgift kommer du att lära dig om användarkonton och filer och kommandon som visar användarkontoinformation.

Användar- och systemkonton definieras i filerna `/etc/passwd` och `/etc/shadow`. Visa de första tio raderna från `/etc/passwd`-filen. Medan `passwd`-filen innehåller allmän information om en användare såsom användarnamn, UID, GID, hemkatalog och inloggningsskal, har den moderna skuggfilen ytterligare detaljer inklusive krypterat lösenord och lösenordspolicy:

```
head /etc/passwd
```

```
sysadmin@localhost:~$ head /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
```

Observera att denna fil innehåller en kolonavgränsad databas över alla användar- och systemkonton som finns tillgängliga på detta system.

Användarkonton tilldelas användare för att ge dem tillgång till operativsystemet.

Systemadministratörskontot du använde för att logga in i systemet är ett typiskt användarkonto.

Systemkonton används av operativsystemet eller tjänster som kör processer på det för att utföra bakgrundsfunktioner. Dessa konton behöver ofta tillgång till hårdvaru- eller systemfiler som normalt bara skulle vara tillgängliga för root-användaren. Standardbehörigheterna för dessa konton ger normalt tillgång till endast de känsliga områden som behövs istället för bred åtkomst som ett root- eller administratörskonto, vilket begränsar skador som ett komprometterat tjänstekonto kan orsaka. Systemkonton används aldrig direkt av vanliga användare.

Använd `grep`-kommandot för att se posten för ditt sysadmin-konto:

```
grep sysadmin /etc/passwd
```

```
sysadmin@localhost:~$ grep sysadmin /etc/passwd
sysadmin:x:1001:1001:System Admin,,,:/home/sysadmin:/bin/bash
```

Genom att använda `grep`-kommandot innehåller utdata endast kontoinformationen för det användarnamnet.



Lösenord

Filen `/etc/shadow` innehåller information om användarnas lösenord. I denna övning kommer du att använda flera kommandon för att visa datan i denna fil.

Försök att se de första raderna i `/etc/shadow-filen`, en fil som innehåller användarnas krypterade lösenord och information om hur de åldras:

```
head -3 /etc/shadow
```

```
sysadmin@localhost:~$ head -3 /etc/shadow
head: cannot open `/etc/shadow' for reading: Permission denied
```

Lägg märke till felmeddelandet som `head`-kommandot visar. Detta beror på att `sysadmin`-användaren inte har rätt att se denna fil. Root-användaren kan dock visa denna fil.

Observera att behörigheterna i `/etc/shadow`-filen anger att endast medlemmar i `shadow`-gruppen har behörighet att se filen:

```
ls -l /etc/shadow
```

```
sysadmin@localhost:~$ ls -l /etc/shadow
-rw-r----- 1 root shadow 968 Feb  8 2021 /etc/shadow
```

Tänk på att root-användaren kan se vilken fil som helst. Detta beror på att root-kontot har särskilda privilegier som överskrider vanliga filbehörigheter.

Använd kommandot `sudo` för att visa de första raderna i `/etc/shadow`-filen. Ange lösenordet till `sysadmin`-användaren, när du blir tillfrågad.

```
sudo head -3 /etc/shadow
```

```
sysadmin@localhost:~$ sudo head -3 /etc/shadow
[sudo] password for sysadmin:
root:$6$HHJ0w8Vo$qB1f7KzPjrjBr1rkZuFC60oRbX4Rq0:18666:0:99999:7:::
daemon:*:18645:0:99999:7:::
bin:*:18645:0:99999:7:::
```

Viktigt

Lösenordet du angav var för ditt `sysadmin`-konto, inte root-kontot. När `sudo` har konfigurerats för ditt konto behöver du inte känna till root-lösenordet för att köra `sudo`-kommandon som root-användare.

Ett annat sätt att hämta kontoinformationen för en användare är att köra följande kommando: `getent passwd username`. Kommandot `getent` har fördelen jämfört med `grep`-kommandot eftersom det också kan komma åt användarkonton som inte är lokalt definierade. Med andra ord kan kommandot `getent` hämta användarinformation för användare som kan vara definierade på nätverkskatalogservrar såsom LDAP, NIS, Windows Domain eller Active Directory Domain-servrar.

Använd `getent`-kommandot för att hämta informationen om `sysadmin`:

```
getent passwd sysadmin
```



```
sysadmin@localhost:~$ getent passwd sysadmin
sysadmin:x:1001:1001:System Admin,,,:/home/sysadmin:/bin/bash
```

Notera

I det här fallet har vi inga nätverkskonton, så utdata som visas är precis som att titta på `/etc/passwd`-filen.

