Universitatea Tehnică a Moldovei

Facultatea Calculatoare Informatică şi Microelectronică

Departamentul Ingineria Software și Automatică

**RAPORT**

Lucrarea de laborator nr. 1

# La disciplina „ Metode și mijloace tehnice de protecție a informației”

**Tema:** Principalele soft-uri destinate protecției calculatorului

A efectuat: st. gr. SI-211 A. Chihai

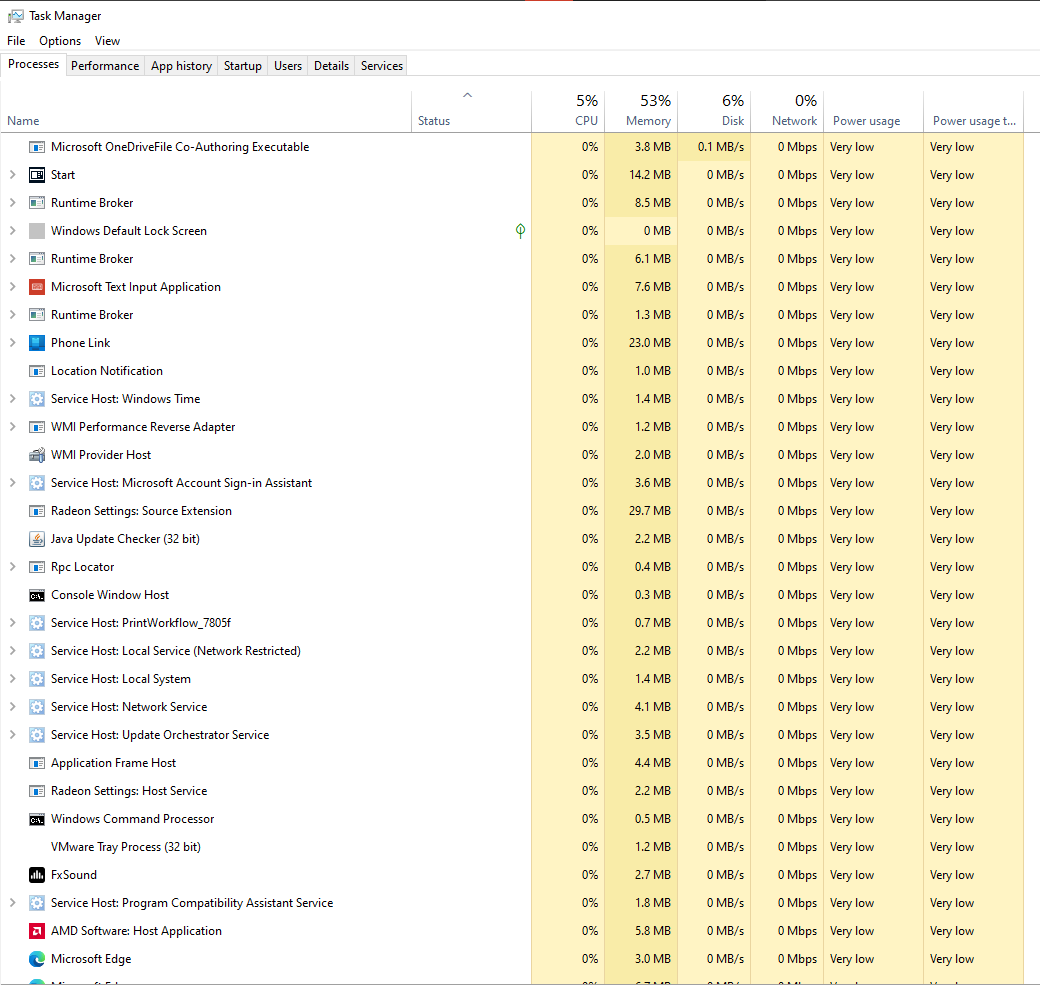
A verificat: V. Coleșnic

Chișinău – 2024

**Scopul lucrării**: Abilități practice de utilizare a soft-ului destinat protecției calculatorului instalat în sistemul de operare Windows.

