Universitatea Tehnică a Moldovei

Facultatea Calculatoare Informatică şi Microelectronică

Departamentul Ingineria Software și Automatică

**RAPORT**

Lucrarea de laborator nr. 1

*Metode și mijloace tehnice de protecție a informației.*

A efectuat: st. gr. SI-211 Chirița Stanislav

A verificat: dr. conf.univ. Colesnic Victor

Chișinău – 2024

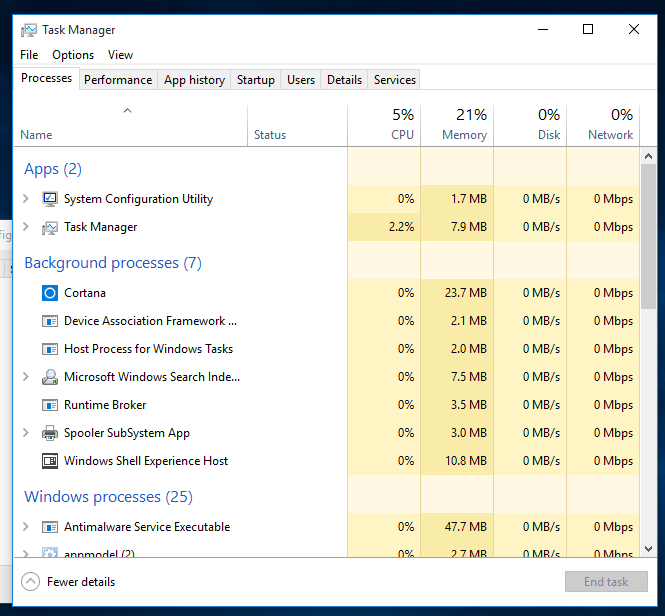
**LUCRAREA DE LABORATOR NR.1**

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

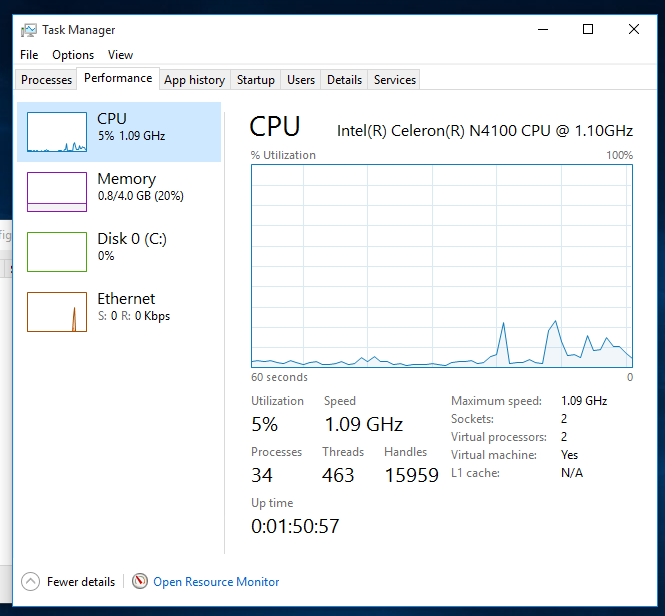
**Scopul lucrării**: Abilități practice de utilizare a soft-ului destinat protecției calculatorului instalat în sistemul de operare Windows.

**1. Sarcina 1: Procese suspecte**

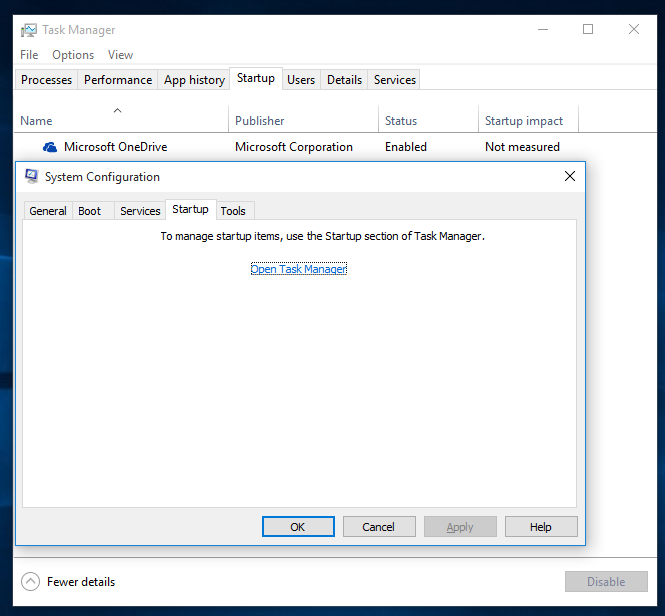
Imaginea arată fereastra „Task Manager” din Windows, afișând procesele active. În partea de sus, se poate observa utilizarea resurselor: 5% CPU și 21% memorie. Două aplicații sunt active: „System Configuration Utility” și „Task Manager”, acestea folosind resurse minime. Mai jos, în secțiunea proceselor de fundal, sunt afișate aplicații precum „Cortana” și „Microsoft Windows Search Indexer”, dar fără un consum semnificativ de resurse. În secțiunea proceselor de Windows, apare „Antimalware Service Executable”, cu o utilizare notabilă de memorie. Fereastra oferă o imagine generală asupra stării curente a sistemului.

