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

Sistem integrat pentru interceptarea și analiza traficului de rețea

Practica de licență

Student(ă): _____ **Chirița Stanislav, SI-211**

Coordonator întreprindere: _____ **Jovmir Cristina, Head of CERT Gov**

Coordonator de licență: _____ **Masiutin Maxim, asist.univ.**

Coordonator universitate: _____ **Bulai Rodica, lector universitar**

Chişinău, 2024

CUPRINS

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)

INTRODUCERE

Practica desfășurată în cadrul **Serviciului Tehnologia Informației și Securitate Cibernetică (STISC)** a avut ca obiectiv principal aprofundarea cunoștințelor teoretice și aplicarea acestora într-un mediu real de lucru, în domeniul securității cibernetice și al analizei traficului de rețea. Activitatea s-a desfășurat pe parcursul perioadei **03.02.2025 – 28.03.2025**, timp în care am avut ocazia să mă familiarizez cu tehnologiile și metodele utilizate pentru interceptarea și analiza traficului de rețea, un domeniu esențial pentru asigurarea securității informaționale la nivel național.

Scopul principal al practicii a fost dezvoltarea unui **sistem integrat pentru interceptarea și analiza traficului de rețea**, utilizând tehnici avansate de captare și interpretare a pachetelor de date. Prin această experiență, am urmărit să înțeleg mai bine structura și vulnerabilitățile rețelelor, metodele de detecție a amenințărilor și utilizarea instrumentelor specifice pentru monitorizarea traficului. Importanța acestui subiect este majoră, având în vedere creșterea constantă a atacurilor cibernetice și necesitatea implementării unor soluții eficiente de protecție în infrastructurile critice.

1 ANALIZA DOMENIULUI DE STUDIU

Analiza traficului de rețea are un rol important în securitatea cibernetică, permițând identificarea atacurilor și optimizarea performanței rețelelor. În cadrul practicii desfășurate la **Serviciul Tehnologia Informației și Securitate Cibernetică (STISC)**, am utilizat instrumente specializate pentru interceptarea și analiza pachetelor de date, având ca scop implementarea unui sistem integrat de monitorizare a traficului.

Am folosit tehnologii precum **Wireshark, tcpdump, Zeek și Suricata**, fiecare având roluri specifice în captarea și interpretarea traficului de rețea. Aceste instrumente au fost utilizate pentru a analiza avantajele și limitările fiecăruia, în scopul dezvoltării unei soluții proprii optimizate. Testele efectuate au permis identificarea punctelor forte și a aspectelor care necesită îmbunătățiri, oferind o bază solidă pentru crearea unui instrument personalizat, capabil să răspundă cerințelor specifice de securitate și monitorizare a rețelei.

Rezultatele au demonstrat eficiența unei soluții automatizate pentru detectarea amenințărilor. Optimizările viitoare pot include integrarea algoritmilor de **machine learning** pentru îmbunătățirea detecției anomaliilor. Această practică a oferit o înțelegere practică asupra monitorizării traficului și a metodelor de protecție a rețelelor informatice.

1.1 Importanța temei

Implementarea unui sistem integrat pentru interceptarea și analiza traficului de rețea contribuie la identificarea anomaliilor și la reacția rapidă împotriva incidentelor de securitate. Prin monitorizarea fluxului de date, se poate determina comportamentul anormal al utilizatorilor sau dispozitivelor dintr-o rețea, prevenind astfel compromiterea infrastructurii IT. De asemenea, analiza traficului permite optimizarea performanței rețelelor și asigurarea respectării politicilor de securitate și a reglementărilor legale.

Prin această lucrare, se urmărește testarea și compararea unor instrumente existente de analiză a traficului, identificarea punctelor lor slabe și dezvoltarea unei soluții îmbunătățite, capabile să ofere o detecție mai rapidă și mai precisă a amenințărilor. Astfel, cercetarea contribuie la îmbunătățirea metodelor de protecție a rețelelor informatice și la dezvoltarea unor tehnologii mai eficiente în domeniul securității cibernetice.

1.2 Sisteme similare cu proiectul realizat

În domeniul securității cibernetice, există numeroase sisteme dezvoltate pentru interceptarea și analiza traficului de rețea. Acestea sunt utilizate atât pentru monitorizare pasivă, cât și pentru detecția activă a amenințărilor. Printre cele mai relevante soluții similare cu proiectul realizat se numără:

Wireshark – Unul dintre cele mai populare instrumente de analiză a traficului de rețea. Permite captarea și inspecția detaliată a pachetelor, fiind utilizat atât pentru depanare, cât și pentru identificarea

vulnerabilităților. Totuși, Wireshark necesită o analiză manuală intensă, ceea ce poate fi un dezavantaj pentru detecția rapidă a atacurilor. Wireshark oferă o flexibilitate remarcabilă prin posibilitatea de a defini filtre personalizate pentru captarea și analizarea pachetelor, facilitând o înțelegere mai detaliată a traficului de rețea. Datorită acestei granularități, un administrator poate identifica exact sursa problemelor de conectivitate sau poate descoperi comportamente suspecte cu precizie ridicată.

Cu toate acestea, utilizarea Wireshark necesită timp și expertiză pentru interpretarea corectă a datelor. În cazul unui volum mare de trafic, o echipă de securitate poate fi copleșită de cantitatea de informații brute, ceea ce face dificilă detectarea rapidă a atacurilor sofisticate. Din acest motiv, Wireshark este adesea folosit în combinație cu alte soluții – de exemplu, sisteme de detectare a intruziunilor (IDS/IPS) care asigură monitorizare în timp real și alerte automate.

Astfel, Wireshark rămâne un instrument esențial pentru investigații post-eveniment și pentru dezvoltarea abilităților de analiză a securității rețelei, dar nu trebuie privit ca un mijloc unic de protecție. Într-un mediu complex, el reprezintă doar o parte dintr-un ecosistem mai larg de soluții de securitate, completat de automatizări, monitorizare continuă și controale adecvate la nivelul infrastructurii.

