**Ministerul Educaţiei și Cercetării al Republicii Moldova**

**Universitatea Tehnică a Moldovei**

**Facultatea Calculatoare, Informatică și Microelectronică**

**RAPORT**

Lucrarea de laborator nr.3

*la Tehnologii a Securitatii Informationale*

A efectuat:

st. gr. TI-216 Rosca Dorin

A verificat: Zalesciuc Maxim

Chişinău – 2023

**Lucrare de laborator nr. 3**

**Tema:**Configurarea drepturilor de acces în Windows și Linux.

**Scopul lucrării:** Gestionarea drepturilor de acces în sistemele de operare Windows și Linux

1. Tipuri de conturi de utilizator (Administrator, Guest, Standart)

**Sistemele de operare moderne, cum ar fi Windows și Linux, includ mai multe tipuri de conturi de utilizator pentru a permite o administrare și o utilizare mai eficientă și sigură a sistemelor. În acest articol, vom explora cele trei tipuri principale de conturi de utilizator: Administrator, Guest și Standard, în contextul sistemelor de operare Windows și Linux.**

**Administrator:Un cont de administrator este cel mai puternic tip de cont de utilizator disponibil pe un sistem de operare. De obicei, acesta este creat la instalarea sistemului de operare și are acces la toate resursele sistemului. Acestea includ permisiuni complete pentru a modifica și instala software-ul, a administra fișiere și directoare, a crea și șterge conturi de utilizator și a efectua alte sarcini administrative. Este important să menționăm că, deoarece contul de administrator are atât de multe privilegii, trebuie utilizat cu precauție pentru a evita orice modificări sau acțiuni nedorite care pot afecta funcționarea sistemului.**

**În Windows, utilizatorii pot crea mai mulți administratori și pot schimba nivelurile de acces al fiecărui cont de utilizator.**

**În Linux, utilizatorii pot accesa contul de administrator prin intermediul terminalului, unde trebuie să introducă comanda "su" (abrevierea de la "switch user" - schimbă utilizatorul) și să introducă parola de administrator.**

**Standard: Contul standard, cunoscut și sub numele de cont limitat, este un tip de cont de utilizator care are acces la un set limitat de resurse și permisiuni de sistem. Aceasta este o opțiune ideală pentru utilizatorii obișnuiți care nu au nevoie de privilegii administrative sau de acces la fișiere sau setări sensibile ale sistemului. Un utilizator standard poate utiliza în continuare majoritatea aplicațiilor și poate accesa majoritatea fișierelor și directoarelor, dar nu poate face modificări care pot afecta sistemul.**

**În Windows, conturile standard pot fi create prin intermediul Panoului de control sau al aplicației Setări.**

**În Linux, utilizatorii pot crea un cont standard prin intermediul terminalului sau al interfeței grafice.**

**Guest: Un cont de utilizator Guest este un cont temporar creat pentru utilizatori care nu au un cont permanent pe sistemul de operare. Acest tip de cont de utilizator este ideal pentru oaspeți sau utilizatori temporari, deoarece nu necesită o parolă și limitează accesul la anumite resurse și permisiuni de sistem. În Windows, utilizatorii pot activa contul de utilizator Guest prin intermediul Panoului de control sau al aplicației Setări.**

**În Linux, utilizatorii pot crea un cont Guest prin intermediul terminalului sau al interfeței grafice.**

1. **Dreptul de Acces la fisiere si dosare:**

**Drepturile de acces la fișiere și dosare sunt un aspect important al securității sistemelor de operare. Aceste drepturi determină cine poate accesa, modifica sau șterge anumite fișiere sau directoare pe un sistem. În cadrul unui sistem de operare, aceste drepturi sunt gestionate prin intermediul permisiunilor. Există trei tipuri principale de permisiuni care pot fi aplicate la fișiere și directoare: Permisiuni de citire: Acest tip de permisiune permite utilizatorului să citească conținutul fișierului sau dosarului. Utilizatorul nu poate modifica sau șterge fișierul sau dosarul. Permisiuni de scriere: Acest tip de permisiune permite utilizatorului să modifice sau să scrie în fișierul sau dosarul respectiv. Utilizatorul poate crea, edita sau șterge fișierele sau directoarele pentru care are această permisiune. Permisiuni de execuție: Acest tip de permisiune permite utilizatorului să ruleze fișierele executabile sau scripturile aflate în dosarul respectiv. În plus, există două tipuri de drepturi de acces pentru utilizatori:**

**Drepturi de acces bazate pe utilizator: Aceste drepturi de acces sunt atribuite fiecărui utilizator în mod individual. Acest tip de drepturi permite gestionarea accesului individual al fiecărui utilizator la fișierele și directoarele sistemului.**

