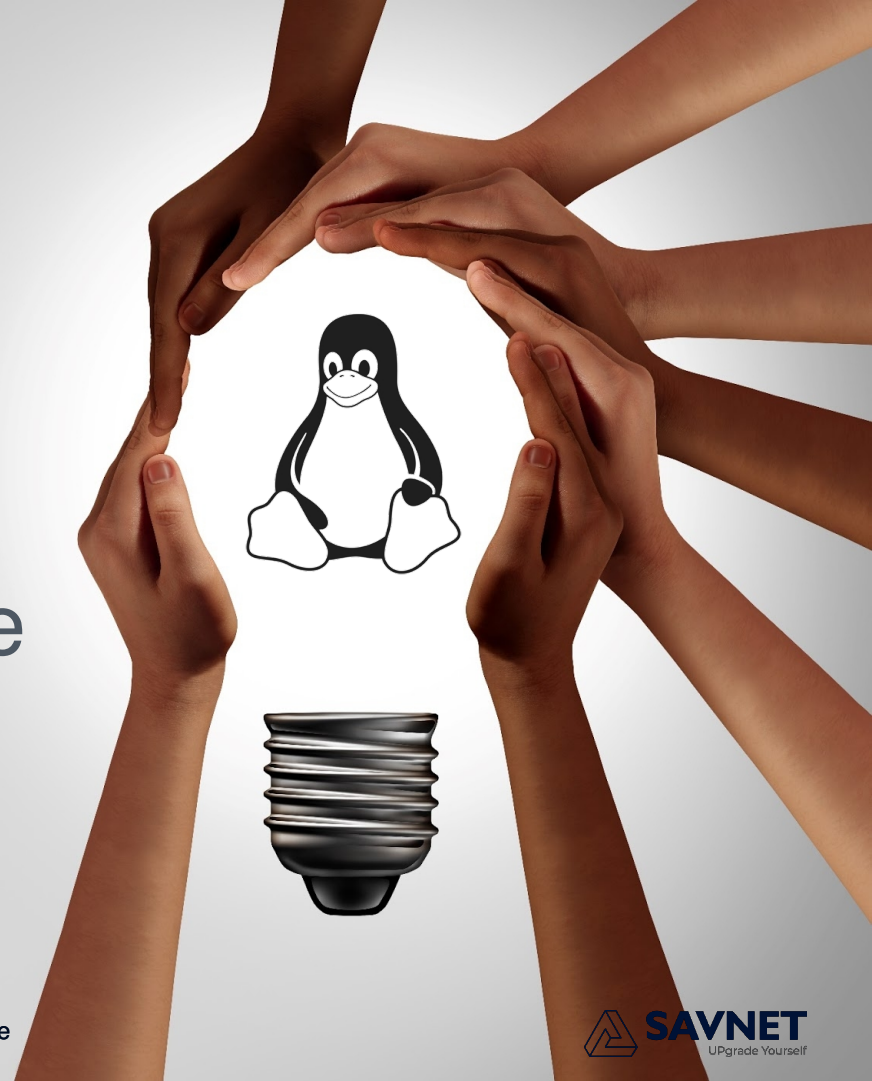
SAVNET
UPgrade Yourself

Linux

Administrare și Securitate



SAVNET
UPgrade Yourself

Ce vom învăța în acest curs?

- Gestionarea utilizatorilor şi grupurilor
- Permisiuni, autentificare, parolare, sudo.
- Principii de securitate: actualizări, patch-uri, zone de risc, protejarea fişierelor critice.
- Aplicaţii practice: configurarea unui sistem Linux securizat într-o infrastructură de telecomunicaţii

Capitolul 6: Securitatea Sistemului şi Utilizatorilor

Gestionarea utilizatorilor şi grupurilor

Identificarea Conturilor de Utilizator

Utilizatori și Permisiuni

Scopul conturilor de utilizator:

Conturile de utilizator sunt concepute pentru a oferi securitate pe un sistem de operare Linux.

Securitate prin permisiuni:

• Conturile de utilizator permit sau interzic accesul unei persoane la fișiere și directoare folosind permisiunile de fișiere.

• Conturile de utilizator aparțin și grupurilor.

Acest modul acoperă:

• Comenzi pentru vizualizarea informațiilor despre conturi de utilizator și grupuri

• Cum să comutați între conturi de utilizator diferite

Conturi Administrative

Root și Privilegii Administrative:

Unele comenzi necesită privilegii administrative sau root.

Riscuri cu utilizarea root:

- Tot va rula ca root (procese de fundal, executabile)
- Poți uita că ești logat ca root
- Poți rula accidental sarcini non-admin ca root

Recomandare:

Se recomandă utilizarea comenzilor sudo sau su pentru a executa comenzi ca root, în loc să te loghezi direct ca root.

Schimbarea Utilizatorului - su

su - Switch User
Comanda su permite să rulezi un shell ca un utilizator diferit.

```
su [options] [username]
```

Opțiuni importante:
- su - → Login shell complet (cu setările noului utilizator)
- su - username → Comută la utilizatorul specificat
- su - → Fără username - comută la root

Autentificare:
După Enter, trebuie să introduci parola utilizatorului root.

```
student@localhost:~$ su -
Password:
root@localhost:~# exit
logout
```

Utilizați comanda exit pentru a reveni la shell-ul inițial (contul utilizatorului).

Executarea Comenzilor Privilegiate - sudo

Comanda sudo permite utilizatorilor să execute comenzi ca alt utilizator (de obicei root).

```
student@localhost:~$ sudo head /etc/shadow
[sudo] password for student:
```

- Poate fi folosit în distribuții care nu permit login ca root
- Solicită parola PROPRIULUI utilizator, nu a root
- Înregistrare în log pentru responsabilitate
- Reduce riscul asociat cu utilizarea root

Exemplu:

```
sudo apt update
sudo systemctl restart apache2
```

Verificare acces sudo:

```
sudo -l   # Arată ce comenzi poți rula cu sudo
```

Conturi de Utilizator - /etc/passwd

Fișierul /etc/passwd

Directorul /etc conține fișiere cu date despre conturile de utilizatori și grupuri definite pe sistem.
Fișierul /etc/passwd definește informații despre conturile de utilizator.
Fiecare linie conține informații despre un singur utilizator.

