**Ministerul Educaţiei și Cercetării al Republicii Moldova**

**Universitatea Tehnică a Moldovei**

**Facultatea Calculatoare, Informatică și Microelectronică**

**RAPORT**

Lucrarea de laborator nr.3

*la Tehnologii de Securitatea Informațională*

A efectuat:

st. gr. TI-214 Buza Cătălin

A verificat: Bulai Rodica

Chişinău - 2023

**Scopul lucrării:**

1. Gestionarea drepturilor de acces în sistemele de operare Windows și Linux

* Tipuri de conturi de utilizator (Administrator, Guest, Standart)
* Drepturi de acces la fișiere și dosare
* Metodele de autentificare ale utilizatorilor. Autentificare Multi-Factor (TwoFactorAuth.org)
* Information rights management (IRC)

Gestionarea drepturilor de acces în sistemele de operare Windows și Linux este o preocupare importantă pentru orice organizație sau utilizator individual. Drepturile de acces sunt esențiale pentru a asigura confidențialitatea, integritatea și disponibilitatea datelor și resurselor dintr-un sistem.

În sistemele de operare Windows și Linux, există diferite tipuri de conturi de utilizator, inclusiv Administrator, Guest și Standard. Contul de Administrator are drepturi de acces depline la sistem și la toate fișierele și dosarele. Contul de Guest este destinat pentru utilizatori temporari și are drepturi de acces limitate. Contul Standard este destinat pentru utilizatorii obișnuiți și are drepturi de acces limitate la unele resurse din sistem.

Pentru a gestiona drepturile de acces la fișiere și dosare în sistemele de operare Windows și Linux, se pot utiliza diferite metode, cum ar fi atribuirea permisiunilor de acces la nivel de utilizator sau grup, utilizarea listelor de control al accesului (ACL) și utilizarea de grupuri de utilizatori pentru a gestiona drepturile de acces la nivel de resursă.

În figura 1 este reprezentat rezultatul obținut după modificarea drepturilor de acces a utilizatorilor guest și standart în windows 10. Am făcut în așa fel ca nimeni înafară de administrator să poată vedea sau modifica accesul la acest fișier text, când cineva vrea să-l deschidă va vedea un mesaj cei spune ca nu are drept de deschidere a acestui fișier.

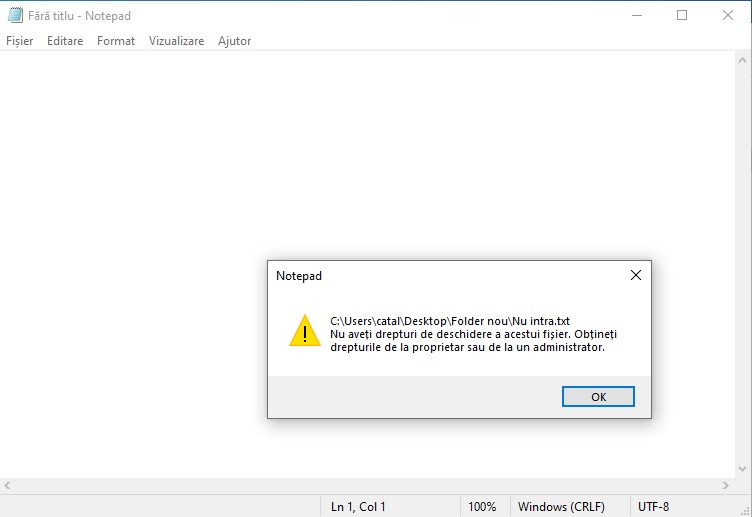


Figura 1- Modificarea drepturilor de acces pe windows 10

Similar ca și pe Windows 10 în linux am folosit fișierul passwords.txt creat pentru a putea realiza o sarcină pentru laboratorul 2, i-am dat permisiunile că doar eu să pot scrie și citi conținutul lui iar alți utilizatori nu-l vor putea deschide. În figurile 2 și 3 sunt reprezentate aceste lucruri.

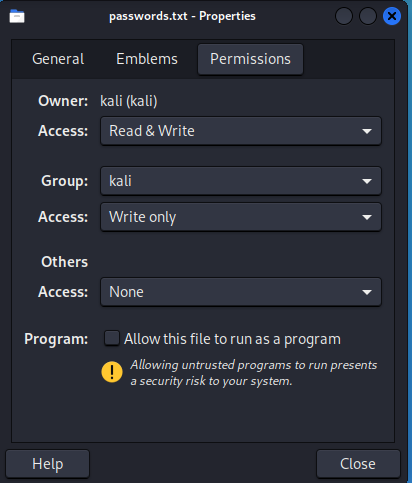


Figura 2- Modificare drepturilor de acces a fișierului passwords.txt

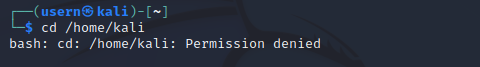


Figura 3- Acces interzis usern

Pentru a îmbunătăți securitatea și a preveni accesul neautorizat, se pot utiliza metodele de autentificare ale utilizatorilor, cum ar fi autentificarea prin parolă, autentificarea prin biometrie, autentificarea prin token-uri de securitate sau autentificarea multi-factor (MFA). Autentificarea multi-factor implică utilizarea a două sau mai multe elemente de autentificare, cum ar fi o parolă și un cod de securitate generat de un dispozitiv separat.

