Universitatea Tehnică a Moldovei

Facultatea *Calculatoare, Informatică și Microelectronică*

Specialitatea *Tehnologii Informaționale*

Raport

la lucrarea de laborator nr. 3

Tema:*"Controlul accesului"*

Disciplina: "Tehnici de securitate informationala"

A efectuat:	Student grupa TI-231 FR	Apareci Aurica
A verificat:	Asistent universitar	Alexandru Tocan

Chișinău 2025

Cuprins

1. Cadru teoretic

Tema lucrării: Controlul accesului

Obiectivele lucrării:

- explicarea conceptelor de bază ale controlului accesului la sistemele de operare;
- familiarizarea cu permisiunile și drepturile utilizatorilor;
- configurarea permisiunilor la fișiere și directoare;
- gestionarea utilizatorilor și grupurilor.

Resurse necesare:

- CSE-LAB VM
- Windows 11 Pro/Entreprise VM

Sarcini:

- Configurare AAA in Windows
- Configurare AAA in Linux

2. Repere teoretice

Controlul accesului în sistemele informatice este esențial pentru securitatea și integritatea acestora, având un impact semnificativ asupra protejării datelor, prevenirii accesului neautorizat și asigurării confidențialității informațiilor. Conceptul AAA (Autentificare, Autorizare, Auditare) reprezintă un concept fundamental în controlul accesului la sistemele informatice:

● Autentificare: se verifică identitatea utilizatorilor și se confirmă că aceștia sunt cine pretind a fi (de exemplu, prin parole, biometrie, chei de autentificare etc).

● Autorizare: se determină ce resurse și privilegii are un utilizator autentificat și care sunt acțiunile pe care le poate efectua (de exemplu, acces la anumite fișiere, funcționalități, servicii etc.).

● Auditare: se monitorizează și se înregistrează activitățile utilizatorilor, precum accesul la resurse, modificările efectuate și alte acțiuni relevante. Auditarea ajută la detectarea și investigarea activităților suspecte sau neautorizate.

Modele de control al accesului

DAC (Discretionary Access Control): Proprietarul resursei stabilește cine are tip de acces.

MAC (Mandatory Access Control): Accesul este controlat de politicile de securitate impuse la nivel de sistem, fără intervenția utilizatorilor.

RBAC (Role-Based Access Control): Permisiunile sunt atribuite pe baza rolurilor utilizatorilor în organizație.

Permisiuni în sistemele de operare

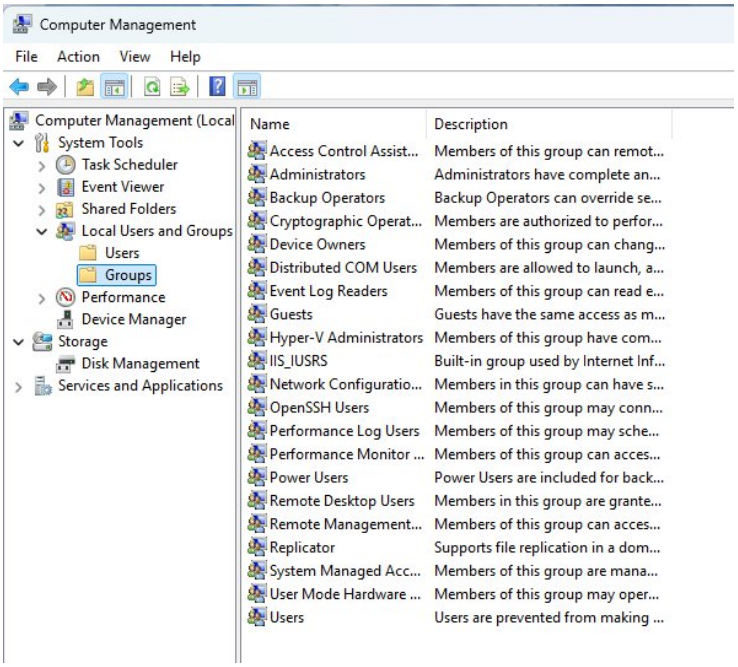
În Windows, drepturile și permisiunile sunt gestionate prin ACL (Access Control List), iar utilizatorii sunt organizați în grupuri locale sau de domeniu.