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

Câmpurile (separate prin două puncte):

- 1. Nume utilizator
- 2. Placeholder parolă (x)
- 3. User ID (UID)
- 4. Primary Group ID (GID)
- 5. Comentariu (nume complet)
- 6. Director home
- 7. Shell

Verificare utilizator daca este definit in sistem:

```
grep username /etc/passwd
```

Parole - /etc/shadow

Fișierul /etc/shadow - conține informații despre parolele utilizatorilor (necesită root pentru citire).

```
admin:$6$c75ekQWF$.GpiZpFnIXLzkALjDpZXmjxZcIll14OvL2mFSIfnc1aU2cQ/
221QL5AX5RjKXpXPJRQ0uVN35TY3/..c7v0.n0:16874:5:30:7:60:15050::
```

Câmpurile:

- 1. Username: Numele contului (corespunde cu /etc/passwd)
- 2. Password: Parola criptată
- 3. Last Change: Ultima dată când parola a fost schimbată
- 4. Min: Număr minim de zile între schimbări de parolă
- 5. Max: Număr maxim de zile când parola este validă
- 6. Warn: Zile înainte de expirare când sistemul avertizează
- 7. Inactive: Perioadă de grație pentru schimbare parolă
- 8. Expire: Zile când contul expiră (de la 1 ianuarie 1970)
- 9. Reserved: Rezervat pentru utilizare viitoare

Conturi de Sistem

Tipuri de conturi pe Linux:

- Conturi obișnuite (regular): UID >- 1000
- Cont root special: UID - 0 (acces complet)
- Conturi de sistem: UID 1-999 (pentru servicii)

Caracteristici conturi sistem:

Concepute pentru servicii care rulează pe sistem (Apache, MySQL, etc.)

- Home directory: De obicei nu au sau au /nonexistent
- Shell: Folosesc /usr/sbin/nologin sau /bin/false
- Password: Folosesc * (nu se poate loga direct)

Exemplu:

```
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin   (/etc/passwd)
www-data:*:19411:0:99999:7:::   (/etc/shadow)
```

Conturi de Grup - /etc/group

Grupuri în Linux:

Fiecare utilizator poate fi membru al unuia sau mai multor grupuri.
Fișierul /etc/passwd definește grupul PRIMAR pentru un utilizator.
Fișierul /etc/group definește apartenența la grupuri SUPLIMENTARE (secundare).

```
sudo:x:27:student,alice,ionescu
```

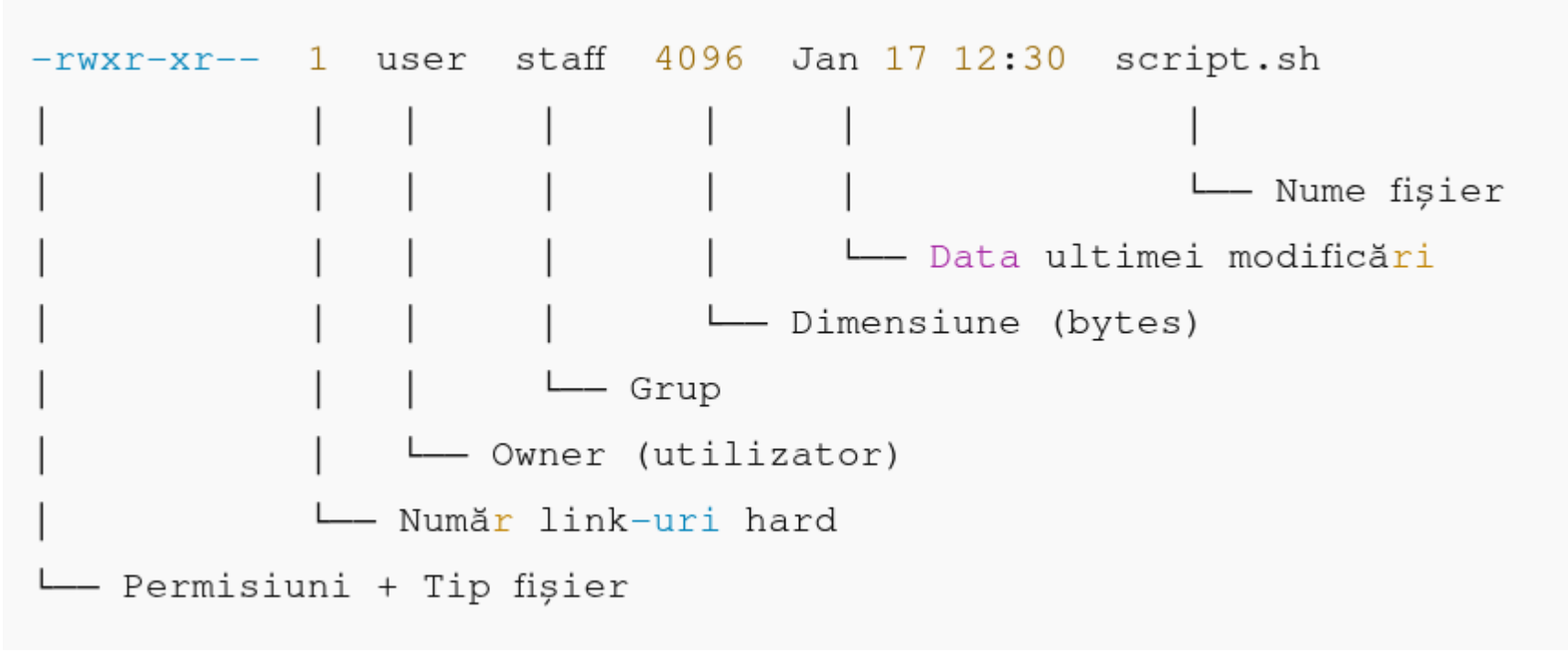
Câmpurile din /etc/group:

