**MINISTERUL EDUCAŢIEI ȘI CERCETĂRII AL REPUBLICII MOLDOVA**

**Universitatea Tehnică a Moldovei**

**Facultatea Calculatoare, Informatică şi Microelectronică**

**Departamentul Ingineria Software și Automatică**

**Programul de studii: Securitatea informațională**

**Aplicație software pentru interceptarea și analiza traficului de rețea în timp real**

|  |  |  |
| --- | --- | --- |
| **Student(ă):** | **\_\_\_\_\_\_\_\_\_\_\_\_\_** | **Chirița Stanislav, SI-211** |
| **Coordonator de licență:** | **\_\_\_\_\_\_\_\_\_\_\_\_\_** | **Masiutin Maxim, asist.univ.** |
| **Coordonator universitate:** | **\_\_\_\_\_\_\_\_\_\_\_\_\_** | **Bulai Rodica, lector universitar** |

**Chişinău, 2025**

# DECLARAȚIA DE ORIGINALITATE

Subsemnatul, Chirița Stanislav, declar pe proprie răspundere, că lucrarea de față este rezultatul muncii mele, realizată pe baza propriilor cercetări și pe baza informațiilor obținute din surse care au fost citate și indicate conform normelor etice în note și în bibliografie.

Declar că lucrarea nu a mai fost prezentată sub această formă la nici o instituție de învățământ superior în vederea obținerii titlului de inginer licențiat.

*Semnătura autorului \_\_\_\_\_\_\_\_\_\_\_*

CUPRINS

[DECLARAȚIA DE ORIGINALITATE 2](#_Toc198653524)

[ABREVIERI 4](#_Toc198653525)

[INTRODUCERE 5](#_Toc198653526)

[1 ANALIZA DOMENIULUI DE STUDIU 6](#_Toc198653527)

[**1.1 Importanța temei** 6](#_Toc198653528)

[**1.2 Sisteme similare cu proiectul realizat** 7](#_Toc198653529)

[**1.3 Scopul, obiectivele și cerințele sistemului** 11](#_Toc198653530)

[**2.1 Descrierea comportamentală a sistemului** 14](#_Toc198653531)

[2.1.1 Imaginea generală asupra sistemului 15](#_Toc198653532)

[2.1.2 Modelarea vizuală a fluxurilor 16](#_Toc198653533)

[**2.1.3 Descrierea scenariilor de utilizare a aplicaţiei** 18](#_Toc198653534)

[**2.2 Descrierea structurală a sistemului** 19](#_Toc198653535)

[2.2.1 Descrierea structurii statice a sistemului 20](#_Toc198653536)

[2.2.2 Relatiile de dependență între componentele sistemului 21](#_Toc198653537)

[3.1 Structura sistemului 23](#_Toc198653538)

[3.2 Integrarea serviciilor externe 24](#_Toc198653539)

[**3.3 Implementarea cerințelor funcționale** 25](#_Toc198653540)

[**3.4 Arhitectura modulară a aplicației** 26](#_Toc198653541)

[**3.5 Modelul de date și structura bazei de date** 27](#_Toc198653542)

[**3.6 Fluxul de execuție în aplicație** 28](#_Toc198653543)

[**3.7 Sistemul de alertare și detectare a comportamentelor suspecte** 29](#_Toc198653544)

[**3.8 Generarea de rapoarte și vizualizări** 30](#_Toc198653545)

[4 DOCUMENTAREA SISTEMULUI 33](#_Toc198653546)

[**4.1 Interfața de autentificare** 33](#_Toc198653547)

[**4.3 Interacțiunea cu baza de date** 34](#_Toc198653548)

[**4.4 Interfața principală a aplicației** 35](#_Toc198653549)

[**4.5 Capturarea traficului de rețea** 35](#_Toc198653550)

[5 Analiza de risc, evaluarea și impactul proiectului 37](#_Toc198653551)

[În cadrul dezvoltării și testării modulului *PacketSentinel*, componentă centrală a aplicației *Sentinel Traffic Analyzer*, au fost identificate o serie de riscuri tehnice și de utilizare, care pot influența performanța, securitatea și etica utilizării aplicației. Acest capitol are ca scop prezentarea riscurilor întâmpinate, a soluțiilor aplicate, precum și evaluarea funcționalităților realizate și impactul proiectului asupra formării academice, cercetării și carierei profesionale. 37](#_Toc198653552)

[**5.1 Riscuri tehnice** 37](#_Toc198653553)

[**5.6 Contribuția în activitatea de cercetare** 38](#_Toc198653554)

[BIBLIOGRAFIE 39](#_Toc198653555)

# ABREVIERI

**IPS (Intrusion Prevention System)** – Sistem de prevenire a intruziunilor

**IDS (Intrusion Detection System)** – Sistem de detecție a intruziunilor

**SIEM (Security Information and Event Management)** – Soluție integrată pentru gestionarea informațiilor și evenimentelor de securitate

**GUI (Graphical User Interface)** – Interfață grafică pentru utilizator

**HTTP (Hypertext Transfer Protocol)** – Protocol pentru transferul de date în format hipermedia pe web

**DNS (Domain Name System)** – Sistem distribuit care traduce numele de domeniu în adrese IP

**SSL (Secure Sockets Layer)** – Protocol criptografic pentru securizarea comunicațiilor pe internet (în prezent înlocuit în mare parte de TLS – Transport Layer Security)

**TCP (Transmission Control Protocol)** – Protocol de transport orientat pe conexiune

**UDP (User Datagram Protocol)** – Protocol de transport fără conexiune

**IP (Internet Protocol)** – Protocol de rutare a pachetelor de date în rețea

**MAC (Media Access Control)** – Adresă fizică unică a interfeței de rețea

**ARP (Address Resolution Protocol)** – Protocol de rezolvare a adreselor IP în adrese MAC

**ICMP (Internet Control Message Protocol)** – Protocol pentru mesaje de control și diagnostic (ex. ping)

**DHCP (Dynamic Host Configuration Protocol)** – Protocol pentru alocarea automată a adreselor IP

**MITM (Man-In-The-Middle)** – Tip de atac ce interceptează comunicația dintre două părți

**DoS (Denial of Service)** – Atac care urmărește blocarea unui serviciu

**DDoS (Distributed Denial of Service)** – Atac DoS lansat din mai multe locații simultan

**TLS (Transport Layer Security)** – Protocol criptografic pentru comunicații securizate, succesorul SSL

**SHA (Secure Hash Algorithm)** – Familie de algoritmi de hash criptografic

**MD5 (Message Digest 5)** – Algoritm de hash criptografic, considerat vulnerabil

**PCAP (Packet Capture)** – Format standard pentru fișiere de captură de trafic de rețea

# INTRODUCERE

În lumea digitală actuală, rețelele de calculatoare joacă un rol central în funcționarea instituțiilor, a întreprinderilor și a societății în ansamblu. Din ce în ce mai multe procese critice se bazează pe infrastructurile IT, iar fluxurile de date devin din ce în ce mai dense, variate. În acest context, protejarea traficului de rețea și asigurarea integrității comunicațiilor reprezintă provocări majore în materie de securitate cibernetică.

Lucrarea de față se concentrează pe proiectarea și implementarea unei aplicații software pentru interceptarea și analiza traficului de rețea în timp real, în vederea identificării comportamentelor suspecte, a posibilelor atacuri și a activităților anormale în cadrul unei rețele locale sau extinse. Aplicația asigură o interfață grafică intuitivă (GUI) prin intermediul căreia utilizatorul poate iniția sesiuni de captură, vizualiza pachetele interceptate, interpreta informații din diferite protocoale (TCP, UDP, HTTP, DNS etc.) și poate genera rapoarte și alerte bazate pe criterii predeterminate.

Motivul alegerii acestei teme provine din nevoia tot mai mare de a înțelege și contracara în timp util amenințările cibernetice. Având în vedere că atacurile de tip phishing, malware, port scanning sau DoS devin din ce în ce mai frecvente, implementarea unor soluții proactive de monitorizare a traficului devine practic pentru prevenirea incidentelor și protejarea datelor. Acest proiect contribuie în această direcție prin oferirea unui instrument capabil să ofere o imagine vizibilă asupra activității rețelei, inclusiv prin evidențierea protocoalelor utilizate, a surselor de trafic și a volumelor de date prelucrate.

Implementarea aplicației implică includerea tehnologiilor open-source și a metodelor eficiente de analiză, cum ar fi utilizarea bibliotecii Scapy pentru capturarea pachetelor în Python, prelucrarea și salvarea datelor relevante în format PCAP și JSON și implementarea unui sistem personalizat de detectare a anomaliilor bazat pe reguli. O parte importantă este capacitatea de a salva sesiuni și de a genera rapoarte PDF cu statistici detaliate.

Lucrarea evidențiază, de asemenea, procesul de proiectare modulară a aplicației și abordarea orientată spre utilizator, astfel încât sistemul să fie ușor de utilizat, dar suficient de flexibil pentru a putea fi extins în viitor. Prin această contribuție, se dorește oferirea unui exemplu concret de aplicație practică în domeniul securității cibernetice, care poate fi utilizată atât în scop educațional, cât și ca bază pentru soluții mai complexe de tip IDS (Intrusion Detection System) sau SIEM (Security Information and Event Management).

În concluzie, această lucrare se înscrie în eforturile curente de creștere a rezilienței rețelelor informatice și de susținere a securității infrastructurilor digitale, prin realizarea unei aplicații funcționale, bine documentate și cu un impact practic real în domeniul monitorizării traficului de rețea.

# 1 ANALIZA DOMENIULUI DE STUDIU

În realizarea proiectului propus, s-a acordat o atenție deosebită procesului de capturare și analiză a traficului de rețea, utilizând o serie de tehnologii și instrumente consacrate în domeniul securității cibernetice. Activitatea s-a concentrat pe înțelegerea funcționării protocoalelor de rețea și a mecanismelor prin care pachetele de date pot fi interceptate, clasificate și evaluate în timp real.

Pentru a construi o bază solidă în procesul de dezvoltare a aplicației, au fost analizate și comparate diverse soluții existente, precum Wireshark, tcpdump, Zeek și Suricata. Acestea au oferit repere importante în ceea ce privește abordările utilizate în captarea și interpretarea traficului, precum și în gestionarea volumului ridicat de date ce circulă prin rețele moderne. Prin testarea funcționalităților acestor instrumente, au fost identificate metode eficiente de prelucrare a informațiilor, dar și limitări care au stat la baza motivării dezvoltării unui instrument propriu.

Aplicația propusă în cadrul acestei lucrări a fost proiectată pornind de la nevoia de a crea o soluție personalizabilă, accesibilă și ușor de utilizat, care să permită monitorizarea activității din rețea, detectarea anomaliilor și înregistrarea evenimentelor relevante. Accentul a fost pus pe flexibilitate și extensibilitate, cu posibilitatea de adăugare a unor componente noi, precum sistemele de alertare sau modulele de export și raportare.

În urma procesului de testare și validare, s-a demonstrat că implementarea unei aplicații proprii aduce beneficii semnificative în ceea ce privește înțelegerea fluxurilor de date, localizarea surselor de trafic suspect și evidențierea tiparelor de comunicație. În perspectivă, soluția poate fi extinsă prin integrarea unor funcții avansate de analiză comportamentală, inclusiv prin utilizarea unor algoritmi de învățare automată pentru detecția proactivă a riscurilor.

## **1.1 Importanța temei**

În contextul digitalizării accelerate a proceselor economice, administrative și sociale, rețelele de calculatoare au devenit coloana vertebrală a infrastructurilor moderne. Odată cu această expansiune, au crescut și riscurile asociate traficului de date, iar protecția rețelelor a devenit o preocupare centrală în domeniul securității cibernetice. Implementarea unui sistem capabil să intercepteze și să analizeze traficul de rețea oferă posibilitatea de a observa în timp real comportamentul comunicațiilor și de a identifica activitățile neobișnuite care pot semnala tentative de compromitere, abuzuri sau defecțiuni.

Monitorizarea atentă a fluxurilor de date permite nu doar identificarea rapidă a anomaliilor, dar și adoptarea unor măsuri de remediere înainte ca un incident să devină critic. Prin evidențierea comportamentelor suspecte ale utilizatorilor, dispozitivelor sau aplicațiilor, se pot preveni atacuri precum exfiltrarea de date, escaladarea privilegiilor, scanările de porturi sau atacurile de tip denial-of-service. Totodată, analiza traficului contribuie la optimizarea utilizării resurselor rețelei, ajutând la identificarea segmentelor congestionate sau a configurărilor ineficiente.

Importanța acestei teme derivă și din necesitatea de a respecta reglementările naționale și internaționale privind protecția datelor, auditul rețelelor și trasabilitatea evenimentelor digitale. Organizațiile sunt din ce în ce mai supuse verificărilor privind conformitatea cu standarde precum ISO/IEC 27001, NIS2 sau GDPR, iar un sistem eficient de monitorizare a traficului joacă un rol important în acest sens.

Lucrarea de față propune o abordare aplicativă, axată pe compararea unor instrumente consacrate (precum Wireshark, tcpdump, Zeek și Suricata) în vederea identificării limitărilor acestora, precum și pe proiectarea și implementarea unei soluții proprii care să ofere o detecție mai rapidă, mai clară și mai ușor de integrat într-un mediu operațional. În acest mod, cercetarea contribuie la dezvoltarea de metode și instrumente moderne în sprijinul securității rețelelor informatice.

