Universitatea Tehnică a Moldovei

Aplicație de interceptare și analiză a traficului de rețea

Network Traffic Interception and Analysis Application

Student: **gr. SI-211,**
Chirița Stanislav

Coordonator: **Masiutin Maxim,**
asistent universitar

Chișinău, 2025

MINISTERUL EDUCAȚIEI ȘI CERCETĂRII AL REPUBLICII MOLDOVA
Universitatea Tehnică a Moldovei
Facultatea Calculatoare Informatică și Microelectronică
Departamentul Ingineria Software și Automatică

Aprob
Șef departament:
Fiodorov Ion dr., conf.univ.
_____

„_____” _____ 2025

Aplicație de interceptare și analiză a traficului de rețea
Teză de licență

Student: **Chirița Stanislav, SI-211**
Coordonator: **Masiutin Maxim, lector univ.**
Consultant: **Bulai Rodica, lector univ.**

Chișinău, 2025

Universitatea Tehnică a Moldovei
Facultatea Calculatoare Informatica și Microelectronica
Departamentul Ingineria Software și Automatica
Programul de studii Securitate Informațională

Aprob
Șef departament:
Fiodorov Ion dr., conf.univ.

1 noiembrie 2024

CAIET DE SARCINI
pentru proiectul/teza de licenţă al/a studentului

Chirița Stanislav

1. Tema proiectului/tezei de licenţă Aplicație de interceptare și analiză a traficului de rețea
confirmată prin hotărârea Consiliului facultăţii nr. 2 din „ 1 ” noiembrie 2024
2. Termenul limită de prezentare a proiectului/tezei de licență „ 24 ” mai 2025
3. Date iniţiale pentru elaborarea proiectului/tezei de licență Studiul instrumentelor de analiză a traficului de rețea (Wireshark, tcpdump, Zeek, Suricata), identificarea limitărilor acestora și necesitatea dezvoltării unei aplicații proprii. Proiectarea și implementarea unei aplicații numite Sentinel Traffic Analyzer, care permite capturarea și analizarea traficului de rețea în timp real, cu interfață grafică (Tkinter), module de alertare (detecție port scanning, flood, spoofing), salvare în fișiere .pcap, .json, .pdf, și integrare cu baze de date și API-uri externe. Evaluarea performanței aplicației prin testare în medii simulate și reale.

4. Conţinutul memoriului explicativ

1. Introducere
2. Analiza domeniului de studiu
3. Realizarea sistemului
4. Documentarea sistemului
5. Estimarea costurilor și evaluarea proiectului

Concluzii

5. Conţinutul părţii grafice a proiectului/tezei de licență

Partea grafică a tezei include modelarea structurală și funcțională a aplicației dezvoltate, realizată prin diagrame UML relevante precum cea de context, componente, clasă, stare și secvență. Sunt prezentate grafice de performanță care reflectă volumul de trafic analizat, numărul de alerte detectate și timpul de procesare în funcție de dimensiunea sesiunii. De asemenea, sunt incluse capturi de ecran reprezentative cu

interfața aplicației în funcțiune, evidențiind procesul de captură, afișarea pachetelor, generarea alertelor și exportul rapoartelor, pentru a ilustra funcționalitatea completă a sistemului.

6. Lista consultanţilor

Consultant	Capitol	Confirmarea realizării activităţii	
		Semnătura consultantului (data)	Semnătura studentului (data)
Bulai Rodica	*Standarde tehnologice, Estimarea costului proiectului*		