- 1. Group Name: Numele grupului
- 2. Password Holder: x (parola nu e stocată aici)
- 3. GID: ID-ul unic al grupului
- 4. User List: Lista membrilor grupului (separați prin virgulă)

Vizualizarea Informațiilor despre Utilizatori

Recapitulare

Pentru a afișa metadatele importante, folosiți comanda ls -l / ls -ld:



Comanda id - Informații Utilizator

id - Identificare utilizator și grupuri

Comanda id afișează informații despre utilizator și grupurile sale.

Sintaxa:

```
id                  # Info despre utilizatorul curent
id username         # Info despre un utilizator specific
id -G               # Doar ID-urile grupurilor secundare
id -Gn              # Doar numele grupurilor secundare
```

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

Interpretare:

- uid=1001(student) → ID utilizator și nume
- gid=1001(student) → Grupul primar
- groups=... → Toate grupurile (primar + secundare)

Comanda who - Utilizatori Logați

who - Cine este logat si sesiunile active

Comanda who listează utilizatorii care sunt logați în prezent, precum și unde și când s-au logat.

Sintaxa:

```
who             # Lista utilizatori logați
who -H          # Cu header (antet)
who -b          # Data ultimului boot
```

```
student@localhost:~$ who
root        tty2         2013-10-11 10:00
student     tty1         2013-10-11 09:58 (:0)
student     pts/0        2013-10-11 09:59 (:0.0)
```

Câmpurile:

- Username: Utilizatorul logat
- Terminal: tty - login local, pts - pseudo terminal (SSH)
- Date: Când s-a logat
- Location: :0 - grafic local, IP - remote

Comanda w - Informații Detaliate

w - Who și What

Comanda w oferă informații mai detaliate despre utilizatorii curenți pe sistem. Include și informații despre starea sistemului (uptime, load average).

Sintaxa:

```
w               # Toate informațiile
w username      # Pentru un utilizator specific
```

```
student@localhost:~$ w
 10:44:03 up 50 min,  4 users,  load average: 0.78, 0.44, 0.19
USER        TTY      FROM             LOGIN@   IDLE       JCPU        PCPU    WHAT
root        tty2     -                10:00    43:44  0.01s       0.01s   -bash
student     tty1     :0               09:58    50:02  5.68s             0.16s   pam: gdm-password
student     pts/0    :0.0             09:59    0.00s   0.14s      0.13s   ssh 192.168.1.2
student     pts/1    example.com 10:00    0.00s             0.03s       0.01s   w
```

- Linie 1: Ora curentă, uptime, utilizatori logați, load average
- IDLE: Timp de la ultima activitate / WHAT: Comanda curentă executată

Comanda last - Istoric Login-uri

last - Istoric autentificări

Comanda last citește fișierul /var/log/wtmp pentru a afișa toate înregistrările de login. Arată sesiunile de login anterioare, precum și informații despre login-ul curent.

Sintaxa:

```
last                # Tot istoricul
last username       # Istoric pentru un utilizator
last -n 10          # Ultimele 10 intrări
last reboot         # Istoricul reboot-urilor
```

```
student@localhost:~$ last

student console Tue Sep 14 05:31   still logged in

student console                    Tue Sep 14 05:31 - 05:31  (00:00)

wtmp begins Tue Sep 14 05:31:57 2025
```

Informații afișate:

- Username, terminal, IP/hostname
- Data și ora login-ului
- Durata sesiunii
- Status: still logged in sau logged out

Rezumat - Securitate Utilizatori

Comenzi esențiale:

```
su -                # Comută la root (login shell)
sudo command        # Execută comandă ca root
id                  # Info utilizator curent
who                 # Cine e logat
w                   # Detalii utilizatori + activitate
last                # Istoric login-uri
```

Fișiere importante:

- /etc/passwd → Info conturi utilizator
- /etc/shadow → Parole criptate (root only)
- /etc/group → Apartenență la grupuri

Securitate:

- Folosește sudo în loc de su când e posibil
- Monitorizează login-urile cu who, w, last

Crearea Utilizatorilor și Grupurilor

Introducere

Informațiile despre conturile de utilizator și autentificare sunt stocate în fișierele /etc/passwd și /etc/shadow.

Adăugare utilizatori/grupuri:

- Folosirea directă a acestor fișiere pentru adăugare este posibilă, dar NU este recomandată.
- Utilizarea comenzilor este abordarea mai potrivită.

User Private Group (UPG):

Când creezi un nou utilizator, unele distribuții creează automat un User Private Group (UPG) - un grup privat cu același nume ca utilizatorul.

Notă: Înainte să începi să creezi utilizatori, ar trebui să planifici cum vei folosi grupurile.

Crearea Grupurilor

De ce grupuri?

Grupurile oferă o modalitate pentru utilizatori să partajeze fișiere.

Verificare configurare:

- Comanda grep poate fi folosită pentru a verifica configurarea și modificările.
- Comanda getent poate fi folosită pentru a afișa grupuri locale și bazate pe rețea.