## **1.2 Sisteme similare cu proiectul realizat**

În domeniul securității informatice, au fost dezvoltate numeroase aplicații destinate supravegherii și interpretării traficului de rețea. Aceste soluții sunt folosite atât în scopuri de monitorizare pasivă, cât și pentru identificarea în timp util a activităților neobișnuite sau potențial periculoase. Printre cele mai cunoscute și utilizate instrumente în acest sens se numără **Wireshark**, un software consacrat pentru inspecția detaliată a pachetelor transmise în cadrul rețelelor IP.

Wireshark oferă posibilitatea de a captura pachetele de date și de a le examina în profunzime, permițând utilizatorilor să aplice filtre personalizate pentru o analiză direcționată. Această funcționalitate este deosebit de utilă pentru depanarea problemelor de conectivitate, analiza performanței aplicațiilor sau investigarea traficului neobișnuit. Nivelul de detaliu disponibil este ridicat, iar interfața grafică ajută la structurarea datelor într-un mod accesibil. În **figura 1.1**, este ilustrat un exemplu de interfață Wireshark cu pachete capturate și decodificate la nivel de protocol.

Cu toate avantajele sale, Wireshark prezintă și unele limite, mai ales în situațiile în care este necesară o reacție rapidă la incidente. Procesul de analiză este predominant manual și poate deveni dificil de gestionat în rețele mari, unde volumul traficului este ridicat. În astfel de cazuri, interpretarea datelor brute necesită cunoștințe avansate din partea operatorilor și poate consuma timp important, ceea ce afectează capacitatea de reacție la evenimentele de securitate.

De aceea, în practică, Wireshark este adesea utilizat împreună cu alte sisteme care dispun de funcționalități automate de alertare și clasificare, cum ar fi sistemele de detectare și prevenire a intruziunilor (IDS/IPS). Acestea pot prelua sarcina de supraveghere continuă, în timp ce Wireshark este folosit pentru investigații detaliate post-eveniment sau pentru instruirea personalului în analiza comunicațiilor digitale.

Prin urmare, Wireshark reprezintă un instrument valoros în procesul de învățare și explorare a arhitecturii rețelelor, dar nu este suficient de eficient în mod izolat pentru a acoperi cerințele unui sistem de apărare complet. Utilizarea sa într-un cadru mai larg, alături de alte soluții specializate, permite o abordare mai echilibrată a protecției infrastructurilor de rețea.

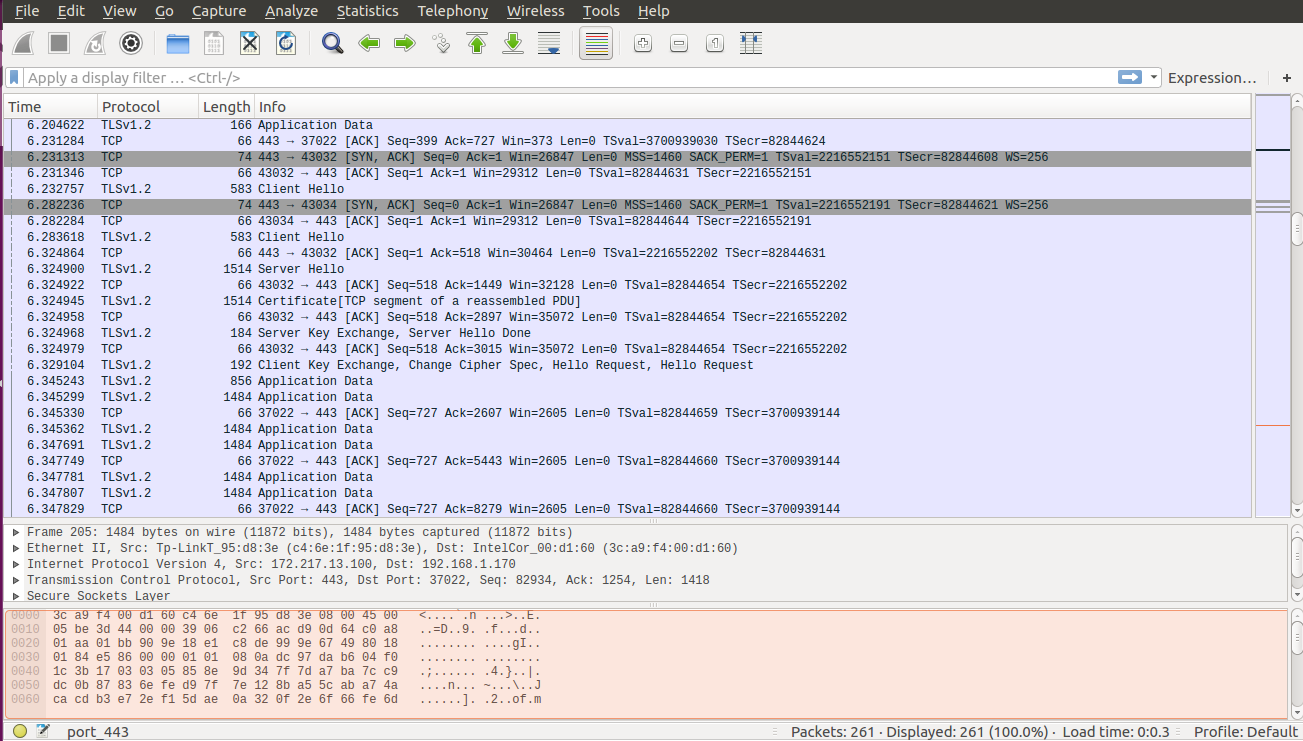


Figura 1.1 – Wireshark

Pe lângă instrumentele cu interfețe grafice, în analiza traficului de rețea sunt frecvent utilizate și soluții în linie de comandă, apreciate pentru flexibilitatea lor și pentru integrarea facilă în procese automatizate. Aceste unelte sunt preferate mai ales în medii server-based sau în situații în care se dorește monitorizarea discretă și consum redus de resurse. Una dintre cele mai cunoscute aplicații din această categorie este **tcpdump**, descrisă mai jos.

**tcpdump** este un utilitar în linie de comandă, frecvent utilizat pentru captarea și filtrarea traficului de rețea în timp real. Acesta funcționează prin monitorizarea pachetelor transmise prin interfețele de rețea ale sistemului și permite afișarea detaliată a acestora direct în consolă. Din cauza simplității sale și a consumului redus de resurse, tcpdump este adesea ales pentru diagnosticare rapidă în medii bazate pe Linux sau Unix, în special în scenarii în care interfețele grafice nu sunt disponibile sau nu sunt necesare.

Interfața sa text-based îl face potrivit pentru utilizatorii care dețin cunoștințe solide de rețea, deoarece interpretarea ieșirilor presupune înțelegerea structurii pachetelor și a protocoalelor implicate (IP, TCP, UDP, ICMP etc.). tcpdump suportă o varietate de filtre care permit selectarea traficului relevant, ceea ce îl transformă într-un instrument versatil pentru monitorizarea activității în rețele locale sau distribuite. În **figura 1.2**, este prezentat un exemplu de rulare a tcpdump într-un terminal, cu afișarea detaliată a pachetelor capturate.

Totuși, tcpdump nu include facilități grafice sau mecanisme automate de analiză, iar utilizarea sa eficientă presupune familiaritate cu expresiile de filtrare și structura internă a protocoalelor. Pentru investigații mai aprofundate sau pentru revizuirea capturilor într-un format vizual, fișierele .pcap generate de tcpdump sunt adesea analizate ulterior în aplicații precum Wireshark, care oferă o reprezentare mai accesibilă a traficului.

Deși reprezintă o soluție viabilă pentru inspecția manuală și rapidă a comunicațiilor de rețea, tcpdump nu este conceput pentru a înlocui sistemele de detecție automată. Lipsa unor componente de alertare sau clasificare în timp real limitează utilizarea sa în strategii complexe de apărare. Astfel, în practica securității informatice, tcpdump este cel mai eficient atunci când este integrat într-un cadru mai larg de monitorizare, în combinație cu alte instrumente precum IDS/IPS sau platforme SIEM.

Изображение выглядит как текст, снимок экрана, Шрифт, число

Автоматически созданное описание

Figura 1.2 – tcpdump

În analiza comportamentală a traficului de rețea, sunt necesare instrumente care să ofere mai mult decât capturarea brută a pachetelor. Unele soluții se concentrează pe interpretarea fluxurilor în context, generând informații utile despre activitatea desfășurată în rețea. Un exemplu reprezentativ în această categorie este **Zeek**, cunoscut anterior sub denumirea **Bro**.

Zeek este o platformă de monitorizare a rețelei care combină funcționalitatea clasică de captare a pachetelor cu un sistem avansat de analiză comportamentală. Pe lângă interceptarea datelor, Zeek poate interpreta protocoale de nivel superior (precum HTTP, DNS, SSL), extrăgând informații relevante care sunt ulterior organizate în fișiere jurnal structurate. Aceste fișiere descriu interacțiunile detectate și pot fi folosite pentru investigarea activităților suspecte sau pentru auditul comunicațiilor din rețea. În **figura 1.3** este ilustrată interfața de lucru asociată jurnalelor generate de Zeek.

Spre deosebire de sistemele bazate exclusiv pe semnături, Zeek se concentrează pe observarea comportamentelor și pe corelarea evenimentelor. Astfel, poate surprinde modele de acțiune care nu corespund unor amenințări cunoscute, oferind o perspectivă mai extinsă asupra tacticilor și tehnicilor utilizate de actori rău-intenționați. De exemplu, analiza conținutului cererilor DNS, a sesiunilor SSL sau a tranzacțiilor HTTP poate indica prezența unui canal de comunicație ascuns sau a unei tentative de comandă și control.

Un alt avantaj important al Zeek constă în suportul pentru scripturi personalizate, care permit ajustarea regulilor și comportamentului aplicației în funcție de nevoile specifice ale administratorilor sau ale politicilor de securitate adoptate. Prin aceste scripturi, utilizatorii pot defini condiții de alertare, extragere a anumitor câmpuri sau integrare cu alte sisteme, precum platforme SIEM sau soluții de orchestrare și automatizare.

Zeek este, așadar, potrivit pentru medii în care este necesară o înțelegere detaliată a traficului și o capacitate de adaptare continuă. Jurnalele și alertele pe care le produce pot sprijini analiza post-eveniment, oferind date clare despre tipurile de activitate care au avut loc într-o rețea într-un anumit interval de timp.

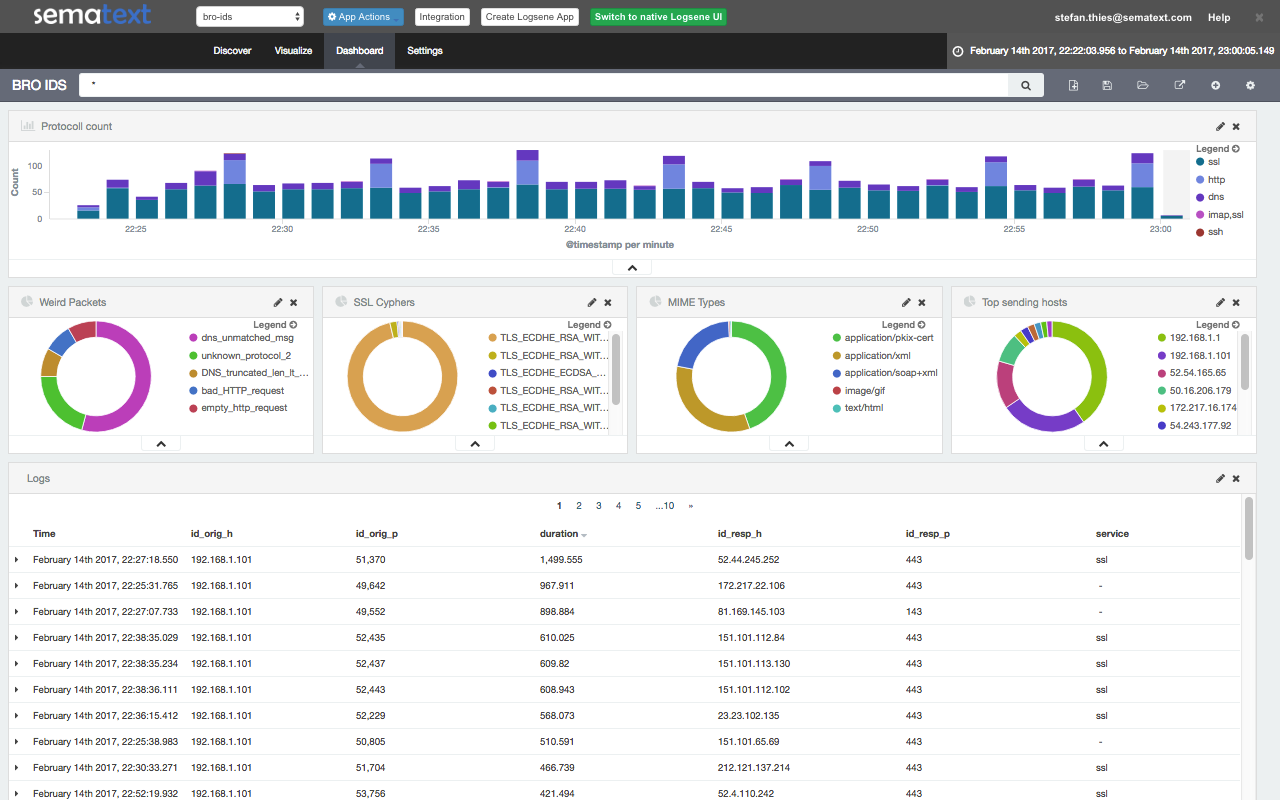


Figura 1.3 – Zeek

În completarea soluțiilor dedicate analizei pasive, există și instrumente care combină capacitățile de monitorizare cu acțiuni concrete de răspuns la incidente. Un exemplu în această direcție este **Suricata**, o platformă care funcționează atât ca sistem de detecție a intruziunilor (IDS), cât și ca sistem de prevenire (IPS), fiind capabilă să analizeze traficul de rețea în timp real și să aplice politici de filtrare sau blocare automată.

