Ministerul Educaţiei, Culturii și Cercetării
Universitatea Tehnică a Moldovei

Faculatea Calculatoare, informatică și microelectronică
Departamentul Ingineria Software și Automatică

RAPORT

Lucrare de Laborator nr.1
Disciplina: Proiectarea sistemelor informaționale
Tema : Analiza și definirea domeniului de studiu

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

A verificat:
asist. univ. Tocan Alexandru

Chişinău 2024

Introducere

În era actuală a digitalizării, rețelele de date reprezintă coloana vertebrală a tuturor proceselor tehnologice, conectând dispozitive, utilizatori și servicii la nivel global. Creșterea rapidă a volumului de informații care circulă prin rețelele de calculatoare aduce nu doar beneficii extraordinare, ci și provocări majore în ceea ce privește securitatea și controlul datelor. În acest context, dezvoltarea unui sistem integrat pentru interceptarea și analiza traficului de rețea devine o necesitate stringentă pentru protejarea informațiilor sensibile și garantarea securității cibernetice.

Interceptarea și analiza traficului de rețea se referă la procesele de captare, examinare și interpretare a pachetelor de date care tranzitează o rețea. Un astfel de sistem permite administratorilor de rețea și specialiștilor în securitate să identifice activități suspecte, să detecteze breșele de securitate și să prevină atacurile cibernetice înainte ca acestea să provoace daune majore. În plus, analiza traficului de rețea poate oferi informații valoroase despre performanța infrastructurii, identificând blocaje sau utilizări ineficiente ale resurselor.

Pe măsură ce complexitatea și dimensiunea rețelelor continuă să crească, este esențial ca soluțiile de interceptare și analiză să fie suficient de robuste și scalabile pentru a răspunde cerințelor variate ale mediilor corporative, guvernamentale și chiar ale utilizatorilor individuali. Un sistem integrat, care îmbină tehnologiile de monitorizare pasivă și activă, poate oferi o imagine completă a traficului de rețea, asigurând o protecție eficientă împotriva amenințărilor interne și externe.

Dezvoltarea unui astfel de sistem implică integrarea mai multor componente esențiale: captarea traficului în timp real, filtrarea datelor relevante, identificarea anomaliilor, și generarea de rapoarte și alerte personalizate. Aceste procese permit atât analiza în timp real, cât și investigarea ulterioară a incidentelor de securitate. Prin intermediul unui astfel de sistem, organizațiile pot obține o transparență totală asupra fluxului de date din rețea, consolidându-și strategiile de apărare cibernetică.

Astfel, un sistem integrat pentru interceptarea și analiza traficului de rețea nu doar că răspunde provocărilor legate de securitate și performanță, ci contribuie și la crearea unui mediu digital mai sigur și mai eficient, reducând riscul de atacuri cibernetice și minimizând impactul acestora asupra afacerilor și utilizatorilor.

1.Analiza domeniului si analiza antreprizei

În dezvoltarea unui **sistem integrat pentru interceptarea și analiza traficului de rețea**, analiza domeniului și antreprizei reprezintă pași cruciali pentru a înțelege provocările și cerințele acestui sector. Domeniul principal al acestui proiect este securitatea cibernetică, cu un accent special pe monitorizarea și analiza rețelelor de date, atât în timp real, cât și retrospectiv. Scopul unui astfel de sistem este de a detecta, analiza și preveni eventualele amenințări cibernetice, protejând integritatea, confidențialitatea și disponibilitatea datelor care circulă în rețea.

Analiza domeniului implică examinarea contextului general al securității rețelelor și a evoluției amenințărilor cibernetice. Pe măsură ce tot mai multe organizații își desfășoară activitățile în mediul online, atacurile cibernetice, cum ar fi atacurile de tip DDoS, interceptarea pachetelor, exploatarea vulnerabilităților și injectarea de malware, au devenit tot mai frecvente și sofisticate. Acest context subliniază importanța unui sistem robust și integrat care să permită monitorizarea constantă a rețelei și detectarea timpurie a activităților suspecte.

