

אפיון פרויקט

הגנת סייבר

**מגיש: עומר כפיר (330869017) תיכון הרצוג כפר סבא יב'3**

**שם פרויקט: Silent Net**

**שם מנחה: אופיר שביט**

**שם חלופה: הגנת סייבר ומערכות הפעלה**

**תאריך הגשה: 00/05/2025**

תוכן עניינים

[**מבוא** 4](#_Toc196754897)

[**תיאור כללי** 4](#_Toc196754898)

[**מטרות ויעדים** 4](#_Toc196754899)

[**בעיות תועלות וחסכונות** 5](#_Toc196754900)

[**סקר שוק – חקירת פתרונות קיימים** 5](#_Toc196754901)

[**סקירת טכנולוגיית הפרויקט** 7](#_Toc196754902)

[**תיחום פרויקט** 7](#_Toc196754903)

[**פירוט תיאור המערכת (אפיון)** 8](#_Toc196754904)

[**תיאור מפורט של המערכת** 8](#_Toc196754905)

[**פירוט על יכולות שהיא תעניק לכל סוג משתמש** 9](#_Toc196754906)

[**פירוט יכולות המערכת** 10](#_Toc196754907)

[**בדיקות, לו"ז וסיכונים** 17](#_Toc196754908)

[**פירוט בדיקות שמתוכננות לפרויקט** 17](#_Toc196754909)

[**תכנון וניהול לוז** 20](#_Toc196754910)

[**סיכונים** 21](#_Toc196754911)

[**תיאור ארכיטקטורה המערכת** 23](#_Toc196754912)

[**תיאור החומרה** 23](#_Toc196754913)

[**מראה גרפי של קשרי החומרה** 24](#_Toc196754914)

[**תיאור טכנולוגיות רלוונטיות** 25](#_Toc196754915)

[**שפות תכנות** 25](#_Toc196754916)

[**מערכת הפעלה** 26](#_Toc196754917)

[**תחומי עניין** 29](#_Toc196754918)

[**תיאור זרימת המידע במערכת** 30](#_Toc196754919)

[**האזנה שקטה על מחשב המשתמש** 30](#_Toc196754920)

[**איסוף מידע בזמן אמת מן מחשב המשתמש** 31](#_Toc196754921)

[**גיבוי נתונים אצל המשתמש בעת שרת כבוי** 32](#_Toc196754922)

[**שליחת מידע המשתמש אל המנהל** 33](#_Toc196754923)

[**איסוף המידע במחשב השרת ל DB** 34](#_Toc196754924)

[**הצגת המידע באופן נגיש במחשב המנהל** 35](#_Toc196754925)

[**הגדרת רמת בטיחות אצל המנהל** 36](#_Toc196754926)

[**ניסוח וניתוח של הבעיה האלגוריתמית** 37](#_Toc196754927)

[**אלגוריתמים קיימים לפתרון הבעיה** 37](#_Toc196754928)

[**סקירת הפיתרון הנבחר** 37](#_Toc196754929)

[**הפנייה למקור רלוונטי** 37](#_Toc196754930)

[**תיאור סביבת הפיתוח** 38](#_Toc196754931)

[**תיאור פרוטוקול התקשורת** 39](#_Toc196754932)

[**דוגמה להודעות:** 39](#_Toc196754933)

[**טבלת הודעות פרוטוקול** 40](#_Toc196754934)

[**תיאור מסכי המערכת** 42](#_Toc196754935)

[**מסך פתיחה** 42](#_Toc196754936)

[**מסך הגדרות** 43](#_Toc196754937)

[**מסך ראשי** 44](#_Toc196754938)

[**מסך אישי** 44](#_Toc196754939)

[**מסך יציאה** 45](#_Toc196754940)

[**מסך טעינה** 45](#_Toc196754941)

[**מסך שגיאה** 46](#_Toc196754942)

[**מסך 404** 47](#_Toc196754943)