Spre deosebire de aplicațiile precum Wireshark sau tcpdump, care sunt axate în principal pe inspecția manuală a traficului capturat, Suricata poate interpreta fluxurile de date în mod automatizat, identificând semnale de atacuri cunoscute și comportamente suspecte, pe baza unor reguli configurabile. Această abordare permite o reacție mai rapidă în fața riscurilor detectate, fără a necesita intervenție directă imediată din partea unui operator uman.

Suricata folosește o bază extinsă de semnături, compatibilă cu formatul Snort, dar și mecanisme avansate de analiză, inclusiv suport pentru decodarea pachetelor la nivel de aplicație și pentru extragerea conținutului. În plus, oferă posibilitatea de a lucra cu fișiere jurnal structurate (JSON, EVE logs) care pot fi integrate ușor în soluții externe de analiză sau vizualizare, precum ELK Stack (Elasticsearch, Logstash, Kibana).

Sistemul propus în cadrul lucrării de față urmărește să combine punctele forte identificate în aplicații precum Wireshark, tcpdump, Zeek și Suricata, într-o platformă unificată, cu o interfață grafică accesibilă și funcționalități avansate de filtrare și clasificare. În locul unei analize brute, consumatoare de timp și expertiză, soluția implementată oferă o abordare orientată pe eficiență, care reduce efortul necesar pentru interpretarea datelor și scurtează timpul de reacție la evenimentele relevante.

Prin corelarea automată a informațiilor din trafic și generarea de rapoarte sintetice, sistemul oferă un sprijin consistent în procesul de decizie. Acest tip de integrare permite adaptarea mai bună la cerințele moderne de securitate, unde viteza de reacție și acuratețea detecției joacă un rol important în menținerea stabilității infrastructurii de rețea.

## **1.3 Scopul, obiectivele și cerințele sistemului**

Proiectul de față are ca direcție principală dezvoltarea unei aplicații software capabile să intercepteze, analizeze și prezinte informațiile rezultate din traficul de rețea într-un mod accesibil și structurat. Prin această abordare, se urmărește construirea unui instrument funcțional care să contribuie la supravegherea comunicării dintre dispozitive și la identificarea comportamentelor care pot ridica semne de întrebare din perspectiva securității.

Soluția implementată trebuie să ofere o modalitate rapidă și automatizată de captare a datelor, să filtreze conținutul nerelevant și să evidențieze acele interacțiuni care pot indica nereguli, configurări greșite sau tentative de acces neautorizat. În plus, sistemul va permite păstrarea istoricului comunicațiilor și prezentarea acestora într-o formă care facilitează luarea de decizii.

Pentru atingerea acestor obiective, proiectul propune următoarele componente funcționale:

**a) Captarea traficului de rețea:** Realizarea unui modul care să permită monitorizarea în timp real a datelor transmise între nodurile din rețea, cu ajutorul unor tehnologii consacrate precum tcpdump, Wireshark, Zeek sau Suricata, în funcție de contextul de utilizare;

**b) Filtrarea și clasificarea pachetelor:** Introducerea unor mecanisme care să selecteze doar acele informații relevante pentru analiză, înlăturând traficul de fundal sau datele irelevante pentru scopul propus. Aceasta presupune interpretarea pachetelor după protocol, port, adresă IP sau alte criterii specific;

**c) Detecția activităților suspecte:** Integrarea unor metode de observare a comportamentului traficului, prin reguli statice sau modele configurabile, pentru a semnala posibile acțiuni nedorite sau ieșite din tiparele obișnuite;

**d) Stocarea și gestionarea datelor:** Proiectarea unui sistem de înregistrare a informațiilor colectate, fie în fișiere de tip log, fie într-o bază de date structurată, pentru a facilita analiza ulterioară și generarea de statistici;

**e) Interfață de utilizator (GUI):** Dezvoltarea unei componente vizuale care să permită utilizatorului să interacționeze facil cu datele procesate, să filtreze și să navigheze printre înregistrări, dar și să genereze rapoarte sintetice pentru documentare;

**f) Automatizarea procesului:** Reducerea dependenței de intervenții manuale prin integrarea unor funcții automate de declanșare a capturilor, aplicare a filtrelor, clasificare și alertare, astfel încât utilizatorii să poată gestiona cu eficiență situațiile apărute;

Pentru ca acest sistem să funcționeze corespunzător, este necesar să îndeplinească o serie de cerințe care pot fi împărțite în două categorii: funcționale și nefuncționale.

Din punct de vedere funcțional, aplicația trebuie să capteze datele în timp real, să le interpreteze corect în funcție de contextul rețelei și să permită diferențierea între fluxuri normale și cele care pot indica riscuri. Aceasta presupune atât aplicarea unor filtre bazate pe protocoale, cât și capacitatea de a corela diferite pachete sau sesiuni pentru a înțelege intenția comunicației. Informațiile obținute trebuie să poată fi salvate și consultate ulterior, iar utilizatorul trebuie să dispună de un mediu vizual unde poate explora conținutul și genera documente utile pentru analiză sau raportare.

Din perspectiva cerințelor nefuncționale, sistemul trebuie să poată fi extins în viitor, în funcție de apariția unor nevoi noi sau de modificări în structura rețelei. De asemenea, aplicația trebuie să funcționeze stabil și să evite supraîncărcarea resurselor, în special în rețele mari sau cu trafic intens. Interfața trebuie să fie clară și bine organizată, pentru a permite o utilizare cât mai eficientă, inclusiv în condiții de presiune operațională. Nu în ultimul rând, sistemul trebuie să fie proiectat în conformitate cu normele legale privind supravegherea comunicațiilor, în special cele legate de confidențialitate și protecția datelor cu caracter personal.

Prin respectarea acestor cerințe, aplicația poate fi utilizată atât pentruactivități de instruire și testare, cât și ca punct de plecare pentru soluții mai complexededicate mediilor operaționale în care vizibilitatea asupra traficului de rețea este indispensabilă pentru luarea deciziilor.2  MODELAREA ȘI PROIECTAREA SISTEMUL INFORMATIC

În cadrul procesului de dezvoltare a unui sistem informatic complex, modelarea și proiectarea reprezintă etape fundamentale care permit structurarea logică și tehnică a soluției propuse. Aceste activități au un rol decisiv în definirea funcționalităților, stabilirea relațiilor dintre componente și anticiparea modului în care sistemul va reacționa în diverse scenarii de operare. În cazul de față, sistemul vizează interceptarea și analiza traficului de rețea, ceea ce presupune un nivel ridicat de coerență între modulele funcționale și o integrare eficientă a tehnologiilor implicate.

Modelarea sistemului se concentrează pe identificarea entităților care compun aplicația, precum și a fluxurilor de date care circulă între acestea. Este vorba despre o etapă în care se construiește o reprezentare conceptuală a arhitecturii, menită să asigure o înțelegere comună între toți membrii echipei de dezvoltare. În această reprezentare se includ atât elementele care preiau informațiile din rețea (modulele de captură), cât și cele care analizează, clasifică, salvează și prezintă aceste date (componentele de procesare, de stocare și de vizualizare).

Proiectarea, pe de altă parte, are în vedere transpunerea acestei arhitecturi conceptuale într-o structură tehnică clară. Se stabilesc astfel componentele software care vor alcătui sistemul, se determină modul în care acestea vor comunica între ele și se aleg tehnologiile corespunzătoare. Acest demers include, de asemenea, analiza cerințelor de performanță, scalabilitate și interoperabilitate, astfel încât soluția să fie adaptabilă și eficientă în contexte variate de utilizare.

Pentru a facilita această etapă, este utilizat **Limbajul Unificat de Modelare (UML)**, o metodă standardizată care permite descrierea vizuală a structurii și comportamentului sistemului. UML oferă un set de diagrame care ajută la documentarea precisă a procesului de dezvoltare, precum:

* **Diagramele de clasă**, care reflectă entitățile-cheie ale sistemului (de exemplu, modulele de captare, analiză, stocare și raportare) și relațiile dintre acestea. Aceste diagrame permit evidențierea proprietăților și metodelor fiecărei componente și modul în care acestea interacționează;
* **Diagramele de activitate**, care oferă o reprezentare a fluxurilor operaționale din cadrul sistemului. Acestea pot descrie pașii necesari pentru captarea traficului, prelucrarea acestuia, detecția anomaliilor și generarea alertelor;
* **Diagramele de secvență**, care ilustrează schimburile de mesaje între obiecte sau module într-un scenariu concret, cum ar fi inițierea unei sesiuni de analiză sau salvarea automată a unui fișier cu date procesate.

Utilizarea acestor diagrame permite nu doar documentarea clară a arhitecturii, ci și validarea deciziilor de proiectare. Ele pot fi analizate pentru identificarea timpurie a eventualelor probleme de compatibilitate, redundanță sau lipsă de coerență logică între componente. În plus, diagramele UML pot sta la baza planificării activităților de testare, contribuind la stabilirea unor scenarii relevante de verificare a funcționării sistemului.

De asemenea, modelarea și proiectarea favorizează o mai bună colaborare între dezvoltatori, specialiști în rețelistică și securitate, și alți factori implicați în procesul decizional. Prin definirea clară a responsabilităților fiecărui modul și a interfețelor de comunicare, se reduce semnificativ riscul apariției neînțelegerilor în timpul implementării.

Un alt beneficiu al acestei abordări este că oferă o bază solidă pentru extinderea ulterioară a aplicației. Pe măsură ce nevoile sistemului evoluează sau apar cerințe suplimentare, o arhitectură bine definită permite adăugarea de funcționalități fără a afecta negativ comportamentul general al aplicației.

## **2.1** **Descrierea comportamentală a sistemului**

Funcționarea unui sistem informatic dedicat interceptării și analizei traficului de rețea poate fi înțeleasă cel mai bine prin analiza succesiunii de acțiuni desfășurate în cadrul procesului de monitorizare. În centrul acestui comportament se află interacțiunile dintre modulele componente și fluxurile de date care leagă aceste module într-o structură logică coerentă. Aceste activități formează un circuit operațional care pornește de la captarea traficului brut și se încheie cu prezentarea rezultatelor către utilizator într-un format structurat și interpretabil.

Procesul debutează cu interceptarea pachetelor de date la nivelul interfeței de rețea. Sistemul este configurat astfel încât să poată prelua traficul în timp real, fie prin ascultare promiscuă, fie prin aplicarea unor filtre definite anterior. Această primă etapă presupune gestionarea unui flux constant de date, într-un mod care să nu perturbe performanța generală a rețelei. Imediat după preluare, pachetele sunt transmise către componentele care se ocupă cu analizarea și filtrarea acestora.

În etapa de analiză, pachetele sunt supuse unui proces de segmentare logică în funcție de caracteristici precum protocolul, adresa sursă sau destinație ori portul utilizat. Datele considerate nerelevante sunt trecute în arhivă, fără a fi analizate în detaliu, pentru a evita aglomerarea inutilă a sistemului. În schimb, informațiile care indică un potențial comportament neobișnuit sunt procesate în profunzime. Acest proces se bazează fie pe reguli prestabilite, asemănătoare celor utilizate de sistemele de tip Suricata, fie pe modele de analiză comportamentală, inspirate de abordarea adoptată de Zeek. Datele considerate importante sunt apoi transmise către un sistem de stocare, unde sunt reținute pentru examinări ulterioare sau pentru generarea de rapoarte.

Interacțiunea cu utilizatorul se realizează prin intermediul unei interfețe grafice care permite vizualizarea datelor prelucrate, filtrarea acestora și exportul în diverse formate. Această componentă oferă o punte între logica internă a sistemului și utilizatorul final, permițându-i acestuia să consulte activitatea rețelei și să intervină, dacă este necesar, asupra unor fluxuri considerate suspecte.

Pentru a oferi o imagine clară și standardizată a comportamentului descris mai sus, sunt utilizate instrumente grafice specifice modelării, precum diagramele UML. Diagramele de activitate permit evidențierea traseului parcurs de pachetele de date în cadrul sistemului, de la momentul captării până la clasificarea lor ca relevante sau neimportante. În completare, diagramele de secvență descriu interacțiunile dintre modulele principale, punând accent pe ordinea schimburilor de informații și pe modul în care acestea colaborează pentru a susține procesul de monitorizare.

Această abordare comportamentală permite nu doar înțelegerea modului în care funcționează aplicația, ci și anticiparea comportamentului acesteia în fața diverselor scenarii de trafic. Totodată, contribuie la verificarea coerenței arhitecturii propuse, oferind un punct de plecare solid pentru etapa următoare de implementare.

