Controlul Accesului

Partea I

Capabilităţi în Linux

Resurse necesare:

- mașină virtuală ce rulează o distribuție de Linux (Ubuntu 14.04, Lubuntu 14.04)
- pachetul `libcap2`

```
sudo apt-get update
sudo apt-get install libcap2
```

Observație:

Comenzile din cadrul acestui laborator vor fi rulate doar pe mașina virtuală creată, având nevoie de acces de tip `root`.

Introducere

In orice sistem de operare există o serie de operații ce pot fi realizate doar de către utilizatorul root (configurare interfață rețea, back-up fișiere, etc.). Acestea corespund programelor Set-UID (fișiere ce au ca proprietar utilizatorul root și au bitul Set-UID setat). Astfel, pe parcursul executării acestor operații, utilizatorul normal devine temporar root, ceea ce reprezintă o vulnerabilitate de securitate a sistemului.

Intr-un sistem bazat pe capabilități, la executarea unui program, procesul corespunzător este inițializat cu o listă de *capabilități*. In momentul în care procesul respectiv încearcă să acceseze o resursă, sistemul de operare verifică dacă procesul are capabilitățile necesare și decide acordarea/interzicerea accesului la resursa solicitată.

Acordarea de capabilități în Linux

În Linux, capabilitățile sunt disponibile prin intermediul pachetului `libcap`. Comenzi disponibile:

- `setcap` - acordare de capabilități unui fișier;
- `getcap` - afișarea capabilităților asociate unui fișier;
- `getpcaps` - afișarea capabilităților asociate unui proces.

Asignarea de capabilități unui executabil se realizează prin comanda `setcap`:

```
setcap lista_capabilitati=flaguri_capabilitati program
```

- `lista_capabilitati`: lista de nume de capabilități, separate prin virgulă;
- `flaguri_capabilitati`: `p` (permitted), `e` (effective), `i` (inheritable).

Ștergerea capabilităților asociate unui program:

```
setcap -r program
```

Observație:

- comanda `setcap` trebuie rulată cu drepturi de `root`.

Obținerea listei de capabilități asociate unui program:

```
getcap program
```

Pentru mai multe detalii, precum și lista capabilităților existente în Linux:

- `man capabilities`
- `less /usr/include/linux/capability.h`