[**דיאגרמת מסכים** 48](#_Toc196754944)

[**תיאור מבני נתונים** 49](#_Toc196754945)

[**סקירת חולשות ואיומים** 51](#_Toc196754946)

# **מבוא**

* **ייזום**

## **תיאור כללי**

הפרויקט הינו פלטפורמה שמאפשרת למנהל של חברה להשגיח על פעילות לקוחותיו מרחוק ולוודא שהם מבצעים את העבודה כראוי. הפלטפורמה על המחשבים של העובדים מסתירה את עצמה כך שהעובדים בחברה לא יוכלו להסיר את התוכנית מהמחשב שלהם לבד או לשבש פעילותה.

בחרתי בפרויקט זה מכיוון שהוא אינו פשוט ויהווה לי אתגר ואף בנוסף הוא עוסק בעיקרו בעולם מערכות ההפעלה, עולם שמרתק אותי. הפרויקט דורש למידה על התנהגות של מערכת ההפעלה והתעסקות עם קוד של מערכת ההפעלה. המטלה הינה לא פשוטה ומביאה עימה מספר אתגרים: הסתרת הליך במערכת הפעלה והאזנה לפעולות שונות מבלי פגע ויכולות של המשתמש לדעת, העברת מידע אמין למחשב המנהל אשר משמש בתור שרת, תצוגה גרפית בצורה נוחה אצל מחשב המנהל ועוד...

## **מטרות ויעדים**

לפרויקט מספר מטרות, חלק מן המטרות עוסקות בכל הנוגע למערכות הפעלה והכוונה להסתיר באופן מוחלט מן העובד בחברה את אותו תהליך בכדי שלא יוכל להסיר אותו/לשנות אותו, בו זמנית המנהל ישלוט באופן מלא על אותם תהליכים ויוכל לעשות בהם כרצונם. על המערכת להיות נגישה כמה שיותר למנהל החברה וביחד עם זאת להיות מוסתרת כמה שיותר מהעובד בחברה שהתוכנה רצה אצלו במחשב.

## **בעיות תועלות וחסכונות**

המערכת באה לחסוך זמנים בשביל מנהלים בחברות. חברות אשר ישתמשו במערכת זו יוכלו באופן נגיש להאזין למחשבים של העובדים בחברה שלהם מבלי שהעובדים יוכלו לעשות דבר כנגד לכך. העובדים לא יוכלו למצוא או לשנות את התוכנית המאזינה בכדי "לעבוד" על המנהל שלהם, המנהל יידע על שלל פעילות המחשב שלהם מבלי יוצא מן הכלל (כמובן הפרטים החשובים, לא האזנה מלאה לכל event). המערכת תפתור את הבעיה שנוצרת אצל עובדים בחברות שאינם מנצלים את זמן העבודה באופן מיטבי ואף גם לעיתים לא מבצעים את העבודה הצפויה מהם במהלך העבודה. זוהי הינה בעיה חמורה שמפסידה כסף רב לחברות, וכאן בדיוק מגיעה המערכת שלי. מבלי ידיעת העובדים המנהל יכול בכל רגע נתון להסתכל על נתוני המחשב של העובד אצלו בתוכנה, ומכך להבין אם העובד מבצע את עבודתו כראוי או שצריך להעיר לו ואף אם הדבר מתמשך לפטר את העובד מהחברה. המערכת תנגיש את המידע על הלקוחות השונים למנהל של החברה בכדי שיוכל לתצפת על עובדיו באופן נוח ויעיל, מבלי שיצטרך להתקשות עם תוכנה מסובכת, כמו שידוע כיום הרבה תוכנות בעלות פונקציונליות רבה מתקשות בלשמור על ממשק משתמש נוח וקל לשימוש, ולכן המערכת תדע להציג את המידע באופן נוח מבלי שמנהל החברה יצטרך להתקשות איתה.