7. Data înmânării caietului de sarcini 02.09.2024

Coordonator Masiutin Maxim _____

semnătura

Sarcina a fost luată pentru a fi executată de studentul Chirița Stanislav

_____

semnătura, data

PLAN CALENDARISTIC

No. crt.	Denumirea etapelor de elaborare/proiectare	Termenul de realizare a etapelor	Nota
1.	Definirea temei și stabilirea cerințelor funcționale	*02.09.24 – 31.10.2024*	10 %
2.	Analiza soluțiilor existente și a domeniului de aplicabilitate	*01.11.2024 – 15.12.2024*	15 %
3.	Modelarea arhitecturii și proiectarea funcțională a sistemului	*16.12.2024 – 31.12.2024*	15 %
4.	Dezvoltarea aplicației (captură, analiză, alertare, interfață)	*01.01.2025 – 15.04.2025*	30 %
5.	Integrarea funcțiilor avansate și testarea funcționalităților	*16.04.2025 – 30.04.2025*	10 %
6.	Documentarea tehnică și generarea rapoartelor de testare	*01.05.2025 – 15.05.2025*	5 %
7.	Redactarea finală a tezei și pregătirea susținerii	*16.05.2025 – 24.05.2025*	5 %

Student Chirița Stanislav(_____)

Coordonator de proiect/teză de licență Masiutin Maxim(_____)

Declarația Studentului

UNIVERSITAEA TEHNICĂ A MOLDOVEI

FACULTATEA CALCULATOARE INFORMATICA ȘI MICROELECTRONICA
DEPARTAMENTUL INGINERIA SOFTWARE ȘI AUTOMATICA
PROGRAMUL DE STUDII SECURITATE INFORMAȚIONALA

AVIZ

la proiectul/teza de licenţă

Titlul: Aplicație de interceptare și analiză a traficului de rețea
Studentul(a) Chirița Stanislav, grupa SI-211

1. Actualitatea temei: În contextul creșterii numărului de atacuri cibernetice și al complexității rețelelor moderne, monitorizarea traficului de rețea în timp real a devenit esențială pentru asigurarea securității informaționale. Tema propusă este relevantă și actuală, răspunzând nevoii de identificare rapidă a comportamentelor suspecte în rețelele informatice.
2. Caracteristica proioectului/tezei de licenţă: Lucrarea propune proiectarea și implementarea unei aplicații denumite *Sentinel Traffic Analyzer*, care interceptează și analizează traficul de rețea, oferind o interfață grafică intuitivă, un sistem de alertare în timp real, integrare cu formate de raportare standard (PDF, JSON) și salvare a sesiunilor de trafic în fișiere .pcap.
3. Analiza prototipului: Aplicația a fost testată în medii reale și simulate, demonstrând capacitatea de a capta trafic pe interfețe locale, de a semnala comportamente de tip flood, scanare de porturi și spoofing, și de a genera rapoarte automatizate. Sistemul funcționează fluent, cu actualizare dinamică a pachetelor și alerte vizuale clare, păstrând un consum redus de resurse.
4. Estimarea rezultatelor obţinute: Rezultatele indică funcționalitatea completă a sistemului, corectitudinea detecției comportamentelor suspecte și eficiența procesului de captură/analyză. Aplicația răspunde cerințelor de bază ale unui sistem de tip IDS (Intrusion Detection System) și poate fi extinsă cu ușurință.
5. Corectitudinea materialului expus: Materialul este bine structurat, susținut de surse academice, cu prezentarea clară a componentelor tehnice, argumentarea deciziilor de proiectare și justificarea tehnologiilor utilizate.
6. Calitatea materialului grafic: Diagramele UML și capturile de ecran oferă o reprezentare clară și coerentă a funcționalităților aplicației, completate de grafice relevante privind performanța și distribuția traficului analizat.
7. Valoarea practică a proiectului/tezei: Aplicația poate fi utilizată ca instrument educațional pentru învățarea analizării traficului, dar și în scopuri practice pentru testare de rețea, simulări de securitate și audit de trafic.
8. Observaţii şi recomandări: Se recomandă extinderea aplicației cu un sistem de învățare automată pentru detecția anomaliilor și integrarea unei componente de răspuns automatizat la incidente.
9. Caracteristica studentului şi titlul conferit: Pe parcursul realizării tezei de licență studentul a dat dovadă de responsabilitate și a aplicat cunoștințele tehnice necesare pentru realizarea sarcinilor propuse. Din cele relatate lucrarea de licență poate fi admisă spre susținere cu nota _____.