Figura 1 – Task Manager

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

Figura 2 - Performance

În imagine se vede din nou „Task Manager”, dar de această dată pe tab-ul „Performance”. Verific utilizarea procesorului, care este un Intel Celeron N4100, și observ că e la 5% utilizare, cu o viteză de 1.09 GHz. Am deschise 34 de procese, 463 de fire (threads) și 15959 de handle-uri. Utilizarea memoriei este la 20%, adică 0.8 GB din 4 GB disponibili. Discul nu este folosit, iar conexiunea Ethernet nu are trafic. În partea de jos văd că sistemul a fost pornit de aproximativ o oră și 50 de minute. Totul pare să funcționeze bine și resursele sunt utilizate moderat.

Figura 3 – Start Up

În această imagine, am deschis „Task Manager” pe tab-ul „Startup” pentru a vedea aplicațiile care se pornesc automat odată cu Windows. În listă apare doar „Microsoft OneDrive”, publicat de Microsoft Corporation, care este activat la pornire, dar impactul său asupra timpului de pornire nu este măsurat. În fundal, am și fereastra „System Configuration” deschisă, pe tab-ul „Startup”, unde mi se spune că pentru a gestiona elementele de pornire trebuie să folosesc secțiunea corespunzătoare din „Task Manager”, cu un link care îmi permite să accesez rapid acest tab. Totul pare destul de simplu de gestionat din această interfață.

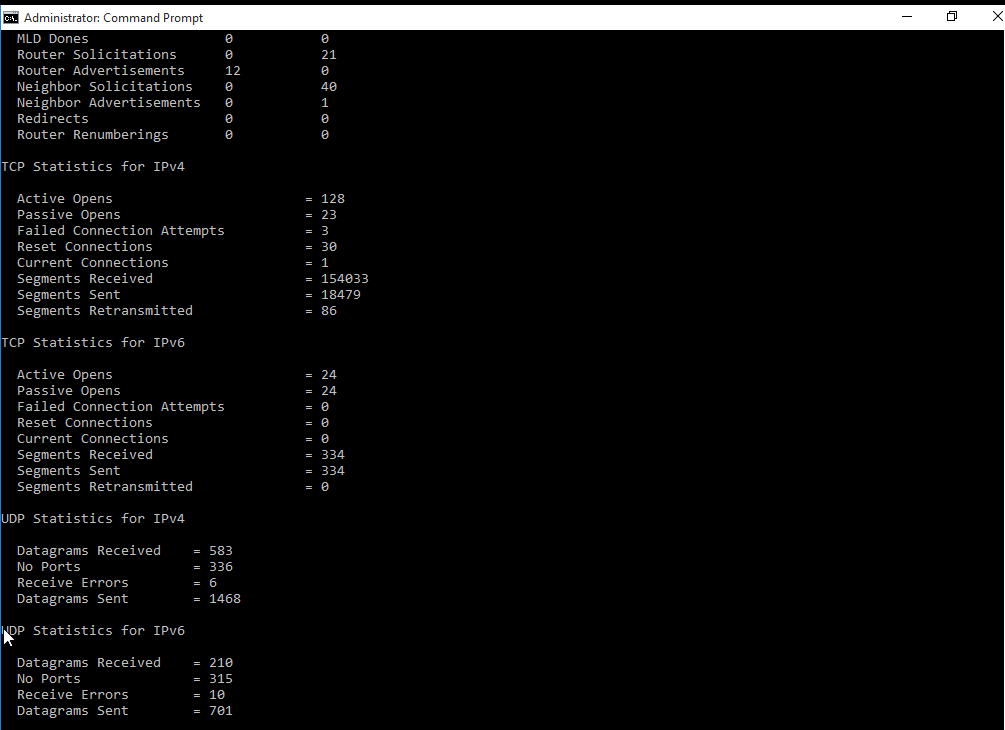
# **Sarcina 3 Activitatea rețelei**

**Comanda** netstat -b afișează conexiunile active la un anumit moment dat, incluzând informații despre protocolul utilizat, adresele IP locale și externe, starea conexiunii și procesul care a inițiat conexiunea.

