UNIUNEA EUROPEANĂ

GUVERNUL ROMÂNIEI

Instrumente Structurale
2007-2013

Platformă de e-learning și curriculă e-content pentru învățământul superior tehnic

Utilizarea Sistemelor de Operare

25. Securitate în Linux

Securitatea sistemului de fișiere

- Aspecte importante
  - directorul HOME al fiecărui utilizator
    - drepturi depline
    - utilizatorul poate sau nu permite accesul altor utilizatori
  - doar utilizatorul privilegiat are acces la anumite intrări
    - fișiere de configurare, programe executabile
- Cum se implementează securitatea fișierelor?
  - drepturi de acces (sau liste de acces)
    - pentru fiecare intrare se precizează drepturile utilizatorilor
    - formă redusă pe Unix (user, group, others)

umask

- Restricția drepturilor de creare a intrărilor în sistemul de fișiere
- Valori tipice pentru umask: 022, 027, 077
- Drepturi de creare implicite
  - 666 pentru fișier
  - 777 pentru director
- Drepturi de creare efective
  - ȘI logic între permisiunile implicite și masca inversată

umask (2)

- director: implicit 777
- umask: 077 → (777 & ~077) 700 (rwx --- ---)

```
razvan@anaconda:~/junk$ umask
0027
razvan@anaconda:~/junk$ mkdir uso7_dir1
razvan@anaconda:~/junk$ ls -ld uso7_dir1
drwxr-x---  2 razvan razvan 4096 Nov 10 17:29 uso7_dir1
razvan@anaconda:~/junk$ umask 077
razvan@anaconda:~/junk$ mkdir uso7_dir2
razvan@anaconda:~/junk$ ls -ld uso7_dir2
drwx------  2 razvan razvan 4096 Nov 10 17:29 uso7_dir2
```

- fișier: implicit 666
- umask: 027 → (666 & ~027) 640 (rw- r-- ---)

```
razvan@anaconda:~/junk$ umask
0022
razvan@anaconda:~/junk$ touch uso7_test1
razvan@anaconda:~/junk$ ls -l uso7_test1
-rw-r--r--  1 razvan razvan 0 Nov 10 17:28 uso7_test1
razvan@anaconda:~/junk$ umask 027
razvan@anaconda:~/junk$ touch uso7_test2
razvan@anaconda:~/junk$ ls -l uso7_test2
-rw-r-----  1 razvan razvan 0 Nov 10 17:28 uso7_test2
```

setuid

- Anumite aplicații neceistă acces la resurse privilegiate
  - ping, traceroute, passwd, su
- Soluție
  - utilizarea unui bit special denumit setuid (suid)
  - execuția unui program cu drepturile deținătorului (root)

```
razvan@anaconda:~/junk$ ls -l /bin/ping
-rwsr-xr-x  1 root root 30764 Dec 23  2003 /bin/ping
```

- Activarea bitului de setuid
  - o valoare în octal suplimentară la chmod

```
razvan@anaconda:~/junk$ ls -l a.out
-rwxr-xr-x  1 razvan razvan 13564 Jul  9 20:49 a.out
razvan@anaconda:~/junk$ chmod 4755 a.out
razvan@anaconda:~/junk$ ls -l a.out
-rwsr-xr-x  1 razvan razvan 13564 Jul  9 20:49 a.out
```

- Potențial risc de securitate
  - un utilizator poate obține drepturi privilegiate

Parole în Unix

- La început parolele se păstrau criptat în /etc/passwd
- Fisierul /etc/passwd conține și alte informații
  - numele utilizatorilor
  - directorul home
  - shell-ul folosit
- Multe programe au nevoie de informațiile de mai sus
  - fișierul /etc/passwd este citibil de toți utilizatorii

```
razvan@anaconda:~/junk$ ls -l /etc/passwd
-rw-r--r--  1 root root 2147 Nov  4 15:35 /etc/passwd
```

- Parola criptată este vizibilă
  - potențial risc de spargere prin încercări

Parole în Unix (cont.)

- Fișierul /etc/shadow
  - accesibil numai de root
  - intrare în /etc/passwd

```
razvan@anaconda:~/junk$ cat /etc/passwd | grep guest
guest:x:1001:1001:Guest,EF
 303,,,Test:/home/guest:/bin/bash
```

  - intrare în /etc/shadow

```
razvan@anaconda:~/junk$ cat /etc/shadow | grep guest
cat: /etc/shadow: Permission denied
anaconda:/home/razvan/junk# cat /etc/shadow | grep guest
guest:$1$jv4hP2au$BSrUDS0J7LhJv8PrCFltU/:13124:0:99999:7:
 ::
```

- Parola ar putea fi spartă prin încercări de login repetate
  - timeout între încercările de autentificare

Contul de root/Administrator

- Controlul absolut al sistemului
  - obținerea contului de superuser înseamnă spargerea sistemului
- Trebuie folosit _numai_ atunci când este nevoie
  - pentru operații obișnuite, folosiți contul _neprivilegiat_
  - o bună parte din atacurile pe Windows se bazează pe faptul că utilizatorii folosesc numai contul de Administrator
- sudo
  - permite unui utilizator obișnuit (dar de încredere) rularea unui set restrâns de comenzi cu privilegii de root
  - privilege separation

Evitarea accesului la contul de root

- Principiul “least privilege” (privilege separation)
  - folosește numai atât cât este nevoie
  - bitul setuid încalcă acest privilegiu
- Linux
  - folosirea sudo pentru rularea unui set restrâns de comenzi
    - fișierul de configurare /etc/sudoers
  - folosirea de capabilități
    - unele programe pot avea acces numai la o parte din privilegiile root
- Windows
  - folosirea Power Users
    - utilizatori de sistem care au acces la câteva din privilegiile Administrator