Lucrarea în forma electronică corespunde originalului prezentat către susținere publică.

Coordonatorul proiectului/tezei de licenţă lector univ. Masiutin Maxim, _____
(titlul ştiinţifico-didactic, titlul ştiinţific, semnătura, data, numele, prenumele

REZUMAT

În contextul actual al creșterii exponențiale a traficului de date și al intensificării atacurilor cibernetice, monitorizarea în timp real a comunicațiilor de rețea a devenit esențială pentru protejarea infrastructurilor informatice. Lucrarea de față propune proiectarea și implementarea unei aplicații denumite **Sentinel Traffic Analyzer**, care permite interceptarea, analiza și vizualizarea traficului de rețea într-un mod eficient, flexibil și extensibil.

Aplicația dezvoltă funcționalități avansate de captare a pachetelor în timp real prin biblioteci precum *Scapy*, oferind utilizatorului o interfață grafică prietenoasă (Tkinter) care permite controlul procesului de monitorizare, configurarea de filtre personalizate, vizualizarea traficului în detaliu, precum și generarea de alerte automate în caz de comportamente suspecte (flood, scanări de porturi, spoofing etc.).

Pe lângă aceste capabilități, aplicația integrează module de **geolocalizare a IP-urilor**, analiză a fluxurilor de comunicație (Follow Stream), vizualizare topologică a rețelei și generare de rapoarte automate în formate PDF și JSON. De asemenea, este inclus un sistem de stocare a sesiunilor în fișiere .pcap și integrare cu baze de date externe prin API, facilitând arhivarea și analiza ulterioară.

Arhitectura modulară și codul sursă organizat pe componente independente permit extinderea ușoară a aplicației. Testele efectuate în rețele reale și simulate au demonstrat stabilitatea, performanța și utilitatea practică a sistemului, confirmând valoarea sa ca instrument de învățare, cercetare sau audit de securitate. Proiectul poate fi integrat în scenarii educaționale sau operaționale, și servește drept bază pentru dezvoltarea ulterioară a unor soluții IDS/SIEM.

Prin această lucrare se evidențiază importanța unei abordări proactive în supravegherea traficului de rețea, susținută de tehnologii open-source și metode de analiză avansate, contribuind la creșterea rezilienței și securității în mediile digitale moderne.

ABSTRACT

In the current landscape marked by the exponential growth of data traffic and increasing cybersecurity threats, real-time monitoring of network communications is essential for protecting IT infrastructures. This thesis introduces the design and implementation of a software application called Sentinel Traffic Analyzer, which enables the interception, analysis, and visualization of network traffic in a flexible, efficient, and extensible manner.

The application integrates advanced packet capturing capabilities using tools such as *Scapy* and offers a user-friendly graphical interface (built with Tkinter). Users can control the monitoring process, define custom filters, view detailed traffic information, and receive automated alerts in response to suspicious behaviors such as floods, port scanning, and spoofing.

Additionally, the system incorporates features like IP geolocation, communication stream analysis (Follow Stream), topological network visualization, and automatic report generation in PDF and JSON formats. It also supports session saving in .pcap files and integration with external databases via API, facilitating long-term storage and retrospective traffic analysis.

Built with a modular architecture and well-structured source code, the application ensures ease of maintenance and future expansion. Testing conducted in both real and simulated environments confirmed the system's stability, performance, and practical utility. The project serves as a reliable tool for learning, research, or security auditing, and lays the groundwork for further development into IDS or SIEM solutions.

This work highlights the importance of proactive approaches in network traffic surveillance, powered by open-source technologies and advanced analysis techniques, contributing to greater resilience and cybersecurity in modern digital infrastructures.