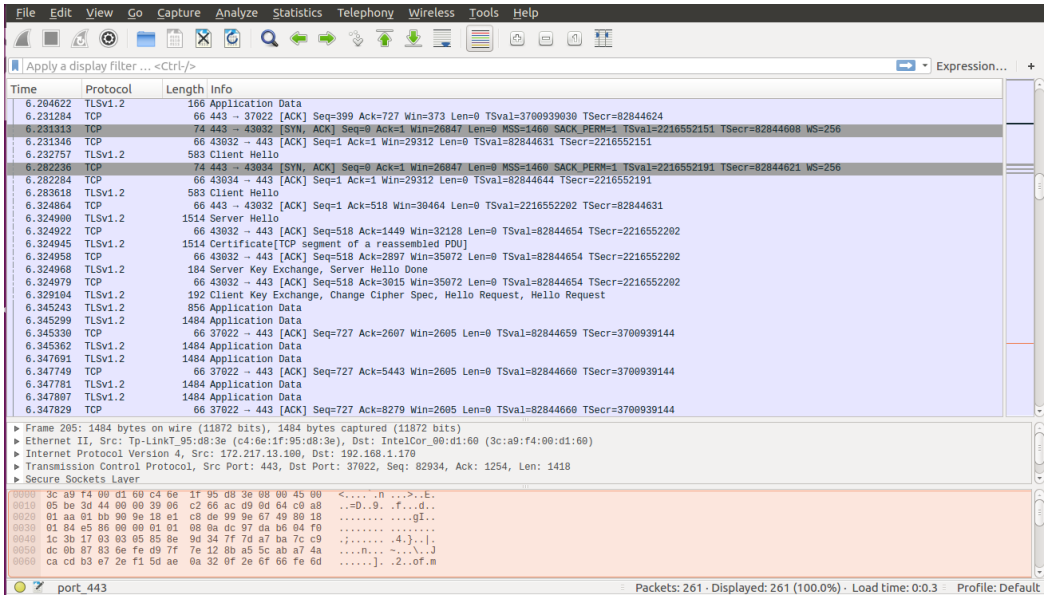

Figura 1.1 – Wireshark

tcpdump – Un instrument în linie de comandă care permite captarea și filtrarea pachetelor de date. Este eficient pentru analiza traficului în timp real, dar are o interfață limitată și necesită cunoștințe avansate pentru interpretarea rezultatelor. **tcpdump** este un instrument pentru specialiștii în securitate și administrare de rețea, însă se folosește exclusiv din linia de comandă. Datorită simplității și a consumului redus de resurse, este deseori preferat în diagnosticarea rapidă a problemelor de rețea și monitorizarea traficului în timp real, mai ales pe sisteme Linux/Unix.

Cu toate acestea, tcpdump oferă doar o interfață textuală, care poate părea intimidantă pentru utilizatorii neexperimentați. Pentru a utiliza eficient filtrele și pentru a interpreta corect datele capturate, este necesar un nivel avansat de cunoștințe de rețea (protocoale, formate de pachete etc.). În plus, pentru

analiza post-captură și interpretarea avansată a vulnerabilităților, se recomandă exportarea fișierelor pcap către soluții cu interfață grafică (de exemplu, Wireshark).

Ca și în cazul oricărui instrument de analiză a traficului, tcpdump nu oferă un mecanism automat de detectare a atacurilor. Este util în identificarea problemelor punctuale și în înțelegerea traficului la nivel de pachete, dar nu poate înlocui soluțiile automatizate de monitorizare și securitate (IDS/IPS, SIEM etc.). Prin urmare, implementarea tcpdump în cadrul unei strategii mai ample de securitate trebuie să fie dublată de alte instrumente și procese de detecție și răspuns la incidente.

```
root@kali:~# tcpdump -i eth0 -s 0
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
04:57:29.856624 IP 192.168.20.1.40816 > 192.168.20.255.40816: UDP, length 131
04:57:29.857265 IP kali.58048 > _gateway.domain: 22425+ PTR? 255.20.168.192.in-addr.arpa. (45)
04:57:29.858650 IP _gateway.domain > kali.58048: 22425 NXDomain 0/1/0 (80)
04:57:29.859271 IP kali.42264 > _gateway.domain: 27790+ PTR? 1.20.168.192.in-addr.arpa. (43)
04:57:29.860750 IP _gateway.domain > kali.42264: 27790 NXDomain 0/1/0 (78)
04:57:29.861150 IP kali.43676 > _gateway.domain: 36900+ PTR? 2.20.168.192.in-addr.arpa. (43)
04:57:29.862288 IP _gateway.domain > kali.43676: 36900 NXDomain 0/1/0 (78)
04:57:29.862621 IP kali.46656 > _gateway.domain: 19118+ PTR? 136.20.168.192.in-addr.arpa. (45)
04:57:30.638164 ARP, Request who-has _gateway tell kali, length 28
04:57:30.638292 ARP, Reply _gateway is-at 00:50:56:fd:dc:24 (oui Unknown), length 46
04:57:34.506805 IP 192.168.20.1.40816 > 192.168.20.255.40816: UDP, length 131
^C
11 packets captured
12 packets received by filter
1 packet dropped by kernel
```

Figura 1.2 - tcpdump

Zeek (Bro) – Un sistem de monitorizare a rețelei care nu doar capturează traficul, ci și analizează comportamentul acestuia pentru detectarea anomaliilor. Comparativ cu alte soluții, Zeek oferă un nivel mai ridicat de automatizare și posibilitatea de a genera rapoarte detaliate despre activitatea rețelei. Pe lângă rolul său de **capturare** a traficului la nivel de rețea, **Zeek (cunoscut anterior sub denumirea Bro)** se diferențiază printr-un **motor sofisticat de analiză a comportamentului**. Practic, Zeek corelează evenimentele de la nivelul aplicațiilor (HTTP, DNS, SSL etc.), transformând fluxurile de trafic în **informații structurate** care pot fi folosite pentru a identifica anomalii și potențiale amenințări de securitate.

