**Remote Administration Tool**



Îndrumător: Realizat de:

Slt**. VAMAN** Adina Sd. Sg. **HIUHIU** Bianca

Sd. Sg. **GUCEANU** Bianca

Grupa C113D

# Capitolul 1 - Introducere

## Scopul proiectului

Scopul proiectului este dezvoltarea unui sistem de administrare de la distanță: permiterea unui utilizator să controleze și să administreze un sistem Linux fără a fi prezent fizic pe mașina respectivă.

## Lista definițiilor

**Acces remote** - gestionarea unui sistem informatic de la distanță. Prin gestionare ne referim prin dispunerea unui terminal care să ofere acces la funcționalitățile celuilalt dispozitiv.

**Socket** - canal de comunicație bidirecțional între două procese care rulează pe rețea și permite schimbul de date între acestea.

**Framework** - un set de biblioteci, module și instrumente care oferă un schelet pentru dezvoltarea de aplicații software.

**CLI(Command Line Interface)** - mecanism de interacțiune cu un computer, un sistem de operare sau un software prin introducerea de comenzi secvențial linie cu linie.

**Network Bridge Adapter** - o configurație care permite mașinii virtuale să comunice direct cu rețeaua fizică. Acest concept este folosit pentru a permite mașinilor virtuale să aibă acces la rețeaua fizică și să comunice cu alte dispozitive din rețea.

**Securitate** - aspectul vital al administrării sistemului de la distanță, care se referă la protejarea datelor și a infrastructurii împotriva accesului neautorizat sau a amenințărilor cibernetice.

**Autentificare cu doi factori (2FA)** - o metodă suplimentară de securitate care necesită două metode separate de autentificare pentru a verifica identitatea unui utilizator, de obicei, o parolă și un factor suplimentar (autentificare pe bază de sesiune).

## Structura documentului

Documentul este împărțit în trei capitole. Capitolul 1 reprezintă introducerea, capitolul 2 cuprinde detalierea generală a produsului software. Capitolul 3 cuprinde o detaliere a cerințelor funcționale și nefuncționale și interacțiunea utilizatorului cu interfața grafică.

# Capitolul 2 - Descrierea generală a produsului software

## 2.1 Descrierea produsului software

Din perspectivă arhitecturală, proiectul va implica două componente distincte: un server, reprezentat de mașina remote care va fi accesată și controlată de la distanță, și un client, reprezentat de dispozitivul de pe care dorim să trimitem comenzi și să interacționăm cu serverul.Utilizatorul va trimite cereri către celălalt dispozitiv, iar acesta va executa comenzile dorite.Cererile utilizatorului pot fi diverse și distincte: acces la terminal la distanță pentru comenzi simple, transferul de fișiere la distanță între sistemul de la distanță și sistemul de control, monitorizarea activității sistemului de la distanță și setări de sistem( pornire și oprire de servicii etc.).

## 2.2 Detalierea platformei HW/SW

Produsul software va fi destinat dispozitivelor care rulează sistemul de operare Linux. Dezvoltarea aplicației principale va fi realizată în limbajul de programare C, iar partea de interfață în linia de comandă (CLI) va fi dezvoltată în Bash pentru Linux. Pentru crearea unui aplicații de tip Console Application care va îndeplini rolul de server în program, se va folosi mediul integrat de dezvoltare Microsoft Visual Studio Code.

## 2.3 Constrângeri

Administrarea unui sistem la distanță necesită implementarea unor măsuri de securitate pentru a proteja atât datele, cât și infrastructura împotriva accesului neautorizat. Toate solicitările efectuate de un utilizator către sistem trebuie să fie precedate de autentificarea în sistem și gestionarea unei sesiuni, asigurând astfel integritatea și securitatea sistemului împotriva potențialelor amenințări.

## 2.4 Listă referințe

* <https://www.cendio.com/blog/10-best-remote-desktop-software-tools-for-linux-users/>
* <https://academic-accelerator.com/encyclopedia/remote-administration>
* <https://ocw.cs.pub.ro/courses/pc/laboratoare/07>

# Capitolul 3 – Detalierea cerințelor specifice

## 3.1 Cerințe funcționale

* Utilizatorului i se va permite acces la mașina remote prin autentificare, pe baza unui nume de utilizator si parola(comandă personalizată).Orice cont introdus ce nu se află în sistemul serverului nu va permite accesul la acesta.Odată introdus corect, se va afișa un mesaj de autentificare cu succes iar utilizatorului i se va permite să trimită cereri catre sistem.Toate conturile vor fi stocate intr-un fisier al serverului.
* Deconectarea de la RAT se va face printr-o comandă și va conduce la afișarea unui mesaj.