Exemplu verificare:

```
grep groupname /etc/group
getent group groupname
```

```
root@localhost:~# grep root /etc/group
root:x:0:
root@localhost:~# getent group root
root:x:0:
```

Crearea unui Grup - groupadd

Comandă de bază:

Execută comanda groupadd ca utilizator root pentru a crea un grup nou.

```
sudo groupadd groupname
```

Specificare GID (Group ID):

Pentru a specifica un ID de grup (GID), folosește opțiunea -g:

```
root@localhost:~# groupadd -g 506 research
```

Comportament implicit:

Dacă opțiunea -g nu este folosită, groupadd va atribui automat un GID cu o valoare mai mare decât ultimul adăugat în fișierul /etc/group.

```
root@localhost:~# grep research /etc/group
research:x:506:
root@localhost:~# groupadd development
root@localhost:~# grep development /etc/group
development:x:507:
```

Considerații privind GID

Reamintire:

În unele distribuții, când un ID de utilizator este creat, un UPG (User Private Group) este creat de asemenea.

Recomandare:

Evită crearea de GID-uri în aceeași gamă ca UID-urile care vor fi create în viitor.

GID-uri rezervate:

- GID-uri sub 1000 sunt rezervate pentru utilizare sistem.
- Pentru a depăși acest lucru și a atribui un GID <1000, folosește opțiunea -r:

```
sudo groupadd -r systemgroup
```

Considerații Denumire Grupuri

Nume portabile:

Un nume de grup portabil funcționează corect cu alte sisteme.

Ghid pentru crearea unui nume de grup portabil:

- Pentru primul caracter: folosește underscore (_) sau alfanumeric mic (a-z)
- După primul caracter: alfanumerice, cratimă sau underscore
- Folosirea a mai mult de 16 caractere poate fi problematică
- Ultimul caracter NU ar trebui să fie o cratimă (-)

Exemple:

- Bine: developers, web_users, db-admin
- Gresit: 1users, very-long-group-name-here, users-

Modificarea unui Grup - groupmod

Comandă groupmod:

Poate fi folosită pentru a schimba numele grupului sau GID-ul.

Schimbare nume (-n):

```
root@localhost:~# groupmod -n clerks sales
```

- Schimbarea numelui grupului NU va cauza probleme cu accesarea fișierelor.

Schimbare GID (-g):

```
root@localhost:~# groupmod -g 10003 clerks
```

- Schimbarea GID-ului va cauza ca fișierele să nu mai fie asociate cu acel grup!

Căutare fișiere orfane:

```
find / -nogroup 2>/dev/null
```

Ștergerea unui Grup - groupdel

Comandă groupdel:

```
sudo groupdel groupname
```

```
root@localhost:~# groupdel clerks
```

Atenție:

- Fișierele din grupul șters vor deveni orfane (fără grup asociat).
- Doar grupurile suplimentare pot fi șterse.
- Nu poți șterge grupul primar al unui utilizator!

Verificare înainte de ștergere:

```
getent group groupname  # Verifică dacă există
grep groupname /etc/group
```

Configurarea Utilizatorilor

Creare utilizatori:

În timpul instalării, este obișnuit să creezi un utilizator normal cu permisiuni root folosind sudo.

Funcționează bine când computerul este folosit de un singur utilizator.

Multiple utilizatori:

Pentru computere cu mai mulți utilizatori, crearea de conturi separate este ideală.

Configurare Utilizatori - useradd -D

Înainte de a crea utilizatori:

Verifică valorile implicite folosind comanda useradd

Vizualizare setări implicite:

`useradd -D`

Opțiunea -D permite vizualizarea sau schimbarea unor valori implicite.

Aceste setări pot fi modificate și prin manipularea fișierului /etc/default/useradd.

```
root@localhost:~# useradd -D
GROUP=100
HOME=/home
INACTIVE=-1
EXPIRE=
SHELL=/bin/bash
SKEL=/etc/skel
CREATE_MAIL_SPOOL=yes
```

Valori importante:

- GROUP - Grupul primar implicit pentru un utilizator nou
- HOME - Directorul de bază sub care va fi creat directorul home al utilizatorului
- INACTIVE - Zile după expirarea parolei când contul este dezactivat
- EXPIRE - Data de expirare (implicit nu este setată)
- SHELL - Shell-ul implicit când utilizatorul se loghează
- SKEL - Directorul skeleton (conținutul copiat în home-ul noului utilizator)

Configurare Utilizatori

Ce înseamnă valorile comenzii useradd -D:

GROUP - grupul primar implicit pentru un utilizator nou. Această setare afectează câmpul ID-ului grupului primar din fișierul /etc/passwd.

```
GROUP=100
```

```
ionescu:x:600:600:ionescu:/home/ionescu:/bin/bash
```

HOME - directorul de bază implicit sub care va fi creat noul director home al utilizatorului. Această setare afectează câmpul director home din fișierul /etc/passwd.

```
HOME=/home
```

```
ionescu:x:600:600:ionescu:/home/ionescu:/bin/bash
```

Configurare Utilizatori

INACTIVE - Această valoare reprezintă numărul de zile după expirarea parolei în care contul este dezactivat. Această setare afectează câmpul inactive din fișierul /etc/passwd.

```
INACTIVE=-1
```

```
ionescu:x:600:600:ionescu:/home/ionescu:/bin/bash
```

EXPIRED - În mod implicit, nu există nicio valoare setată pentru data de expirare. Această setare afectează câmpul expire din fișierul /etc/passwd.

```
EXPIRE=
```

```
ionescu:pw:15020:5:30:7:60:15050:
```

Configurare Utilizatori

SHELL - Shell-ul implicit pentru un utilizator atunci când se autentifică în sistem. Această setare afectează câmpul shell din fișierul /etc/passwd.

```
SHELL=/bin/bash
```

```
ionescu:x:600:600:ionescu:/home/ionescu:/bin/bash
```

SKELETON DIRECTORY - Conținutul acestui director este copiat în directorul home al noului utilizator. Această setare afectează câmpul expire din fișierul /etc/passwd.

```
SKEL=/etc/skel
```

CREATE MAIL SPOOL - Fișierul în care este plasat emailul primit.

```
CREATE_MAIL_SPOOL=yes
```

Configurare Utilizatori - /etc/login.defs

Fișierul /etc/login.defs:

Stabilește parametrii impliciți pentru comenzi precum useradd, login, passwd și alte utilitare legate de administrarea utilizatorilor.