Spre deosebire de alte unelte de tip IDS/IPS care se bazează preponderent pe semnături, Zeek adoptă o abordare **mai flexibilă**, analizând semnalele comportamentale și colectând metadate valoroase, cum ar fi cererile DNS sau parametrii tranzacțiilor HTTP. Această abordare face posibilă **detectarea atacurilor necunoscute** sau a tacticilor avansate folosite de atacatori, în condițiile în care semnăturile tradiționale nu ar oferi rezultate.

Beneficiind de un **sistem de scripturi** extensibil, Zeek permite personalizarea regulilor de monitorizare în funcție de nevoile organizației, precum și **integrarea cu alte soluții** de securitate (SIEM, platforme de automatizare etc.). Rapoartele generate de Zeek oferă o **imagine detaliată** asupra activității rețelei, fiind extrem de utile în investigațiile post-eveniment și în luarea deciziilor strategice de securitate. Astfel, Zeek reprezintă o componentă solidă într-o arhitectură de securitate modernă,

funcționând atât ca instrument de monitorizare continuă, cât și ca bază pentru detecția proactivă a amenințărilor.

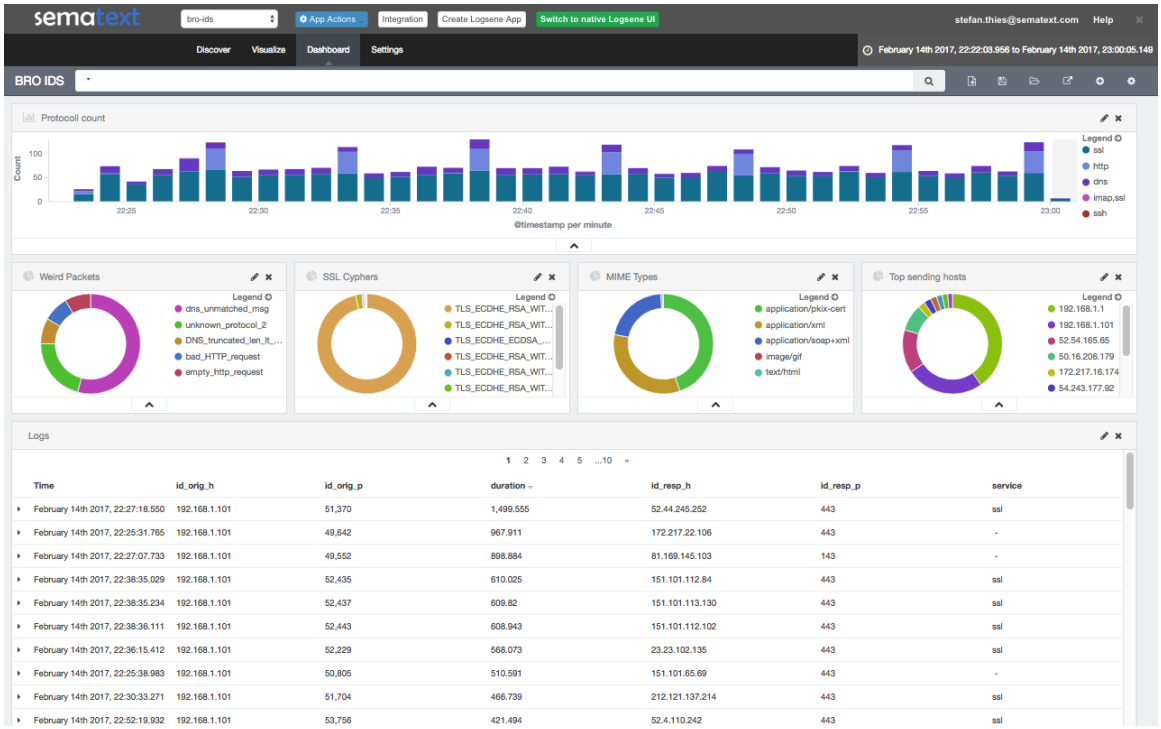

Figura 1.3 – Zeek

Suricata – Un sistem de detecție și prevenire a intruziunilor (IDS/IPS) care analizează traficul în timp real. Spre deosebire de Wireshark și tcpdump, care sunt axate pe captare, Suricata este capabilă să blocheze traficul suspect, având o abordare mai proactivă în securitatea rețelei.

Sistemul propus se bazează pe îmbinarea celor mai relevante caracteristici din diverse soluții de monitorizare și analiză a traficului (precum Wireshark, tcpdump sau Zeek), pentru a oferi o **platformă unitară și eficientă**. În loc să se limiteze la captarea pachetelor brute și la o analiză manuală extensivă, noul proiect introduce **funcționalități de filtrare și clasificare avansată**, concepute să reducă semnificativ timpul și expertiza specializată necesare în interpretarea datelor.

Prin agregarea și corelarea informațiilor din surse multiple, sistemul oferă **rapoarte sintetice** care sprijină luarea rapidă de decizii și permite **detecția proactivă** a potențialelor incidente de securitate. Astfel, **abordarea propusă** depășește limitele instrumentelor tradiționale, facilitând un **proces de analiză mai fluid și mai bine integrat** în cadrul infrastructurii de rețea.

1.3 Scopul, obiectivele și cerințele sistemului

Scopul principal al acestui proiect este dezvoltarea unui **sistem integrat pentru interceptarea și analiza traficului de rețea**, care să permită monitorizarea și detecția eficientă a activităților suspecte. Sistemul trebuie să ofere o metodă rapidă și automatizată de captare, filtrare și interpretare a pachetelor de

date, contribuind astfel la îmbunătățirea securității cibernetice prin prevenirea și investigarea amenințărilor informatice.

a) **Captarea traficului de rețea** – Dezvoltarea unui modul care să intercepteze pachetele de date în timp real folosind tehnologii precum **tcpdump, Wireshark, Zeek** sau **Suricata**;
b) **Filtrarea și clasificarea pachetelor** – Implementarea unor algoritmi care să extragă și să analizeze doar informațiile relevante, eliminând traficul nesemnificativ;
c) **Detecția activităților suspecte** – Identificarea anomaliilor și a potențialelor atacuri informatice prin metode bazate pe semnături și comportament;
d) **Stocarea și gestionarea datelor** – Crearea unei baze de date sau a unui sistem de logare pentru păstrarea și analizarea ulterioară a traficului interceptat;
e) **Interfață de utilizator (GUI)** – Dezvoltarea unei interfețe intuitive care să permită utilizatorilor să vizualizeze datele capturate și să genereze rapoarte relevante;
f) **Automatizarea procesului** – Integrarea unor funcționalități care să reducă necesitatea intervenției manuale, crescând astfel eficiența detecției.