Utilizatorul care deține accesul la terminal poate executa comenzi direct pe sistemul de la distanță. Aceasta poate include comenzi de sistem, comenzi de gestionare a fișierelor, comenzi pentru configurarea rețelei.

* Execuția de comenzi de sistem: Prin intermediul accesului la terminal, utilizatorul poate executa comenzi de sistem pentru a controla și gestiona resursele sistemului. Aceasta include comenzi precum **`ls`** pentru a afișa conținutul unui director, **`ps`** pentru a lista procesele în execuție, `**mkdir`** pentru a crea directoare, `**rm`** pentru a șterge fișiere și multe altele.
* Utilizatorul poate utiliza terminalul pentru a monitoriza starea sistemului, pentru a urmări jurnalele de evenimente și pentru a efectua diagnosticări ale problemelor sau erorilor.
* Transfer de fișiere: prin comenzi sau instrumente de transfer de fișiere, utilizatorul poate trimite un fisier catre sistemul remote.De asemenea, utilizatorul poate alege un fisier aflat pe sistemul remote pe care sa il descarce in propriul calculator. Acest lucru este util pentru gestionarea și actualizarea datelor și a conținutului.
* Informații de sistem: Afișarea informațiilor de bază despre sistem, cum ar fi sistemul de operare, versiunea kernelului, arhitectura hardware și altele.
* Gestionarea proceselor: Capacitatea de a lista, opri sau porni procese în execuție pe sistem.
* Comenzi personalizate: Permite utilizatorului să definească și să execute comenzi personalizate pentru sarcini specifice.

## 3.2. Cerințe nefuncționale

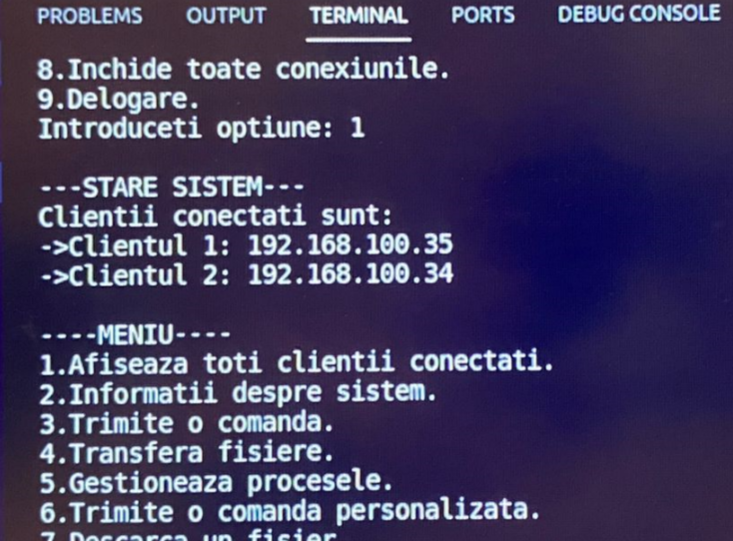
* **Cerințe de implementare:** utilizarea limbajului C, serverul și clientul vor fi realizate în mediul de dezvoltare Microsoft Visual Studio Code in mediul Linux și se va utiliza un server de baze de date MySQL.//user si parola
* **Cerințe de interfață:** sistemul de operare pe care va putea rula aplicația este Linux.
* **Cerințe de performanță:** asigurarea unei conexiuni cat mai eficiente atât pentru client și server, cât și pentru baza de date și a unui feedback cât mai rapid pentru client.Existența unui mecanism de excepții pentru prevenirea utilizării necorespunzătoare a aplicației, prin care utilizatorul va fi avertizat de eroarea produsă. (Ex: introducerea unui ID necorespunzător sau a unei cereri incorecte sau nerealizabilă).

**3.3 Teste**

**Notă:** După câteva opțiuni adăugate din meniu, la un moment dat, serverul se blochează și necesită delogarea clientului și oprirea serverului, iar apoi din nou pornirea lui și conectarea clienților(comenzi: make, ./server, ./client). Toate opțiunile din meniu sunt funcționale.