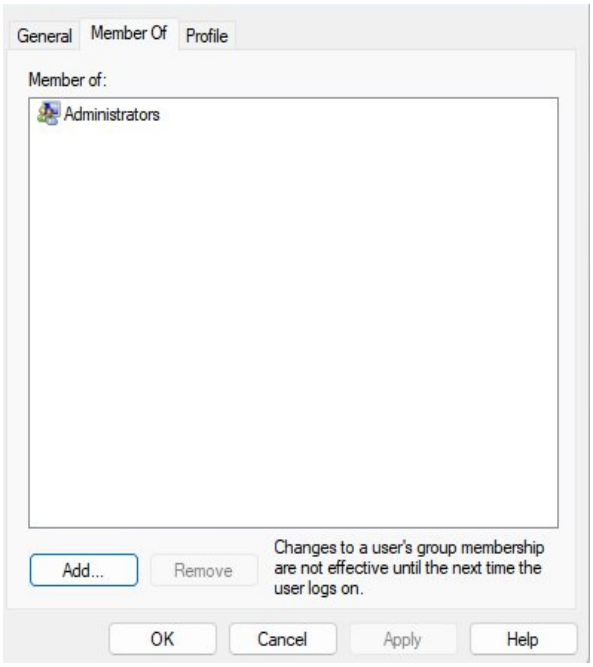
În Linux, sistemul de fișiere utilizează permisiuni de tip rwx (read, write, execute) pentru trei categorii: utilizator (owner), grup (group), alții (others).

Gestionarea eficientă a utilizatorilor și a grupurilor este esențială pentru a preveni accesul neautorizat și pentru a implementa politici de securitate coerente.