Antrepriza – sau entitatea care ar beneficia de implementarea acestui sistem – poate varia de la companii mici și mijlocii, la corporații multinaționale și instituții guvernamentale, care dețin date sensibile și au nevoie de soluții avansate pentru a preveni pierderile de date sau accesul neautorizat. Securitatea rețelelor reprezintă o prioritate strategică pentru orice organizație, deoarece breșele de securitate nu doar că pot cauza pierderi financiare, ci și deteriorarea reputației.

În urma acestei analize, putem evidenția câteva **nevoi cheie** ale antreprizei:

- **Monitorizare în timp real**: Organizațiile au nevoie de un sistem care să captureze și să analizeze traficul în timp real pentru a detecta rapid amenințările și a reduce timpul de răspuns.
- **Analiză detaliată**: Identificarea comportamentelor anormale sau activităților suspecte în rețea necesită un nivel ridicat de detalii, ceea ce implică o soluție capabilă să proceseze un volum mare de date și să ofere alerte precise.
- **Prevenire proactivă**: Sistemul ar trebui să poată identifica tipare și să prevină posibilele atacuri prin analizarea traficului istoric și a anomaliilor comportamentale.
- **Scalabilitate**: Cu extinderea constantă a infrastructurilor IT, soluția trebuie să fie scalabilă pentru a gestiona un volum variabil de trafic de rețea.

Oportunitatea principală pe care o prezintă un astfel de sistem constă în capacitatea sa de a transforma modul în care organizațiile își securizează rețelele. Prin integrarea interceptării și analizei traficului într-o soluție unică și automatizată, organizațiile pot reduce semnificativ riscul de atacuri cibernetice și pot gestiona mai eficient incidentele de securitate. Într-un context în care costurile provocate de incidentele de securitate sunt în continuă creștere, implementarea unui astfel de sistem poate aduce economii importante și un avantaj competitiv pentru antrepriză.

1.1 Cercetarea sistemelor informaționale existente

Pentru a dezvolta un sistem integrat pentru interceptarea și analiza traficului de rețea, este esențial să înțelegem soluțiile disponibile în prezent în acest domeniu și modul în care acestea funcționează. Fiecare soluție are propriile sale avantaje, dezavantaje și tehnologii utilizate, iar aceste aspecte trebuie analizate în detaliu pentru a stabili cum pot fi îmbunătățite sau integrate într-o nouă aplicație.

Una dintre cele mai cunoscute aplicații pentru analiza traficului de rețea este Wireshark, un instrument extrem de popular datorită capacității sale de a captura pachetele de date în timp real și de a le analiza cu o precizie incredibilă. Wireshark este folosit pe scară largă datorită suportului său extins pentru un număr foarte mare de protocoale de rețea și a interfeței sale grafice intuitive, care permite utilizatorilor să vizualizeze și să filtreze traficul pe baza unor criterii specifice. Prin intermediul Wireshark, inginerii de rețea și experții în securitate pot analiza fluxurile de date în detaliu, identificând comportamentele anormale sau problemele de performanță ale rețelei. Cu toate acestea, complexitatea acestui instrument poate fi descurajantă pentru utilizatorii care nu au experiență în analiza detaliată a protocoalelor, iar funcționalitățile sale sunt limitate la nivelul de captură și analiză a pachetelor, fără a oferi o detecție automată a amenințărilor.