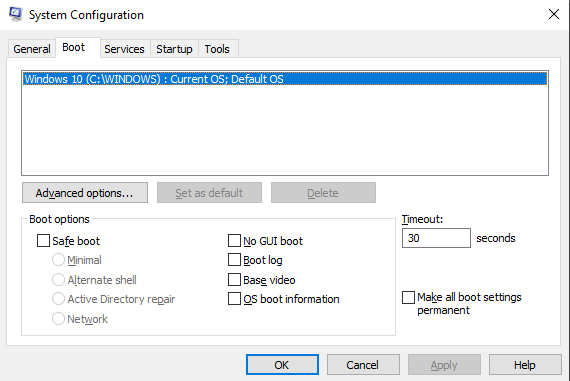
**Sarcina 1: Procese suspecte**

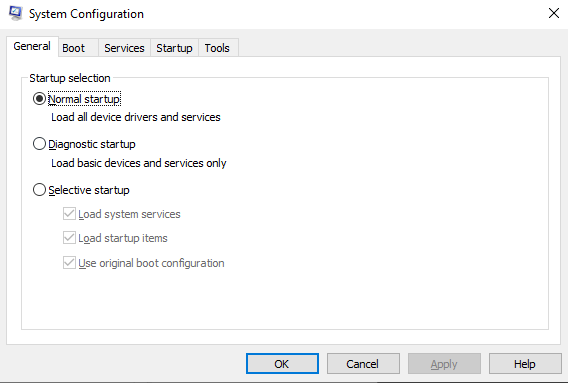
Task Manager este un instrument din Windows care oferă informații despre performanța sistemului și detalii despre procesele active. Acesta permite utilizatorului să monitorizeze și să gestioneze resursele precum CPU, memorie, și rețea. Pentru a identifica un proces suspect, se poate urmări consumul neobișnuit de resurse (CPU sau memorie ridicate) și se pot verifica procesele necunoscute prin căutarea lor online sau utilizând software antivirus pentru detectarea potențialelor amenințări.

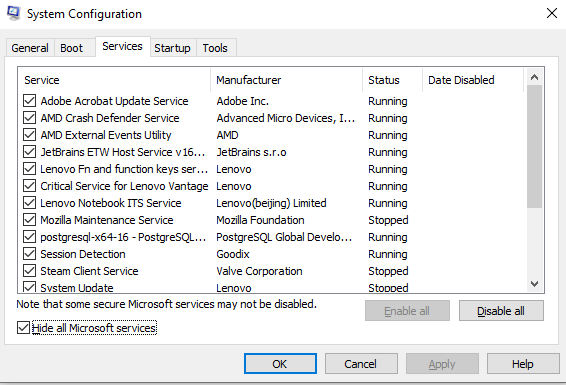


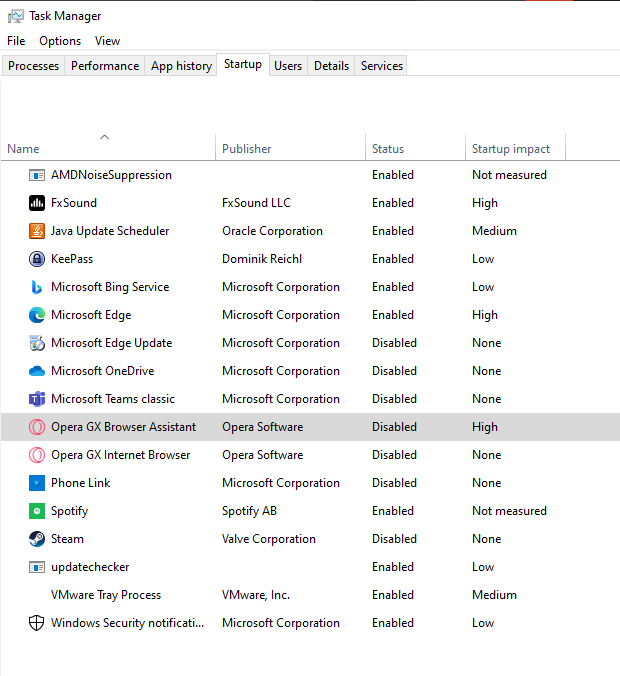
**Sarcina 2. Elemente de Startup (pornire)**

Elementele de Startup sunt aplicații care se pornesc automat atunci când sistemul de operare Windows este pornit. Acestea pot include programe utile, dar și malware sau aplicații nedorite, care pot încetini sistemul. Gestionarea elementelor de Startup prin instrumente ca „msconfig” sau din Task Manager ajută la îmbunătățirea performanței și la reducerea riscului de compromitere a securității.