### 2.1.1 Imaginea generală asupra sistemului

Modul în care utilizatorul final interacționează cu aplicația dedicată interceptării și analizei traficului de rețea poate fi reprezentat vizual printr-o diagramă de caz de utilizare. În **Figura 2.1 – Interacțiune cu utilizatorul/analistul**, este ilustrat setul principal de acțiuni pe care un analist le poate executa în cadrul sistemului. Aceste funcționalități reflectă relația directă dintre utilizator și componentele aplicației și sunt necesare pentru a configura, monitoriza și evalua activitatea rețelei.

Изображение выглядит как текст, снимок экрана, диаграмма, линия

Контент, сгенерированный ИИ, может содержать ошибки.

Figura 2.1 - Interacțiune cu utilizatorul/analistul

Una dintre opțiunile disponibile este **adăugarea unui filtru**, care permite selectarea traficului în funcție de criterii definite, precum adrese IP, protocoale utilizate sau porturi de destinație. Această funcție contribuie la focalizarea procesului de captură asupra informațiilor relevante, reducând volumul de date inutile.

O altă funcționalitate importantă este **configurarea alertelor**, care oferă posibilitatea stabilirii unor condiții declanșatoare pentru semnalarea activităților anormale. Acest mecanism de alertare automată sprijină identificarea rapidă a incidentelor potențiale și îmbunătățește capacitatea de reacție a operatorului.

Vizualizarea istoricului alertelor permite revizuirea evenimentelor detectate anterior, oferind o imagine de ansamblu asupra comportamentului rețelei în timp și facilitând recunoașterea unor tipare recurente asociate cu riscuri sau abuzuri.

Prin pregătirea raportului, utilizatorul poate genera documente care sintetizează rezultatele sesiunilor de monitorizare. Aceste rapoarte pot conține statistici, diagrame și descrieri ale alertelor, fiind utile în contextul auditării, al raportării către management sau al investigațiilor ulterioare.

De asemenea, configurarea dispozitivului de interceptare oferă control asupra parametrilor tehnici ai capturii, cum ar fi interfața de rețea folosită, modul promiscuu de funcționare sau aplicarea de filtre la nivel hardware/software, asigurând astfel eficiența și acuratețea procesului de colectare a datelor.

Prin urmare, diagrama din Figura 2.1 oferă o perspectivă clară asupra punctelor de contact dintre utilizator și sistem, ilustrând modul în care analiza traficului este inițiată, controlată și documentată de către operator, în cadrul unei aplicații concepute pentru supraveghere și detecție.

### 2.1.2 Modelarea vizuală a fluxurilor

Pentru a înțelege funcționarea internă a sistemului informatic propus, este necesară reprezentarea grafică a modului în care datele sunt procesate în funcție de alegerile făcute la nivelul configurației inițiale. Un exemplu elocvent este oferit de Figura 2.2 – Procesul de interceptare, care prezintă o diagramă de activitate ce urmărește traseul logic parcurs de aplicație în procesul de captare și partajare a traficului de rețea.

Diagrama începe prin verificarea existenței unor filtre de captare definite de utilizator. În cazul în care aceste filtre sunt prezente, sistemul inițiază interceptarea doar a pachetelor care corespund criteriilor stabilite. Acest tip de filtrare direcționează captarea către fluxurile considerate relevante pentru analiza de securitate, reducând semnificativ volumul de date care necesită prelucrare ulterioară. Dacă nu au fost configurate filtre, sistemul trece automat la captarea integrală a traficului, asigurând astfel o acoperire completă a activității de rețea.

Ulterior, indiferent de tipul de captare inițial selectat, sistemul parcurge o a doua decizie logică, referitoare la aplicarea unei filtrări personalizate. Această etapă suplimentară permite rafinarea suplimentară a datelor, aplicând reguli mai detaliate în funcție de nevoile de investigare. Atunci când aceste reguli sunt active, traficul partajat este cel care respectă condițiile impuse, oferind un grad ridicat de specificitate în analiza ulterioară. În lipsa unei astfel de filtrări, tot traficul capturat este partajat, păstrând caracterul complet al sesiunii de monitorizare.

cИзображение выглядит как текст, снимок экрана, диаграмма, линия

Контент, сгенерированный ИИ, может содержать ошибки.

Figura 2.2 – Procesul de interceptare

Modelul prezentat în diagramă evidențiază flexibilitatea arhitecturii sistemului și permite o mai bună adaptare la diferite contexte operaționale. Alegerea între captarea completă și cea filtrată, urmată de opțiunea unei filtrări avansate, constituie o abordare care încurajează controlul progresiv asupra datelor procesate. În mod particular, această metodă este benefică în scenariile în care analiza trebuie să fie orientată fie pe trafic general, în scop de audit, fie pe fluxuri specifice, în cazul investigațiilor privind comportamente suspecte sau atacuri punctuale.

Prin intermediul acestei reprezentări grafice, este subliniată importanța definirii inițiale a regulilor de captare, precum și a capacității sistemului de a ajusta în mod dinamic volumul și tipul datelor analizate. Această abordare permite echipei de securitate să adapteze rapid setările aplicației la schimbările de context din rețea, fără a necesita intervenții complexe asupra structurii sistemului. În același timp, modelarea fluxurilor oferă o bază solidă pentru testare, întreținere și eventuală extindere a funcționalităților, sprijinind astfel un proces de dezvoltare sustenabil și bine documentat.

## **2.1.3 Descrierea scenariilor de utilizare a aplicaţiei**

Pentru a evidenția succesiunea logică a pașilor executați în cadrul aplicației și modul în care actorii interacționează cu componentele sistemului, este utilă reprezentarea procesului printr-o diagramă de secvență. În Figura 2.3 – Diagrama de secvență pentru configurarea, capturarea și analiza traficului de rețea, sunt ilustrate schimburile de mesaje dintre analist, sistem, componenta responsabilă de accesarea sursei de trafic și modulul de analiză.

Scenariul începe cu inițierea de către utilizator a procesului de configurare a filtrelor de captare. Aceste filtre pot viza anumite protocoale, adrese IP sau alte criterii relevante în contextul supravegherii rețelei. Odată ce aceste setări sunt definite, sistemul validează configurația și trece la inițierea procesului de captare a pachetelor.

Изображение выглядит как текст, снимок экрана, диаграмма, Параллельный

Контент, сгенерированный ИИ, может содержать ошибки.

Figura 2.3 - Diagrama de secvență pentru configurarea, capturarea și analiza traficului de rețea

După pornirea capturii, sistemul formulează o solicitare către componenta care gestionează traficul de rețea, în vederea obținerii datelor corespunzătoare. Aceste date, odată colectate, sunt transmise către modulul de analiză, care le examinează pentru a identifica eventuale comportamente neobișnuite, semnale de alertă sau tentative de acces neautorizat. Rezultatul acestei analize este returnat sistemului, împreună cu informațiile relevante privind posibilele riscuri.

În etapa următoare, analistul solicită generarea unui raport, ceea ce determină sistemul să adune și să structureze datele obținute anterior. Modulul de analiză este implicat și în această etapă, furnizând date suplimentare sau agregate, care contribuie la realizarea unei sinteze finale a sesiunii de monitorizare. În cele din urmă, sistemul returnează raportul final, care este prezentat utilizatorului într-un format accesibil și interpretabil, contribuind la documentarea rezultatelor și la luarea unor decizii informate privind securitatea rețelei.

Structura acestei diagrame permite înțelegerea clară a fluxului de date și a rolului fiecărui component în cadrul sistemului. De asemenea, scoate în evidență caracterul secvențial și coordonat al acțiunilor, subliniind coeziunea dintre fazele de configurare, captare, analiză și raportare. Acest mod de reprezentare este util atât în documentarea arhitecturii aplicației, cât și în etapele ulterioare de testare și validare a funcționalităților implementate.

## **2.2** **Descrierea structurală a sistemului**

Structura unui sistem informatic destinat monitorizării și analizei traficului de rețea trebuie să fie bine definită și organizată astfel încât fiecare componentă să contribuie într-un mod coerent la atingerea scopurilor funcționale. În cazul proiectului de față, sistemul poate fi divizat în mai multe componente principale, fiecare având un rol specific și interacționând cu celelalte într-o manieră logică și previzibilă.

Componenta de **captură** reprezintă punctul de intrare a datelor în sistem și are ca sarcină interceptarea pachetelor de rețea în timp real. Aceasta trebuie să fie suficient de performantă pentru a gestiona volume mari de trafic, fără a pierde informații sau a produce întârzieri semnificative. Pe lângă funcția de colectare, modulul de captură oferă și suport pentru aplicarea filtrelor de selecție, permițând astfel extragerea numai a acelor fluxuri de date care corespund criteriilor definite de utilizator.

Odată ce datele au fost preluate, ele sunt transmise către **modulul de analiză**, responsabil pentru procesarea și interpretarea informațiilor colectate. Acest modul are rolul de a detecta comportamente neobișnuite, posibile amenințări sau abateri față de tiparele normale de trafic. Funcționalitățile sale pot include atât tehnici bazate pe semnături — care presupun compararea cu un set de reguli prestabilite — cât și tehnici de analiză comportamentală, care urmăresc identificarea anomaliilor prin observarea variațiilor în activitatea rețelei.

Pentru ca activitățile să poată fi revizuite, documentate și corelate în timp, sistemul include și o componentă de stocare, reprezentată de o bază de date sau un mecanism echivalent de logare. Aceasta reține informațiile relevante privind sesiunile de trafic, alertele generate, filtrele aplicate, precum și rapoartele produse. Accesul rapid la aceste date este important pentru investigarea ulterioară a evenimentelor și pentru realizarea unor audituri retrospective.

Legătura dintre utilizator și logica internă a aplicației este realizată prin intermediul **interfeței grafice**, care permite configurarea setărilor, inițierea procesului de captură, monitorizarea alertelor și generarea de rapoarte. Această interfață este concepută astfel încât să faciliteze utilizarea intuitivă, reducând curba de învățare și oferind un nivel ridicat de vizibilitate asupra activității desfășurate în cadrul rețelei. Prin intermediul acesteia, utilizatorii pot adapta sistemul la contextul operațional curent și pot reacționa rapid la semnalele generate de procesul de analiză.

Din punct de vedere logic, componentele descrise mai sus sunt interconectate într-o arhitectură modulară, în care fiecare parte contribuie la funcționarea generală a sistemului fără a depinde excesiv de celelalte. Această separare a responsabilităților permite atât dezvoltarea independentă a fiecărei componente, cât și întreținerea sistemului în timp. Comunicarea între module se realizează prin protocoale bine definite sau prin interfețe programatice, ceea ce asigură flexibilitate în cazul în care se dorește extinderea sau înlocuirea unei părți a aplicației.

Pentru a documenta această structură, se utilizează frecvent instrumente vizuale de modelare, precum diagramele de componente sau diagramele de clasă din cadrul limbajului UML. Acestea permit descrierea arhitecturii dintr-o perspectivă abstractă, ușor de înțeles și interpretat atât de către dezvoltatori, cât și de către alți actori implicați în proiect, precum analiștii de securitate sau personalul tehnic de suport.

### 2.2.1 Descrierea structurii statice a sistemului

Pentru a înțelege organizarea internă a componentelor aplicației, este necesar să se analizeze structura statică a sistemului. Aceasta poate fi exprimată eficient printr-o diagramă de clasă UML, care descrie entitățile fundamentale, atributele și metodele aferente, precum și relațiile dintre aceste entități. În Figura 2.4 – Diagrama de clasă a sistemului de interceptare și analiză a traficului, este ilustrată arhitectura logică a sistemului sub forma unui model orientat pe obiecte.

Clasa Utilizator este responsabilă de autentificarea în sistem, configurarea filtrelor pentru captarea traficului și inițierea generării rapoartelor. Această clasă reprezintă interfața dintre operatorul uman și componentele aplicației, asigurând controlul și personalizarea procesului de monitorizare. Atribute precum ID, nume sau rol permit identificarea și diferențierea utilizatorilor, iar metodele disponibile permit realizarea acțiunilor principale asupra sistemului.

Изображение выглядит как текст, диаграмма, снимок экрана, линия

Контент, сгенерированный ИИ, может содержать ошибки.

Figura 2.4 - Diagrama de clasă a sistemului de interceptare și analiză a traficului.

Componenta centrală a aplicației este reprezentată de clasa SistemInterceptat, care intermediază comunicarea dintre utilizator și procesele tehnice de interceptare. Această clasă cuprinde metodele de inițializare și oprire a capturii, precum și funcționalitatea de aplicare a filtrelor configurate. Ea joacă un rol cheie în transmiterea pachetelor captate către componentele de analiză.

Datele colectate din rețea sunt modelate prin clasa Pachet, care conține informații despre sursă, destinație, protocol și alte metadate asociate. Aceste instanțe sunt procesate ulterior de ModulAnaliza, componentă specializată în examinarea conținutului captat pentru identificarea unor comportamente neobișnuite. Modulul de analiză conține metode prin care se efectuează analiza propriu-zisă a pachetelor și se generează alerte atunci când sunt detectate amenințări sau abateri de la comportamentul normal.