- Definește reguli despre:
- Politica parolelor (ex: durata minimă/maximă a parolei)
- Politica expirării parolei și contului
- UID și GID implicite pentru utilizatori și grupuri noi
- Limite pentru numărul maxim/minim de utilizatori
- Căile implicite pentru directoarele home, shell-uri etc.

Configurare Utilizatori - /etc/login.defs

Fișierul /etc/login.defs:

Conține valori care vor fi aplicate implicit utilizatorilor noi creați cu useradd.

Vizualizare fără comentarii:

```
grep -v '^#' /etc/login.defs | grep -v '^$'
```

Valori importante:

- PASS_MAX_DAYS - Număr maxim de zile pentru aceeași parolă
- PASS_MIN_DAYS - Timp minim pentru păstrarea unei parole
- PASS_MIN_LEN - Lungime minimă parolă
- UID_MIN/UID_MAX - Interval UID-uri pentru utilizatori obișnuiți
- GID_MIN/GID_MAX - Interval GID-uri pentru grupuri
- CREATE_HOME - Dacă se creează director home automat
- UMASK - Permisiuni implicite pentru director home

```
~$ grep -v '^#' /etc/login.defs | grep -v '^$'
MAIL_DIR        /var/mail
FAILLOG_ENAB            yes
LOG_UNKFAIL_ENAB        no
LOG_OK_LOGINS           no
SYSLOG_SU_ENAB          yes
SYSLOG_SG_ENAB          yes
FTMP_FILE       /var/log/btmp
SU_NAME         su
HUSHLOGIN_FILE  .hushlogin
ENV_SUPATH      PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
ENV_PATH        PATH=/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/games
TTYGROUP        tty
TTYPERM         0600
ERASECHAR       0177
KILLCHAR        025
UMASK           022
HOME_MODE       0750
PASS_MAX_DAYS   99999
PASS_MIN_DAYS   0
PASS_WARN_AGE   7
UID_MIN                  1000
UID_MAX                 60000
GID_MIN                  1000
GID_MAX                 60000
LOGIN_RETRIES           5
LOGIN_TIMEOUT           60
CHFN_RESTRICT           rwh
DEFAULT_HOME    yes
USERGROUPS_ENAB yes
ENCRYPT_METHOD SHA512
```

Puncte importante pentru crearea conturilor

Informații necesare pentru crearea unui cont:

- Numele contului (obligatoriu)
- UID (opțional, dar util pentru planificare)
- Grupul primar
- Grupurile suplimentare
- Directorul home
- the skeleton directory – stuctura (sablonul) directorului home
- Shell-ul de folosit

Ghid pentru nume utilizator portabil:

- Primul caracter: underscore (_) sau alfanumeric mic (a-z)
- Caractere următoare: alfanumerice, cratimă sau underscore
- Max 16 caractere (pentru compatibilitate)
- Ultimul caracter NU ar trebui să fie cratimă (-)

Crearea unui Utilizator - useradd

Comandă de bază:

```
sudo useradd student
```

Cu opțiuni complete:

```
sudo useradd -u 1500 -g developers -G sudo,docker -s /bin/bash -m -c "student cont" student
```

Opțiuni importante:

- -u UID → Specifică UID
- -g GROUP → Grupul primar
- -G GROUPS → Grupuri suplimentare (separate prin virgulă)
- -s SHELL → Shell-ul utilizatorului
- -m → Creează director home
- -c COMMENT → Comentariu (nume complet)

Ce se întâmplă automat:

- Info adăugate în /etc/passwd și /etc/shadow
- Info grupuri în /etc/group și /etc/gshadow
- Director /home/student creat

Setarea Parolelor

Factori pentru alegerea unei parole:

- Lungime: Minimă specificată în /etc/login.defs
- Compoziție: Combinație de caractere alfabetice, numerice și simbolice
- Durată de viață: Timpul maxim de utilizare ar trebui limitat

Modalități de setare parolă:

- 1. Utilizatorul execută passwd:

```
passwd  # Schimbă propria parolă
```

- 2. Admin execută passwd cu username:

```
sudo passwd student  # Admin setează parola lui student
```

- 3. Unelte grafice (GUI)

Note:

- Utilizatorii trebuie să urmeze ghidurile pentru parole
- Root poate ignora avertismentele

```
root@localhost:~# passwd student
Enter new UNIX password:
BAD PASSWORD: it is WAY to shortc
BAD PASSWORD: is too simple
Retype new UNIX password:
```

Modificarea unui Utilizator - usermod

Verificare înainte de modificare:

```
who     # Verifică dacă utilizatorul e logat
w
last username
```

Comandă usermod:

Oferă multiple opțiuni pentru modificarea utilizatorilor.

Opțiuni comune:

```
sudo usermod -d /home/old_home_new -m old_home    # Schimbă home
sudo usermod -l newname oldname                   # Schimbă username
sudo usermod -u 2000 student                         # Schimbă UID
sudo usermod -g newgroup student                     # Schimbă grup primar
sudo usermod -aG sudo student                        # Adaugă la grup suplimentar
sudo usermod -s /bin/zsh student                     # Schimbă shell
sudo usermod -L student                              # Lock cont (disable)
sudo usermod -U student                              # Unlock cont
```

Atenție:

• Modificările majore (UID, username) pot cauza probleme cu fișierele existente!

Ștergerea unui Utilizator - userdel

Decizie importantă:

Când ștergi un cont de utilizator, trebuie să decizi dacă ștergi și directorul home.