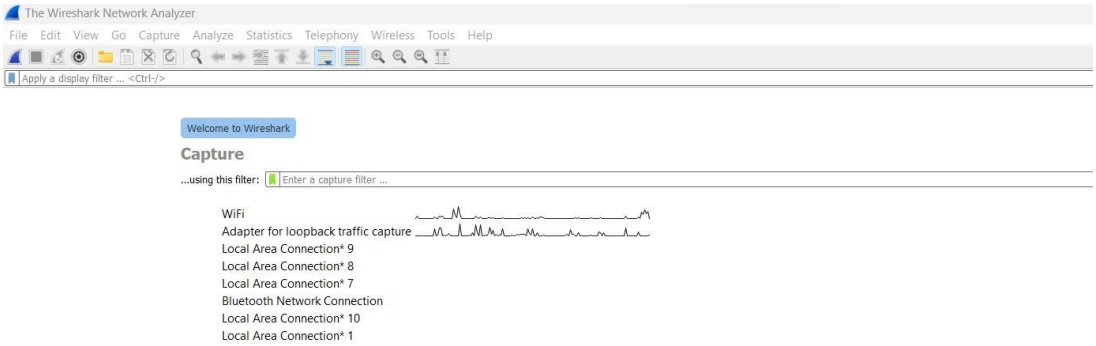

Figura 1.1 – Wireshark

Pe de altă parte, Zeek (cunoscut anterior ca Bro IDS) reprezintă un pas înainte în ceea ce privește detecția și analiza traficului de rețea. Spre deosebire de Wireshark, care se concentrează pe analiza pasivă a pachetelor, Zeek este un sistem orientat spre securitate, capabil să detecteze activități neobișnuite și amenințări complexe în rețea. Cu ajutorul scripturilor personalizate, Zeek permite utilizatorilor să

monitorizeze rețelele într-un mod mai dinamic și să identifice anomalii comportamentale care ar putea indica o intruziune sau alte amenințări cibernetice. În același timp, această capacitate avansată vine cu un preț: utilizarea Zeek necesită o învățare și o configurare mai complexă, iar pentru rețele mari, poate deveni resursiv, necesitând infrastructuri hardware mai performante.

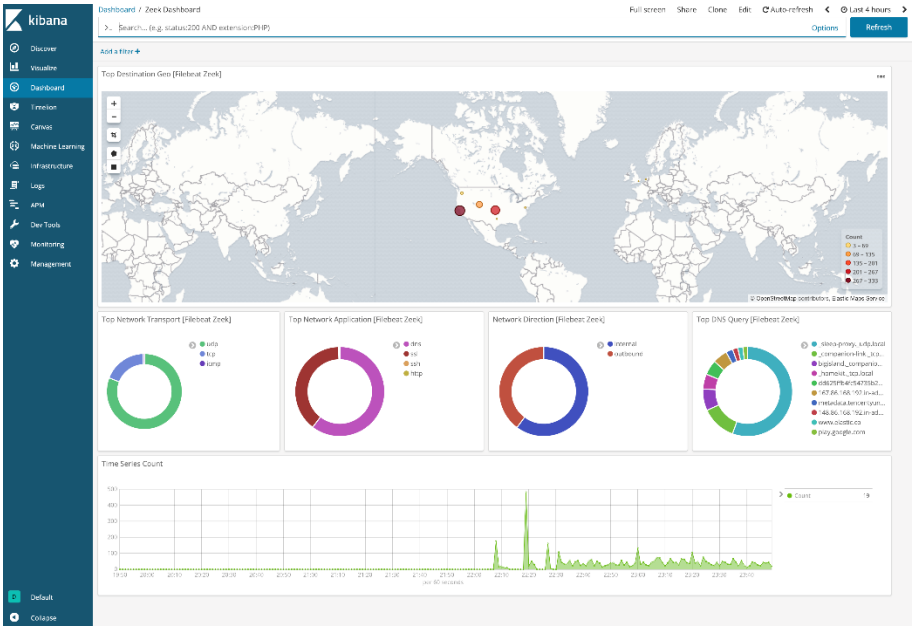

Figura 1.2 – Zeek/Bro

Un alt sistem esențial în domeniul monitorizării și analizei rețelelor este Snort, care a devenit un standard în detecția și prevenirea intruziunilor (IDS/IPS). Snort funcționează prin analiza traficului de rețea în timp real și detectarea semnăturilor specifice asociate cu diferite tipuri de atacuri cibernetice. Această capacitate de a detecta rapid atacurile cunoscute îl face un instrument puternic pentru protecția rețelelor, dar și unul limitat la detectarea amenințărilor bazate pe semnături predefinite. În contextul atacurilor zero-day, care nu au încă o semnătură definită, Snort poate deveni ineficient, iar acest aspect trebuie luat în considerare de către organizațiile care se bazează pe acest tip de soluție.