Rezultatul procesului analitic este agregat în obiecte de tip RezultatAnaliza, care sintetizează datele obținute: numărul de pachete analizate, descrierea anomaliilor și volumul traficului suspect. Aceste rezultate pot fi transmise clasei Raport, responsabilă de generarea documentației aferente fiecărei sesiuni de monitorizare. Clasa respectivă include metode pentru exportul și pregătirea conținutului într-un format accesibil și utilizabil de către specialiști.

Un alt element important în structură este clasa Filtru, care determină criteriile de selecție a pachetelor procesate. Prin parametri precum adresa IP, tipul protocolului sau portul utilizat, această componentă contribuie la focalizarea procesului de captare asupra unor zone de interes și la reducerea volumului de date irelevante.

Pentru păstrarea informațiilor referitoare la alertele generate și la activitățile sistemului, se utilizează clasa BazaLogurilor. Aceasta asigură înregistrarea și accesarea ulterioară a evenimentelor, oferind un istoric valoros pentru audituri de securitate sau investigații. Evenimentele sunt stocate alături de datele asociate, iar metoda SalvareEveniment() permite persistarea acestora în mod controlat.

Clasa Alerta este generată în momentul în care sistemul detectează o amenințare. Aceasta cuprinde informații precum descrierea alertei, severitatea și identificatorul unic, fiind asociată automat cu evenimentul detectat. Sistemul poate notifica operatorul în baza acestor alerte, ceea ce sprijină luarea rapidă a unor măsuri de răspuns.

### 2.2.2 Relatiile de dependență între componentele sistemului

O componentă importantă în proiectarea unui sistem informatic o reprezintă modelarea stărilor interne prin care acesta trece în funcție de acțiunile utilizatorului și condițiile de execuție. Un exemplu relevant în acest sens este procesul de autentificare și autorizare, care determină accesul la funcționalitățile aplicației și stabilește drepturile de utilizare pentru fiecare categorie de utilizator.

În Figura 2.5 – Diagrama de stare pentru procesul de logare, este prezentat modul în care sistemul evoluează din momentul în care utilizatorul inițiază accesul până la finalizarea procesului de autentificare și tranziția către zona de funcționare a aplicației. Diagrama este structurată sub forma unei mașini de stare UML, care include atât stări simple, cât și un stat compozit, reflectând structura internă a sistemului în timpul autentificării.

Procesul debutează dintr-un nod de început, moment în care aplicația direcționează utilizatorul către interfața de logare. Aici, sistemul așteaptă introducerea unor date de identificare, precum nume de utilizator și parolă. Această fază este encapsulată într-un stat compozit intitulat „Sistemul”, care cuprinde mai multe stări intermediare. După ce utilizatorul completează câmpurile de autentificare și inițiază procesul printr-un buton dedicat, sistemul trece în starea de verificare a datelor introduse.

Изображение выглядит как текст, снимок экрана, диаграмма, линия

Контент, сгенерированный ИИ, может содержать ошибки.

Figura 2.5 - Diagrama de stare pentru procesul de logare

În cazul în care informațiile furnizate nu corespund unor înregistrări valide, sistemul generează o tranziție către starea anterioară, semnalizată printr-un eveniment de tip „Login Failed”. Această revenire permite utilizatorului să încerce din nou, fără a părăsi cadrul aplicației. Dacă autentificarea este reușită, se inițiază automat procesul de autorizare, prin care se verifică nivelul de acces atribuit utilizatorului. Această etapă este necesară pentru a determina ce componente ale aplicației pot fi accesate și ce acțiuni pot fi efectuate.

Finalizarea cu succes a procesului de autorizare conduce la ieșirea din statul compozit și la trecerea într-o nouă stare activă, care corespunde utilizării normale a aplicației. În această etapă, utilizatorul are acces la funcțiile disponibile conform rolului său (de exemplu, vizualizarea rapoartelor, configurarea filtrelor, inițierea capturii de trafic etc.). Diagrama se încheie cu un nod final, care marchează încheierea procesului de autentificare și trecerea completă în mediul operațional al sistemului.

Această reprezentare evidențiază interdependențele dintre componentele de autentificare și celelalte module ale sistemului, precum și condițiile care trebuie îndeplinite pentru a permite accesul. Prin utilizarea stărilor și tranzițiilor, este oferită o imagine clară asupra modului în care sistemul reacționează la acțiunile utilizatorului și asupra logicii interne de control a accesului.

Modelarea procesului de logare în acest mod contribuie nu doar la înțelegerea mecanismului de control al accesului, ci și la identificarea punctelor în care pot fi aplicate politici de securitate, optimizări sau mecanisme suplimentare de verificare, cum ar fi autentificarea în doi pași sau înregistrarea tentativelor nereușite. În plus, această abordare poate sta la baza testării funcționale, asigurând că sistemul reacționează corect în toate scenariile posibile legate de identificarea utilizatorilor.

3 REALIZAREA SISTEMULUI

Procesul de construire a aplicației pentru interceptarea și analiza traficului de rețea a presupus parcurgerea mai multor etape succesive, de la proiectarea arhitecturii generale și definirea funcționalităților, până la implementarea concretă a componentelor și integrarea acestora într-un ansamblu coerent. Acest capitol prezintă în mod detaliat modul în care a fost realizată aplicația, punând accent pe organizarea modulară, alegerea tehnologiilor, structura internă și fluxul de funcționare.

Aplicația a fost concepută pentru a permite monitorizarea traficului din rețele locale, oferind utilizatorului posibilitatea de a vizualiza în timp real informații despre pachetele capturate. Aceasta este alcătuită din trei componente principale: motorul de captură și analiză a traficului, interfața grafică de utilizator (GUI) și un modul de stocare locală a datelor. Toate aceste componente au fost dezvoltate utilizând limbajul Python, datorită portabilității, suportului extins pentru biblioteci externe și ușurinței în implementarea funcțiilor specifice de rețea.

Pentru partea de captare a traficului, au fost utilizate bibliotecile scapy și socket, care permit interceptarea pachetelor la nivelul rețelei și extragerea caracteristicilor de bază ale acestora (IP sursă/destinație, porturi, protocoale, timestamps). Informațiile obținute sunt prelucrate și afișate prin intermediul unei interfețe grafice create cu Tkinter, organizată într-un mod intuitiv, sub forma unei ferestre de autentificare stilizate, însoțită de un panou principal de control și afișare a traficului.

Datele rezultate din sesiunile de monitorizare sunt salvate local într-o bază de date, permițând atât consultarea ulterioară, cât și exportul în formate standard, cum ar fi .pcap sau .txt. Acest mecanism oferă persistență și sprijină procesul de analiză post-eveniment, contribuind la o evaluare mai detaliată a comportamentului rețelei.

Aplicația a fost construită într-un mod flexibil și modular, astfel încât fiecare componentă să poată fi întreținută sau extinsă separat. În cadrul acestui capitol sunt prezentate în detaliu structura proiectului, modul de organizare a codului, integrarea cu servicii externe, și modul în care cerințele funcționale au fost transpuse în implementare concretă.

## 3.1 Structura sistemului

Aplicația „Sentinel Traffic Analyzer” a fost dezvoltată într-un mod modular, respectând o arhitectură clară și extensibilă. Codul sursă este organizat în mai multe fișiere Python, fiecare responsabil de un set specific de funcționalități. Această abordare permite întreținerea eficientă a aplicației și adăugarea ulterioară a unor noi componente fără a afecta funcționarea generală.

Captura traficului de rețea este realizată prin intermediul clasei TrafficAnalyzerCore din fișierul core.py. Metoda start\_capture() utilizează biblioteca scapy pentru a intercepta pachetele în timp real, după cum se observă în fragmentul următor:

# core.py

def start\_capture(self, iface, callback, bpf\_filter=None):

self.stop\_sniff = False

sniff(

iface=iface,

prn=lambda pkt: self.\_handle\_packet(pkt, callback),

stop\_filter=lambda x: self.stop\_sniff,

filter=bpf\_filter if bpf\_filter else None)

După captură, pachetele sunt procesate intern de metoda \_handle\_packet(), care extrage date precum IP sursă, destinație, protocol, și le trimite spre interfața grafică:

# core.py

def \_handle\_packet(self, packet, callback):

self.captured\_packets.append(packet)

callback(self.format\_packet(packet))

Interfața grafică (GUI), implementată în fișierul gui.py, este construită folosind Tkinter și oferă utilizatorului funcționalități complete: pornirea și oprirea capturii, alegerea interfeței de rețea, salvarea sesiunilor, încărcarea fișierelor .pcap, generarea rapoartelor și vizualizarea alertelor.

După pornirea capturii, datele interceptate sunt afișate în timp real într-un widget de tip text, gestionat de clasa PacketDisplay din packet\_display.py:

# packet\_display.py

def write(self, line, packet\_obj=None):

self.packets.append(line)

self.text\_widget.insert(tk.END, line)

self.text\_widget.see(tk.END)

Toate datele capturate sunt păstrate într-o structură proprie de raportare (ReportData din report\_generate.py), care permite generarea de fișiere PDF și JSON cu informații detaliate despre sesiunea analizată.

# report\_generate.py

def export\_pdf\_report(self, path="raport\_final.pdf"):

self.generate\_graphs()

pdf.output(path)

## 3.2 Integrarea serviciilor externe

Pentru a oferi o funcționalitate extinsă și pentru a îmbunătăți experiența utilizatorului, aplicația *Sentinel Traffic Analyzer* integrează mai multe servicii și biblioteci externe care contribuie semnificativ la precizia și ușurința în utilizare a platformei.

Una dintre cele mai importante integrări este utilizarea bazei de date **GeoLite2-City.mmdb**, furnizată de MaxMind. Aceasta este o bază de date geografică care permite maparea adreselor IP către locații geografice estimative, incluzând informații precum țara, orașul, regiunea, coordonatele GPS și zona de timp.

Integrarea cu GeoLite2 este realizată în fișierul network\_discovery\_view.py, în cadrul metodei load\_geoip\_data(). Această metodă utilizează biblioteca geoip2.database.Reader pentru a accesa fișierul .mmdb și pentru a parcurge toate adresele IP detectate în cadrul unei sesiuni de analiză. Informațiile obținute sunt apoi atașate fiecărui IP și utilizate ulterior în vizualizarea geografică a rețelei, precum și în tabelul de hosturi detectate.

reader = geoip2.database.Reader("PacketSentinel/GeoLite2-City.mmdb")

all\_ips = set(report\_data.sources.keys()) | set(report\_data.destinations.keys())

for ip in all\_ips:

response = reader.city(ip)

country = response.country.name

city = response.city.name

lat = response.location.latitude

lon = response.location.longitude

Această integrare permite afișarea automată a locației IP-urilor implicate în sesiunile de trafic, oferind analistului o perspectivă suplimentară asupra distribuției geografice a dispozitivelor sau serverelor implicate în comunicare. În cazul în care o adresă IP nu poate fi localizată, sistemul completează automat cu valori „N/A”, asigurând astfel continuitatea afișării fără a întrerupe funcționarea aplicației.

Datele geografice sunt afișate într-un tab dedicat al ferestrei de descoperire a rețelei („Hartă Rețea”), unde IP-urile sunt reprezentate grafic ca noduri interconectate. Fiecare nod include, alături de IP, țara și orașul corespunzătoare, precum și – dacă este disponibil – organizația asociată adresei IP:

labels[node] = "\n".join(filter(None, [

node,

f"{loc.get('country', '')}, {loc.get('city', '')}",

f"{loc.get('org')}" if loc.get('org', '') != "N/A" else ""

]))

Această reprezentare ajută la identificarea rapidă a legăturilor geografice între gazdele detectate și oferă un punct de plecare valoros în investigarea sursei unor activități suspecte.

## **3.3 Implementarea cerințelor funcționale**

Pentru ca aplicația *Sentinel Traffic Analyzer* să răspundă obiectivelor propuse, s-a urmărit transpunerea concretă a unui set de cerințe funcționale în funcționalități directe, accesibile utilizatorului. Fiecare dintre aceste cerințe a fost abordată în mod practic, cu scopul de a asigura controlul complet asupra unei sesiuni de monitorizare, de la inițiere până la generarea de rapoarte și salvarea rezultatelor.

Un prim aspect urmărit a fost **captura traficului în timp real**, care se realizează la nivelul unei interfețe de rețea selectate de utilizator. Captura este gestionată asincron, ceea ce permite aplicației să funcționeze fluent indiferent de volumul de date. Procesul poate fi întrerupt și reluat fără pierderi, iar selecția traficului poate fi restrânsă prin aplicarea de filtre BPF.

Vizualizarea interactivă a datelor capturate a fost implementată pentru a facilita analiza în timp real. Pachetele interceptate sunt afișate progresiv într-un tabel grafic, cu actualizare dinamică, iar informațiile afișate sunt prezentate într-un format condensat, cu evidențierea protocoalelor. Acest mecanism permite utilizatorului să observe imediat variații în comportamentul rețelei sau prezența unor fluxuri neobișnuite.

Un element important îl constituie **sistemul de alertare**, activ automat în fundal. Acesta analizează traficul în mod continuu și declanșează notificări în cazul identificării unor modele care pot indica activități potențial periculoase. Printre aceste modele se regăsesc scanări de porturi, flood-uri de diverse tipuri, spoofing ARP și trafic provenind de la IP-uri marcate ca periculoase. Alertele sunt prezentate vizual în interfață și salvate în fișiere de tip .log și .json.