Ștergere fără director home:

```
root@localhost:~# userdel student
```

- Directorul /home/student rămâne intact
- Fișierele utilizatorului devin orfane (UID fără nume)

Ștergere cu director home:

```
root@localhost:~# userdel -r student
```

- Șterge utilizatorul ȘI directorul home /home/student
- Șterge și fișierul mail /var/spool/mail/student

Verificare după ștergere:

```
grep student /etc/passwd  # Nu ar trebui să returneze nimic
ls /home/student          # Verifică dacă a fost șters
```

Rezumat - Comenzi Esențiale

Grupuri:

```
groupadd [-g GID] groupname     # Creează grup
groupmod -n newname oldname     # Redenumește
groupmod -g newGID groupname    # Schimbă GID
groupdel groupname              # Șterge grup
```

Utilizatori:

```
useradd -D                      # Vezi setări implicite
useradd [opțiuni] username      # Creează utilizator
passwd username                 # Setează parolă
usermod [opțiuni] username      # Modifică utilizator
userdel [-r] username           # Șterge utilizator
```

Fișiere importante:

- /etc/passwd, /etc/shadow, /etc/group, /etc/gshadow
- /etc/default/useradd, /etc/login.defs

Opțiuni utile useradd:

- -u UID, -g grup_primar, -G grupuri_suplimentare, -s shell, -m (creează home)

Principii de securitate

Directoare și Fișiere Speciale / Permisiuni Speciale

Permisiuni Setuid

Ce este Setuid?

Această permisiune este setată pe utilitățile de sistem astfel încât să poată fi rulate de utilizatori normali, dar executate cu permisiunile root.
Oferă acces la fișiere de sistem la care un utilizator normal nu are acces.

Exemplu:

Utilizatorul student încearcă să vizualizeze conținutul fișierului /etc/shadow:

```
student@localhost:~$ cat /etc/shadow
cat: /etc/shadow: Permission denied
```

Cum poate un utilizator obișnuit să modifice fișierul /etc/shadow când execută comanda passwd?

• Comanda passwd are permisiunea specială setuid:

```
student@localhost:~$ ls -l /usr/bin/passwd
-rwsr-xr-x 1 root root 31768 Jan 28 2010 /usr/bin/passwd
```

Permisiuni Setuid - Reprezentare

Reprezentarea permisiunii setuid:

Permisiunea setuid este reprezentată de un caracter s în permisiunile de executare ale utilizatorului.

```
-rwsr-xr-x    # setuid și execute pentru user (s mic)
-rwSr-xr-x    # doar setuid, fără execute (S mare)
```

Diferența între s și S:

- s mic (lowercase s) - setuid și user execute sunt ambele setate
- S mare (uppercase S) - doar setuid este setată, nu și user execute

Permisiuni Setuid - Setare

Setarea permisiunilor speciale:

Permisiunile speciale pot fi setate cu comanda chmod, folosind fie metoda simbolică, fie metoda octală.

Pentru a adăuga permisiunea setuid simbolic:

```
chmod u+s file
```

Pentru a adăuga permisiunea setuid numeric:

Adaugă 4000 la permisiunile existente ale fișierului (presupunem că fișierul de mai jos avea inițial 775):

```
chmod 4775 file
```

Pentru a elimina permisiunea setuid simbolic:

```
chmod u-s file
```

Pentru a elimina permisiunea setuid numeric:

Scade 4000 din permisiunile existente ale fișierului:

```
chmod 0775 file
```

Permisiuni Setgid pe un Fișier

Permisiunea setgid este similară cu setuid, dar pentru permisiunile de grup.
Există două tipuri de permisiuni setgid: setgid pe fișiere și setgid pe directoare

Setgid pe un fișier:
Permite utilizatorului să ruleze un fișier binar executabil oferind acces temporar de grup.
Reprezentat de s în permisiunile de grup:

```
-rwxr-sr-x
```

Exemplu - comanda /usr/bin/wall:

```
-rwxr-sr-x. 1 root tty 10996 Jul 19  2011 /usr/bin/wall
```

Acest fișier executabil este deținut de grupul tty. Când un utilizator execută această comandă, va putea accesa fișiere care sunt deținute de grupul tty.

Permisiuni Setgid pe un Director

Ce face Setgid pe un director?

Setgid pe un director face ca fișierele create în director să fie deținute automat de grupul care deține directorul.

Reamintire:

În mod normal, fișierele noi sunt deținute de grupul primar al utilizatorului care a creat fișierul.

Moștenire:

Dacă un director este setgid, orice directoare create în acel director vor moșteni permisiunea setgid.

Vizualizare permisiuni director:

```
ls -ld directoryname
```

Două modalități de reprezentare a permisiunii setgid:

s mic (lowercase s):

`drwxrwsrwx` - Înseamnă că atât setgid cât și permisiunea de executare pentru grup sunt setate.

S mare (uppercase S):

`DrwxrwSr-x` - Înseamnă că doar setgid este setată și nu permisiunea de executare pentru grup

Permisiuni Setgid pe un Director - Setare

Pentru a adăuga permisiunea setgid pe un director simbolic:

```
chmod g+s directory
```

Pentru a adăuga permisiunea setgid numeric:

Adaugă 2000 la permisiunile existente ale directorului (presupunem că directorul de mai jos avea inițial 775):

```
chmod 2775 directory
```

Pentru a elimina permisiunea setgid simbolic:

```
chmod g-s directory
```

Pentru a elimina permisiunea setgid numeric:

Scade 2000 din permisiunile existente ale directorului:

```
chmod 0775 directory
```

Permisiunea Sticky Bit

Ce este Sticky Bit?

Permisiunea sticky bit permite ca fișierele dintr-un director să fie partajate, dar doar proprietarul fișierului sau root pot șterge.
Fără această permisiune, utilizatorii ar putea șterge orice fișiere din acest director, inclusiv cele care aparțin altor utilizatori.