****

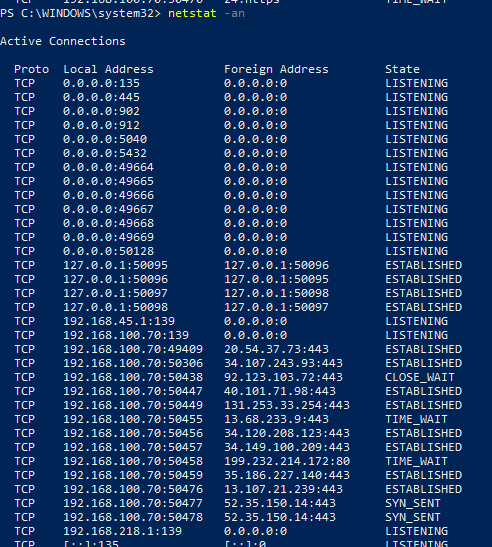


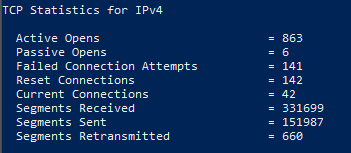


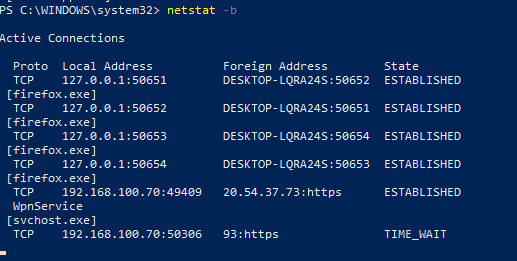


**Sarcina 3 Activitatea rețelei**

Monitorizarea activității rețelei este esențială pentru a detecta traficul neobișnuit, ce poate indica prezența unor aplicații malefice sau încercări de acces neautorizat. Instrumente precum „Network Monitor” din Task Manager sau aplicații dedicate oferă o imagine clară asupra pachetelor de date trimise și primite. Identificarea traficului neobișnuit poate preveni atacuri de tip DDoS, furturi de date sau alte activități malițioase.