## **סקר שוק – חקירת פתרונות קיימים**

כידוע כיום עולם אבטחת המידע הוא נושא מבין הנושאים שמעסיקים אותנו ביום יום. קיימים מאות אלפי אם לא מיליוני כלים באינטרנט לאבטחת סייבר. כלים אשר מדמים את פעולות של המערכת הם כלים כמו Anti-Virus/Anti-cheat. אותם כלים לרוב יהיו KLM (Kernel Loadable Module) והם יודעים להאזין לפעילויות המערכת, קלטים שונים, תהליכים כאלו ואחרים, ואף להתריע ולשלוח לאדם חיצוני בעת זיהוי סכנה. דרך פעולה זו מדמה את פעולות המערכת בפרויקט שלי, אשר המערכת יודעת לשבת בליבת מערכת ההפעלה, ולשלוח מידע לאדם חיצוני, האומנם המערכת שלי אינה מנתחת את פעילות המחשב ומתריעה רק בעת סכנה, אך היא יודעת להאזין לליבת מערכת ההפעלה ולשלוח את המידע לאדם חיצוני. Silent Net מתמקדת לא רק בהאזנה דיסקרטית אלא גם במניעת חשיפה שעלולה לאפשר התערבות חיצונית.

המערכת מתוכננת כך שהמשתמש לא יוכל להשיג כל מידע מהותי שיאפשר לו לזהות, לאתר או לחסום את פעילותה. לשם כך, Silent Net שמה דגש על טשטוש סימנים מזהים כמו שמות מודולים, נתיבי קבצים, כתובות תקשורת ופרטים נוספים. בכך, גם אם המשתמש ינסה לנתח את המערכת, לא יימצאו רמזים ברורים שיאפשרו לו להפעיל אמצעים נגדיים. גישה זו מייחדת את Silent Net ממערכות אבטחה קלאסיות, שכן המטרה אינה להתריע על סכנות אלא לשמר פעילות סמויה לאורך זמן מבלי לאפשר גילוי או שיבוש.



## **סקירת טכנולוגיית הפרויקט**

במערכות הפעלה קיימת שונות רבה בין מערכות שונות ואפילו בין גרסאות שונות של אותה מערכת הפעלה. ועל כך, יש חשיבות ותלות רבה בסביבה בה תורץ המערכת. מכיוון שהמערכת עוסקת בלב ליבה של מערכת ההפעלה, קיים קושי בלהפוך אותה דינמית לשלל גרסאות של מערכת הפעלה, ולכן המערכת תהייה מחויבת לרוץ על אותה סביבת עבודה. (בדגש רק צד הלקוח, על צד השרת לא תקפים החוקים הללו). דבר זה יכול להתקיים על ידי הרצה של VMים כאלו ואחרים. הפרויקט יהיה מחוייב לרוץ על הגרסה בה פותח, ללא אפשרות להריץ על גרסאות אחרות של אותה מערכת הפעלה, ולכן חובה על כל מחשב שהמערכת תרוץ עליו להתאים לגרסת מערכת ההפעלה עליה הפרויקט תוכנן לרוץ.

## **תיחום פרויקט**

הפרויקט הולך לעסוק בשלל של נושאים שעליהם אפרט:

* + מערכות הפעלה – hook שונים של פונקציות במערכת ההפעלה, הסתרת מידע בפני תהליכים, האזנות לדרייברים, ועוד...
  + רשתות – על מנת להעביר את המידע שנאסף מן מערכת ההפעלה על הפרויקט להשתמש ב socket, בדגש על שימוש בפרוטוקול TCP אשר יעביר את המידע בצורה אמינה למחשב השרת.
  + על הפרויקט להשתמש בסוגי הצפנות שונים בכדי לתקשר בצורה מאובטחת עם צד השרת.
  + המערכת איננה עוסקת באבטחה של מערכות הפעלה (כמו שצוין AntiVirus), שמירת סיסמאות בתוך DB ועוד...