Pentru ca sistemul să funcționeze eficient, acesta trebuie să îndeplinească o serie de cerințe esențiale, atât funcționale, cât și non-funcționale. Din punct de vedere funcțional, sistemul trebuie să fie capabil să captureze și să analizeze traficul de rețea în timp real, asigurând în același timp filtrarea și clasificarea pachetelor de date pe baza protocoalelor utilizate și a adreselor IP. De asemenea, este necesară integrarea unor mecanisme eficiente de detecție pentru identificarea anomaliilor sau a posibilelor atacuri informatice. Un alt aspect important este posibilitatea de stocare și raportare a datelor relevante, permițând astfel investigarea ulterioară a incidentelor de securitate. Pentru a facilita utilizarea, sistemul trebuie să dispună de o interfață grafică care să permită analiza și gestionarea traficului interceptat într-un mod intuitiv.

Pe lângă cerințele funcționale, sistemul trebuie să respecte și o serie de cerințe non-funcționale. Acesta trebuie să fie scalabil, astfel încât să permită extinderea funcționalităților în funcție de necesități. Performanța trebuie optimizată pentru a evita introducerea unor latențe semnificative în rețea, menținând un echilibru între eficiența analizelor și resursele consumate. Interfața utilizatorului trebuie să fie intuitivă și ușor de utilizat, astfel încât specialiștii în securitate să poată interpreta rapid datele obținute. Nu în ultimul rând, sistemul trebuie să respecte normele legale privind interceptarea și analiza traficului de rețea, asigurând conformitatea cu reglementările în vigoare.

2 MODELAREA ȘI PROIECTAREA SISTEMUL INFORMATIC

Modelarea și proiectarea sunt etape centrale în dezvoltarea oricărui sistem informatic, inclusiv a unui sistem integrat pentru interceptarea și analiza traficului de rețea. În această fază, se stabilește în detaliu modul în care sistemul își va îndeplini funcționalitățile, se definesc structurile interne și se proiectează interacțiunile dintre componente.

Modelarea datelor implică crearea unei reprezentări arhitecturale a funcționalităților și a fluxurilor de date. Aceasta se realizează prin identificarea entităților-cheie (de exemplu, module de interceptare a pachetelor, componente de analiză și raportare) și definirea relațiilor dintre acestea. Proiectarea se concentrează pe determinarea arhitecturii generale, a modulelor, interfețelor și tehnologiilor care vor asigura îndeplinirea cerințelor de securitate, performanță și scalabilitate.

Un instrument de mare importanță în procesul de modelare și proiectare este limbajul unificat de modelare (UML). Acesta oferă un set de diagrame și simboluri standardizate pentru descrierea și documentarea aspectelor funcționale și structurale ale sistemului. De exemplu:

- Diagrame de clasă - evidențiază entitățile (modul de interceptare, modul de analiză, modul de stocare a datelor) și relațiile dintre acestea;
- Diagrame de activitate - ilustrează fluxurile de lucru, cum ar fi procesul de captare a traficului și secvența operațiunilor de analiză;
- Diagrame de secvență - evidențiază interacțiunile dintre componente într-un anumit scenariu de interceptare sau de analiză.

Prin utilizarea UML, echipa de dezvoltare a proiectului și părțile interesate relevante (de exemplu, departamentul IT, specialiștii în securitate) obțin o viziune comună asupra modului în care va funcționa sistemul și asupra modului în care diferitele componente vor comunica între ele. Această abordare standardizată îmbunătățește comunicarea și coordonarea, contribuind la identificarea potențialelor incertitudini sau probleme într-un stadiu incipient. Diagramele UML pot servi, de asemenea, ca bază pentru testare, permițând identificarea și corectarea rapidă a erorilor și optimizarea performanței sistemului.

Prin urmare, modelarea și proiectarea sistemului integrat de interceptare și analiză a traficului de rețea oferă o structură clară și eficientă, asigurând îndeplinirea cerințelor funcționale și nefuncționale. Utilizarea în consecință a UML și a metodelor de proiectare adecvate asigură un proces de dezvoltare coerent, permițând ulterior implementarea, testarea și întreținerea ușoară a instalației.

2.1 Descrierea comportamentală a sistemului

Comportamentul sistemului integrat de interceptare și analiză a traficului de rețea poate fi înțeles cel mai bine prin ilustrarea modului în care componentele sale interacționează și colaborează pentru a realiza obiectivele de monitorizare și detecție. În această etapă, accentul cade pe definirea fluxurilor de

activități și pe evidențierea modului în care datele parcurg succesiv diferitele module ale sistemului. Pentru a asigura o reprezentare clară și standardizată a comportamentului, sunt utilizate diagrame UML (diagrame de activitate, diagrame de secvență), care fac posibilă identificarea pașilor logici și a interacțiunilor relevante.

Din punct de vedere comportamental, sistemul poate fi descris în trei etape majore:

Captarea traficului de rețea

– Modulul de interceptare preia pachetele care trec prin interfața de rețea, fie în mod promiscuu (prin care se colectează toate pachetele), fie pe baza unor filtre specifice;

– Interceptarea pachetelor se realizează în timp real, iar sistemul trebuie să gestioneze aceste date rapid, fără a introduce latențe considerabile în rețea;

– Acest flux inițial reprezintă punctul de intrare în sistem și declanșează următoarele activități, precum filtrarea și clasificarea datelor;

Analiza și filtrarea datelor

– Odată ce pachetele au fost colectate, modulul de analiză preliminară le segregă după criterii precum tipul protocolului (TCP, UDP, ICMP, HTTP etc.), sursa și destinația.

