פרויקט גמר

הנדסאי תוכנה

**DPI Over Linux Firewall**

מגיש

אריאל אילון – 215537176

מנחה – אייל יעקב יחיאלי

מכללת אורט רחובות

שנה"ל תשפ"ד

30.09.2024

# תוכן העניינים

[תוכן העניינים 2](#_Toc178592802)

[1. פרק ראשון: הצעת הפרויקט 3](#_Toc178592803)

[1.1. תיאור פרויקט 3](#_Toc178592804)

[2.1. תיאור הטכנולוגיה 4](#_Toc178592805)

# 1. פרק ראשון: הצעת הפרויקט

## 1.1. תיאור פרויקט

1.1.1. הצורך המבצעי

בחיל האוויר ישנן מספר רב מאוד של רשתות בעלות רמות סיווג שונות. כל אחת מן השרתות הללו מבודדות, והמעבר של מידע והוראות בין הרשתות הללו מוגבל מאוד כך שבמידה ותוקף הצליח לחדור לאחת מן הרשתות, לא תהיה פגיעה באבטחת שאר הרשתות.

בכדי למנוע מתוקף להשיג גישה למערכות מבצעיות ומידע מסווג, נוצרו מספר מערכות שונות, כגון: חומות אש, ערוצי תקשורת מוצפנים, קווי תקשורת מוגנים וכו'.

מטרת הפרויקט הזה, היא לספק שכבת הגנה אחרונה (חומת אש) בנקודות הקצה של המערכת, בעלת יכולת של קריאת פקטות עמוקה – DPI כך, שמערכת מבצעית תוכל להגן על עצמה ממתקפת "איש באמצע" (MITM).

2.1.1. מענה לצורך המבצעי

הפרויקט יהיה מורכב מ3 חלקים עקרים. חומת האש עצמה, שתבצע DPI, ממשק משתמש גרפי (GUI) ומוסד נתונים מבוסס SQL. אפליקציית המשתמש תאפשר להגדיר את הפורטים, פרוטוקולים ותבניות הסינון שבהן ישתמש שירות הDPI.

שירות ה DPI ייעזר בממשק סינון פקטות שהינו חלק מהקרנל של מערכת ההפעלה כדי לתפוס את הפקטות שנכנסות למחשב ויעזר במידע ממסד הנתונים בכדי לקבוע האם לאפשר לפקטה לעבור או לא (הוורדיט/Verdict).

3.1.1. רקע תיאורטי וידע נדרש למטרת מימוש הפרויקט

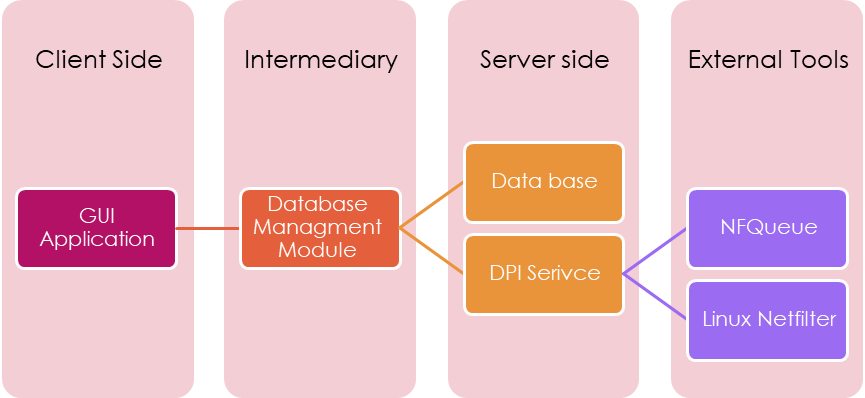
* תכנות בשפות C, .C++
* ניהול מסד נתונים, SQL.
* עבודה במרחב קרנל (KERNEL\_SPACE).
* תכנון מערכות.
* ידע והבנה של עקרונות תקשורת מחשבים ורשתות.
* עבודה עם ממשקי NetFilter ו- NF queue.
* תכנון ובנייה של GUI.
* תכנות בשפת C# וספריית Avalonia.
* בניית אפליקציה אגנוסטית למערכת הפעלה (בשל השימוש ב#C).  
  Platform Agnostic / Cross – Platform.
* מבנה Linux Kernel.
* פיתוח Kernel Module.

4.1.1. תהליכים עיקריים בפרויקט

* תפיסה וסינון פקטות בעזרת DPI.
* ניהול וסנכרון מסד הנתונים.
* תקשורת בין ממש משתמש לצד השרת.
* תפיסה וזיהום פקטות בכדי לדמות תוקף MITM.

## 2.1. תיאור הטכנולוגיה

1.2.1. תרשים להמחשת המערכת



MITM Simulation via a kernel module

2.2.1. טכנולוגיות עזר נדרשות

* Linux (Debian distribution) Operating System.
* C Programing language.
* C++ Programing language.
* C# Programing language.
* Avalonia library.
* Linux Netfilter.
* SQLite.