Reprezentare:

Permisiunea sticky bit este afișată ca un t în partea de executare a permisiunilor pentru others:

```
drwxrwxrwt
```

Diferența între t și T:

- t mic (lowercase t) - atât sticky bit cât și execute sunt setate
- T mare (uppercase T) - doar sticky bit este setat

Permisiunea Sticky Bit - Setare

Pentru a adăuga permisiunea sticky bit simbolic:

```
chmod o+t directory
```

Pentru a adăuga permisiunea sticky bit numeric:

Adaugă 1000 la permisiunile existente ale directorului (presupunem că directorul de mai jos avea inițial 775):

```
chmod 1775 directory
```

Pentru a elimina permisiunea sticky bit simbolic:

```
chmod o-t directory
```

Pentru a elimina permisiunea sticky bit numeric:

Scade 1000 din permisiunile existente ale directorului:

```
chmod 0775 directory
```

Link-uri

Hard Links și Symbolic Links

Problema:

Există fișiere care se află adânc în sistemul de fișiere și au pathname-uri lungi.

• Unele fișiere nu pot fi copiate într-un alt director deoarece alți utilizatori actualizează fișierul.

Soluția:

Poți crea un fișier care va fi legat (linked) la cel care este "îngropat adânc" și plasa link-ul în directorul tău.

Două tipuri de link-uri:

• Hard Links - pointează la același inode (fiecare fisier, director are un indentificator unic in sistemul de fisiere si informatii relevante despre el)

• Symbolic Links (Soft Links) - pointează la un alt fișier prin pathname

Despre inode (index node):

Un inode reține informatiile: tipul fișierului (fișier normal, director, link etc.), drepturile de acces (permisiuni), UID-ul și GID-ul proprietarului, dimensiunea fișierului, data creării, modificării și accesării, numărul de link-uri către fișier, locația fizică pe disc (blocurile unde este stocat conținutul)

Crearea Hard Links

Fiecare fișier pe o partiție are un număr de identificare unic numit inode.

Vizualizare număr inode:

```
ls -i filename
```

Ce sunt Hard Links?

Hard links sunt două nume de fișiere care pointează la același inode.

Exemplu - fișierele passwd și mypasswd:

```
Nume Fișier          Număr Inode
passwd               123
mypasswd             123
```

Poți accesa datele fișierului folosind oricare dintre cele două nume deoarece au același număr inode.

Crearea Hard Links - Comandă

Vizualizare link count:

Poți vizualiza numărul de link count al unui fișier executând comanda ls -li:

```
student@localhost:~$ ls -li file.*
278772 -rw-rw-r--. 1 student student 5 Oct 25 15:42 file.original
```

Pentru a crea un hard link:

Folosește comanda ln cu două argumente:

`ln source_file link_name`

```
student@localhost:~$ ln file.original file.hard
student@localhost:~$ ls -li file.*
278772 -rw-rw-r--. 2 student student 5 Oct 25 15:53 file.hard
278772 -rw-rw-r--. 2 student student 5 Oct 25 15:53 file.original
```

Crearea unui Symbolic (soft) Link

Ce este un Symbolic Link?

Un symbolic link, numit și soft link, este un fișier care pointează la un alt fișier.

```
student@localhost:~$ ls -l /etc/grub.conf
lrwxrwxrwx. 1 root root 22 Feb 15  2011 /etc/grub.conf -> ../boot/grub/grub.conf
```

În exemplul de mai sus, fișierul /etc/grub.conf "pointează la" fișierul ../boot/grub/grub.conf

Pentru a crea un symbolic link:

Folosește opțiunea -s cu comanda ln:

`ln -s target_file link_name`

```
student@localhost:~$  ln -s /etc/passwd mypasswd
student@localhost:~$  ls -l mypasswd
lrwxrwxrwx. 1 student student 11 Oct 31 13:17 mypasswd -> /etc/passwd
```

Compararea Hard și Symbolic Links

Deși au același rezultat, fiecare produce rezultate diferite și au avantaje și dezavantaje.

Avantajul Hard Link:

Dacă există multiple fișiere cu același hard link, ștergerea oricăruia dintre aceste fișiere nu va rezulta în ștergerea conținutului actual al fișierului. Cu un soft link, dacă fișierul original este eliminat, atunci orice fișiere legate de el vor eșua.

Avantajele Soft Link:

• Soft link-urile sunt mai ușor de văzut.
• Soft link-urile pot lega la orice fișier deoarece folosesc un pathname. Hard link-urile nu pot fi create pentru a traversa sisteme de fișiere deoarece fiecare sistem de fișiere are un set unic de inode-uri.
• Soft link-urile se pot lega la un director.

Rezumat - Permisiuni Speciale și Link-uri

Permisiuni Speciale:

- Setuid (4000): Execută cu permisiuni proprietar → chmod u+s sau chmod 4xxx
- Setgid (2000): File → grup temporar; Directory → moștenire grup → chmod g+s sau chmod 2xxx
- Sticky Bit (1000): Doar owner/root pot șterge → chmod o+t sau chmod 1xxx

Link-uri:

```
ln source hardlink          # Hard link (același inode)
ln -s target symlink        # Symbolic link (pathname)
```

Verificare:

```
ls -li file     # Vezi inode și link count
ls -l file      # Vezi symbolic links (l și ->)
```

Hard vs Soft:

- Hard: Rezistent la ștergere, nu traversează filesystems, nu poate lega directoare
- Soft: Ușor de văzut, poate traversa filesystems, poate lega directoare, vulnerabil la ștergerea originalului