– Pachetele identificate ca fiind irelevante (de exemplu, trafic de rutină, fără semnificație pentru securitate) pot fi trecute direct în arhivă, pentru a nu încărca modulul de detecție.

– Pachetele considerate potențial suspecte sunt supuse unei analize mai aprofundate, cu ajutorul mecanismelor bazate pe semnături (compararea cu reguli cunoscute, după modelul Suricata) sau pe comportament (analiza anomaliilor, după modelul Zeek).

– Datele considerate importante sunt transferate către modulul de stocare și raportare, unde sunt păstrate pentru investigații ulterioare.

Prin intermediul diagramelor de activitate (Activity Diagrams) sunt reprezentate succesiunea și ramificarea fluxurilor ce descriu traseul pachetelor, de la momentul captării până la eventuala lor marcare ca „suspecte” sau „inofensive”. În plus, diagramele de secvență (Sequence Diagrams) oferă o perspectivă detaliată asupra modului în care componentele (modulul de captare, modulul de filtrare, modulul de detecție, baza de date și interfața de utilizator) interacționează în timp, punând în evidență ordinea exactă a apelurilor și a transferurilor de date.

2.1.1 Imaginea generală asupra sistemului

În **Figura 2.1** („Interacțiune cu utilizatorul/analistul”), se observă diagrama de caz de utilizare care ilustrează principalele acțiuni pe care un analist le poate întreprinde în cadrul aplicației pentru interceptarea și analiza traficului de rețea. Actorul, reprezentat de „Utilizatorul/Analistul”, interacționează cu sistemul printr-o serie de funcționalități esențiale:

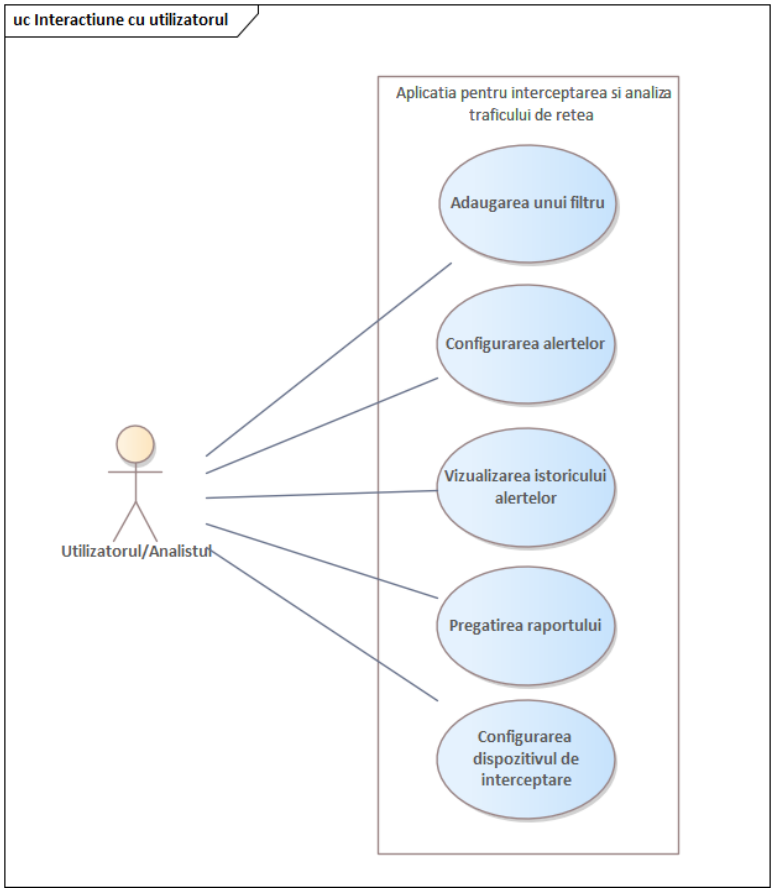

Figura 2.1 - Interacțiune cu utilizatorul/analistul

Funcționalitatea de adăugare a unui filtru oferă posibilitatea personalizării modului de captare a traficului, prin specificarea unor reguli precise de filtrare bazate, de exemplu, pe adrese IP, protocoale sau porturi, astfel încât analistul să poată izola informațiile relevante. Opțiunea de configurare a alertelor reprezintă o modalitate de stabilire a unor praguri și condiții ce declanșează notificări automate, utile pentru depistarea rapidă a activităților suspecte și a anomaliilor. În plus, vizualizarea istoricului alertelor permite accesul la evenimentele de securitate semnalate anterior, contribuind la identificarea tiparelor de atac și la evaluarea riscurilor asociate. Prin funcția de pregătire a raportului, se pot genera documente detaliate despre activitățile de monitorizare, statisticile traficului și potențialele incidente de securitate. De asemenea, configurarea dispozitivului de interceptare facilitează gestionarea setărilor tehnice ale echipamentului sau aplicației de captare, asigurând că datele sunt preluate eficient și corespunzător nevoilor de analiză.

2.1.2 Modelarea vizuală a fluxurilor

În **Figura 2.2**, este ilustrat un exemplu de diagramă de activitate care reflectă procesul de interceptare și partajare a traficului în funcție de filtrele definite. Diagrama pune în evidență pașii logici parcurși de aplicație imediat după inițierea filtrelor de captare: dacă sunt introduse reguli de filtrare, sistemul începe procesul de interceptare a traficului conform acestora, iar în absența unor reguli specifice, se optează pentru captarea completă (tot traficul). Ulterior, există o decizie suplimentară privind aplicarea unei filtrări personalizate înainte de partajarea fluxului de date; în cazul în care se optează pentru filtrarea

suplimentară, se partajează doar traficul care corespunde criteriilor stabilite, în timp ce, în absența acestor criterii, se partajează integral pachetele colectate. Această modelare vizuală a fluxurilor ajută la înțelegerea mai clară a logicii interne a sistemului și oferă o structură ușor de urmărit atunci când se dorește extinderea sau optimizarea procesului de monitorizare și prelucrare a datelor.

