**General Proxy**

**-Proiect PSO-**

Prof. Coord.: Avram Dan

Grupa: C113 A

Studenți: Bălăcescu Anamaria

Dima Vlăduț Vasile



**Cuprins**

[**Diagrama Generală de Comunicație** 3](#_Toc150365094)

[**Descrierea interacțiunii cu aplicația** 3](#_Toc150365095)

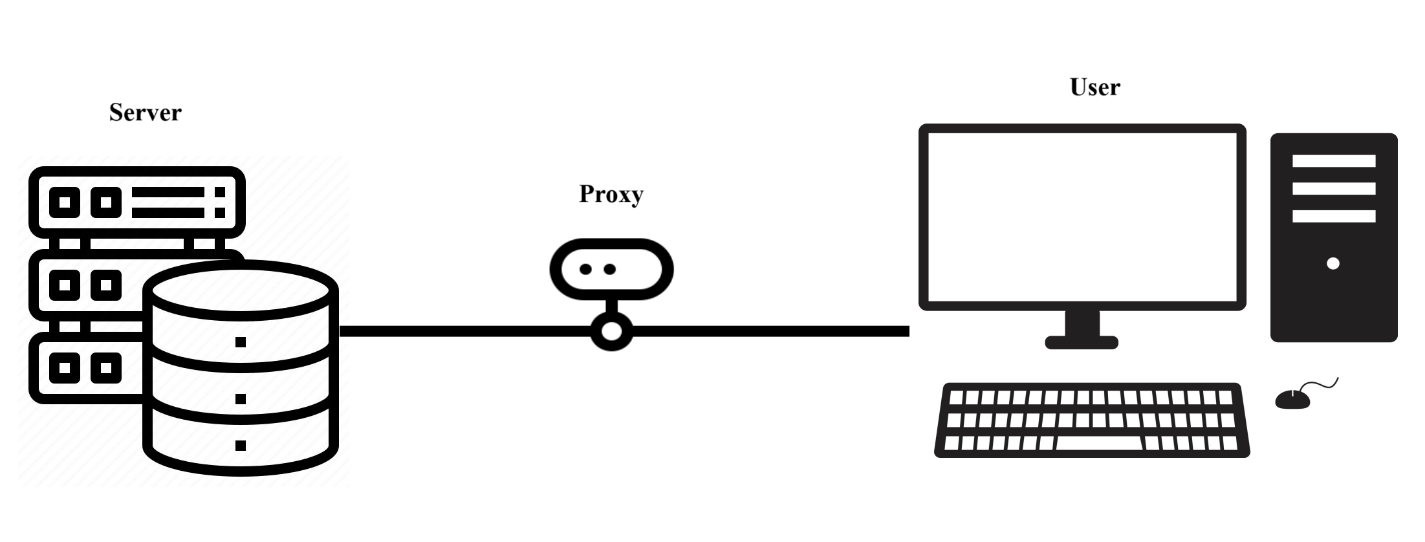
[**Descrierea cerințelor** 3](#_Toc150365096)

[1. Cerințele funcționale 3](#_Toc150365097)

[2. Cerințele non-funcționale 3](#_Toc150365098)

[**Bibliografie** 4](#_Toc150365099)

# **Diagrama Generală de Comunicație**



# **Descrierea interacțiunii cu aplicația**

Aplicția prezentată este un General Proxy care acționează ca un MITM între client și server.

În ecranul de pornire se stabilește adresa ip a serverului și portul pe care se interceptează traficul și fișierul de reguli pentru gestionarea acestuia. Aplicația așteaptă răspunsul de acceptare a conexiunii din partea serverului și începe interceptarea traficului pe portul stabilit.

După pornirea interceptării, la pachetele primite utilizatorul va primi codul hexazecimal și opțiunea de forward, drop sau modify. De asemena, se vor detecta caracteristici ale protocoalelor de comunicație cum ar fi nume, dimensiune.

În sprijinul detecției protocoalelor custom, se vor compara string-urile de date ale pachetelor trimise pentru a identifica secvențele comune ce pot reprezentare un warning.

# **Descrierea cerințelor**

## 1. Cerințele funcționale

* Interceptarea și afișarea traficului care intră pe un port specific al sistemului
* Afișarea codului hexazecimal
* Modificarea pachetelor în timp real - blocarea, înlocuirea sau injectarea de date în pachete
* Detectarea pattern-urilor – compararea pachetelor primite la nivel de date și detectarea octeților care se repetă.
* Sprijin pentru protocoale custom – gestionarea traficului în funcție de regulile primite prin fișierul transmis la pornirea aplicației.
* Detecție automată de protocoale – ex: detecția secvenței GET implică protocol HTTP
* Multi threading – gestionarea mai multor clienți simultan
* White list (opțional) – se acceptă comunicare de la adresele ip specificate în lista data și se blochează traficul de la orice altă adresă
* Posibilitatea utilizatorului de creare de reguli de drop/replacing pe anumite pattern-uri.

## 2. Cerințele non-funcționale

* + actualizarea automată a listei de pachete interceptate
  + înregistrarea acțiunilor în cadrul aplicației (History Log) - modificările, transmiterea sau blocarea de pachete se vor înregistra automat la nivelul fișierelor interne ale aplicației.

# **Bibliografie**

1. https://youtu.be/j9-Y0KWVJ1k?si=\_qeVLQfjj9qJT2Qq
2. https://youtu.be/qcXO93wgSQk?si=OBq3y1BQrjFWwXRN
3. https://youtu.be/QuCzG04Gypk?si=S5VfYtJUA9nRm4JC
4. https://youtu.be/g2iSPBmRZ7M?si=IF94-yCE3\_1DoVh9
5. https://youtu.be/btr3mj4DOjU?si=Vc5mt\_ndKYeXts8V
6. https://youtu.be/KOibBdrdyY0?si=CDcKvxM3kRKrrKwX
7. https://www.youtube.com/watch?v=ibnUI-amsj8&pp=ygUOdGNwIHByb3h5IGluIGM%3D&ab\_channel=HusseinNasser
8. <https://www.youtube.com/watch?v=iApNzWZG-10&pp=ygUZcHJveHkgc2VydmVyIHByb3h5IGNsaWVudA%3D%3D&ab_channel=LiveOverflow>
9. https://www.geeksforgeeks.org/proxy-design-pattern/
10. https://javascript.plainenglish.io/build-your-own-forward-and-reverse-proxy-server-using-node-js-from-scratch-eaa0f8d69e1f
11. https://www.winpcap.org/docs/docs\_412/html/funcs\_2pcap\_8h.html
12. https://github.com/the-tcpdump-group/libpcap/blob/master/pcap/pcap.h
13. https://www.tcpdump.org/pcap.html
14. https://www.cloudflare.com/learning/network-layer/what-is-a-computer-port/#main-content
15. https://cromwell-intl.com/networking/protocols.html
16. https://www.winpcap.org/docs/docs\_40\_2/html/functions\_vars.html