**În cazul acesta:**

* **O singură conexiune activă:** Se observă o singură conexiune TCP stabilită către adresa IP externă a92-123-103-80 pe portul HTTPS (443).
* **Procesul inițiator:** Conexiunea a fost inițiată de procesul SearchUI.exe, care este asociat cu funcția de căutare a Windows.

**Comanda** netstat -s furnizează statistici detaliate despre traficul de rețea, cum ar fi numărul de pachete trimise și primite, erori, fragmentare etc.

Figura 4 - netstat

Imaginea prezintă o fereastră de comandă (Command Prompt) într-un sistem de operare Windows, mai precis în directorul C:\Windows\system32. În această fereastră a fost executată comanda netstat -b.

**Comanda** netstat -b este utilizată pentru a afișa o listă a tuturor conexiunilor de rețea active pe un computer la un moment dat. Ea furnizează informații detaliate despre fiecare conexiune, cum ar fi:

* **Protocolul** utilizat (în acest caz, TCP - Transmission Control Protocol).
* **Adresa IP locală** și **portul** de pe care computerul inițiază conexiunea.
* **Adresa IP externă** și **portul** la care se conectează computerul.
* **Starea conexiunii** (în acest caz, ESTABLISHED - adică conexiunea este activă și datele pot fi transferate în ambele sensuri).
* **Procesul** care a inițiat conexiunea (în acest caz, SearchUI.exe, care este asociat cu funcția de căutare a Windows).

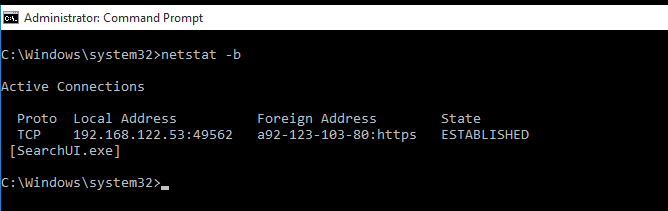
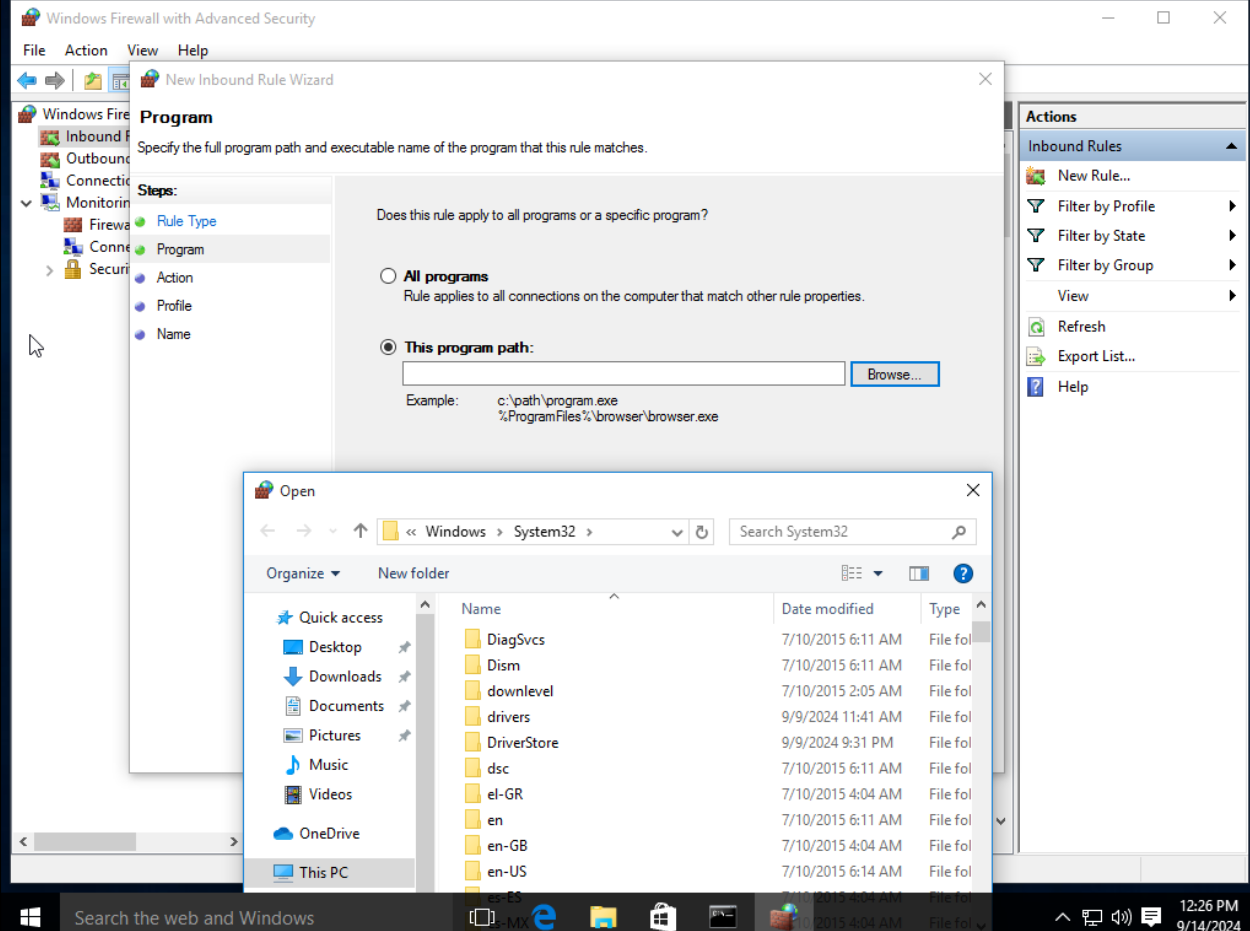
****