Pentru a proteja informațiile împotriva accesului neautorizat, se poate utiliza Information Rights Management (IRM). IRM implică utilizarea de politici de securitate care restricționează drepturile de acces la documente sau alte resurse din sistem, permițând doar utilizatorilor autorizați să acceseze și să utilizeze aceste resurse.

În general, gestionarea drepturilor de acces în sistemele de operare Windows și Linux este esențială pentru a proteja informațiile și resursele din sistem. Utilizarea metodelor de autentificare multi-factor și IRM poate îmbunătăți securitatea și a preveni accesul neautorizat la informații și resurse din sistem.

Managerul de parole

La pornirea programului python va fi afișat la ecran un generator de parole care arată ca în figura 4.În această fereastră avem posibilitatea să primim o parolă de lungime minimă 9 și în care putem selecta numărul de litere, cifre sau simbolu speciale pe care le vrem ca parola să le aibe. Dacă apăsăm butonul autentificare se va deschide fereastra unde trebuie să punem parola pentru a putea ajunge la seiful cu parole.În figura 5 este reprezentat acest lucru.

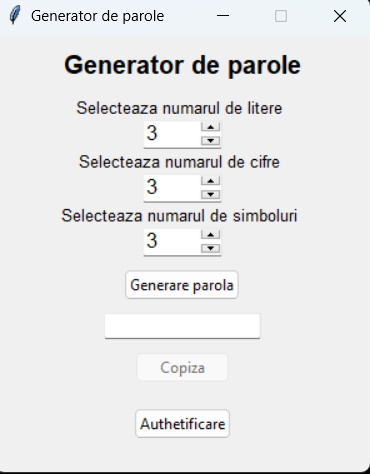


Figura 4 -Generatorul de parole

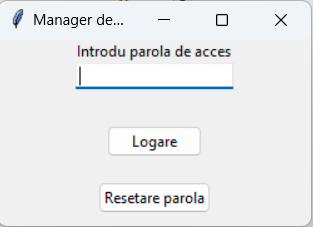


Figura 5- Autentificarea pentru a intra în seif

În figura 6 este reprezentat seiful cu parole. El este unul simplu, pentru a adauga un nou cont este doar necesar de a apăsa butonul *Adauga noua intrate*. După care vom introduce fiecare informație pe rând iar la final acestă nouă intrare va fi adăugată la final. Fiecare intrare adăugată conține alte 4 metode pentru a ușura muncă. Pentru a șterge o intrare apasăm pe *Sterge,* pentru a actualiza o intrare apăsăm *actualizare*, iar dacă dorim să copiem Parola sau Username apăsăm butoanele respective.

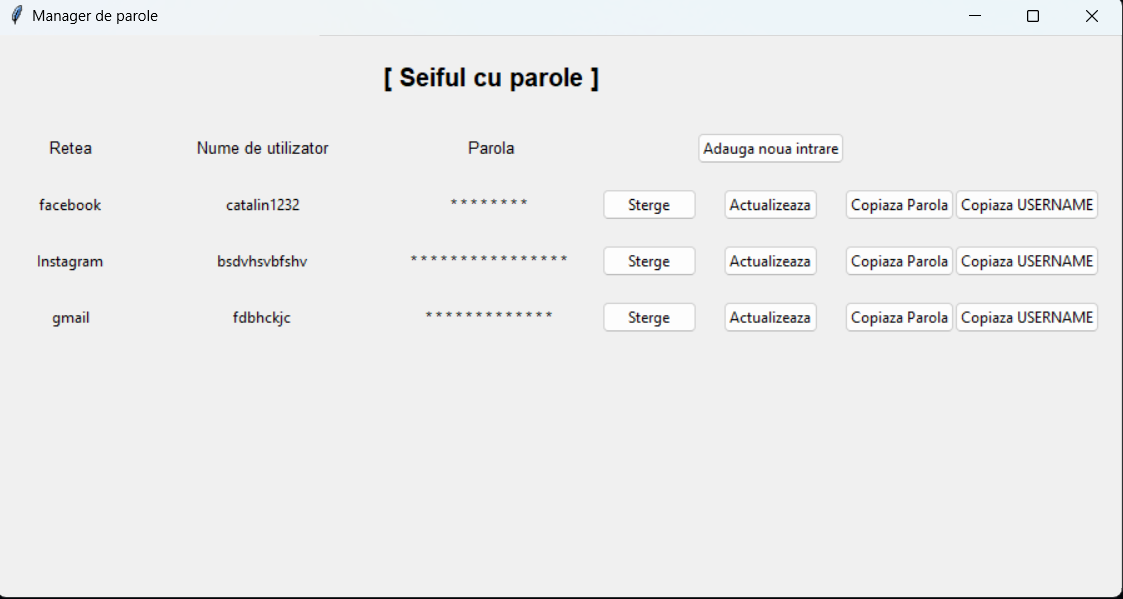


Figura 6 – Seiful cu parole

Metode principale

window=Tk()

window.geometry('300x350')

window.style=ttk.Style(window)

window.title("Generator de parole")