**Drepturi de acces bazate pe grup: Acest tip de drepturi de acces se aplică întregului grup de utilizatori. Aceste drepturi de acces sunt utile pentru gestionarea accesului la fișierele și directoarele care trebuie partajate între un grup de utilizatori.**

**Astfel, administratorul poate gestiona drepturile de acces pentru un întreg grup în loc să le configureze individual. În sistemele de operare moderne, precum Windows sau Linux, administratorii pot configura drepturile de acces pentru fiecare fișier și dosar în parte prin intermediul permisiunilor de acces.**

1. **Metodele de autentificare ale utilizatorilor. Autentificare Multi-Factor (TwoFactorAuth.org)**

**Metodele de autentificare a utilizatorilor sunt utilizate pentru a confirma identitatea unei persoane care accesează un sistem sau o aplicație. Aceste metode pot include autentificarea prin parolă, autentificarea prin biometrie, autentificarea prin token-uri sau autentificarea prin autentificare multi-factor (MFA).**

**Autentificarea multi-factor este o metodă de autentificare care utilizează cel puțin două elemente diferite pentru a confirma identitatea utilizatorului. Aceste elemente pot fi, de exemplu, o parolă și o cheie de securitate hardware sau o amprentă digitală și o întrebare secretă.**

**Autentificarea multi-factor oferă un nivel suplimentar de securitate, deoarece utilizatorul trebuie să aibă în posesie ambele elemente pentru a confirma identitatea lor. TwoFactorAuth.org este o organizație care promovează utilizarea autentificării multi-factor pentru a proteja conturile online ale utilizatorilor.**

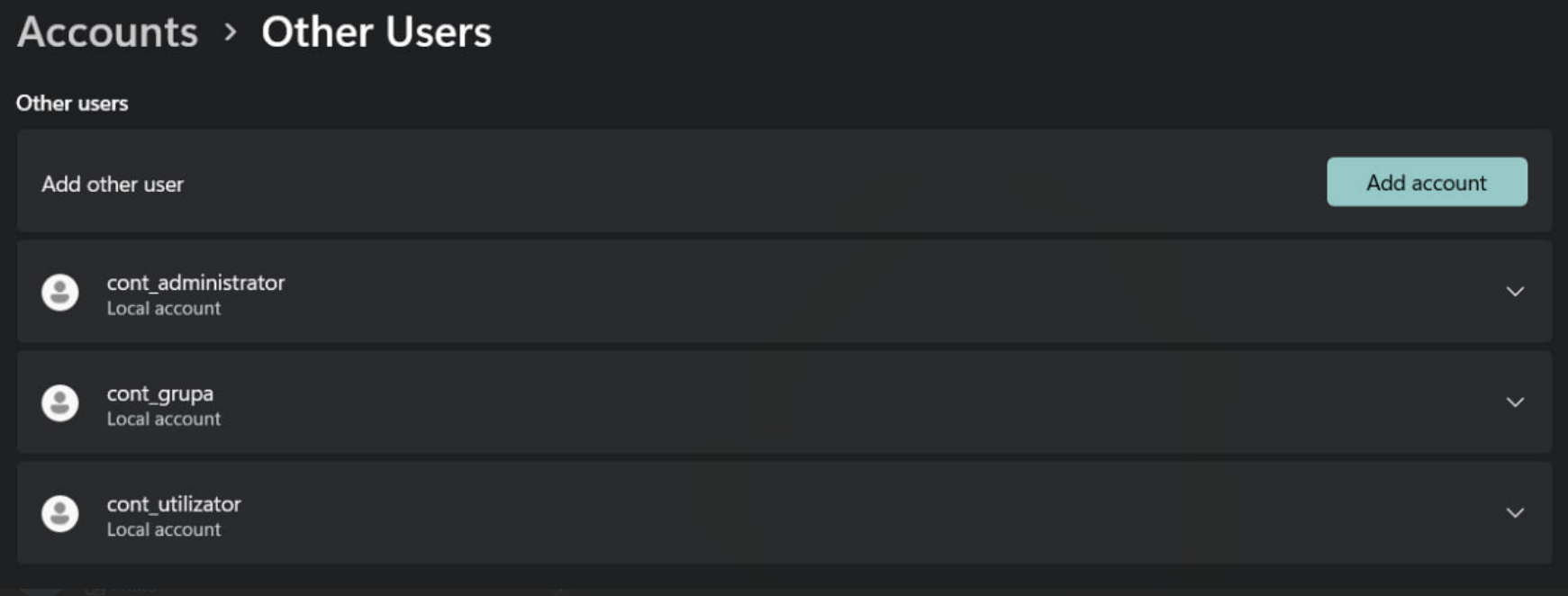
**Această metodă de autentificare este considerată mai sigură decât autentificarea prin parolă simplă și poate fi implementată cu ușurință prin intermediul unor aplicații sau dispozitive hardware. Implementarea autentificării multi-factor poate ajuta la reducerea riscului de acces neautorizat la conturile utilizatorilor și poate îmbunătăți securitatea în mediul online.**