# **פירוט תיאור המערכת (אפיון)**

## **תיאור מפורט של המערכת**

המערכת המדוברת היא מערכת האזנה שקטה ובלתי נראית, אשר פועלת על מחשבי קצה המריצים את מערכת ההפעלה לינוקס. מטרת העל של המערכת היא לפקח על פעולתם התקינה והשוטפת של המחשבים, תוך שמירה על סודיות מוחלטת וללא כל אפשרות למשתמשי המערכת לזהות את נוכחותה. המערכת תופעל ברקע ותנטר בצורה שקטה מתודות שונות המבוצעות על ידי תוכניות שונות שרצות על המחשב, וזאת במטרה לאפשר מעקב רציף, מדויק ויסודי אחרי כל פעולה המתבצעת במערכת.

באמצעות מנגנוני האזנה מתקדמים, המערכת תוכל לעקוב אחרי מגוון רחב של פעולות, ביניהן הרצת תוכניות חדשות, יצירת ושימוש בחיבורים לרשת, ועוד. המידע שייאסף יאפשר לקבל תמונה מלאה, מקיפה ורציפה על כל מה שמתרחש במחשב בזמן אמת, כך שכל פעילות תדווח למחשב השרת והמנהל יוכל לבחון זאת בעצמו ולהחליט על עבודת העובד.

הייחודיות של המערכת טמונה בכך שהיא לא רק מבצעת מעקב אלא גם שומרת על עצמה מוסתרת לחלוטין. גם אם עובד יידע מראש על קיומה, הוא לא יוכל לזהות אותה, להסיר אותה או להפריע לפעולתה. לשם כך, המערכת תשתמש בטכניקות חכמות ומתקדמות, כמו שינוי מודולים קיימים של מערכת ההפעלה, שינוי דינמי של קריאות מערכת והתחמקות מגילוי או אמצעי ניטור אחרים.

המערכת תעבוד באופן קבוע לאיסוף מידע, אשר ייארז בצורה מסודרת, מאורגנת ויעילה, תוך שמירה על הפרדה בין משתמשים שונים. המידע יישלח למחשב שרת מרכזי שאיתו המנהלים יוכלו ליצור תקשורת ולהשיג את הנתונים ממנו השמורים על כל מחשב ומחשב, הנתונים שמורים בצורה ברורה, נוחה ונגישה. המידע יוצג לפי משתמשים ומחשבים, עם אפשרויות סינון מתקדמות, הצגת נתונים בזמן אמת, כולל הפקת דו"חות מפורטים לפי הצורך.

באופן כללי, המערכת מהווה פתרון טכנולוגי מתקדם שמפשט ומייעל את ניהול העובדים והמשאבים הדיגיטליים של הארגון. בזכות אוטומציה של תהליכי הפיקוח ושמירה על דיסקרטיות מוחלטת, המערכת מאפשרת למנהל לקבל שליטה מלאה, לצפות בהתנהלות העובדים, לאתר בעיות במהירות, וכל זאת תוך שמירה על רמת ביצועים גבוהה מאוד וללא השפעה ניכרת על המערכת הנבדקת.