# window.iconbitmap(True,'H:/prem college/qt\_5.12/login\_window\_fl/login\_img/f\_logo.ico')

window.resizable(0,0)

no\_of\_letters=IntVar()

no\_of\_letters.set(3)

no\_of\_digits=IntVar()

no\_of\_digits.set(3)

no\_of\_symbols=IntVar()

no\_of\_symbols.set(3)

heading = ttk.Label(window, text = 'Generator de parole' , font ='arial 15 bold').pack(pady=10)

letter\_spinbox\_label=ttk.Label(window,text="Selecteaza numarul de litere ",font=Font(family='arial 10 bold', size=10)).pack()

letter\_spinbox=ttk.Spinbox(window,from\_=3,to=11,textvariable=no\_of\_letters,width=5,font=Font(family='Helvetica', size=12)).pack()

digit\_spinbox\_label=ttk.Label(window,text="Selecteaza numarul de cifre ",font=Font(family='arial 10 bold', size=10)).pack()

digit\_spinbox=ttk.Spinbox(window,from\_=3,to=11,textvariable=no\_of\_digits,width=5,font=Font(family='Helvetica', size=12)).pack()

symbol\_spinbox\_label=ttk.Label(window,text="Selecteaza numarul de simboluri ",font=Font(family='arial 10 bold', size=10)).pack()

symbol\_spinbox=ttk.Spinbox(window,from\_=3,to=11,textvariable=no\_of\_symbols,width=5,font=Font(family='Helvetica', size=12)).pack()

password\_string=StringVar()

def Copy\_password():

    pyperclip.copy(password\_string.get())

    copy['state']=DISABLED

def generate() :

    copy['state']=NORMAL

    password=[]

    digits=['1','2','3','4','5','6','7','8','9','0']

    letters=['a', 'b', 'c', 'd', 'e', 'f', 'g','h', 'i', 'j', 'k', 'l', 'm', 'n', 'o',  'p', 'q', 'r', 's', 't', 'u', 'v', 'w', 'x', 'y', 'z','A', 'B', 'C', 'D', 'E', 'F', 'G', 'H', 'I', 'J', 'K', 'L', 'M', 'N', 'O', 'P', 'Q', 'R', 'S', 'T', 'U', 'V', 'W', 'X', 'Y', 'Z']

    symbols=['#','$','%','&','(',')','\*','+','-','.','/',':','<','=','>','?','@','[',']','^','\_','{','}','/' ]

    for x in range(no\_of\_letters.get()):

        password.append(random.choice(letters))

    for x in range(no\_of\_digits.get()):

        password.append(random.choice(digits))

    for x in range(no\_of\_symbols.get()):

        password.append(random.choice(symbols))

    random.shuffle(password)

    password\_string.set("".join(password))

copy=ttk.Button(window, text = 'Copiza', command = Copy\_password,state=DISABLED)

def checkPassword():

            match=getMasterPassword()

            if match:

                global encryptionkey

                encryptionkey= base64.urlsafe\_b64encode(kdf.derive("PremWagh2210".encode('utf-8')))

                passwordvault()

            else:

                Mstr\_pass\_txt.delete(0,'end')

                lbl1.config(text="Parola gresita !")

Concluzie

În cadrul laboratorului numărul 3 la Tehnologii de Securitate Informațională, am avut ocazia să învățăm despre gestionarea drepturilor de acces în sistemele de operare Windows și Linux. Am explorat tipurile de conturi de utilizator, cum ar fi Administrator, Guest și Standard, precum și drepturile de acces la fișiere și dosare.

De asemenea, am discutat despre diferite metode de autentificare ale utilizatorilor, inclusiv autentificarea prin parolă, autentificarea prin biometrie, autentificarea prin token-uri de securitate sau autentificarea multi-factor (MFA). Am aflat cum utilizarea autentificării multi-factor poate îmbunătăți securitatea și a preveni accesul neautorizat la informații și resurse din sistem.

În plus, am învățat despre Information Rights Management (IRM), o metodă de protejare a informațiilor prin utilizarea de politici de securitate care restricționează drepturile de acces la documente sau alte resurse din sistem. Astfel, am înțeles cum gestionarea drepturilor de acces este esențială pentru protejarea informațiilor și resurselor din sistem, și am învățat cum să utilizăm diferite metode pentru a îmbunătăți securitatea.

În general, acest laborator ne-a ajutat să înțelegem importanța gestionării drepturilor de acces în sistemele de operare, precum și să dobândim cunoștințe și abilități practice în utilizarea de metode de autentificare multi-factor și Information Rights Management pentru a proteja informațiile și resursele din sistem.