1. **Information rights Management(IRC)**

**Information Rights Management (IRM) este o metodă de protejare a datelor care permite proprietarilor de informații să controleze accesul, utilizarea și distribuirea informațiilor lor digitale. Acest sistem se bazează pe criptarea datelor, oferind utilizatorilor dreptul de a accesa și utiliza informațiile numai în conformitate cu permisiunile setate de proprietar. Prin utilizarea IRM, proprietarii de informații pot seta drepturi de acces, de editare și de distribuire pentru documentele lor digitale, limitând accesul la acestea numai la utilizatorii autorizați și în scopuri specifice. În acest fel, IRM ajută la protejarea informațiilor sensibile, limitând riscul de pierdere, furt sau dezvăluire neautorizată a datelor.**

1. **Sarcina:**

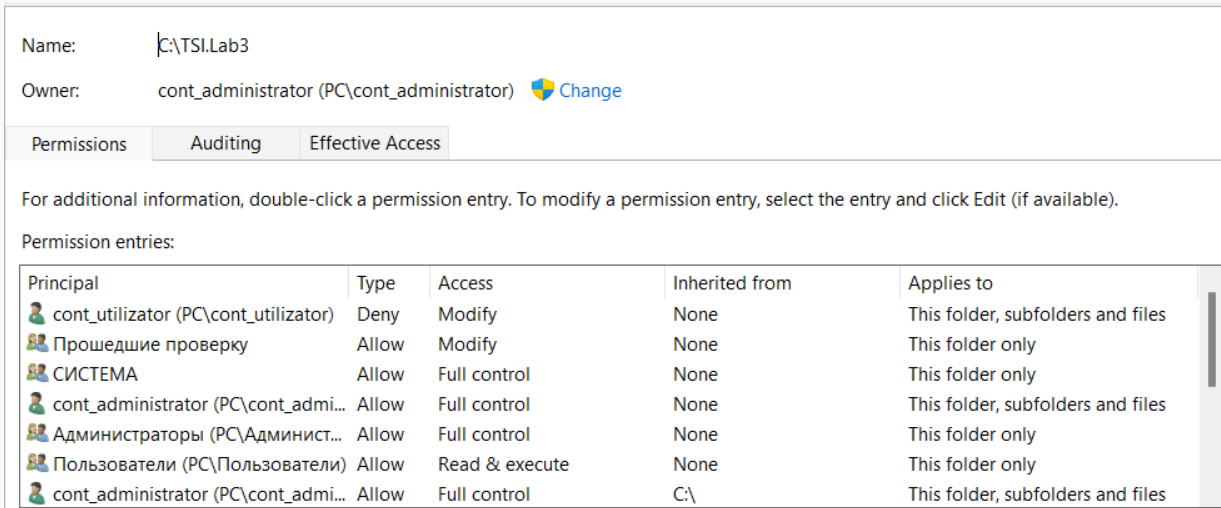
Pentru a efectua lucrarea va avea nevoie de două conturi - cont\_administrator și cont\_utilizator, care nu face parte din grupul de administratori.