Den kolonavgränsade filen `/etc/passwd` har följande fält:

```
name:password:UID:GID:Comment:directory:shell
```

En uppdelning av dessa områden:

Name

```
sysadmin:x:1001:1001:System Administrator,,,:/home/sysadmin:/bin/bash
```

Password Placeholder

```
sysadmin:x:1001:1001:System Administrator,,,:/home/sysadmin:/bin/bash
```

User ID

```
sysadmin:x:1001:1001:System Administrator,,,:/home/sysadmin:/bin/bash
```

Primary Group ID

```
sysadmin:x:1001:1001:System Administrator,,,:/home/sysadmin:/bin/bash
```

Comment

```
sysadmin:x:1001:1001:System Administrator,,,:/home/sysadmin:/bin/bash
```

Home Directory

```
sysadmin:x:1001:1001:System Administrator,,,:/home/sysadmin:/bin/bash
```

Shell

```
sysadmin:x:1001:1001:System Administrator,,,:/home/sysadmin:/bin/bash
```

Du kan se dokumentationen för fälten i `/etc/passwd`-filen med följande kommando:

```
man 5 passwd
```



```
PASSWD(5) File Formats and Conversions PASSWD(5)

NAME
passwd - the password file

DESCRIPTION
/etc/passwd contains one line for each user account, with seven fields
delimited by colons (":"). These fields are:

o login name
o optional encrypted password
o numerical user ID
o numerical group ID
```

Viktigt

Kom ihåg att när du tittar på en man-sida, tryck **Enter** för att gå framåt rad för rad, **Mellanslag** sida för sida och **q** för att avsluta.

Du kan se kontoinformation för ditt konto, eller ett angivet användarkonto, med kommandot **id**:

```
id
id root
```

```
sysadmin@localhost:~$ id
uid=1001(sysadmin) gid=1001(sysadmin) groups=1001(sysadmin),
4(adm), 27(sudo)
sysadmin@localhost:~$ id root
uid=0(root) gid=0(root) groups=0(root)
```

Utdata från kommandona visar följande:

Användaridentitet:

```
uid=1001(sysadmin) gid=1001(sysadmin) groups=1001(sysadmin),4(adm),27(sudo)
```

Primär gruppidentitet:

```
uid=1001(sysadmin) gid=1001(sysadmin) groups=1001(sysadmin),4(adm),27(sudo)
```

Grupper du tillhör:

```
uid=1001(sysadmin) gid=1001(sysadmin) groups=1001(sysadmin),4(adm),27(sudo)
```

I det här fallet tillhör ditt användarkonto bara tre grupper.

Notera

Filen **/etc/group**, tillsammans med **/etc/passwd**, avgör dina gruppmedlemskap. Din standardprimärgrupp bestäms genom att matcha din GID som finns i **/etc/passwd** med GID som definierats för en grupp i **/etc/group**. Alla sekundära gruppmedlemskap definieras i **/etc/group**-filen.



Formatet för poster i `/etc/group`-filen för varje rad är:

```
group_name:password:GID:user_list
```

Vem är inloggad

I denna uppgift kommer du att utföra några kommandon för att se vem som är inloggad i systemet.

Använd kommandot `who` för att få den aktuella listan över användare i systemet:

```
who
```

```
sysadmin@localhost:~$ who
sysadmin pts/0      Feb 23 19:48
sysadmin@localhost:~$
```

Utdata från `who`-kommandot har fyra kolumner:

Username

```
sysadmin console   Apr 11 14:32
```

Denna kolumn anger namnet på användaren som är inloggad.

Terminal

```
sysadmin console   Apr 11 14:32
```

Denna kolumn visar vilket terminalfönster användaren arbetar i.

Date

```
sysadmin console   Apr 11 14:32
```

Denna kolumn anger när användaren loggade in.

Host

Även om det inte finns någon utdata för den fjärde kolumnen i detta fall, kan det vara namnet eller IP-adressen till en lokal eller fjärrvärd.

Använd kommandot `w` för att få en mer detaljerad bild av de användare som för närvarande är på ditt system:

```
w
```

```
sysadmin@localhost:~$ w
15:17:08 up 6 days, 15 min,  1 user,load average: 0.39, 0.34,0.37
USER      TTY      FROM          LOGIN@      IDLE        JCPU   PCPU   WHAT
sysadmin  pts/0    -             14:32       4.00s      0.16s  0.00s  w
sysadmin@localhost:~$
```

Utdata från `w`-kommandot visar en sammanfattning av hur länge systemet har varit igång, hur många användare som är inloggade och genomsnittliga systembelastningsciffror för de senaste 1, 5 och 15 minuterna.



Det visas också en post för varje användare med deras inloggningsnamn, tty-namn (terminalnamn), värd, inloggningstid, inaktiva tid, JCPU (CPU-tid som används av bakgrundsjobb), PCPU (CPU-tid som används av den aktuella processen) och vad som körs på den aktuella kommandoraden.

Visa logghändelser

`last` kommandot läser hela inloggningshistoriken från `/var/log/wtmp`-filen och visar alla inloggningar och omstartsposter som standard.

Använd `last` kommandot för att se filen `/var/log/wtmp` som håller en logg över alla användare som har loggat in och ut ur systemet.

```
last
```

```
sysadmin@localhost:~$ last
sysadmin pts/0          Fri Feb 23 19:48   still logged in

wtmp begins Fri Feb 23 19:48:19 2024
sysadmin@localhost:~$
```