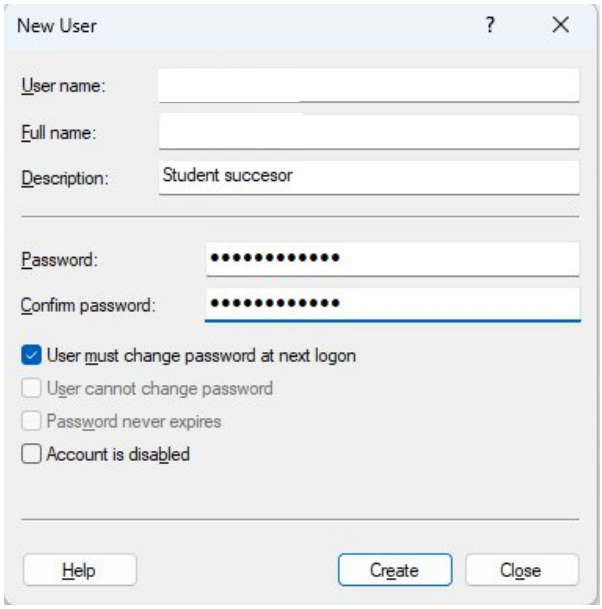
3. Sarcini practice

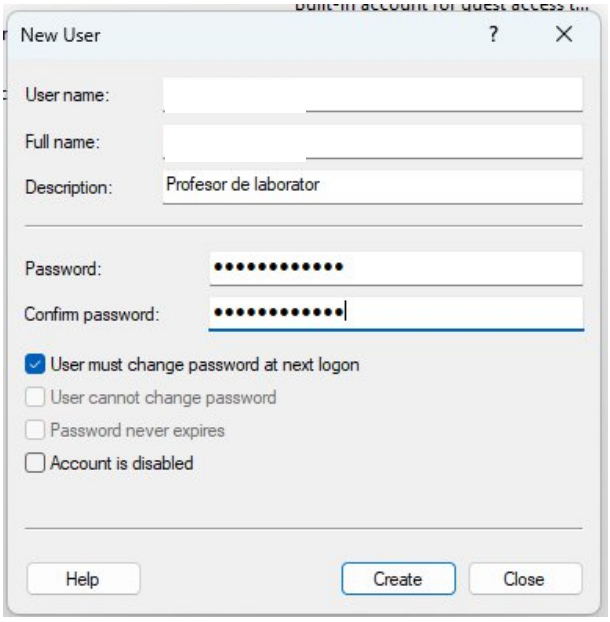
Pasul 1: *Crearea utilizatorilor noi*



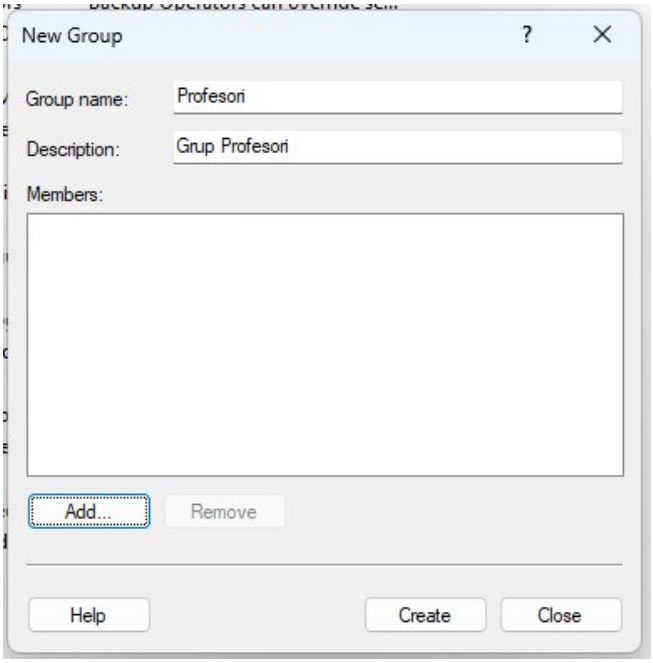


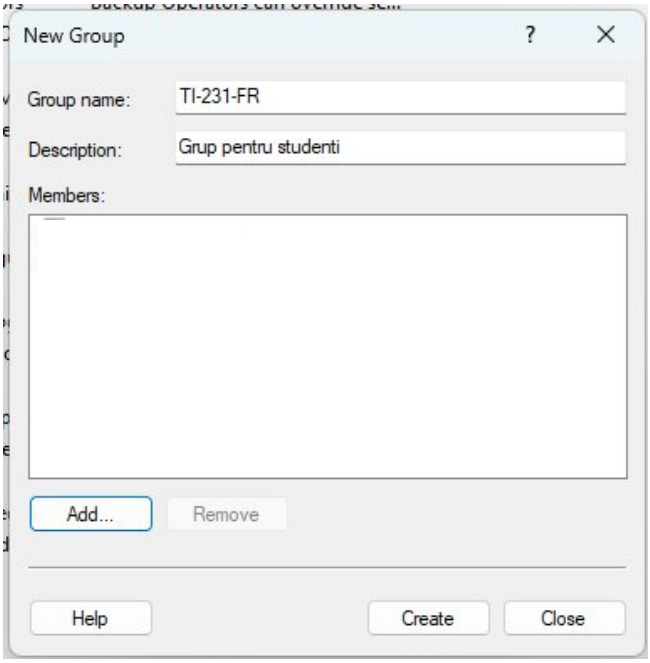
Verificarea utilizatorilor si a grupurilor existente



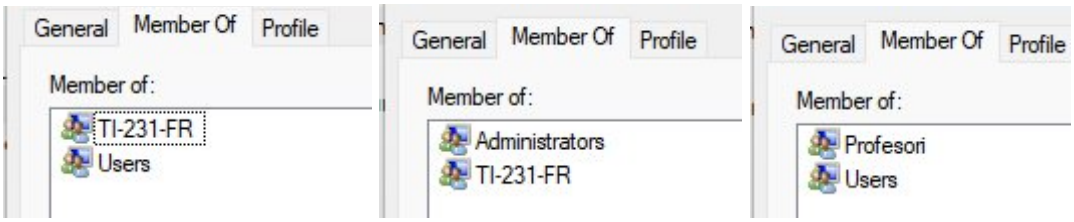


Pasul 2: *Crearea grupurilor noi pentru Studenți și Profesori și atribuire utilizatori*

