**Aplicație destinata capturarii și analizei traficului dintr-o rețea de calculatoare**

|  |  |
| --- | --- |
| **Autor:** | **Damian Tudor Constantin** |
| **Îndrumător:** | **Prof. Dr. Eng. Bogdan Iancu** |

# Scopul și obiectivele proiectului

Această lucrare își propune dezvoltarea unei aplicații capabile să captureze și să analizeze traficul dintr-o rețea de calculatoare, oferind administratorilor de rețea o unealtă eficientă pentru monitorizare. Prin utilizarea Scapy pentru captură și procesare și integrarea cu ELK Stack pentru analiză și vizualizare, proiectul își propune să ofere o soluție scalabilă și performantă.

Obiective principale:

* Dezvoltarea unui modul pentru identificarea și listarea interfețelor de rețea disponibile pe sistem.
* Implementarea unui sistem de captură de pachete de pe una sau mai multe interfețe utilizând Scapy.
* Analiza protocoalelor fundamentale: IPv4, IPv6, TCP, UDP, ICMP.
* Clasificarea traficului în funcție de fluxuri (IPsrc, Portsrc, IPdst, Portdst, Protocol) sau alte criterii (DSCP, Porturi, IP).
* Filtrarea traficului conform criteriilor definite de utilizator.
* Captura și stocarea pachetelor într-un fișier PCAP pentru analiză ulterioară.
* Procesarea fișierelor PCAP utilizând Logstash, cu indexare în Elasticsearch și vizualizarea datelor capturate și analizate prin Kibana.
* Dezvoltarea unei interfețe web pentru acces la distanță și analiză în timp real.

# Rezultate așteptate / livrabile

Proiectul constă în dezvoltarea unei aplicații funcționale pentru captură și analiză de trafic de rețea. Acesta va permite administratorilor de rețea să monitorizeze traficul și să obțină statistici relevante în timp real. Aplicația va integra o interfață web pentru accesibilitate sporită și va permite salvarea datelor în format PCAP pentru analiză ulterioară. Se va furniza, de asemenea, documentație tehnică detaliată despre implementare și utilizare.

# Metode (abordarea tehnică)

Pentru a asigura eficiența și scalabilitatea aplicației, aceasta este organizată în mai multe componente:

1. Subsistemul de captură de trafic – utilizează Scapy pentru colectarea și stocarea pachetelor în fișiere PCAP.

2. Subsistemul de analiză și procesare – fișierele PCAP sunt încărcate și procesate în Logstash, apoi indexate în Elasticsearch.

3. Subsistemul de vizualizare și acces remote – utilizarea Kibana pentru afișarea statisticilor și dezvoltarea unei interfețe web pentru acces de la distanță.

Tehnologii utilizate:

• Scapy pentru capturarea și analiza pachetelor de rețea.

• Logstash, Elasticsearch, Kibana (ELK Stack) pentru procesarea și vizualizarea traficului.

• Spring Boot (Java) pentru backend-ul interfeței web.

• React.jspentru frontend-ul web.

Resurse necesare

Hardware: Sistem compatibil cu Scapy, spațiu de stocare suficient pentru fișiere PCAP.

Software: Java, Spring Boot, Scapy, Logstash, Elasticsearch, Kibana, React.js.

# Planificarea proiectului

**A graph with a number of letters and numbers

AI-generated content may be incorrect.**

# Cuprins lucrare

1. Introducere
2. Obiectivele Proiectului
3. Studiu Bibliografic
4. Analiza si Fundamentare Teoretica
5. Testare si Validare
6. Concluzii
7. Bibliografic