O altă funcționalitate implementată este gestionarea sesiunilor de captură și exportul datelor. Utilizatorul poate salva sesiunile în format .pcap, utilizabil ulterior în instrumente de analiză precum Wireshark, dar și în format .txt sau .json, pentru prelucrare personalizată. La finalul fiecărei sesiuni, aplicația poate genera automat un raport în format PDF, care include grafice și sinteze ale sesiunii curente.

Aplicația include și o serie de **verificări și măsuri de protecție** în interfața grafică, care previn apariția unor erori de utilizare. De exemplu, nu este permisă pornirea capturii fără selectarea unei interfețe valide, iar dacă utilizatorul nu are drepturi suficiente, aplicația notifică acest lucru în mod explicit. Aceste mecanisme contribuie la fiabilitatea aplicației și reduc riscul de funcționare defectuoasă în condiții necontrolate.

## **3.4 Arhitectura modulară a aplicației**

Aplicația *Sentinel Traffic Analyzer* a fost construită pe baza unui model arhitectural modular, în care fiecare componentă îndeplinește un rol distinct și interacționează cu celelalte prin mecanisme bine delimitate. Această abordare a permis o dezvoltare controlată și organizată, precum și posibilitatea extinderii funcționalităților fără a afecta stabilitatea aplicației.

Structura modulară este vizibilă în separarea logică a funcțiilor principale. Captura traficului de rețea este gestionată de un modul dedicat, care preia pachetele transmise prin interfața selectată, le interpretează și le transmite mai departe spre analiză și afișare. Procesarea acestora se desfășoară în paralel cu activitatea interfeței grafice, evitând astfel blocarea aplicației în timpul capturii.

Analiza comportamentală a traficului se realizează într-un modul distinct, care primește pachetele capturate și aplică asupra lor reguli de identificare a anomaliilor. Dacă sunt detectate comportamente suspecte, acestea sunt înregistrate sub formă de alerte și pot fi vizualizate în timp real, precum și stocate pentru analiză ulterioară. Interfața grafică joacă rolul de punct de interacțiune între utilizator și logica aplicației, permițând configurarea procesului de captură, declanșarea acțiunilor de export sau generare de rapoarte și monitorizarea în timp real a traficului.

Pe lângă componenta vizuală principală, aplicația conține un modul specializat pentru afișarea pachetelor interceptate, într-o formă structurată și lizibilă. Acesta menține o listă a datelor capturate și permite operațiuni precum marcare, comentarii sau salvarea individuală a pachetelor. Sistemul de raportare funcționează în strânsă legătură cu motorul de captură și cu baza de date, extrăgând informațiile relevante și prezentându-le sub formă de documente PDF sau fișiere JSON, alături de reprezentări grafice generate automat.

Pentru a facilita procesul de selecție a sursei de trafic, aplicația include și o componentă de identificare a interfețelor de rețea, care extrage denumirile reale ale acestora, îmbunătățind astfel experiența de utilizare. Persistența datelor este asigurată printr-un sistem de stocare local, care permite salvarea sesiunilor și alertelor într-o bază de date, structurată astfel încât să poată fi interogată ulterior în funcție de mai mulți parametri.

Prin această distribuție clară a responsabilităților între componente, arhitectura aplicației reușește să asigure echilibrul între flexibilitate, performanță și mentenabilitate. Fiecare modul poate fi modificat, testat sau extins în mod independent, fără a afecta funcționarea celorlalte părți ale aplicației. Astfel, *Sentinel Traffic Analyzer* devine un cadru robust și extensibil, capabil să răspundă eficient cerințelor actuale și viitoare din domeniul analizei traficului de rețea.

## **3.5 Modelul de date și structura bazei de date**

Persistența datelor în cadrul aplicației *Sentinel Traffic Analyzer* este asigurată printr-un sistem de stocare care combină două componente principale: o bază de date locală, utilizată pentru gestionarea sesiunilor, pachetelor și alertelor, și un serviciu API extern, prin care fișierele .pcap sunt salvate fizic și înregistrate într-o bază de date relațională (PostgreSQL).

Aplicația locală stochează temporar datele capturate în fișiere de tip .pcap, precum și metadatele asociate acestora (timestamp, interfață utilizată, durată, volum de trafic). Aceste date sunt ulterior disponibile pentru analiză post-eveniment, fie prin interfața grafică, fie prin exportul în formate standardizate. Pentru o utilizare avansată și centralizată, aplicația oferă și posibilitatea de a trimite aceste fișiere către un API extern, unde sunt gestionate în mod persistent.

Componenta de backend este realizată folosind frameworkul Flask și oferă un punct de acces HTTP la ruta /upload, unde fișierele .pcap sunt transmise prin metode POST. La primirea unui fișier valid, acesta este salvat local într-un director dedicat pe server (/server\_storage/pcaps), iar referința către fișierul salvat este înregistrată într-o bază de date PostgreSQL. Acest proces asigură atât păstrarea fișierelor brute, cât și posibilitatea de a le identifica și regăsi prin interogări directe în baza de date.

Conexiunea cu baza de date este gestionată prin modulul psycopg2, iar parametrii de autentificare sunt încărcați dintr-un fișier .env, pentru a păstra securitatea datelor de acces. Structura tabelului pcap\_metadata este simplă și eficientă, incluzând câmpuri precum filename (numele generat al fișierului) și filepath (calea completă de stocare pe server).

Fragmentul de cod de mai jos ilustrează acest proces:

@app.route("/upload", methods=["POST"])

def upload\_file():

file = request.files['file']

timestamp = datetime.now().strftime("%Y%m%d\_%H%M%S")

filename = f"capture\_{timestamp}.pcap"

filepath = os.path.join(UPLOAD\_FOLDER, filename)

file.save(filepath)

conn = get\_db\_connection()

cur = conn.cursor()

cur.execute(

"INSERT INTO pcap\_metadata (filename, filepath) VALUES (%s, %s)",

(filename, filepath)

)

conn.commit()

Această abordare permite scalarea aplicației pentru utilizare în rețele mai mari sau în scenarii distribuite, unde mai mulți clienți pot încărca capturi spre un punct centralizat de stocare și analiză. În același timp, sistemul rămâne compatibil cu rularea locală, pentru cazurile în care rețelele nu permit acces extern sau se dorește rularea aplicației în mod izolat.

În ceea ce privește modelul de date local utilizat în aplicație, structura este orientată pe sesiuni. Fiecare sesiune de monitorizare este identificată printr-un ID unic și conține o listă de pachete capturate, salvate în structuri serializabile. Alertele generate în timpul sesiunii sunt asociate cu aceste capturi și stocate în fișiere .log și .json, iar datele semnificative extrase din trafic pot fi interogate pe baza unor filtre precum IP sursă, porturi sau protocoale.

Prin această combinație între stocarea locală și integrarea cu servicii externe, aplicația oferă un sistem de persistență flexibil, sigur și scalabil, care răspunde cerințelor de audit, analiză și arhivare a traficului monitorizat.

## **3.6 Fluxul de execuție în aplicație**

Funcționarea aplicației *Sentinel Traffic Analyzer* urmează un flux de execuție bine definit, care acoperă toate etapele de utilizare, de la inițializarea interfeței grafice până la încheierea unei sesiuni și generarea unui raport. Acest flux este organizat astfel încât utilizatorul să poată interacționa cu sistemul într-un mod intuitiv, iar toate acțiunile efectuate să se reflecte în mod direct asupra modului de procesare și afișare a traficului de rețea.

La lansarea aplicației, interfața grafică este inițializată și utilizatorului i se prezintă o fereastră principală în care sunt încărcate componentele de control, afișare și configurare. Printre primele acțiuni necesare se numără selectarea unei interfețe de rețea, care este identificată automat de un utilitar intern care utilizează WMI pentru a extrage numele reale ale plăcilor de rețea disponibile în sistem. Această selecție este fundamentală pentru inițierea unei sesiuni de captură.

Odată aleasă interfața, utilizatorul poate lansa procesul de captură. Acesta este pornit prin intermediul unui buton din interfață, care declanșează în fundal activarea modulului de captură. Captura traficului se desfășoară asincron, astfel încât interfața să rămână responsivă. Pe măsură ce pachetele sunt interceptate, acestea sunt procesate în timp real și afișate în zona de vizualizare, într-un tabel cu actualizare progresivă.

În paralel, fiecare pachet procesat este transmis către modulul de analiză comportamentală. Acesta verifică pachetele conform unor reguli prestabilite, detectând activități suspecte precum scanări de porturi sau tentative de flood. În cazul identificării unui eveniment neobișnuit, sistemul generează automat o alertă, care este înregistrată și afișată în interfața grafică, precum și salvată pentru referință ulterioară.

Pe tot parcursul sesiunii, utilizatorul are posibilitatea de a opri temporar capturarea, de a salva traficul sub formă de fișier .pcap și de a efectua filtrări după diverse criterii. La finalul unei sesiuni, toate datele pot fi exportate în diferite formate, iar aplicația oferă posibilitatea de a genera un raport automat. Acest raport conține statistici despre numărul de pachete, tipurile de protocoale întâlnite, alertele generate și o hartă a rețelei detectate, inclusiv cu locații geografice asociate IP-urilor (prin integrarea GeoLite2).

În cazul în care fișierul rezultat este considerat relevant pentru analiză centralizată sau pentru arhivare într-un sistem extern, utilizatorul poate transmite fișierul .pcap către o interfață API. Acest serviciu salvează fișierul pe server și înregistrează metadatele într-o bază de date PostgreSQL, oferind astfel un mecanism suplimentar de stocare și consultare ulterioară.

Întregul flux este însoțit de mecanisme de validare și notificare, care previn acțiunile eronate (de exemplu, pornirea capturii fără interfață selectată) și oferă feedback în timp real cu privire la starea operațiilor efectuate. Finalizarea unei sesiuni este marcată de oprirea capturii, salvarea datelor și revenirea aplicației într-o stare inactivă, în așteptarea unei noi comenzi.

Prin acest flux bine definit, aplicația permite controlul complet asupra unei sesiuni de analiză de rețea, punând la dispoziția utilizatorului instrumentele necesare pentru captură, filtrare, analiză, alertare și raportare, într-un mod unitar și eficient.

## **3.7 Sistemul de alertare și detectare a comportamentelor suspecte**

Un element central al aplicației *Sentinel Traffic Analyzer* este capacitatea de a detecta în timp real comportamente de rețea neobișnuite, asociate potențial cu activități periculoase sau malițioase. Acest mecanism este implementat într-un modul dedicat, detector.py, care rulează în fundal în paralel cu procesul de captură și analiză a traficului. Funcția principală a acestuia este de a analiza fiecare pachet interceptat și de a semnala activități suspecte prin generarea de alerte.

La inițializare, detectorul creează mai multe structuri interne pentru urmărirea comportamentului IP-urilor din trafic. Aceste structuri folosesc colecții de tip defaultdict, unde se păstrează înregistrări temporale pentru fiecare activitate detectată. Această abordare permite o analiză în timp scurt (sliding window), fără stocarea persistentă a întregului istoric.

Fiecare linie analizată este procesată de metoda process\_packet(), care extrage adresa IP sursă și eventual portul de destinație. Pe baza acestor date, sunt aplicate mai multe reguli de detecție care verifică:

* Trafic provenit de la adrese IP aflate pe o listă neagră (BLACKLIST). În acest caz, alerta este imediat marcată cu severitate maximă;
* Scanarea de porturi, identificată atunci când un IP accesează mai mult de zece porturi diferite într-un interval scurt;
* Atacuri de tip DNS flood, în care sunt detectate un număr mare de cereri către portul 53 într-o perioadă restrânsă;
* SYN flood, semnalat printr-un volum ridicat de pachete care conțin flag-ul SYN, dar nu și ACK;
* ICMP flood, determinat pe baza numărului de mesaje ICMP primite de la un IP în cinci secunde.
* UDP flood, similar ca structură, dar axat pe traficul UDP;
* ARP spoofing, detectat prin analizarea intensității mesajelor ARP provenite de la o singură sursă.

Dacă oricare dintre aceste condiții este îndeplinită, se generează o alertă sub forma unui mesaj text și a unui nivel de severitate. Alerta este apoi înregistrată simultan în două fișiere: unul de tip .log și altul de tip .json. Această dublă salvare are rolul de a permite atât o inspecție rapidă a jurnalului într-un editor text, cât și o analiză automată ulterioară pe baza formatului structurat JSON.

Mecanismul de înregistrare este implementat în metoda log\_alert(). Aceasta creează automat câte un fișier de alertă pentru fiecare zi de funcționare, utilizând ca denumire data curentă. Astfel, alertele pot fi revizuite și organizate cronologic, iar sistemul poate genera statistici privind frecvența și severitatea incidentelor de rețea.

Prin urmare, modulul detector.py contribuie la transformarea aplicației într-un instrument de detecție activă, capabil să identifice în mod automat semne ale unor atacuri sau disfuncționalități în rețea. Acest subsistem nu doar completează funcționalitatea de monitorizare pasivă, ci oferă și o bază pentru implementarea unor reacții automate în viitor, prin corelarea alertelor cu acțiuni de blocare, notificare sau escaladare.