În ordinea opțiuniilor din meniu:

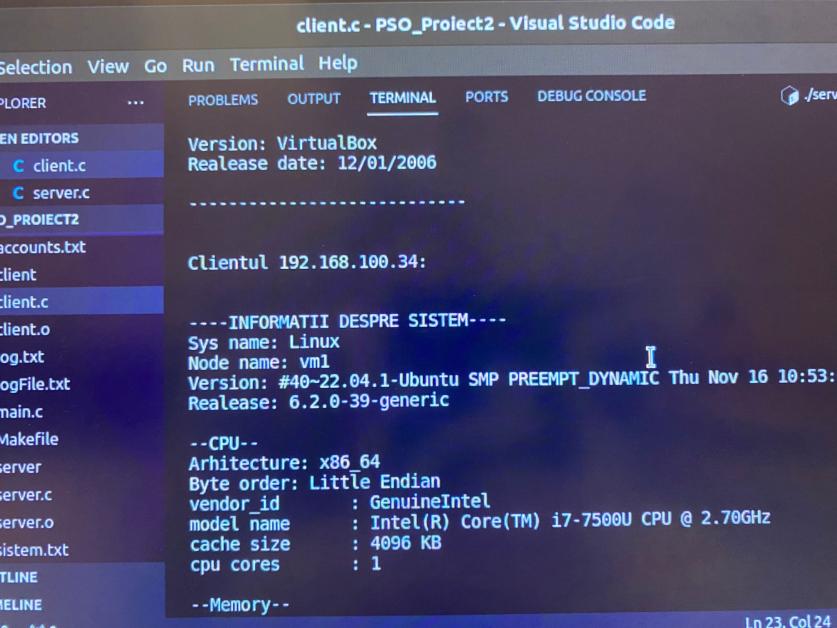
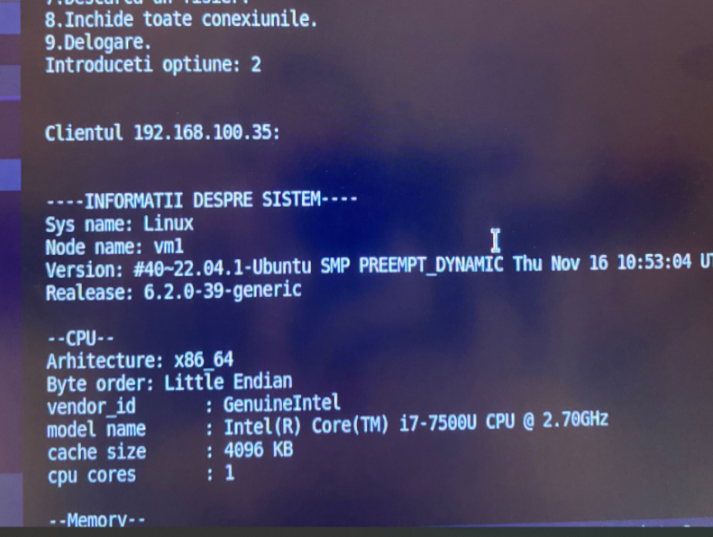
1. Pentru prima opțiune avem :



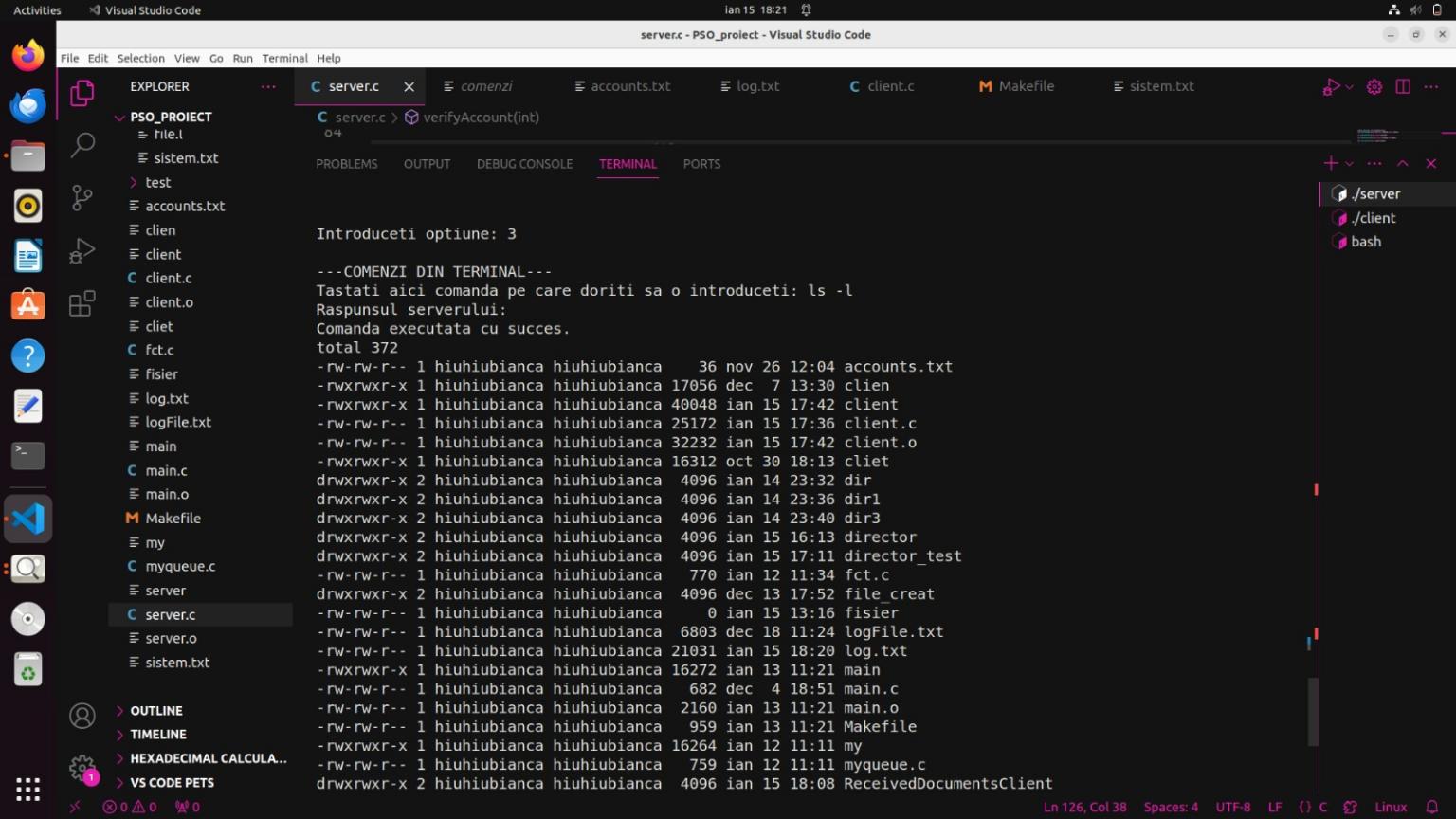
Afișarea clienților care s-au conectat la server-ul pornit. Server-ul trimite comenzi clienților în ordinea conectării lor .