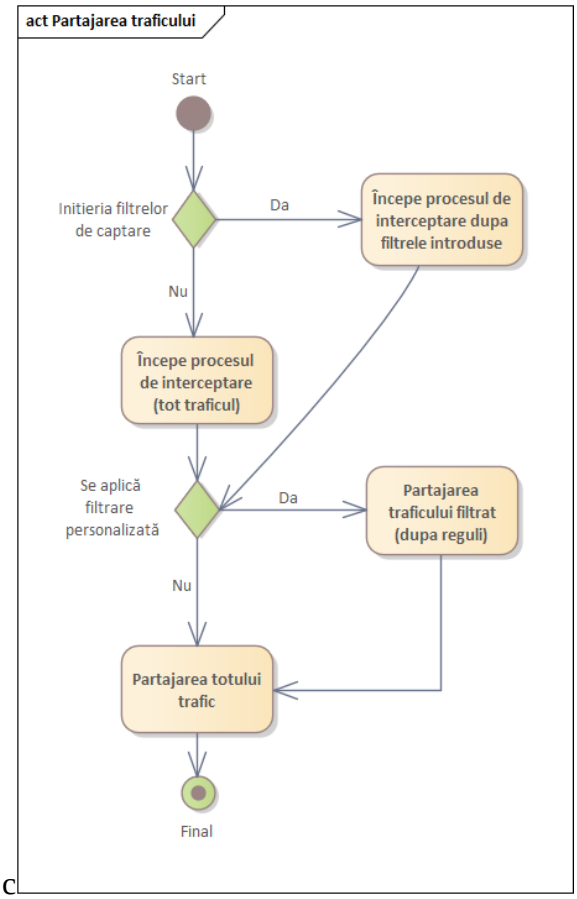

Figura 2.2 – Procesul de interceptare

Fluxul prezentat subliniază conceptul de „filtrare progresivă” în contextul interceptării datelor de rețea, demonstrând cum, în funcție de setările definite la pornirea aplicației, procesul poate evolua către o captare globală sau, dimpotrivă, către una orientată strict pe tipul de trafic vizat. Parcurgerea decizională din diagrama de activitate scoate în evidență flexibilitatea sistemului, permițând combinarea regulilor de filtrare pentru a obține un control granular asupra pachetelor interceptate. Astfel, dacă echipa de securitate activează anumite condiții de filtrare — cum ar fi protocoalele de comunicare suspecte sau adresele IP țintă — aceste reguli sunt aplicate din momentul inițial al captării, iar fluxul de date este redirecționat automat pentru analiză avansată. În situația opusă, fără introducerea niciunui filtru inițial, aplicația colectează toate pachetele, oferind o imagine de ansamblu cuprinzătoare asupra traficului. Prin prezentarea acestei diagrame, se arată cât de importantă este stabilirea de reguli flexibile încă de la începutul procesului, ceea ce permite adaptarea dinamică la diverse tipare de trafic și nevoi de securitate.

2.1.3 Descrierea scenariilor de utilizare a aplicației

În **Figura 2.4** se regăsește o diagramă de secvență care ilustrează etapele implicate în configurarea și gestionarea traficului de rețea, precum și schimbul de mesaje între actorul „Analist”, „Sistem”, sursa de „Trafic Rețea” și „Modulul Analiză”.

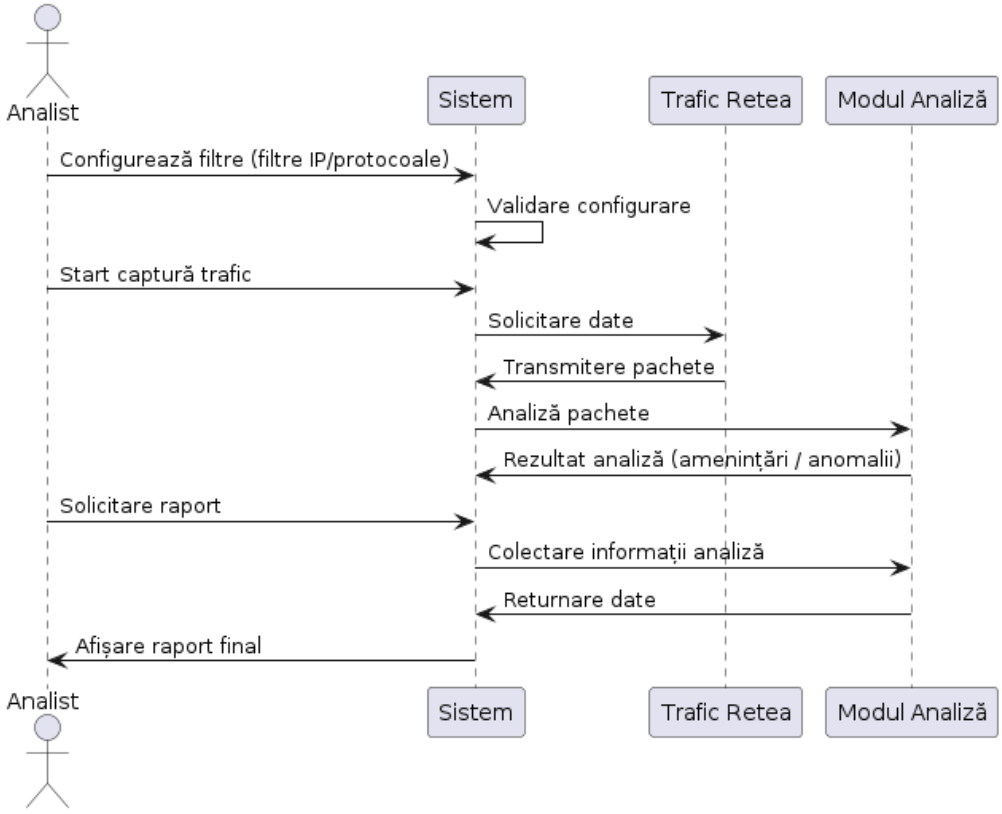

Figura 2.3 - Diagrama de secvență pentru configurarea, capturarea și analiza traficului de rețea

În primă instanță, analistul stabilește filtrele (adrese IP, protocoale) și pornește procesul de captură, moment în care sistemul validează setările și solicită date de la sursa de trafic. Pachetele interceptate sunt apoi transmise modulului de analiză, care verifică eventualele anomalii sau amenințări și returnează rezultatele. Ulterior, la cererea analistului, sistemul colectează informațiile obținute și afișează raportul final. Structura acestei diagrame de secvență subliniază interacțiunile logice dintre componente și evidențiază fluxul complet de acțiuni, de la definirea filtrelor până la prezentarea concluziilor despre securitatea traficului monitorizat.