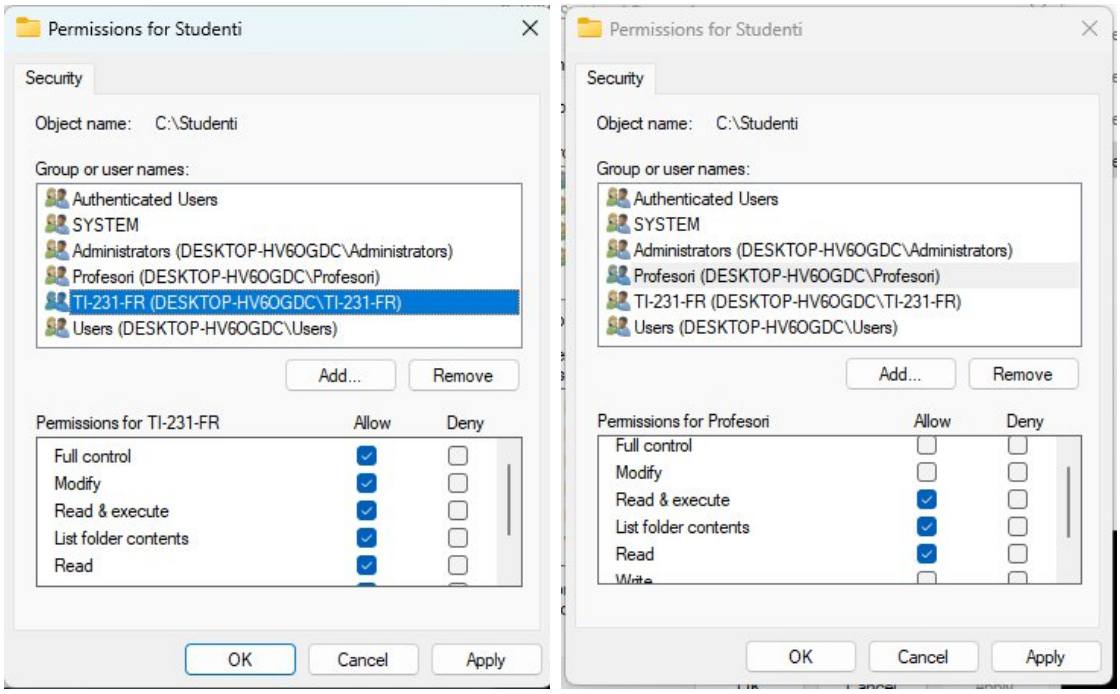




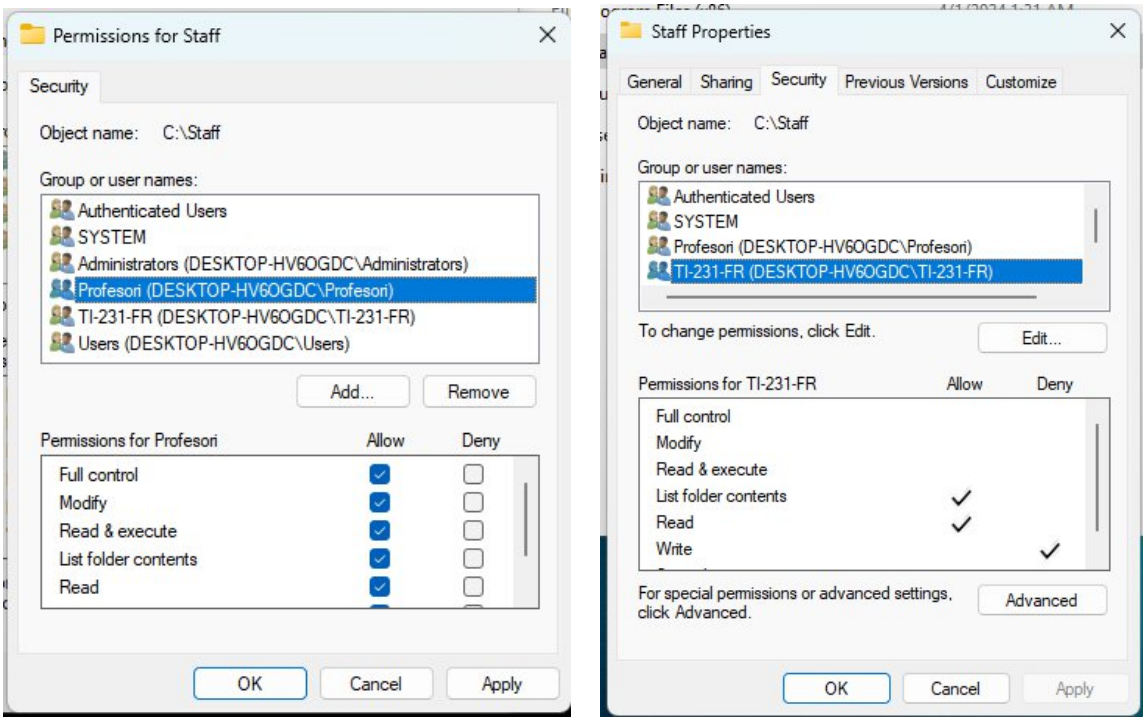
Verificare atribuire la grup:



Pasul 3: *Atribuire permisiuni de grup catre anumite foldere*

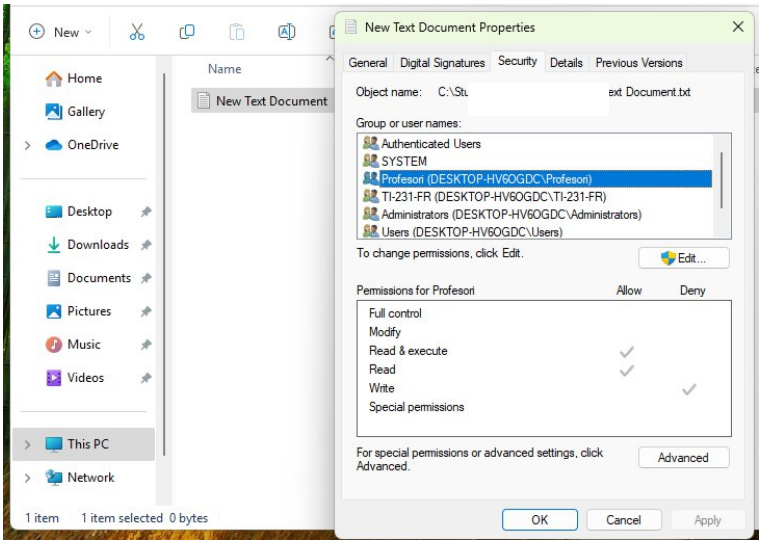


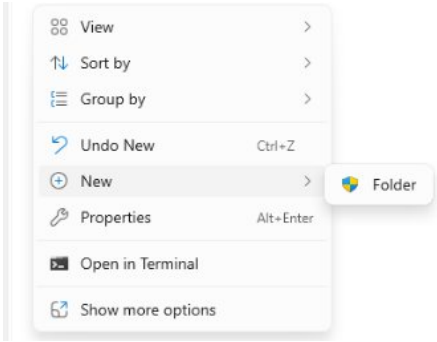
Atribuim Permisiuni pentru mapa „Studenti”