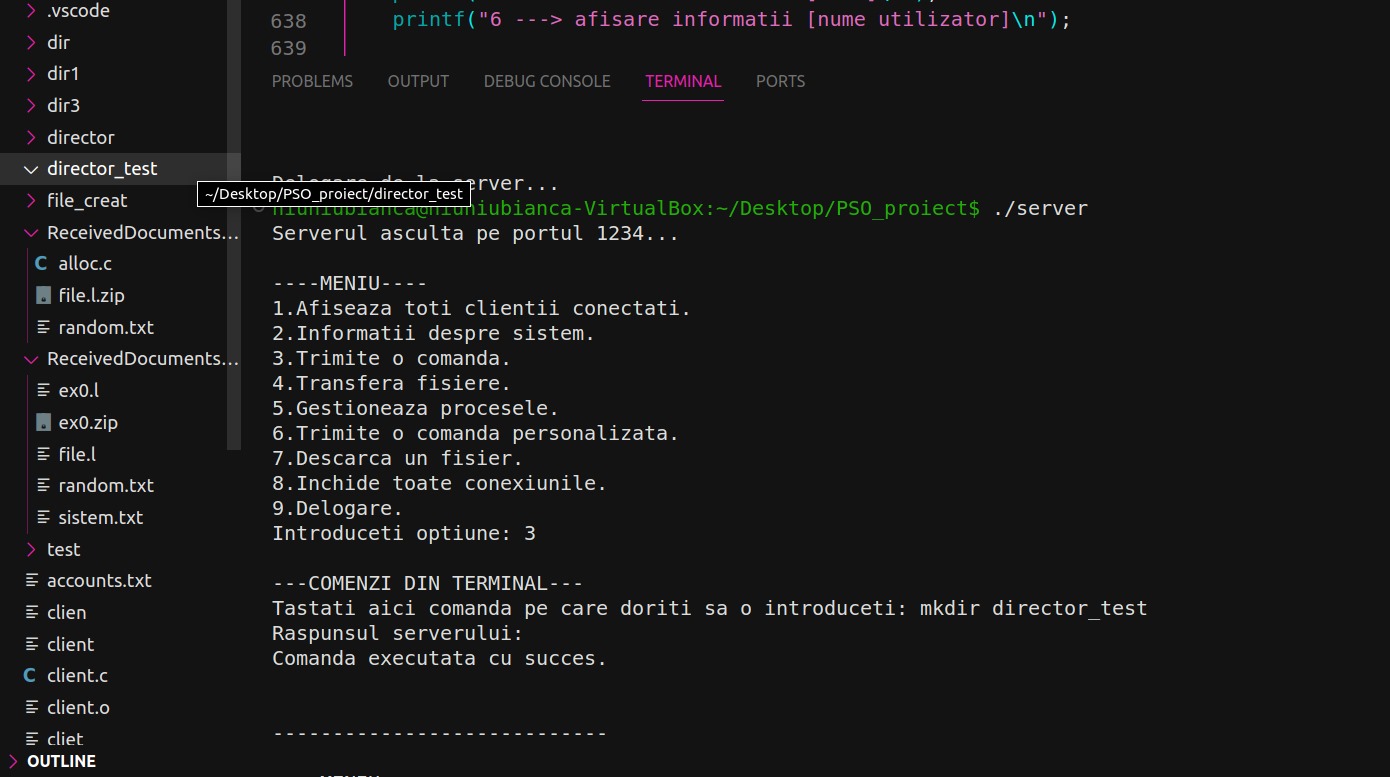
1. Informații despre sistemul clienților :