2.2 Descrierea structurală a sistemului

În prima instanță, sistemul poate fi împărțit în componente precum modulul de captură (responsabil de interceptarea pachetelor de date), modulul de analiză (destinat verificării și detectării anomaliilor), bazele de date pentru logarea activităților și interfața de utilizator, prin care specialiștii configurează filtrele și vizualizează rapoarte. Fiecare dintre aceste componente are un rol bine definit și un set de responsabilități clar delimitate, fiind conectate într-o manieră ierarhică sau prin relații de colaborare.

Pentru ilustrarea acestor legături, se utilizează de regulă diagrame UML adecvate, precum diagrame de componente (Component Diagrams) sau diagrame de clasă (Class Diagrams). Aceste reprezentări grafice asigură o imagine de ansamblu asupra modului în care sunt organizate părțile sistemului și asupra modului în care acestea interacționează pentru a atinge obiectivele de securitate. De pildă, o diagramă de componente poate arăta modulul de captură conectat la modulul de analiză, care, la rândul lui, interacționează cu baza de date și notifică interfața de utilizator în cazul detecției unor comportamente suspecte. Această abordare vizuală facilitează înțelegerea rapidă a structurii interne, fiind un punct de reper pentru echipa de dezvoltare și pentru părțile interesate.

2.2.1 Descrierea structurii statice a sistemului

În **Figura 2.4** este prezentată diagrama de clasă asociată sistemului de interceptare și analiză a traficului, evidențiind principalele entități, atribute și metode implicate. Modelul cuprinde clase precum „Utilizator”, „SistemInterceptare”, „Filtru”, „Pachet”, „ModulAnaliză”, „BazaDateLoguri”, „Raport”, „RezultatAnaliza” și „Alerta”, fiecare având un rol specific în ciclul de captură și procesare. Clasa „Utilizator” administrează configurațiile și rapoartele, în timp ce „SistemInterceptare” inițiază și oprește capturarea, gestionând regulile de filtrare prin obiecte de tip „Filtru”. Pachetele de date interceptate sunt modelate prin clasa „Pachet”, care reține informațiile despre sursa, destinația și protocolul folosit.

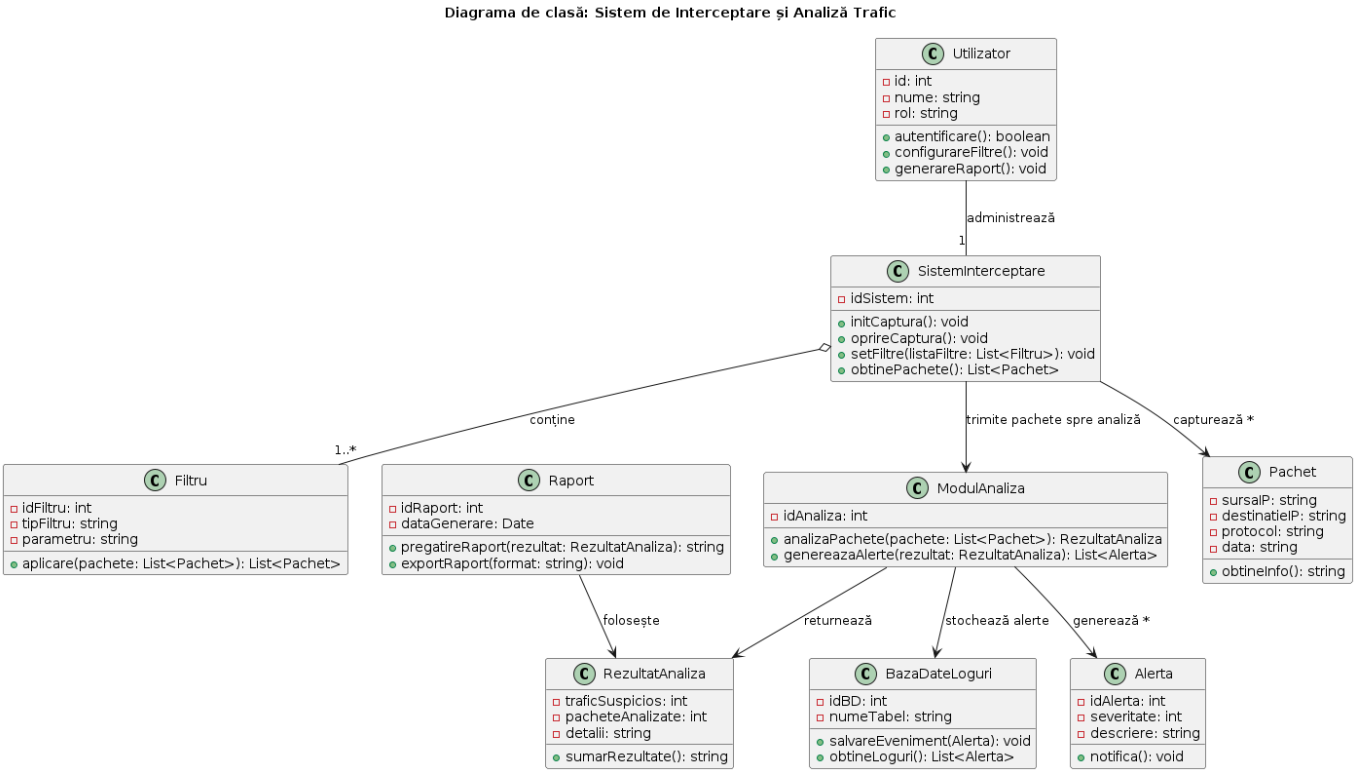

Figura 2.4 - Diagrama de clasă a sistemului de interceptare și analiză a traficului.