Într-un mod similar, Suricata este o soluție IDS/IPS care extinde funcționalitățile Snort, oferind suport pentru multi-threading și capacități avansate de analiză a pachetelor. Suricata este apreciată pentru performanța sa superioară în comparație cu alte soluții, datorită capacității sale de a analiza simultan multiple fluxuri de date, ceea ce îi permite să proceseze volume mari de trafic fără a pierde din detalii. În plus, Suricata oferă suport pentru inspecția profundă a pachetelor (DPI) și poate decoda protocoale complexe, făcându-l un instrument foarte util pentru organizațiile care au nevoie de o soluție robustă pentru monitorizarea și protecția rețelei. Cu toate acestea, utilizarea sa necesită o curba de învățare mai abruptă, iar configurarea sa inițială poate fi dificilă pentru cei care nu sunt familiarizați cu tehnologiile avansate de securitate.

Pe lângă soluțiile axate pe detecția și prevenirea intruziunilor, există și instrumente dedicate monitorizării performanței rețelei, cum ar fi **SolarWinds Network Performance Monitor (NPM)**.

SolarWinds NPM este recunoscut pentru capacitatea sa de a monitoriza în timp real performanța infrastructurii de rețea, oferind informații detaliate despre fluxurile de date și identificând rapid orice probleme de performanță. Soluția este apreciată pentru interfața sa grafică intuitivă, care permite utilizatorilor să acceseze cu ușurință rapoarte și statistici despre starea rețelei. Cu toate acestea, SolarWinds NPM se concentrează mai mult pe analiza performanței decât pe securitate, ceea ce îl face mai potrivit pentru organizațiile care doresc să își optimizeze infrastructura și mai puțin pentru cele care caută o soluție dedicată securității rețelei.

TShark este o variantă a Wireshark care funcționează exclusiv în linia de comandă și reprezintă un instrument puternic pentru capturarea și analiza traficului de rețea. Acesta oferă aceleași capacități avansate de capturare a pachetelor ca Wireshark, dar fără interfața grafică, ceea ce îl face ideal pentru utilizatorii care preferă să lucreze din linia de comandă sau pentru scenarii unde interfața grafică nu este disponibilă sau necesară, cum ar fi în cadrul serverelor sau sistemelor integrate.

Unul dintre avantajele majore ale TShark este flexibilitatea sa. Poate fi utilizat pentru a captura date în timp real sau pentru a analiza fișierele de captură create anterior. Utilizatorii au acces la o gamă largă de opțiuni de filtrare și selecție a datelor care pot fi aplicate fie în timpul capturării, fie ulterior, la procesarea datelor. Filtrele de captură și afișare permit extragerea informațiilor relevante din fluxul de date brut, ceea ce facilitează concentrarea pe aspectele critice, cum ar fi analizarea anumitor protocoale sau identificarea traficului anormal.

TShark este adesea preferat în medii unde automatizarea este esențială, fiind ușor de integrat în scripturi pentru monitorizare automată și analiza periodică a traficului de rețea. De exemplu, poate fi configurat pentru a captura pachete pe anumite interfețe de rețea și pentru a salva capturile într-un fișier, care poate fi analizat ulterior pentru detectarea de erori sau comportamente suspecte.

Un alt avantaj al TShark este faptul că consumă mai puține resurse decât Wireshark, datorită lipsei unei interfețe grafice. Aceasta îl face o opțiune excelentă pentru medii unde resursele hardware sunt limitate sau pentru servere de producție unde eficiența este crucială. Poate fi rulat în fundal fără a afecta în mod semnificativ performanțele sistemului, ceea ce îl face ideal pentru scenarii de monitorizare continuă.

Cu toate acestea, lipsa unei interfețe grafice poate fi un dezavantaj pentru utilizatorii care nu sunt confortabili cu linia de comandă sau pentru cei care doresc o analiză vizuală detaliată a datelor. Deși TShark oferă o gamă completă de funcționalități, interpretarea rezultatelor poate fi mai dificilă în lipsa vizualizărilor grafice și a interacțiunii intuitive oferite de Wireshark.

În concluzie, TShark este un instrument deosebit de util pentru profesioniștii care au nevoie de un instrument flexibil, puternic și eficient pentru capturarea și analiza traficului de rețea, mai ales în scenarii care necesită utilizarea liniei de comandă sau automatizarea sarcinilor. Deși nu are o interfață grafică,

capacitățile sale avansate îl fac o soluție valoroasă pentru analiza rețelelor în timp real sau pentru procesarea unor volume mari de date într-un mod rapid și eficient.