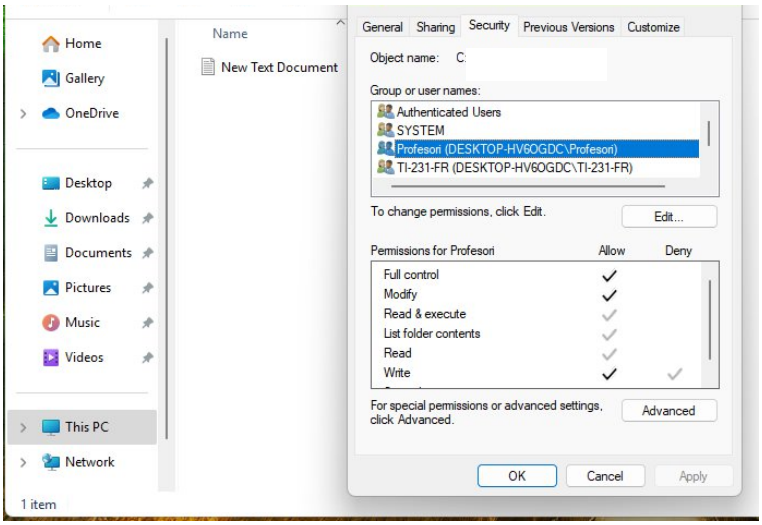


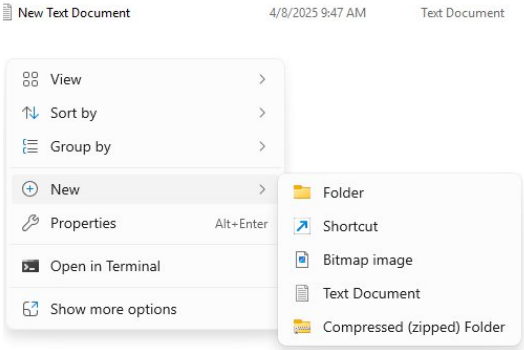
Atribuim Permisiuni pentru mapa „Staff”

Pasul 4: *Modificarea permisiunilor utilizatorilor si grupurilor*









Pasul 5: *Realizarea auditului sistemului de operare Windows 11 Pro*

Se verifică în Event Viewer log-urile pentru acțiunile ce au fost realizate

Pentru filtrare log-uri creem custom view pentru id

Event ID 4720 – Un utilizator a fost creat.

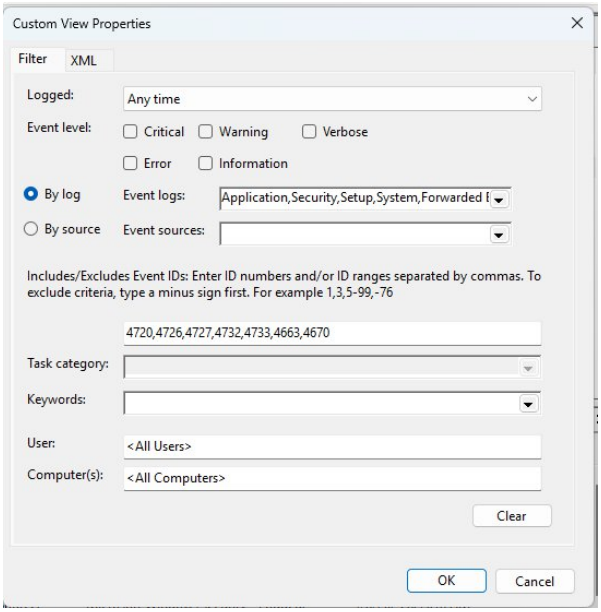
Event ID 4726 – Un utilizator a fost șters.

Event ID 4727 – Un grup de securitate a fost creat.

Event ID 4732 – Un utilizator a fost adăugat într-un grup.

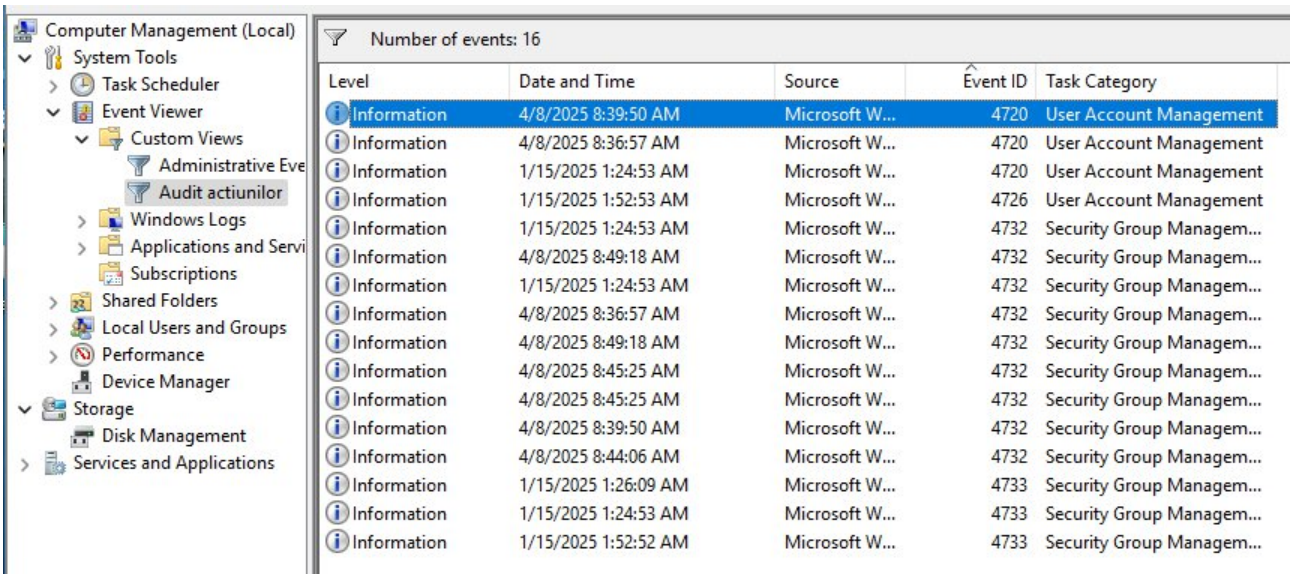
Event ID 4733 – Un utilizator a fost eliminat dintr-un grup.