## **פירוט על יכולות שהיא תעניק לכל סוג משתמש**

היכולות העיקריות שיוסגו מן הפרויקט הינן לצד המנהל. כמו שהוסבר מקודם הפרויקט הוא פרויקט האזנה למחשבים של עובדים בחברה, ומטרת התוכנה הינה להסתתר כמה שיותר במחשבי העובדים. כלומר העובדים לא אמורים כלל להיות מודעים לנוכחות התוכנה על מחשבים, ובמידה וכן, לא יוכלו לעשות דבר בנידון. לכן בשביל צד המשתמש אין לו כלל יכולות שהפרויקט מעניק לו. בניגוד לכך, הפרויקט מעניק שלל יכולות מגוונות למנהל של העובדים. המנהל יוכל בכל רגע נתון לראות את פעילות עובדי החברה במחשביהם, כלומר, אם הוא רוצה לבדוק שעובדיו מבצעים את עבודתם כראוי, יוכל להסתכל בנתוני המערכת אצלו במחשב ולראות נתונים שונים על מחשב העובד. מטרת הפרויקט כפי שהוגדרה הינה לייעל את עבודתו של מנהלים בחברות, והגישה של המנהל לנתונים נגישים בזמן אמת על עובדיו בהחלט מסייעת לכך. אם הנתונים האלו המנהל יכול להבין אילו מעובדיו מבצעים את עבודתם ואילו אינם, ומכיוון שהעובדים לא יכולים לשנות את התוכנה (או שהם בכלל לא מודעים לתוכנה) הם לא יכולים כלל לדעת מתי המנהל מסתכל על הנתונים של מחשביהם, ובכך המנהל יכול לדעת באופן חשאי פרטים על פעילות עובדיו, והאם צריך לשנות נהלים באופן העבודה או בכלל לפטר עובדים שרוב הזמן אינם עובדים לפי הוראות המנהל.

להלן פירוט מפורט יותר של היכולות.

## **פירוט יכולות המערכת**

1.האזנה שקטה על מחשב המשתמש.

2.איסוף מידע בזמן אמת מן מחשב המשתמש.

3.גיבוי נתונים אצל המשתמש בעת שרת כבוי.

4.שליחת מידע של מחשב המשתמש אל מחשב השרת.

5.איסוף המידע במחשב השרת אל תוך DB.

6.הצגת המידע באופן נגיש במחשב המנהל.

7.הגדרת רמת בטיחות אצל המנהל.

|  |  |
| --- | --- |
| האזנה שקטה על מחשב המשתמש | שם היכולת |
| האזנה שקטה על מחשב המשתמש מאפשרת לכך שאין באפשרות העובדים למחוק/לשבש דברים בתוכנה בזמן פעילותה, כלומר התוכנה תמיד תפעל ואך ורק המנהל הוא בעל היכולת לשנות דברים בתוכנה. בכך המנהל יכול בכל זמן נתון לתצפת על עובדיו מבלי שיוכלו "לעבוד" על התוכנית ולגרום לה לשלוח מידע לא אמין. | מהות היכולת |
| **אצל הלקוח**   * ביצוע hookים שונים על פעולות מבלי לפגוע במהות הפעולות * הסתרת התהליך * האזנה "קלה" כך שאינה משפיע על ביצועי המערכת של מחשב המשתמש | אוסף פעולות/יכולות הנדרשות ליכולת הנ"ל |
| * KLM – Kernel Loadable Module, כלומר תהליך בהרשאות הגבוהות ביותר במחשב – קרנל * מחשב לקוח (עם מערכת הפעלה לינוקס) * הרשאות של המנהל על מחשב הלקוח | אובייקטים נחוצים |

|  |  |
| --- | --- |
| איסוף מידע בזמן אמת מן מחשב המשתמש | שם היכולת |
| איסוף מידע בזמן אמת מן המחשב של המשתמש מאפשרת ליכולות אחרות בפרויקט זה, אסיפת המידע היא יכולת קריטית אצל מחשבי המשתמשים, והיא חלק גדול מפרויקט זה. איסוף המידע בזמן אמת יאפשר למנהל לתצפת על עובדיו בזמן אמת (ולא רק לקבל סיכום), כלומר בכל רגע נתון המנהל בעל יכולת לבדוק את עובדיו ואת עבודותיהם. | מהות היכולת |
| **אצל הלקוח**   * ביצוע hookים שונים על פעולות מבלי לפגוע במהות הפעולות * שמירת המידע בצורת טקסט שניתן לקרוא ולהבין בצורה מונגשת * יצירת סדר במידע, כל פעולה שונה במחשב המשתמש עליה להיות מסודרת לפי סוג הפעולה. | אוסף פעולות/יכולות הנדרשות ליכולת הנ"ל |
| * KLM – Kernel Loadable Module, כלומר תהליך בהרשאות הגבוהות ביותר במחשב – קרנל * מחשב לקוח * קבצים/באפרים לאחסון המידע באופן זמני | אובייקטים נחוצים |