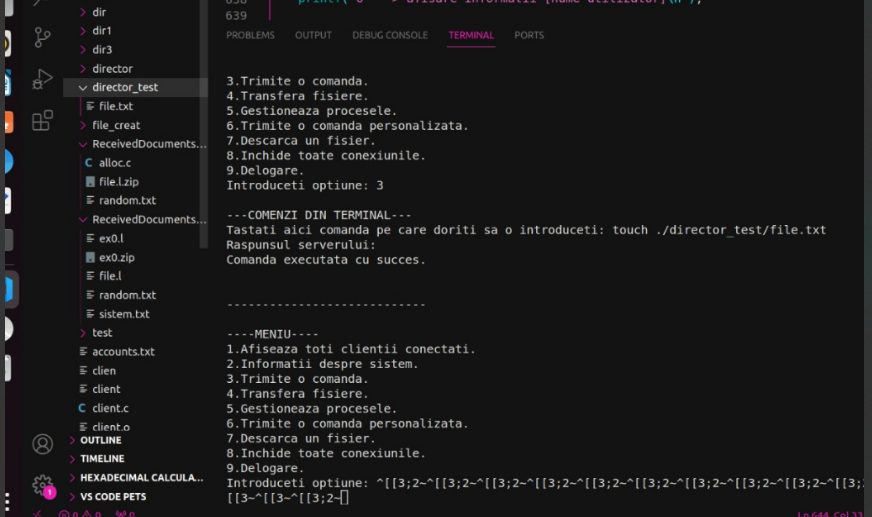
Aceasta se aplică simultan pentru toți clienții autentificați.