## **3.8 Generarea de rapoarte și vizualizări**

Pentru a oferi o imagine de ansamblu asupra traficului capturat și pentru a sprijini procesul de analiză post-eveniment, aplicația *Sentinel Traffic Analyzer* integrează un modul dedicat pentru generarea de rapoarte și vizualizări grafice. Acest modul, implementat în cadrul clasei ReportData, centralizează informațiile colectate în timpul sesiunilor de monitorizare și le transformă într-un format accesibil, lizibil și ușor de distribuit.

Pe durata unei sesiuni active, toate pachetele capturate sunt înregistrate împreună cu metadatele relevante, cum ar fi momentul capturii, IP-ul sursă, IP-ul destinație, protocolul utilizat sau numărul total de pachete. Modulul colectează în paralel informații despre frecvența protocoalelor, distribuția traficului pe IP-uri, alertele generate de modulul de detecție și volumul de trafic în timp. Aceste date sunt stocate în structuri optimizate, cu acces rapid, și pot fi convertite într-un format JSON pentru procesare ulterioară automată sau stocare.

În vederea generării de vizualizări grafice, ReportData utilizează bibliotecile matplotlib și networkx. Se creează astfel grafice de tip bară, care reflectă distribuția protocoalelor și volumul de trafic per IP, grafice liniare pentru evoluția traficului în timp și diagrame circulare care ilustrează proporția alertelor pe categorii. Pe lângă aceste elemente statistice, modulul construiește și o hartă a rețelei, în care IP-urile detectate sunt reprezentate ca noduri conectate în funcție de legăturile observate între ele. Această hartă oferă o perspectivă vizuală utilă pentru înțelegerea topologiei rețelei monitorizate.

Funcția principală de export este export\_pdf\_report, care generează un document PDF cuprinzător. Acesta include, într-o primă parte, un rezumat al sesiunii: numărul total de pachete, momentul de început și sfârșit al capturii, protocoalele utilizate, cele mai frecvente adrese IP sursă și destinație, precum și lista alertelor generate. Informațiile textuale sunt organizate clar, în ordine logică, cu fonturi și formatare specifice, asigurând astfel o prezentare profesională a datelor.

Ulterior, raportul PDF integrează imaginile grafice generate anterior. Acestea sunt inserate automat, pe pagini separate, și includ graficele statistice și harta de rețea. Fișierele grafice sunt selectate din directorul curent, iar denumirile acestora sunt validate pentru a evita introducerea de fișiere lipsă. Pentru a garanta compatibilitatea și lizibilitatea textului în cadrul PDF-ului, este aplicată o funcție de transliterare care înlocuiește caracterele specifice limbii române cu echivalente ASCII.

Raportul final astfel generat poate fi exportat în format .pdf și salvat local sau transmis către un serviciu extern, împreună cu fișierul brut .pcap, pentru arhivare sau audit. Procesul de generare este complet automatizat, astfel încât, odată finalizată sesiunea de monitorizare, utilizatorul să poată obține rapid o sinteză completă a activității de rețea analizate.

Acest sistem de raportare contribuie la extinderea funcționalității aplicației dincolo de analiza în timp real, adăugând o componentă importantă de informare, comunicare și analiză retrospectivă. Prin combinarea datelor brute cu reprezentări grafice intuitive și conținut textual bine structurat, rapoartele produse devin un instrument util atât pentru utilizatorii tehnici, cât și pentru factorii de decizie care evaluează starea rețelei sau investighează incidente de securitate.

**3.9 Probleme întâmpinate și soluții aplicate**

Pe parcursul dezvoltării aplicației *Sentinel Traffic Analyzer*, au existat mai multe provocări tehnice și arhitecturale care au necesitat identificarea unor soluții adaptate contextului platformei și specificului sistemului de operare. Procesul de realizare a unei aplicații complexe, care integrează captură de pachete, analiză în timp real, generare de alerte și interfață grafică reactivă, a implicat luarea unor decizii iterative, în funcție de limitările identificate în fazele de testare și implementare.

Unul dintre cele mai frecvente obstacole întâmpinate a fost legat de accesul la interfețele de rețea pe sistemele Windows. Captura de pachete la nivel scăzut necesită privilegii de administrator și o bibliotecă compatibilă cu driverul rețelei (precum Npcap). În absența acestor condiții, aplicația returna erori critice sau nu detecta nicio interfață disponibilă. Pentru a atenua aceste efecte, a fost integrat un sistem de notificare vizuală, care avertizează utilizatorul cu privire la lipsa privilegiilor sau la imposibilitatea de a accesa resursele necesare.

O altă dificultate a vizat menținerea performanței interfeței grafice în condițiile în care sunt interceptate volume mari de trafic. Inițial, actualizarea vizuală a pachetelor interceptate se realiza direct în threadul principal al interfeței, ceea ce ducea la blocaje și latențe. Soluția adoptată a constat în delegarea capturii către un fir de execuție paralel, cu sincronizare controlată între fluxul de captură și actualizarea interfeței, prin intermediul funcțiilor callback. Această decuplare a îmbunătățit considerabil responsivitatea GUI-ului, chiar și în condiții de trafic ridicat.

În etapa de dezvoltare a sistemului de alertare, s-a constatat că anumite condiții de detecție produceau alerte false pozitive, în special în cazul traficului local cu caracter repetitiv (de exemplu, cereri DNS legitime în buclă). Pentru a filtra acest comportament, s-au implementat ferestre de timp ajustabile și praguri dinamice de declanșare, care evaluează atât frecvența, cât și varietatea evenimentelor suspecte. Astfel, doar comportamentele neobișnuite într-un interval scurt de timp declanșează alerte, reducând zgomotul informațional.

Integrarea componentelor externe, precum biblioteca geoip2 și fișierul GeoLite2-City.mmdb, a adus provocări legate de gestionarea fișierelor lipsă sau corupte. În absența unei verificări corespunzătoare, aplicația putea întâmpina erori la generarea hărților de rețea. Pentru a preveni aceste situații, a fost introdus un mecanism de validare a prezenței fișierului înainte de procesare, iar în cazul lipsei acestuia, aplicația continuă execuția fără a întrerupe fluxul principal, înlocuind informațiile lipsă cu valori implicite (de tip „N/A”).

Un alt aspect important a fost proiectarea unui mecanism de stocare flexibilă și sigură a fișierelor capturate, care să permită transmiterea acestora către un serviciu API. În contextul acestei integrări, au fost necesare ajustări în gestionarea numelor de fișiere, pentru a preveni suprascrierea accidentală, și în validarea formatului .pcap. De asemenea, au fost identificate erori de comunicare între client și server în cazul unor fișiere corupte sau incomplete, care au fost tratate prin introducerea unui sistem de răspuns detaliat, cu coduri de eroare și mesaje informative returnate de API.

În procesul de generare a rapoartelor PDF, utilizarea fonturilor și caracterelor diacritice a ridicat probleme de randare, în special în unele versiuni ale bibliotecii FPDF. Soluția aleasă a fost implementarea unei funcții de transliterare care normalizează caracterele specifice limbii române, pentru a asigura compatibilitatea și lizibilitatea documentelor generate, fără a compromite conținutul semantic.

# 4 DOCUMENTAREA SISTEMULUI

Acest capitol prezintă modalitatea de utilizare a aplicației *Sentinel Traffic Analyzer*, explicând componentele vizuale, fluxurile funcționale și modul în care utilizatorul interacționează cu sistemul. Sunt descrise principalele interfețe ale aplicației, atât cele de conectare și înregistrare, cât și componentele operaționale pentru captură și afișare a traficului de rețea. Documentarea este însoțită de capturi de ecran care exemplifică funcționarea aplicației în diverse stări și acțiuni.

## **4.1 Interfața de autentificare**

Pagina de autentificare oferă punctul de acces în aplicație pentru utilizatorii existenți. Interfața este realizată într-un stil modern și aerisit, cu accent pe claritate vizuală. Formularul include două câmpuri principale: adresa de email și parola. Acestea sunt însoțite de pictograme relevante, care facilitează recunoașterea rapidă a tipului de date solicitate.Изображение выглядит как текст, снимок экрана, Мультимедийное программное обеспечение, программное обеспечение

Контент, сгенерированный ИИ, может содержать ошибки.

**Figura 4.1 –** **Interfața de autentificare în aplicație**

În partea superioară a paginii este prezentat logo-ul aplicației și denumirea completă. Sub formular se regăsesc legături rapide către pagina de înregistrare și funcționalitatea de resetare a parolei. Această interfață este redată în **Figura 4.1**, care ilustrează ecranul de logare în starea inițială.

**4.2 Interfața de înregistrare**

Formularul de înregistrare permite crearea unui cont nou. Acesta este accesibil prin butonul „Sign Up” de pe pagina de autentificare. Utilizatorul este invitat să completeze un set de câmpuri obligatorii, printre care prenumele, numele, adresa de email, parola și confirmarea parolei. Interfața menține același stil vizual ca și pagina de autentificare, cu pictograme intuitive și un layout clar.

Изображение выглядит как текст, снимок экрана, Мультимедийное программное обеспечение, программное обеспечение

Контент, сгенерированный ИИ, может содержать ошибки.

Figura 4.2 – Formularul de creare a unui cont nou în aplicația Sentinel

Butonul de finalizare a înregistrării este evidențiat cromatic, pentru a sublinia funcționalitatea principală a formularului. Această pagină este ilustrată în **Figura 4.2**, care prezintă aspectul complet al interfeței de creare cont.

## **4.3 Interacțiunea cu baza de date**

După completarea formularului de înregistrare, datele sunt validate și procesate în partea de backend. Acestea sunt inserate într-o bază de date PostgreSQL, într-o tabelă denumită users. Structura acestei tabele include un identificator de tip UUID, numele și prenumele utilizatorului, adresa de email și o parolă criptată cu algoritmul SHA-512. Acest model permite gestionarea sigură a datelor personale și a acreditivelor de conectare.

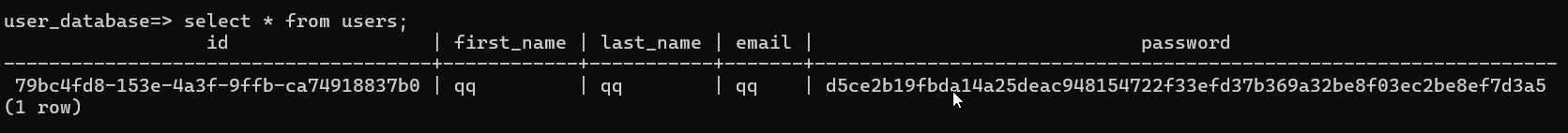


Figura 4.3 - Conținutul bazei de date PostgreSQL după înregistrarea unui utilizator

Validarea datelor și înregistrarea reușită pot fi confirmate și prin interogări directe asupra bazei de date. **Figura 4.3** prezintă rezultatul unei astfel de interogări, evidențiind înregistrarea noului utilizator.

## **4.4 Interfața principală a aplicației**

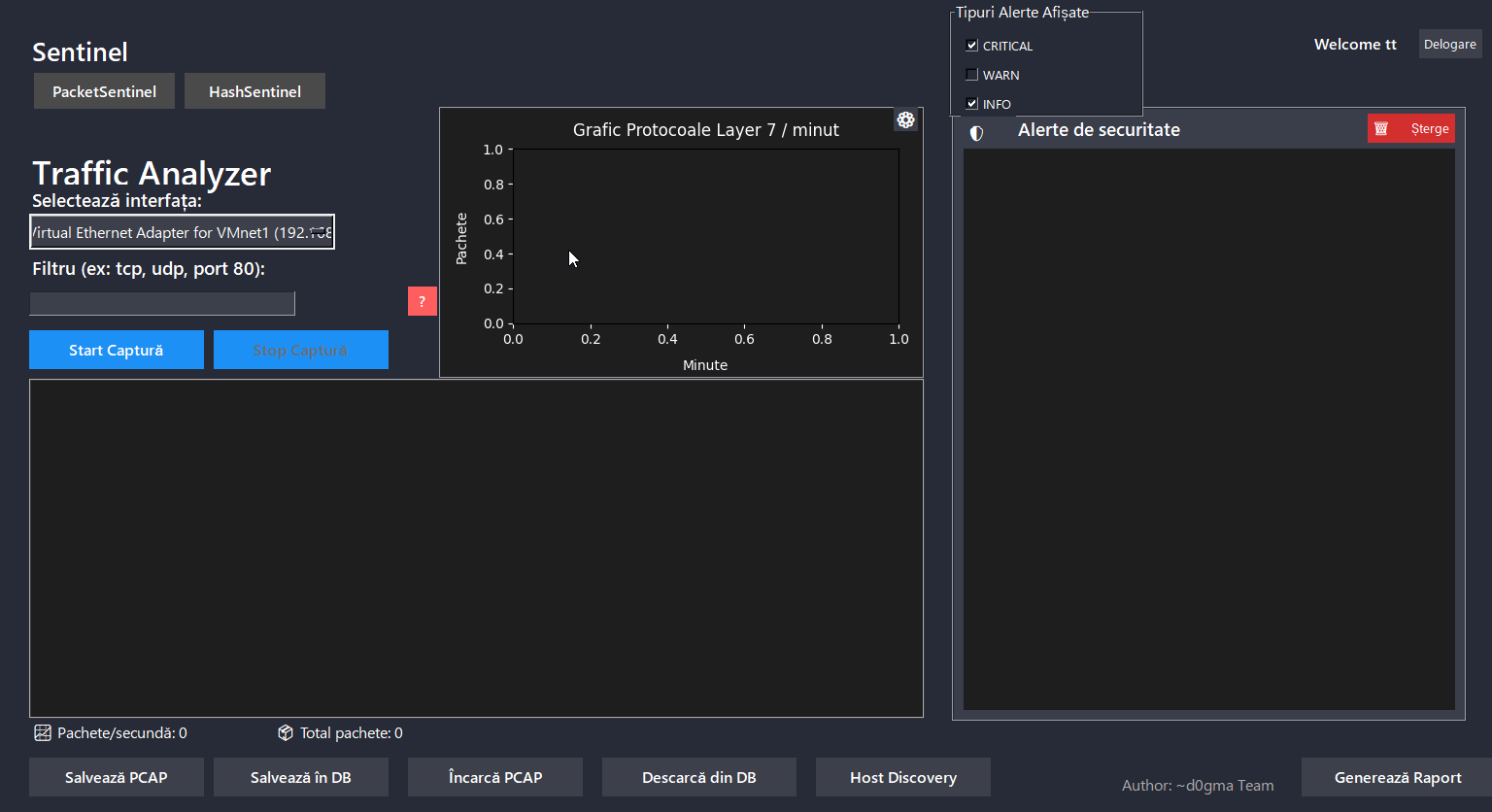
După autentificare, utilizatorul este redirecționat către fereastra principală a aplicației, unde sunt reunite toate modulele disponibile. Această interfață este organizată astfel încât să permită controlul complet asupra procesului de captură a traficului și accesul la funcționalitățile suplimentare.