Event ID 4663 – Tentativă de acces la un obiect (fără succes sau cu succes).



Event ID 4670 – Permisiunile unui obiect au fost modificate.

Event ID 4663 - auditarea accesului la obiecte



Configurare AAA în Linux

Pasul 1: *Crearea de grupuri noi si adaugarea utilizatorilor in noul grup*

1. Comută la utilizatorul root:

```bash
sudo su
```

2. Creează grupurile:

```bash
groupadd studenti
groupadd profesori
```

1. Creează utilizatorul (dacă nu există deja):

```bash
useradd -m auricaa
```

2. Setează parola:

```bash
passwd auricaa
```

3. Adaugă utilizatorul în grupul `studenti`:

```bash
usermod -aG studenti auricaa
```

Pasul 2: *Schimbarea utilizatorului si modificarea permisiunilor*

1. Comută de la root la utilizatorul `auricaa`:

```bash
su - auricaa
```

2. Încearcă să creezi un fișier într-un director al altui utilizator (simulând lipsa permisiunii):

```bash
touch /home/alexandrutocan/test.txt
```

> Această comandă ar trebui să eșueze dacă permisiunile sunt corect setate (de exemplu, `r-x` fără `w` pentru alți utilizatori).

3. Revino la utilizatorul root:

```bash
exit
```

Pasul 3: *Realizarea auditului actiunilor intreprinse*

1. Asigură-te că serviciul audit este instalat și activ:

```bash
sudo apt install auditd
sudo systemctl start auditd
```

2. Adaugă o regulă de audit pentru directorul `auricaa`:

```bash
sudo auditctl -w /home/auricaa -p rwxa -k auricaa_dir
```

3. Consultă evenimentele de audit:

```bash
sudo ausearch -k auricaa_dir
```

4. Concluzii

Lucrarea de laborator a avut ca scop înțelegerea și aplicarea practică a conceptelor fundamentale ale controlului accesului în sistemele de operare. Prin realizarea sarcinilor propuse, s-a evidențiat importanța mecanismelor de autentificare, autorizare și audit (AAA) în asigurarea securității informaționale.

Au fost explorate și aplicate permisiunile și drepturile utilizatorilor în medii Windows și Linux, punând accent pe configurarea corectă a accesului la fișiere și directoare. De asemenea, s-a realizat gestionarea eficientă a utilizatorilor și grupurilor, evidențiind diferențele de implementare și control între cele două sisteme de operare.

În concluzie, laboratorul a contribuit la dezvoltarea abilităților tehnice necesare pentru administrarea și protejarea resurselor sistemului, oferind o bază practică solidă pentru înțelegerea politicilor de control al accesului în contextul securității cibernetice.

5. Bibliografie

- Îndrumar de laborator - Autor: lect.univ., dr. Arina Alexei
- Ghiduri despre securitatea IT de pe platforma ELSE - Autor: lect.univ., dr. Arina Alexei.