1.1 Analiza utilizatorilor potențiali

În analiza unui **sistem integrat pentru interceptarea și analiza traficului de rețea**, este important să definim și să înțelegem utilizatorii potențiali ai acestui sistem, similar modului în care se analizează categoriile de utilizatori pentru o aplicație de monitorizare a animalelor de companie. Un astfel de sistem ar avea utilizatori dintr-o gamă largă de domenii și ar putea servi mai multe scopuri, fiecare grup având nevoi și obiective specifice.

Primul și cel mai evident grup de utilizatori îl reprezintă **administratorii de rețea** și **specialiștii IT** din companii, care se confruntă frecvent cu nevoia de a monitoriza și optimiza performanțele rețelelor lor. Pentru aceștia, un sistem integrat pentru interceptarea și analiza traficului de rețea este un instrument esențial în gestionarea securității și performanței rețelei. Ei vor utiliza sistemul pentru a detecta anomalii, a identifica și izola problemele, și pentru a preveni potențiale atacuri cibernetice sau breșe de securitate. Un astfel de sistem le oferă control și vizibilitate deplină asupra traficului de rețea, ajutându-i să asigure continuitatea activităților și protecția datelor.

Un al doilea grup de utilizatori include **echipele de securitate cibernetică** și **analiștii de securitate**. Aceștia au nevoie de acces constant la datele de rețea pentru a monitoriza amenințările, a răspunde rapid la incidente și pentru a asigura conformitatea cu reglementările în materie de securitate. Un sistem de interceptare a traficului de rețea le permite să obțină date valoroase în timp real, să investigheze activități suspecte și să prevină accesul neautorizat. Utilizarea unui astfel de sistem contribuie la o mai bună protecție împotriva atacurilor, cum ar fi atacurile de tip DDoS sau intruziunile avansate.

Organizațiile mari, în special cele care gestionează cantități masive de date și au rețele complexe, reprezintă un alt grup de utilizatori potențiali. Aceste organizații, precum băncile, instituțiile guvernamentale sau companiile telecom, trebuie să se asigure că traficul lor de rețea este monitorizat constant pentru a preveni pierderile de date, atacurile cibernetice și alte incidente critice. Pentru ele, un sistem de monitorizare a traficului de rețea poate fi integrat în strategiile lor de conformitate și de prevenție a riscurilor, ajutându-le să se asigure că toate datele tranzitate prin rețelele lor sunt sigure și conforme cu legislația în vigoare.

Un alt tip de utilizatori sunt **furnizorii de servicii de internet (ISP)**. Aceștia ar putea folosi un astfel de sistem pentru a analiza și gestiona traficul clienților lor, optimizând performanța rețelelor și oferind o experiență de utilizare îmbunătățită. De asemenea, ISP-urile pot utiliza aceste sisteme pentru a monitoriza și restricționa anumite tipuri de trafic, conform politicilor companiei și cerințelor legale, protejându-se totodată împotriva atacurilor cibernetice care vizează rețelele lor.

Nu în ultimul rând, **companiile care oferă soluții de monitorizare și securitate IT** sunt un grup de utilizatori potențiali, deoarece ele ar putea integra acest sistem în portofoliul lor de servicii pentru a oferi soluții mai avansate și complete clienților. Aceștia pot oferi un astfel de sistem fie ca un serviciu administrat (managed service), fie ca o soluție dedicată, adresându-se astfel nevoilor organizațiilor care nu au resursele interne necesare pentru a gestiona un sistem complex de monitorizare a traficului de rețea.

1.2 Argumentarea necesității dezvoltării sistemului

Dezvoltarea unui **sistem integrat pentru interceptarea și analiza traficului de rețea** este esențială într-un context tehnologic tot mai complex, în care rețelele sunt expuse constant la riscuri și atacuri cibernetice, iar volumul de date transferate crește exponențial. Necesitatea unui astfel de sistem poate fi argumentată din mai multe perspective esențiale pentru companii, organizații și instituții care depind de securitatea și performanța rețelelor lor.