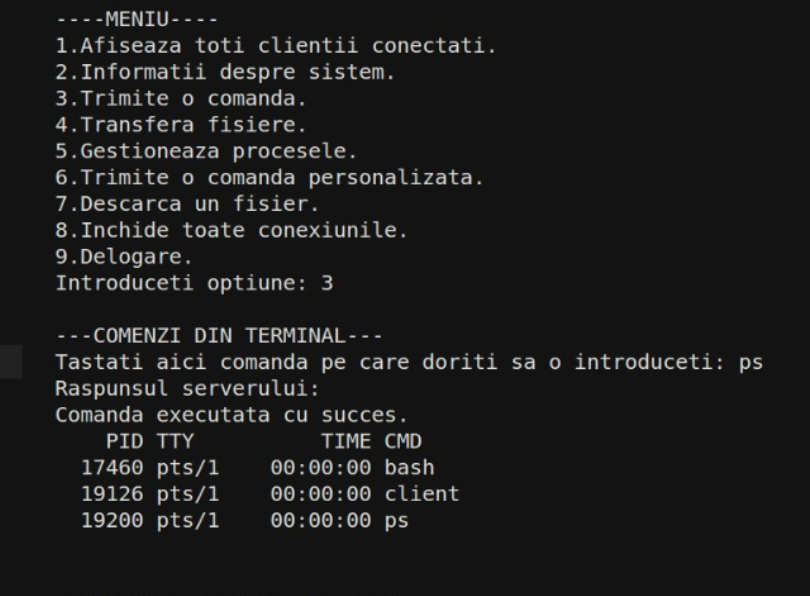


1. Trimiterea de comenzi:



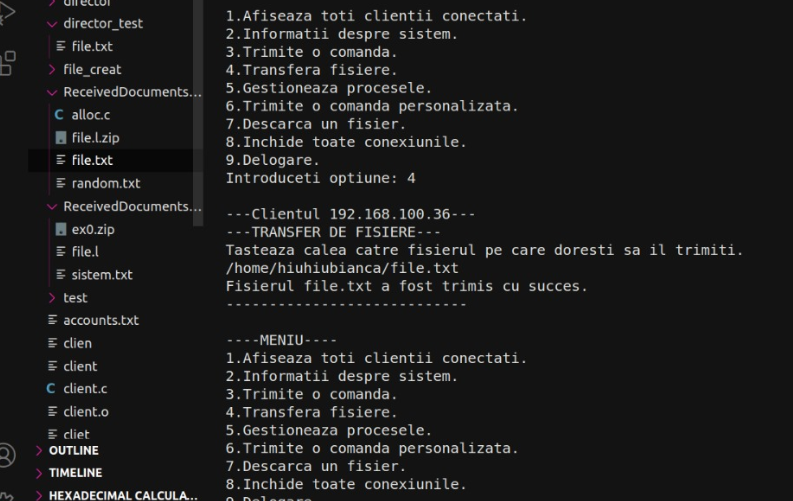




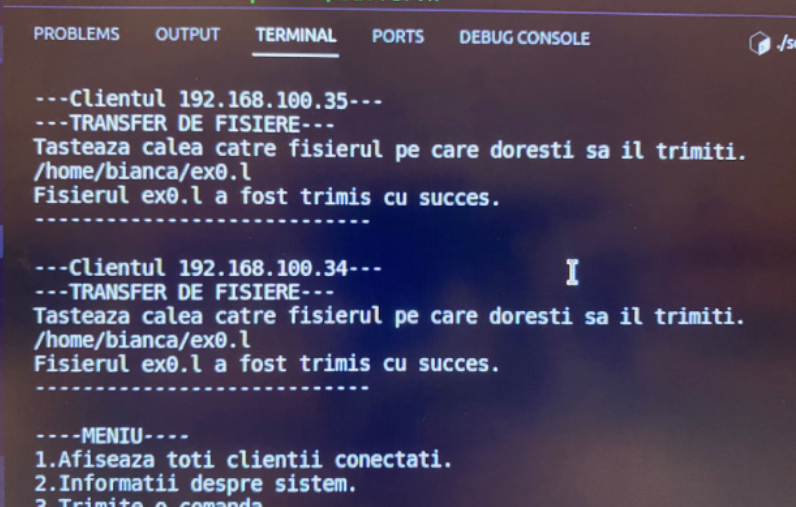


1. Transferul de fișiere:

Pentru un client:

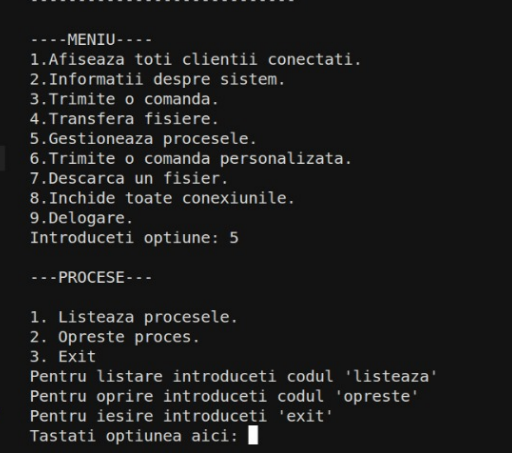


Pentru doi:

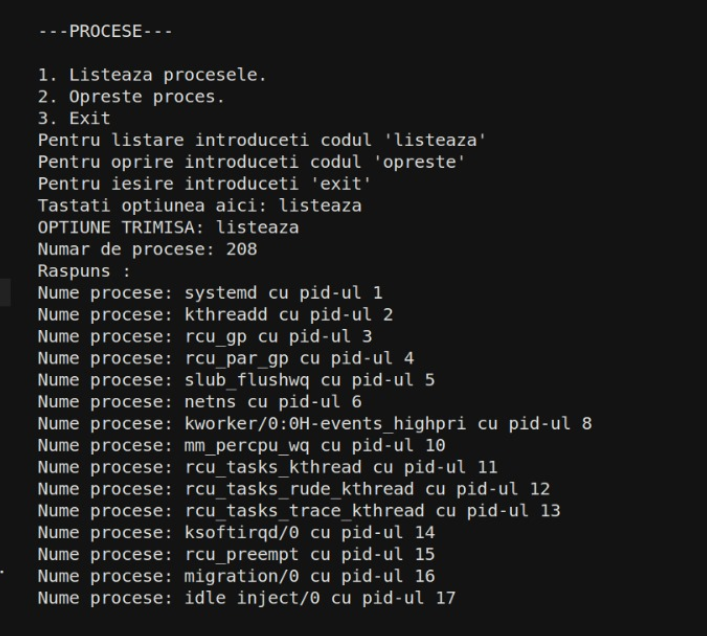


1. Gestionarea proceselor.

Aceasta funcționalitate include un submeniu în care poți alege daca vrei să listezi procesele aflate în execuție la momentul respectiv sau să oprești un proces.