****

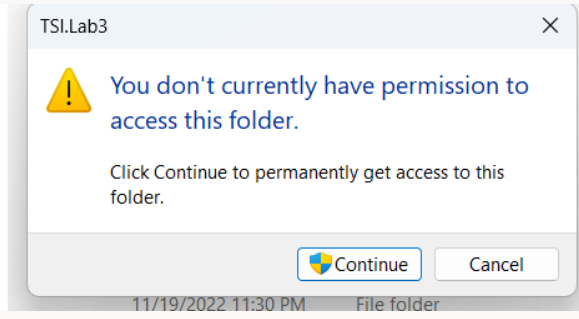
**Fig1.Crearea Conturilor**

****

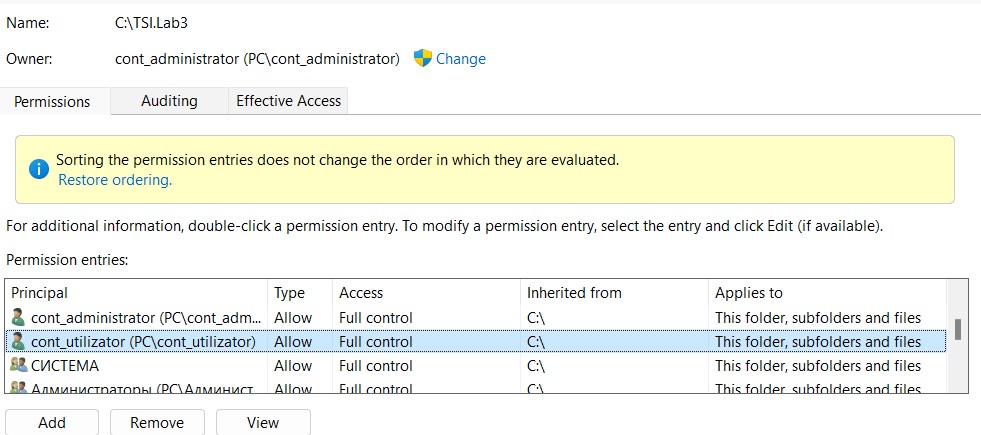
**Fig2.Crearea Folderului**

****

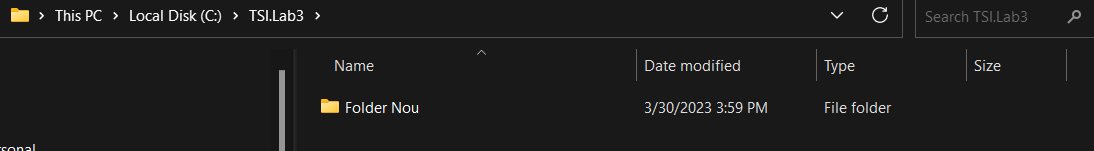
**Fig3.Setarea Drepturilor Utilizator**

****

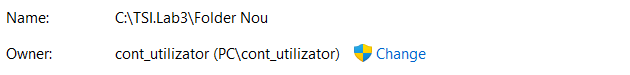
**Fig4.Rezultatul can incerc sa modific Folderul din alt cont**

****

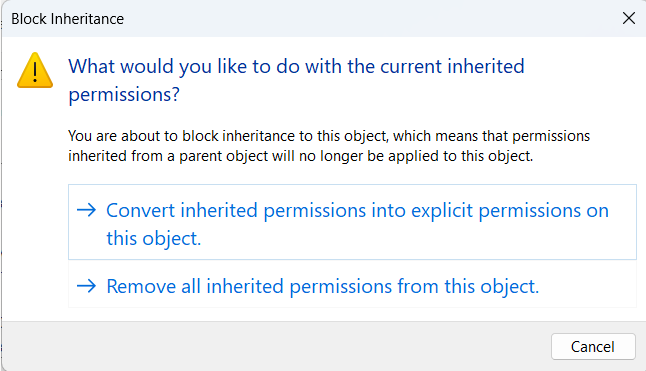
**Fig5.Modificarea drepturilor de acces**

****

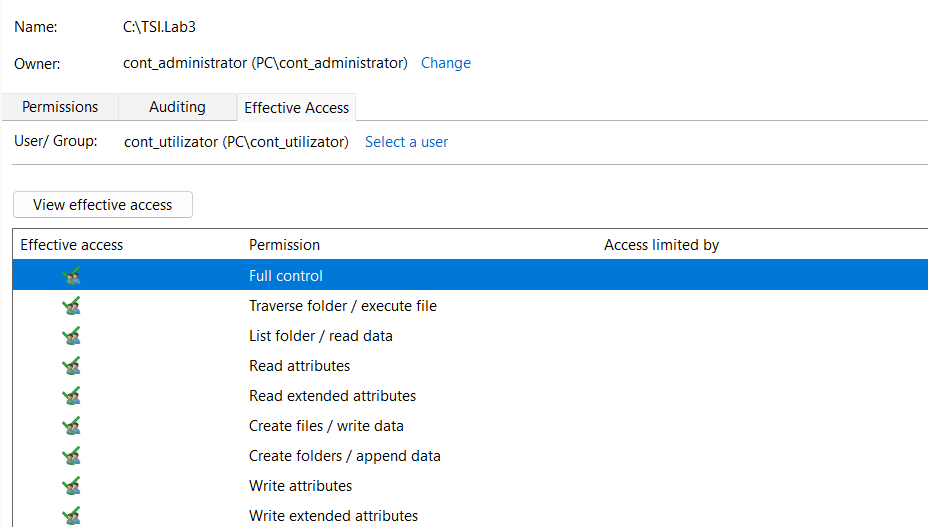
**Fig6.Rezultatul acum**

****

**Fig7. Detalii Folder Creat**

****

**Fig8. Sterge Mostenirea**

****

**Fig9. Vizualizare Permisiuni**

1. **Concluzie:**

Această lucrare de laborator se axează pe gestionarea drepturilor de acces în sistemele de operare Windows și Linux, acoperind tipurile de conturi de utilizator (Administrator, Guest, Standard) și drepturile de acces la fișiere și dosare. Este important să se utilizeze cu precauție contul de administrator, deoarece are acces la toate resursele sistemului, iar permisiunile pentru fișiere și directoare sunt gestionate prin intermediul permisiunilor de citire, scriere și execuție.