În primul rând, **creșterea riscurilor de securitate cibernetică** face ca un astfel de sistem să fie indispensabil. Pe măsură ce rețelele devin mai interconectate, oportunitățile pentru atacatorii cibernetici se multiplică. De la atacuri de tip DDoS la intruziuni avansate și furt de date sensibile, amenințările cibernetice sunt din ce în ce mai sofisticate și greu de detectat fără un instrument dedicat. Un sistem de interceptare a traficului de rețea poate monitoriza activitățile suspecte în timp real, poate identifica comportamente anormale și poate declanșa alerte în cazul detecțiilor de securitate, permițând echipelor IT să acționeze rapid și eficient pentru a preveni daune majore.

Un alt motiv pentru care un astfel de sistem este necesar îl reprezintă **nevoia de conformitate cu reglementările și standardele internaționale de securitate**. Organizațiile din diverse domenii, cum ar fi sectorul financiar, cel guvernamental sau cel de sănătate, sunt obligate să respecte norme stricte în ceea ce privește protecția datelor și confidențialitatea informațiilor transmise prin rețea. Prin utilizarea unui sistem de interceptare și analiză a traficului de rețea, acestea pot monitoriza și audita traficul în mod continuu, demonstrând conformitatea cu regulamente precum GDPR, PCI-DSS, HIPAA sau alte norme relevante. Astfel, organizațiile nu doar că se protejează împotriva riscurilor, dar evită și sancțiuni financiare și legale semnificative.

Din punctul de vedere al **performanței rețelelor**, un sistem de acest tip ajută la optimizarea fluxului de date și la îmbunătățirea calității serviciilor oferite. Monitorizarea constantă a traficului permite identificarea și rezolvarea rapidă a problemelor care pot apărea, precum congestia rețelei, pierderea de pachete sau degradarea performanței. Prin detectarea acestor probleme în timp real, administratorii de rețea pot lua măsuri corective imediat, ceea ce asigură o funcționare stabilă și eficientă a rețelelor, aspect esențial pentru organizațiile care depind de uptime și latență scăzută în activitatea lor zilnică.

Un alt argument puternic este **creșterea complexității rețelelor moderne**. Cu migrarea către cloud, adoptarea masivă a tehnologiilor de tip IoT și dezvoltarea infrastructurilor de rețea hibride, traficul

de rețea este mai dinamic și mai dificil de gestionat ca niciodată. Sistemele tradiționale de monitorizare nu mai sunt suficiente pentru a gestiona eficient această complexitate. Un sistem integrat de interceptare a traficului oferă o soluție avansată pentru vizibilitatea completă asupra rețelei, permițând o mai bună înțelegere a modului în care sunt distribuite datele, cine le accesează și cum pot fi protejate.

Totodată, un astfel de sistem are și **beneficii economice**. Deși implementarea inițială poate presupune costuri semnificative, pe termen lung, un sistem de monitorizare a traficului de rețea contribuie la reducerea pierderilor financiare asociate cu atacurile cibernetice, timpul de nefuncționare (downtime) și pierderea datelor. Investiția într-o soluție avansată pentru interceptarea și analiza traficului se justifică prin economiile realizate prin prevenirea incidentelor și prin optimizarea continuă a performanței rețelei.

În final, dezvoltarea unui **sistem integrat pentru interceptarea și analiza traficului de rețea** răspunde nevoii tot mai mari de securitate, performanță și conformitate în cadrul rețelelor moderne. Atât companiile mici, cât și organizațiile mari au nevoie de vizibilitate completă asupra traficului lor de rețea pentru a asigura funcționarea eficientă și protecția împotriva amenințărilor cibernetice. Un astfel de sistem devine o componentă esențială a infrastructurilor IT, oferind un sprijin crucial în menținerea unui mediu de rețea sigur și performant.

2. Identificarea și declarația problemei

Identificarea Problemei:

În era digitală, rețelele de calculatoare sunt esențiale pentru funcționarea organizațiilor, facilitând comunicarea, colaborarea și accesul la informații. Cu toate acestea, creșterea traficului de rețea și complexitatea infrastructurii IT au condus la provocări semnificative în ceea ce privește monitorizarea și analiza acestuia. Problemele pot include detectarea timpurie a amenințărilor cibernetice, identificarea comportamentului anormal în rețea și asigurarea conformității cu reglementările de securitate. Aceste provocări necesită soluții eficiente pentru a garanta securitatea și performanța rețelelor.