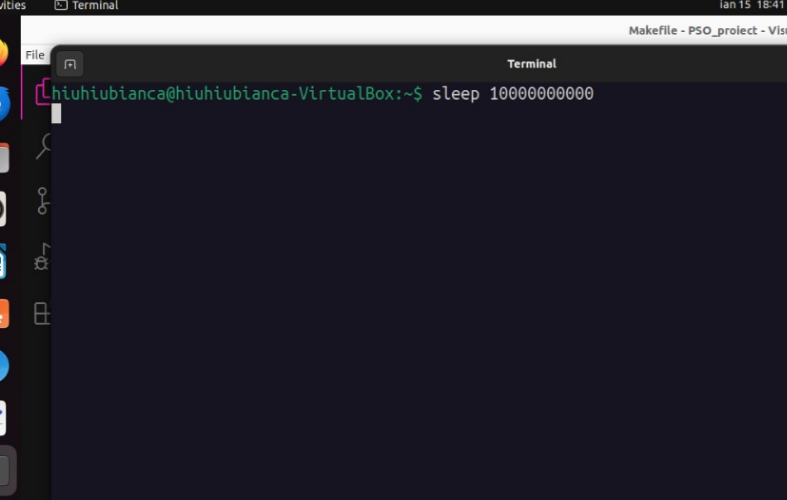


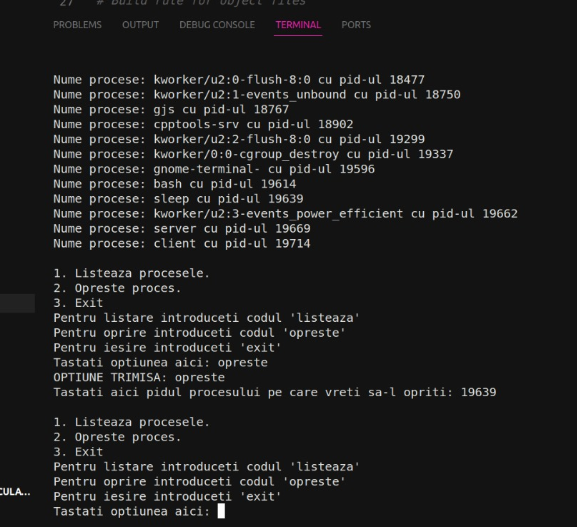
Pentru listare:

z

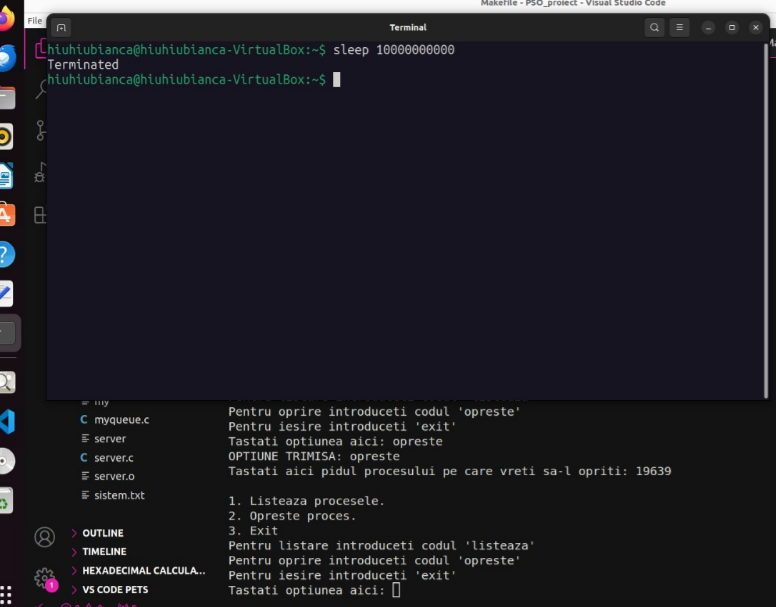
Pentru oprire proces:

Ca exemplu, am creat un sleep într-un terminal linux și voi încerca să-l opresc cu opțiunea pusă la dispoziție.





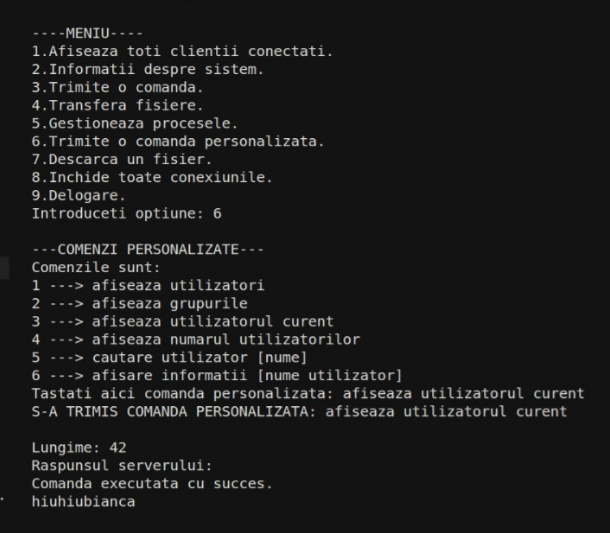
Înainte să-l opresc, am afișat lista cu procese pentru a afla pid-ul procesului sleep pe care vreau să-l opresc.