Principii de securitate în Linux

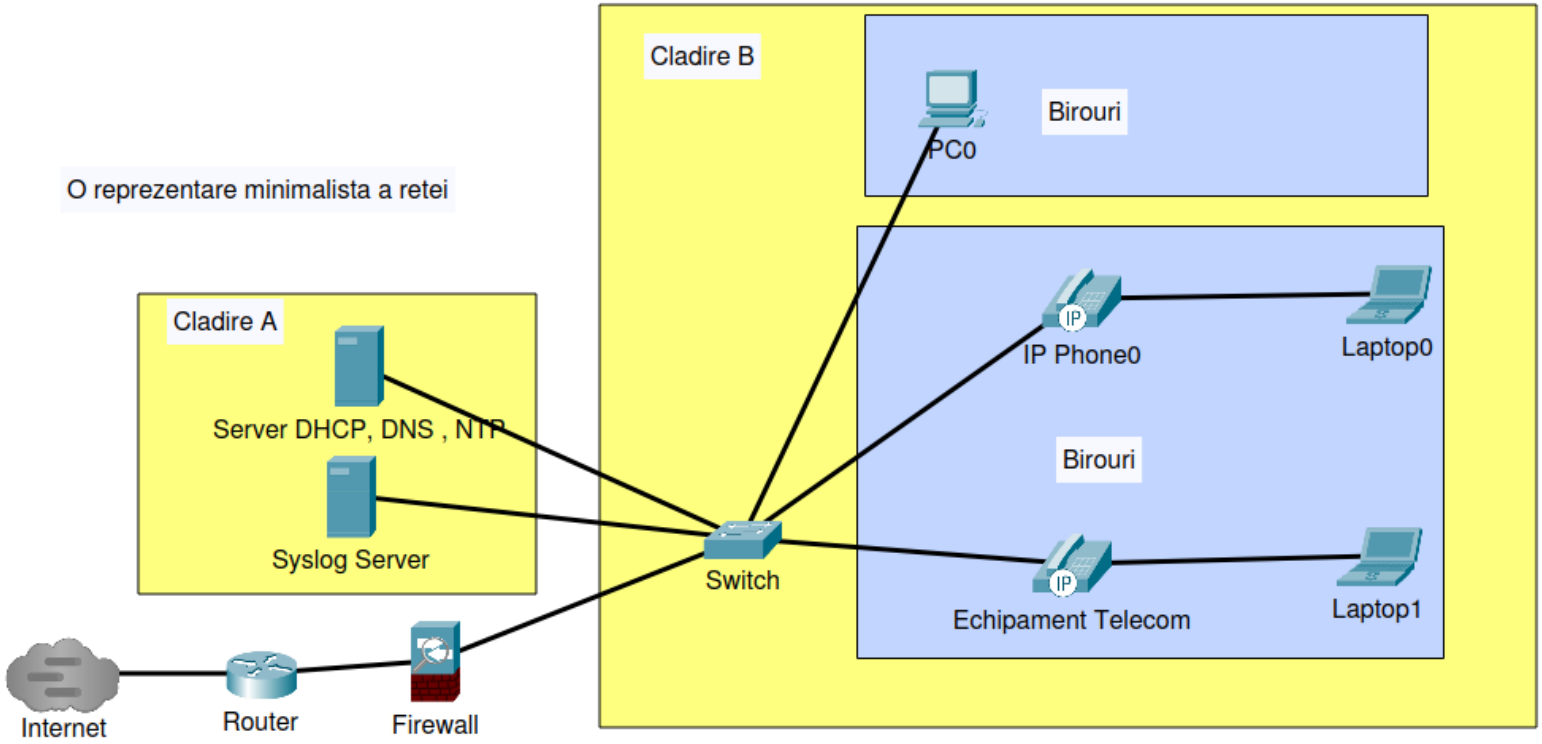
Actualizări și minimizarea suprafeței de atac

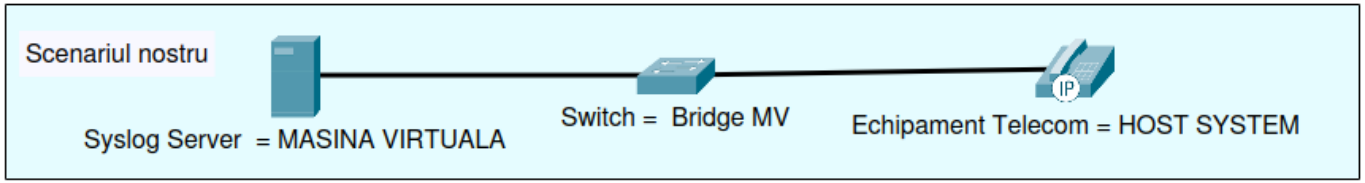
- Menține sistemul actualizat (apt / dnf update)
- Aplică patch-uri de securitate imediat
- Activează actualizări automate
- Identifică și limitează serviciile expuse in retea (e.g. SSH, FTP, web)
- Dezactivează protocoalele nefolosite (e.g. IPv6)
- Dezactivează serviciile inutile (e.g. cups)
- Configurează firewall (e.g. UFW / firewalld)
- Monitorizează logurile sistemului

Protejarea fișierelor critice

- Restricționează accesul la directoare esențiale (/etc, /bin, /usr, /root)
- Setează permisiuni corecte (chmod / chown)
- Utilizează sudo în loc de root
- Dezactivează autentificarea root prin SSH
- Activează SELinux sau AppArmor
- Monitorizează integritatea fișierelor (AIDE / Tripwire)

Aplicaţie practica
Configurarea unui sistem Linux securizat într-o infrastructură de telecomunicaţii

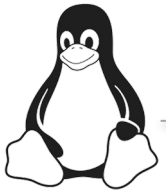

O reprezentare minimalista a retei
Cladire B
Birouri
PC0
Cladire A
Server DHCP, DNS , NTP
Syslog Server
IP Phone0
Laptop0
Birouri
Switch
Echipament Telecom
Laptop1
Internet
Router
Firewall


Scenariul nostru
Syslog Server = MASINA VIRTUALA
Switch = Bridge MV
Echipament Telecom = HOST SYSTEM

Q&A

Activități pentru acasă

Ce urmează?



Învățare constantă = dezvoltare profesională
Succes!


SAVNET
UPgrade Yourself