Declarația Problemei:

Problema fundamentală constă în lipsa unui sistem integrat capabil să intercepteze și să analizeze în mod eficient traficul de rețea, permițând organizațiilor să identifice și să răspundă rapid la amenințările cibernetice. Un astfel de sistem ar trebui să colecteze date din diverse surse de trafic, să le analizeze în timp real și să ofere rapoarte relevante pentru a facilita luarea deciziilor informate. De asemenea, este esențial ca acest sistem să fie scalabil, să se integreze ușor cu infrastructura existentă și să ofere o interfață prietenoasă pentru utilizatori.

Dezvoltarea unui astfel de sistem nu numai că va îmbunătăți securitatea rețelelor, dar va contribui și la optimizarea resurselor și la reducerea timpului de răspuns în fața incidentelor de securitate. Astfel, se va asigura o gestionare proactivă a amenințărilor și o mai bună conformitate cu standardele de securitate cibernetică.

Scopul și Obiectivele:

Scopul principal al dezvoltării acestui sistem este de a oferi o soluție cuprinzătoare pentru interceptarea și analiza traficului de rețea, cu următoarele obiective specifice:

1. **Monitorizarea continuă a traficului de rețea:** Implementarea unui sistem capabil să intercepteze și să analizeze în timp real tot traficul de rețea, identificând activitățile suspecte și anomaliile.
2. **Detectarea și alertarea asupra amenințărilor:** Dezvoltarea de algoritmi eficienți pentru a detecta amenințările cibernetice și a genera alerte în timp real pentru a permite intervenții rapide.
3. **Generarea de rapoarte și analize:** Crearea unei platforme care să permită generarea de rapoarte detaliate asupra traficului de rețea, incluzând statistici și tendințe, pentru a sprijini luarea deciziilor strategice.
4. **Interfață prietenoasă pentru utilizatori:** Asigurarea unei experiențe utilizator intuitive, care să permită utilizatorilor să acceseze rapid informațiile necesare și să navigheze ușor prin funcționalitățile sistemului.
5. **Securitatea datelor și confidențialitatea:** Implementarea celor mai bune practici de securitate pentru a proteja datele sensibile și a asigura confidențialitatea informațiilor analizate.

Prin atingerea acestor obiective, sistemul propus va contribui semnificativ la îmbunătățirea securității rețelelor și la optimizarea gestionării traficului de rețea, răspunzând astfel nevoilor organizațiilor contemporane.

Conlcuzie:

Proiectul „Sistem integrat pentru interceptarea și analiza traficului de rețea” se dovedește a fi o inițiativă esențială în contextul provocărilor curente de securitate cibernetică și al creșterii continue a complexității rețelelor de calculatoare. Într-o lume în care amenințările cibernetice devin din ce în ce mai sofisticate și răspândite, un sistem eficient de monitorizare și analiză a traficului de rețea nu mai este un lux, ci o necesitate.

Dezvoltarea unei astfel de soluții integrate va permite organizațiilor să își protejeze infrastructura, să îmbunătățească securitatea datelor și să asigure conformitatea cu reglementările în vigoare. Prin implementarea tehnologiilor avansate de interceptare și analiză, se va facilita nu doar identificarea rapidă a amenințărilor, ci și o mai bună gestionare a resurselor de rețea, contribuind la optimizarea performanței globale a sistemului.

Obiectivele stabilite, de la monitorizarea continuă a traficului la generarea de rapoarte detaliate, reflectă angajamentul de a oferi o soluție completă, adaptabilă și prietenoasă pentru utilizatori. Securitatea datelor și confidențialitatea utilizatorilor sunt priorități fundamentale, ceea ce asigură că aplicația va respecta cele mai înalte standarde de protecție a informațiilor.

În concluzie, implementarea acestui sistem integrat va transforma modul în care organizațiile abordează securitatea cibernetică, asigurându-le astfel nu doar protecția împotriva amenințărilor actuale, ci și capacitatea de a se adapta rapid la provocările viitoare din domeniul tehnologiei informației.

Bibliografie

1. Wireshark [docs] Disponibil:
   https://www.wireshark.org/docs/