Figura 5 – netstat -b

**Sarcina 4. Windows Firewall**



## Figura 6 – Firewall

## Cum să adaugi o regulă nouă pentru un program în Windows Firewall

**Imaginea pe care o vezi reprezintă un pas crucial în procesul de creare a unei noi reguli în Windows Firewall.** Această regulă va determina modul în care Windows Firewall va gestiona conexiunile către sau de la un anumit program.

**Iată o explicație pas cu pas a ceea ce vezi în imagine și cum să procedezi pentru a adăuga o regulă nouă:**

1. **Accesează Windows Firewall:**
   * Deschideți "Panoul de control" și apoi accesați "Windows Firewall".
   * Căutați opțiunea "Setări avansate".
2. **Alegeți tipul de regulă:**
   * În fereastra care se deschide, veți avea opțiunea de a crea o regulă pentru conexiuni **intrante** (adică conexiuni către computer) sau **ieșite** (conexiuni de la computer).
   * În imaginea ta, este selectată opțiunea "Inbound Rules" (Reguli de intrare).
3. **Pornește "New Inbound Rule Wizard":**
   * Apasă pe butonul "New Rule..." pentru a iniția procesul de creare a unei noi reguli.
4. **Specifică programul:**
   * În primul pas al vrăjitorului, vei fi întrebat dacă regula se aplică tuturor programelor sau unui program specific.
   * Dacă vrei să creezi o regulă pentru un program anume, selectează opțiunea "This program".
   * În câmpul "This program path", introduce calea completă către executabilul programului. Poți face clic pe butonul "Browse" pentru a naviga și a selecta fișierul.
   * **Important:** Calea trebuie să fie completă și corectă. De exemplu, C:\Program Files\MyProgram\myprogram.exe.
5. **Continuă cu următorii pași:**
   * După ce ai specificat programul, vrăjitorul te va ghida prin mai mulți pași, unde vei putea configura alte aspecte ale regulii, cum ar fi:
     + **Acțiunea:** Ce se întâmplă cu conexiunile care se potrivesc regulii (permitere, blocare, solicitare de acțiune etc.)
     + **Profile:** În ce profiluri (de exemplu, domeniu, privat, public) se aplică regula
     + **Porturi:** Dacă vrei să specifici anumite porturi
     + **Scopuri:** Dacă vrei să filtrezi după scopul conexiunii (de exemplu, web server, e-mail etc.)

**Concluzie:** În urma analizei efectuate, se constată că sistemul de operare Windows analizat prezintă o configurație de securitate relativ bună. Procesele active nu indică prezența de malware, iar firewall-ul este configurat pentru a bloca conexiunile neautorizate. Cu toate acestea, se recomandă o evaluare mai amănunțită a setărilor firewall-ului și actualizarea regulată a sistemului de operare și a software-urilor de securitate pentru a preveni potențiale vulnerabilități. De asemenea, este important ca utilizatorul să fie conștient de cele mai bune practici de securitate cibernetică, cum ar fi evitarea deschiderii fișierelor sau a link-urilor suspecte.