**General Proxy**

**-Proiect PSO-**

Prof. Coord.: Avram Dan

Grupa: C113 A

Studenți: Bălăcescu Anamaria

Dima Vlăduț Vasile



Cuprins

Contents

[**Tabel versiuni** 3](#_Toc148893542)

[**Capitolul 1 – Introducere** 4](#_Toc148893543)

[1.1. Scopul proiectului 4](#_Toc148893544)

[1.2. Lista definițiilor 4](#_Toc148893545)

[1.3. Structura DSC 4](#_Toc148893546)

[**Capitolul 2 – Descrierea generală a produsului software** 4](#_Toc148893547)

[2.1. Descrierea produsului software 4](#_Toc148893548)

[2.2. Descrierea platformei HW/SW 5](#_Toc148893549)

[**Capitolul 3 – Descrierea cerințelor** 5](#_Toc148893550)

[3.1. Cerințele funcționale 5](#_Toc148893551)

[3.2. Cerințele non-funcționale 6](#_Toc148893552)

# **Tabel versiuni**

|  |  |  |
| --- | --- | --- |
| Versiune | Client – specificații | Server - specificații |
| Versiune 1.0 |  |  |

# **Capitolul 1 – Introducere**

## 1.1. Scopul proiectului

Programul are ca scop interceptarea traficului primit pe un port și manipularea datelor sale.

Pachetele transmise în rețea sunt detectate în cadrul server-ului Proxy prin pattern-ul lor și trimise spre analiză. În funcție de header-ele transmise se pot identifica tipurile de protocoale de comunicație primite. De asemenea, la primirea pachetului se oferă posibilitatea vizualizării codului hexazecimal și modificarea pachetului în timp real, iar erorile detectate de reguli prestabilitate vor fi remediate automat.

## 1.2. Lista definițiilor

## 

|  |  |
| --- | --- |
| Abreviere | Definiție |
| App | Aplicație |
| DSC | Document Cerințe Software |
| HW | Hardware |
| SW | Software |
| Frame | Cadru de rețea |
| Header | Antet |

## 1.3. Structura DSC

Documentul este împărțit în 3 capitole: capitolul 1 reprezintă Introducerea în tema proiectului (scopul proiectului, lista definițiilor), capitolul 2 prezintă descrierea generală a cerințelor software cu particularitățile stabilite inițial pentru funcționalitățile software, elementele hardware și constrângerile necesare realizării aplicației propriu-zise, urmând o detaliere a cerințelor, funcționale și non-funcționale, în capitolul 3.

# **Capitolul 2 – Descrierea generală a produsului software**

## 2.1. Descrierea produsului software

În prezent, „boom-ul” tehnologic a luat amploare acoperind majoritatea domeniilor de activitate. Odată cu acest progres științific au progresat deopotrivă și amenințările din domeniul cibernetic (exfiltrare de date, impersonare, phishing, etc). Cât timp folosești aplicații, comunici prin intermediul rețelelor de socializare sau pur și simplu ești conectat la internet, ești o țintă aproape sigură a atacatorilor din acest domeniu. Aplicația noastră vizează combaterea încercărilor de infiltrare și asigurarea posibilității de control asupra fluxului de date din rețeaua proprie.

Pentru a asigura o experiență cât mai plăcută, interfața noastră grafică este intuitivă și prietenoasă, cu navigare ușoară, structură logică și un design clar, care nu necesită instrucțiuni complexe pentru utilizare.

După transmiterea unui pachet în rețea acesta va fi interceptat de server-ul Proxy care îl va analiza după regulile predefinite și îl va încadra fie într-o categorie de protocoale cunoscute, fie necunoscute. Utilizatorul va avea posibilitatea de a vedea și evalua codul hexazecimal al pachetului primit, precum și a modifica acțiunea efectuată asupra lui. Astfel, va prelua puterea de decizie în transmiterea, rejectarea sau modificarea pachetului.

Dacă pe parcursul acestei analize sunt sesizate nereguli care contravin retricțiilor stabilite în interiorul programului, server-ul va putea acționa prin apelarea funcțiilor de gestionare a erorilor și va schimba octeții afectați.

De asemenea, protocoalele de categorie specială care nu prezintă risc prin regulamentul după care este concepută aplicația, vor beneficia de sprijin pentru redirecționarea cât mai rapidă pentru a eficientiza procesele de securitate și comunicare.

Pentru a facilita descoperirea unor eventuale acțiuni malițioase sau a persoanelor responsabile de anumite defecțiuni aduse sistemului, fiecare acțiune asupra pachetelor va fi memorată la nivelul bazei de date într-un Histroy log, iar cele considerate malițioase de către app vor genera un mesaj de eroare. De asemenea, pentru a evita pierderea de informații, acest fișier se va actualiza automat după fiecare modificare adusă. Interceptarea, precum și acțiunile decizionale asupra pachetelor vor fi și ele însemnate la nivelul aplicației.

Luând o situație ipotetică, vom considera o firmă multinațională cu angajați din diferite țări care lucrează în regim remote. Albert și John sunt angajați ai acestei firme care își transmit informații prin rețeaua VPN.

Conversațiile lor uzuale sunt înregistrate prin trimitere și acceptare de ambele părți.

1. Albert has sent a packet. 12/03/2023 14:55
2. John has received a packet. 12/03/2023 14:55
3. John has sent a packet. 12/03/2023 14:58
4. Albert has received a packet. 12/03/2023 14:58

. . . . . . . . .

Dar se poate întâmpla ca un atacator să se infiltreze în rețea sub adresa IP a lui John și să îl impersoneze. Albert, folosind Proxy-ul înaintea validării oricărui pachet primit, va analiza protocolul stabilit și codul său hexazecimal, va cere înlocuirea octeților malițioși și va rejecta pachetul. În acest caz istoricul acțiunilor memorate va fi de forma:

. . . . . . . . .

1. John has sent a packet. 12/03/2023 14:58
2. Albert has modified the packet. 12/03/2023 14:59
3. Albert has dropped the packet. 12/03/2023 15:00

. . . . . . . . .

## 2.2. Descrierea platformei HW/SW

Pentru testarea aplicației, atât serverul cât și utilizatorul au nevoie de o conexiune la internet și de platforme de tip Ubuntu Linux.

# **Capitolul 3 – Descrierea cerințelor**

## 3.1. 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 - modificarea octeților din pachet la detectarea erorilor prin reguli prestabilite
* Sprijin pentru protocoale custom - transmitere mai rapidă a unor protocoale prestabilite
* Posibilitatea utilizatorului de creare de reguli de drop/replacing pe anumite pattern-uri

## 3.2. 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.
  + Securizarea informațiilor (Criptarea mejasului din protocolul de comunicație/pachetului) – folosind metode criptografice pentru autenticitate și constanța conținutului datelor.