Figura 4.4 - Interfața principală a aplicației

În partea centrală a ecranului se află panoul de control pentru captură. Utilizatorul selectează interfața de rețea activă, apoi poate porni procesul de monitorizare. Traficul este afișat în timp real în zona de vizualizare. Interfața include butoane pentru oprirea capturii, salvarea sesiunii și generarea de rapoarte. Această zonă de lucru este prezentată în **Figura 4.4**, într-o stare pre-captură.

## **4.5 Capturarea traficului de rețea**

Una dintre funcționalitățile centrale ale aplicației *Sentinel Traffic Analyzer* este capacitatea de a intercepta, analiza și afișa în timp real pachetele care circulă printr-o interfață de rețea selectată. Această funcție devine activă imediat după ce utilizatorul alege o interfață disponibilă din lista detectată de sistem și inițiază procesul de captură prin intermediul butonului dedicat din interfața principală.

Odată activată, aplicația utilizează un modul de captură de joasă nivel (scapy) care rulează într-un fir de execuție separat față de interfața grafică, asigurând astfel fluiditatea interacțiunii utilizatorului chiar și în condițiile în care traficul analizat este intens. Sistemul capturează fiecare pachet în momentul în care acesta trece prin interfață și îl procesează instantaneu, extrăgând metadatele relevante și afișându-le într-o formă structurată.

Pentru fiecare pachet interceptat, aplicația oferă următoarele informații: momentul exact al capturii (timestamp), adresa IP sursă, adresa IP destinație, protocolul utilizat (cum ar fi TCP, UDP sau ICMP), porturile implicate (acolo unde sunt aplicabile), precum și dimensiunea totală a pachetului. Aceste date sunt afișate într-un panou tip consolă, unde fiecare rând corespunde unui pachet individual, iar stilizarea vizuală a protocoalelor facilitează diferențierea rapidă a tipurilor de trafic.

A screenshot of a computer

AI-generated content may be incorrect.

Figura 4.5 - Capturarea traficului în timp real și afișarea în interfață

Captura este realizată în timp real, dar datele afișate pot fi și analizate ulterior. Aplicația oferă posibilitatea de filtrare a pachetelor în funcție de protocoale sau de adrese IP, precum și opțiuni de căutare rapidă în conținutul afișat. În plus, utilizatorul are la dispoziție funcționalități de marcare manuală a pachetelor suspecte, exportul selectiv al acestora, sau vizualizarea detaliilor brute ale conținutului, pentru investigații mai profunde.

Procesul de captură poate fi întrerupt în orice moment, fără pierderi de date sau coruperea sesiunii. Aplicația permite salvarea completă a sesiunii într-un fișier de tip .pcap, compatibil cu aplicații de analiză precum Wireshark. În paralel, există și opțiunea de a exporta datele sub formă text, într-un fișier .txt, pentru consultare directă, partajare sau documentare. Această flexibilitate în export facilitează adaptarea aplicației la diverse scenarii operaționale, fie ele tehnice sau educaționale.

Figura 4.5 prezintă o sesiune de captură în desfășurare, în care se observă interfața selectată (de tip loopback), zona de afișare a pachetelor, precum și starea activă a capturii, indicată vizual prin marcaje cromatice și butoane dinamice.

# 5 Analiza de risc, evaluarea și impactul proiectului

În cadrul dezvoltării și testării modulului PacketSentinel, componentă centrală a aplicației Sentinel Traffic Analyzer, au fost identificate o serie de riscuri tehnice și de utilizare, care pot influența performanța, securitatea și etica utilizării aplicației. Acest capitol are ca scop prezentarea riscurilor întâmpinate, a soluțiilor aplicate, precum și evaluarea funcționalităților realizate și impactul proiectului asupra formării academice, cercetării și carierei profesionale.

## **5.1 Riscuri tehnice**

Una dintre dificultățile frecvente în aplicațiile de analiză a traficului de rețea este reprezentată de restricțiile de acces la interfețele de rețea ale sistemului de operare. Pe platformele Windows, acest tip de acces este condiționat de existența unor privilegii administrative, precum și de funcționarea corectă a serviciilor externe, cum ar fi Npcap. În lipsa acestora, aplicația poate întâmpina blocaje sau returna o listă incompletă a interfețelor disponibile. Această problemă a fost gestionată printr-o verificare automată a interfețelor active și prin introducerea unor mesaje explicite de avertizare pentru utilizator.

Captura în timp real a unui volum ridicat de pachete poate conduce la suprasarcină și, implicit, la pierderi de date. Pentru a preveni această situație, sistemul de captură a fost conceput să funcționeze în paralel cu interfața grafică, fiecare dintre aceste procese desfășurându-se în fire de execuție separate. În plus, a fost adăugat suportul pentru filtrare avansată folosind expresii de tip BPF (Berkeley Packet Filter), ceea ce permite restrângerea traficului capturat la un subset relevant.

Probleme pot apărea și în interpretarea greșită sau lipsită de precizie a pachetelor capturate, în special atunci când utilizatorul introduce filtre de rețea incorecte sau prea generale. Pentru a reduce acest risc, aplicația permite ajustarea dinamică a filtrelor și oferă feedback vizual în timp real cu privire la efectele aplicării acestora.

Selectarea greșită a interfeței de rețea reprezenta un alt risc potențial, generat de faptul că bibliotecile tehnice identifică aceste interfețe prin denumiri tehnice (GUID-uri), care nu sunt intuitive. În acest sens, a fost introdus un mecanism de corelare între denumirea comercială a plăcii de rețea, adresa IP asociată și identificatorul intern, oferind astfel utilizatorului o imagine clară și completă asupra opțiunilor disponibile.

**5.2 Riscuri de utilizare**

Dincolo de aspectele tehnice, o provocare importantă este reprezentată de riscul utilizării aplicației în scopuri neautorizate. Prin natura sa, un analizator de trafic oferă capacitatea de a intercepta comunicații dintr-o rețea, iar dacă este folosit într-un mediu în care utilizatorul nu deține permisiuni, poate genera implicații legale sau etice. Pentru a limita acest risc, aplicația a fost concepută fără posibilitatea de a decodifica conținutul efectiv al datelor transmise (payload), concentrându-se exclusiv pe metadatele pachetului. De asemenea, aplicația este distribuită cu mențiunea clară a scopului său educațional și experimental.

**5.3 Funcționalități implementate**

Funcționalitățile de bază implementate în modulul PacketSentinel au fost verificate prin testare în medii controlate. Sistemul listează toate interfețele de rețea disponibile, afișând numele complet și adresa IP asociate fiecăreia. Utilizatorul poate selecta o interfață și poate iniția o sesiune de captură în timp real în care pachetele sunt interceptate și afișate pe ecran. Aplicația permite aplicarea de filtre precum TCP, UDP, ICMP sau filtre personalizate și oferă o reprezentare grafică a distribuției protocoalelor detectate, precum și a volumului de trafic măsurat în pachete pe minut.

Datele rezultate pot fi salvate într-un format specific pentru analiză ulterioară sau pentru arhivă, sub formă de fișiere .pcap sau .txt. Aceste funcții de export au fost verificate în mai multe sesiuni de testare, în rețele locale, wireless și cu trafic generat manual.

**5.4 Evaluarea performanței**

Testele efectuate au demonstrat că aplicația poate funcționa în condiții stabile pe rețele de tip wireless și cablate, fără a produce un consum excesiv de resurse de sistem. Captura se realizează în timp real, iar interfața grafică rămâne reactivă, chiar și în prezența unui volum ridicat de trafic. În plus, aplicația poate fi utilizată simultan cu alte instrumente de analiză a rețelei, fără interferențe sau conflicte de acces la resurse.

**5.5 Impactul educațional**

Cu interfața sa intuitivă și modul transparent de afișare a informațiilor, PacketSentinel oferă un instrument didactic valoros pentru studenții și profesioniștii care doresc să înțeleagă structura traficului de rețea. Acesta permite observarea în timp real a pachetelor generate de aplicații comune, cum ar fi navigarea pe internet, ping sau interogări DNS, fără a necesita utilizarea unor aplicații comerciale avansate sau greu de configurat. Studenții pot testa ipoteze, analiza fluxuri și învăța concepte de securitate de rețea fundamentale.

## **5.6 Contribuția în activitatea de cercetare**

Proiectul *PacketSentinel*, ca parte a aplicației *Sentinel Traffic Analyzer*, oferă o platformă flexibilă și extensibilă care poate fi adaptată cu ușurință în scopuri de cercetare în domeniul rețelisticii și al securității cibernetice. Prin arhitectura sa modulară și prin funcționalitățile deja implementate, aplicația poate constitui un punct de plecare valoros pentru studii experimentale, dezvoltarea de noi metode de analiză a traficului sau testarea de algoritmi de detecție a anomaliilor și atacurilor cibernetice.

Una dintre cele mai relevante direcții de cercetare în care aplicația poate fi integrată este investigarea comportamentului rețelelor sub influența diferitelor tipuri de atacuri. Modulul de detecție implementat deja în *PacketSentinel* permite recunoașterea unor tehnici de atac precum scanarea de porturi, inundațiile de tip SYN, UDP sau ICMP, precum și tentativele de falsificare a pachetelor ARP. Prin extinderea acestor mecanisme cu reguli personalizabile sau prin integrarea cu sisteme de învățare automată, se poate obține o platformă capabilă să identifice și să clasifice comportamente necunoscute sau subtile, greu de detectat prin metode convenționale.

În același timp, modulul de captură oferă o sursă valoroasă de date pentru generarea unor seturi de date de rețea, utile în simulări, în instruirea modelelor statistice sau în antrenarea algoritmilor de inteligență artificială. Prin utilizarea filtrelor avansate și prin exportul în formate standardizate (precum .pcap și .json), se pot extrage fluxuri specifice de interes, care să fie utilizate în experimente repetitive sau comparabile între scenarii diferite.

# BIBLIOGRAFIE

[1] Bejtlich, R. (2005). *The Tao of Network Security Monitoring: Beyond Intrusion Detection*. Addison-Wesley.

[2] Orebaugh, A., Ramirez, G., & Beale, J. (2006). *Wireshark & Ethereal Network Protocol Analyzer Toolkit*. Syngress.

[3] Scapy Documentation. (2024). [Online]. Available: <https://scapy.readthedocs.io/>

[4] Kurose, J. F., & Ross, K. W. (2021). *Computer Networking: A Top-Down Approach* (8th ed.). Pearson.

[5] Paxson, V. (1999). “Bro: A System for Detecting Network Intruders in Real-Time,” *Computer Networks*, vol. 31, pp. 2435–2463.

[6] Suricata IDS. *Suricata – Open Source Threat Detection Engine*. [Online]. Available: <https://suricata.io/>

[7] Nmap Network Scanning. (2024). *Nmap Guide to Network Discovery and Security Scanning*. [Online]. Available: https://nmap.org/book/

[8] Python Software Foundation. (2024). *Scapy Packet Manipulation Library*. [Online]. Available: <https://pypi.org/project/scapy/>

[9] RFC 791 – *Internet Protocol*. [Online]. Available: https://datatracker.ietf.org/doc/html/rfc791

[10] RFC 793 – *Transmission Control Protocol*. [Online]. Available: https://datatracker.ietf.org/doc/html/rfc793

[11] Go Authors. (2024). *Official Go Documentation*. [Online]. Available: <https://golang.org/doc/>

[12] Tkinter GUI Docs. (2024). *Python Tkinter GUI Reference*. [Online]. Available: <https://docs.python.org/3/library/tkinter.html>

[13] Stallings, W. (2017). *Network Security Essentials* (6th ed.). Pearson.

[14] Wireshark. (2024). *Wireshark User Guide*. [Online]. Available: https://www.wireshark.org/docs/