Analiza pachetelor are loc în cadrul clasei „ModulAnaliză”, rezultatele fiind centralizate în instanțe de tip „RezultatAnaliza” și, dacă e cazul, înregistrate sub forma unor „Alerta” în „BazaDateLoguri”.

Generarea documentației se efectuează prin intermediul clasei „Raport”, responsabilă de compilarea și exportul informațiilor esențiale, astfel încât procesul de monitorizare și investigare a traficului să fie susținut în mod unitar și eficient.

2.2.2 Relatiile de dependență între componentele sistemului

În **Figura 2.5** se observă o diagramă de componente care evidențiază structura modulară a sistemului de interceptare și analiză a traficului. Interfața Utilizator facilitează configurarea și controlul procesului de captură, generând cereri către „Modul Captură” pentru a intercepta pachetele de date. Aceste pachete sunt ulterior transmise către „Modul Analiză”, unde sunt identificate eventualele amenințări sau anomalii. „Generator Rapoarte” accesează rezultatele obținute, oferind utilizatorului posibilitatea de a solicita rapoarte și de a consulta date istorice, în timp ce „Baza de Date Loguri” stochează și pune la dispoziție evenimentele relevante pentru investigații ulterioare. Astfel, componenta fiecărei entități și rutele de comunicație dintre ele asigură o abordare coerentă și scalabilă a monitorizării securității rețelei.

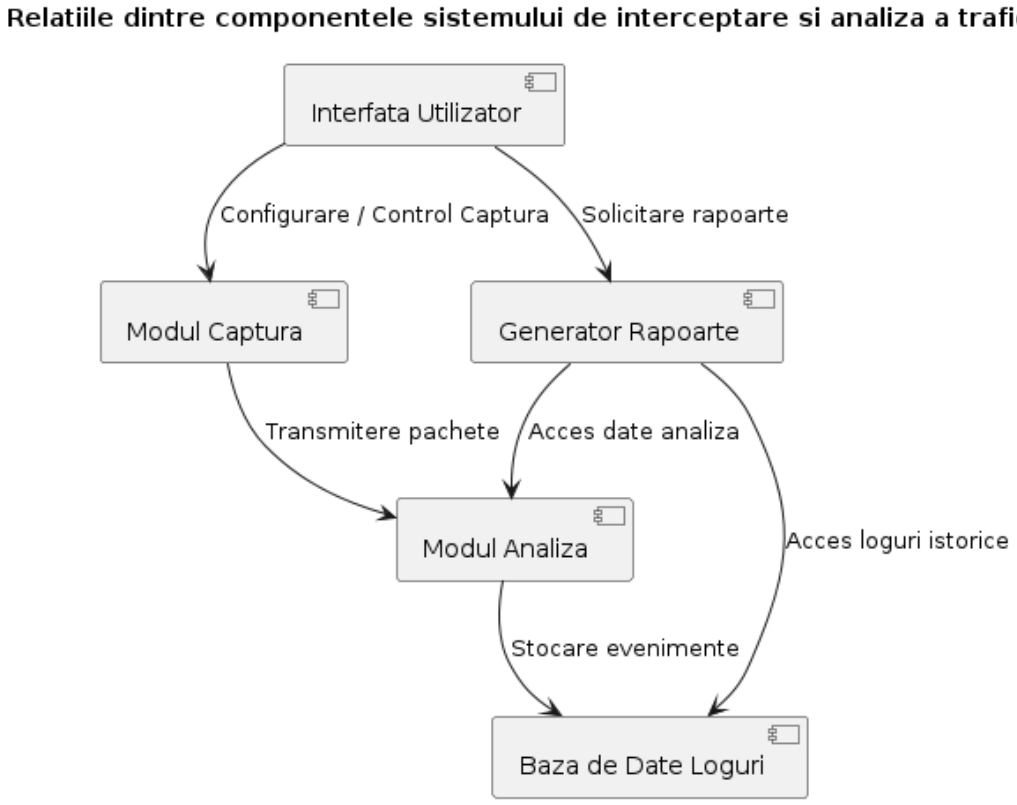

Figura 2.5 - Diagrama de componente a sistemului de interceptare și analiză a traficului.

CONCLUZII

La finalul stagiului, s-a constatat că realizarea unui sistem integrat pentru interceptarea și analiza traficului de rețea contribuie semnificativ la creșterea nivelului de securitate în infrastructurile informatice. Soluția proiectată asigură captarea în timp real a pachetelor, filtrarea lor după criterii relevante (protocol, adrese IP, porturi), precum și analiza automată în vederea identificării potențialelor amenințări. Eficiența unui astfel de sistem constă nu doar în capacitatea de a detecta activități suspecte, ci și în posibilitatea de a furniza rapoarte detaliate și de a stoca istoricul evenimentelor pentru investigații ulterioare.

Pe tot parcursul procesului de dezvoltare, s-a pus accent pe proiectarea modulară și pe modelarea UML, pentru a asigura o implementare coerentă și extensibilă. Utilizarea unor instrumente standardizate precum diagramele de clasă, de componente, de secvență și de activitate a permis o bună înțelegere a relațiilor dintre entități și a fluxurilor de date, contribuind la identificarea timpurie a eventualelor blocaje sau lacune. Testele efectuate au demonstrat că un proces de filtrare progresivă, combinat cu algoritmi de analiză bazată pe semnături și pe comportament, poate asigura un grad ridicat de acuratețe în detectarea anomaliilor.

Prin urmare, rezultatul final al practicii demonstrează cum adoptarea unei strategii de monitorizare continuă și de analiză avansată a traficului de rețea reprezintă un pas esențial pentru protejarea informațiilor sensibile și pentru menținerea integrității infrastructurilor IT. Experiența acumulată în timpul stagiului consolidează cunoștințele în domeniul securității cibernetice și oferă o perspectivă practică asupra abordărilor aplicate în mediul real.