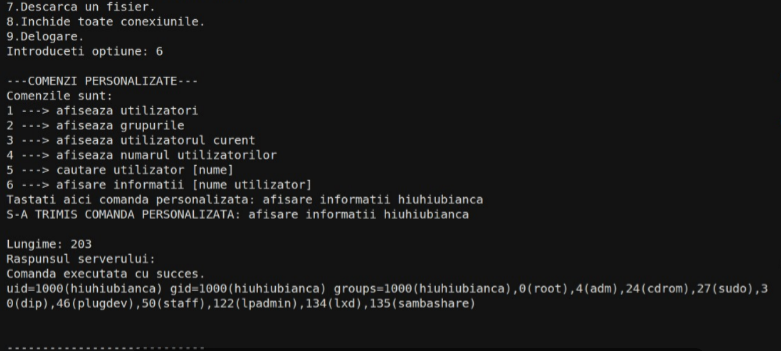


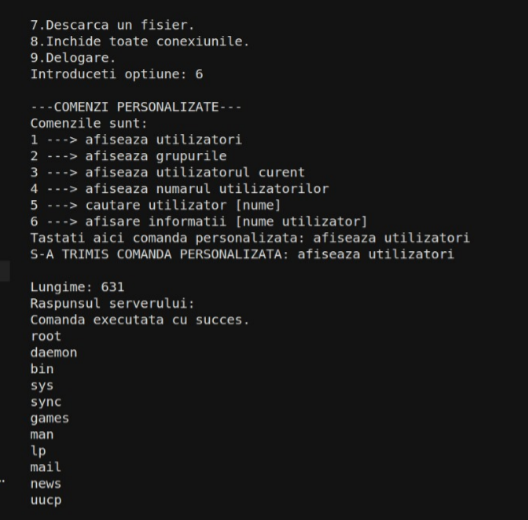
1. Comenzi personalizate.

Comenzi bazate pe utilizatori și grupuri care sunt echivalentul celor din linux mai complexe pentru a lista utilizatorii din sistem, grupurile, utilizatorul curent sau câți utilizatori sunt în sistem. De asemenea, conține și opțiunea pentru căutarea unui user (îi verifică existența) și afișarea informațiilor despre un anumit user.

Exemple:

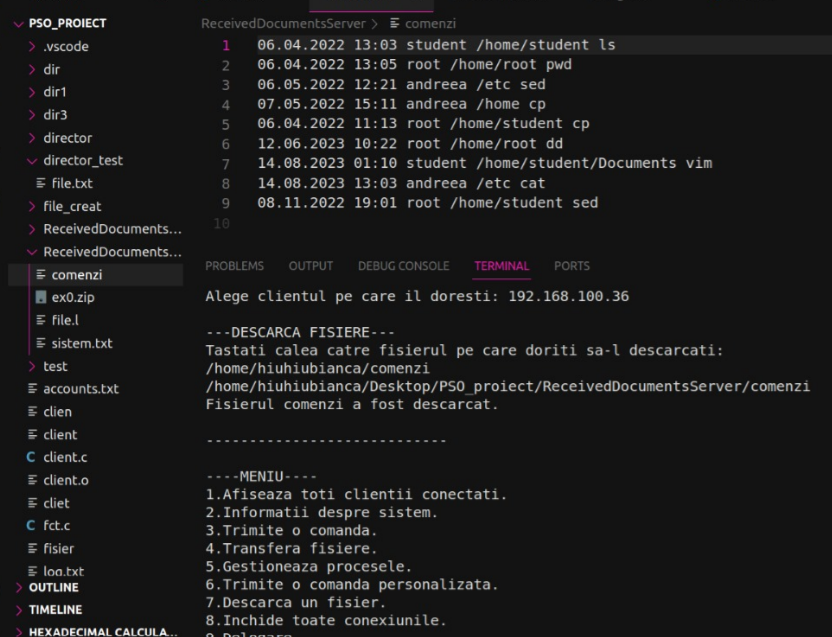






1. Descărcarea unui fișier.

Permite descărcarea unui fișier de pe un client.



De asemenea, clientul se poate deloga de la server dacă tastează ‘exit’