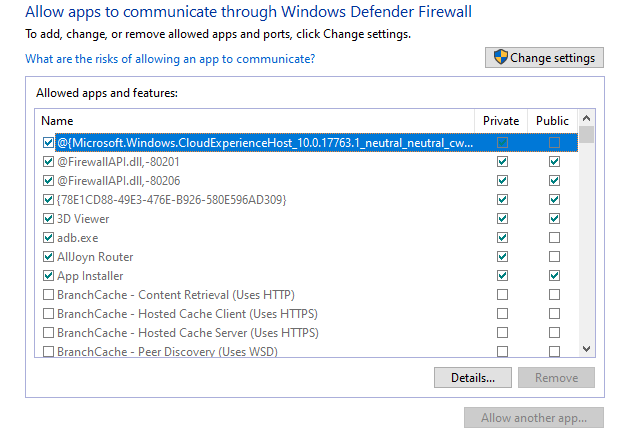
****

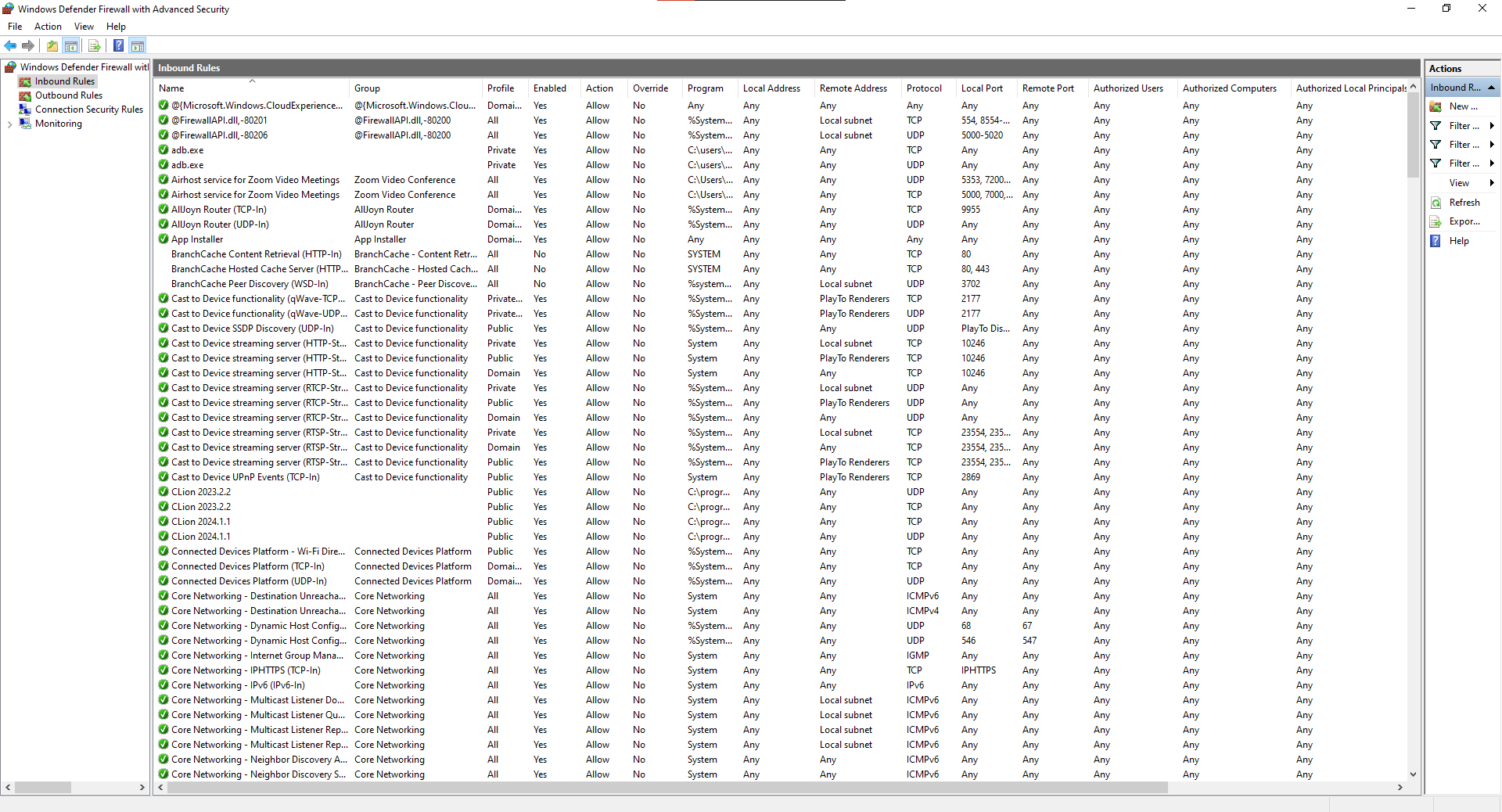
****

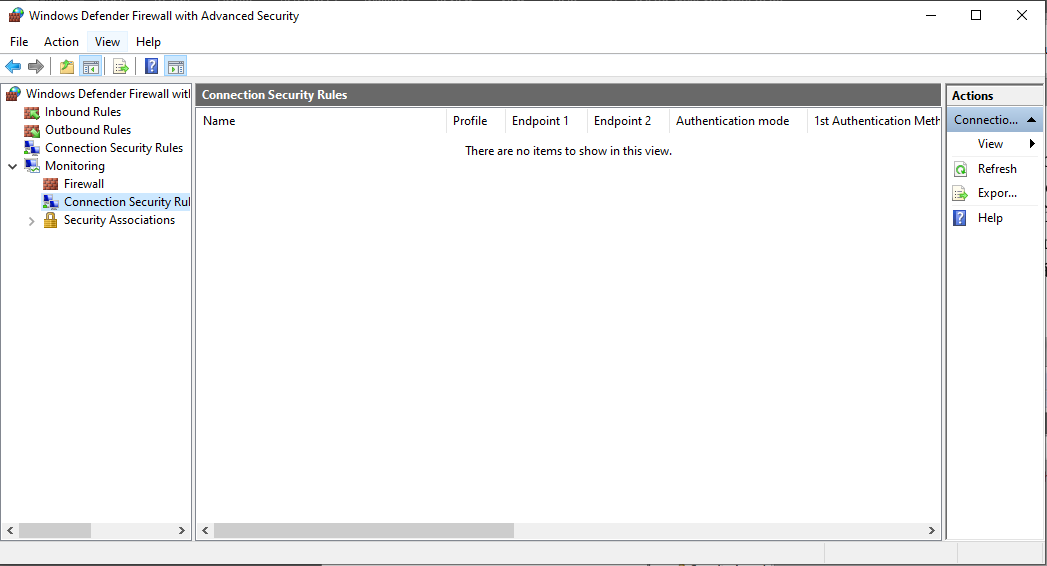
****

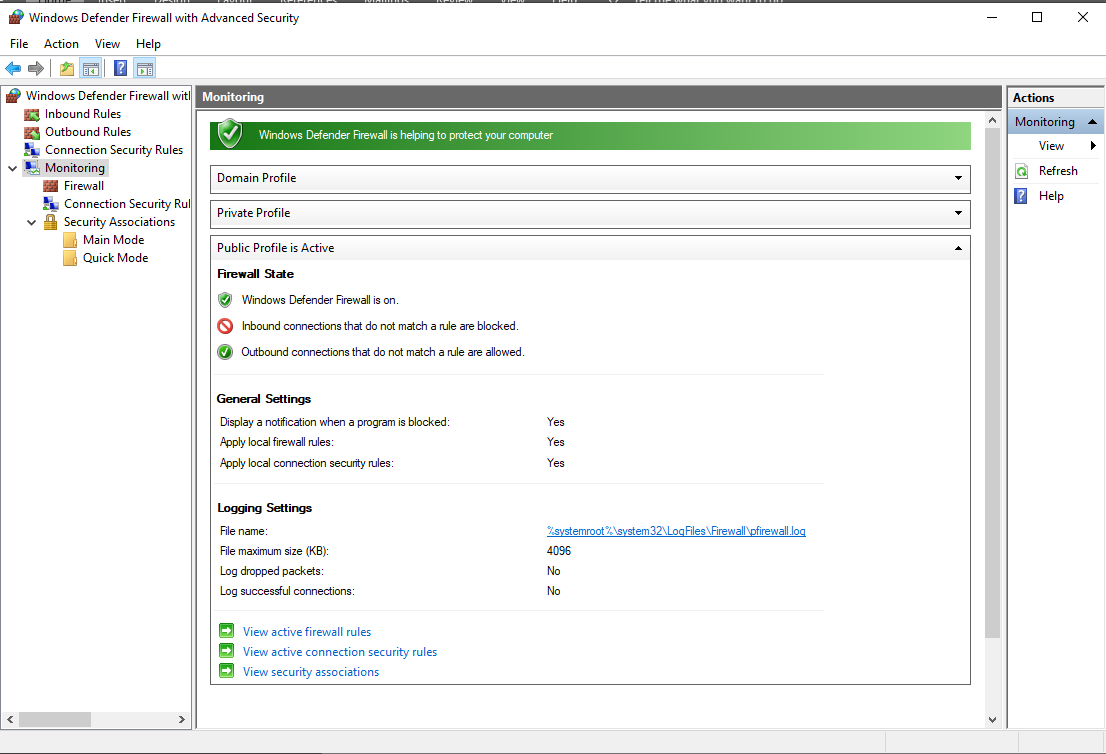
**Sarcina 4. Windows Firewall**

Windows Firewall este o barieră de protecție între computer și rețea. Rolul său este să filtreze traficul de date, permițând doar acele conexiuni care sunt considerate sigure. Firewall-ul poate fi configurat pentru a bloca sau permite aplicații individuale să acceseze internetul. Această funcție previne atacurile externe, dar și scurgerile de date cauzate de programe infectate care încearcă să comunice cu atacatori.

****

****

****

****

**Concluzie:**

Folosind corect instrumentele de securitate din Windows, cum ar fi Task Manager, gestionarea programelor de pornire, monitorizarea traficului de rețea și firewall-ul, poți face computerul mai sigur. Este important să verifici constant procesele și aplicațiile care rulează pentru a identifica orice amenințare. Aceste măsuri nu doar protejează datele tale de atacuri, ci și ajută la menținerea computerului în stare bună, funcționând mai rapid și fără probleme.