|  |  |
| --- | --- |
| גיבוי נתונים אצל המשתמש בעת שרת כבוי | שם היכולת |
| בזכות היכולת של הלקוח לאסוף בזמן אמת נתונים, עליו גם לאחסן אותם אצלו כאשר קיימות תקלות כאלו ואחרות בתקשורת או אפילו מחשב השרת נכבה. יכולת זה מכפה על תקלות כאלו שאינן בשליטת הפרויקט ובאות לפצות עליהן. גיבוי הנתונים אינו אינסופי אך מוגבל בגודלו על ידי המנהל בכדי לא להעמיס על מחשבי הלקוחות, הגודל נקבע לפי רצון המנהל. אם מחשב הלקוח נכבה אף הוא בעצמו מבלי לסגור את התוכנית באופן שלם, התוכנית תדע בעצמה לחזור למצב המקורי של גיבוי המידע, כלומר אין איבוד מידע גם כאשר מחשב הלקוח בעצמו נכבה בבורטליות. | מהות היכולת |
| **אצל הלקוח**   * ביצוע hookים שונים על פעולות מבלי לפגוע במהות הפעולות * שמירת המידע בצורת טקסט שניתן לקרוא ולהבין בצורה מונגשת * יצירת סדר במידע, כל פעולה שונה במחשב המשתמש עליה להיות מסודרת לפי סוג הפעולה. * התממשקות עם קבצים – פתיחה, כתיבה, קריאה, סגירה (ותוך כדי להישאר במצב Kernel). | אוסף פעולות/יכולות הנדרשות ליכולת הנ"ל |
| * KLM – Kernel Loadable Module, כלומר תהליך בהרשאות הגבוהות ביותר במחשב – קרנל * מחשב לקוח * קבצים לאחסון המידע באופן זמני | אובייקטים נחוצים |

|  |  |
| --- | --- |
| שליחת מידע של מחשב המשתמש אל מחשב השרת | שם היכולת |
| שליחת מידע של מחשב המשתמש אל מחשב השרת מאפשרת לשרת/מנהל לקבל את המידע על עובדיו ובכך מקשר את מחשבי העובדים למחשב השרת. המידע שנאסף על המחשבים נשלח בזמן אמת אל השרת ובכך התוכנית יכולה לבצע יכולות רבות על המידע שמתקבל מן המשתמשים. | מהות היכולת |
| **אצל הלקוח**   * תוכנית שמאזינה לפעולות הלקוח. * שליחת המידע מן מחשב המשתמש לשרת.   **אצל השרת**   * איסוף המידע. * קבלת המידע אצל מחשב השרת ופענוח המידע. | אוסף פעולות/יכולות הנדרשות ליכולת הנ"ל |
| * מחשב לקוח * Socket * מחשב שרת * קבצים/באפרים לאחסון המידע באופן זמני | אובייקטים נחוצים |

|  |  |
| --- | --- |
| איסוף המידע במחשב השרת אל תוך DB | שם היכולת |
| איסוף המידע במחשב השרת אל תוך DB מאפשר למחשב השרת לשמור את המידע הנשלח מן הלקוחות בזמן אמת ולהפריד אותו לכל לקוח בנפרד. כלומר כל מחשב של עובד בחברה יהיה שמור בתוך ה DB של כלל העובדים, כך שיהיה ניתן להפריד בין העובדים השונים במערכת. | מהות היכולת |
| **אצל השרת**   * איסוף המידע מן הלקוח. * פענוח המידע לפי הפרוטוקול * הכנסה ל DB את הערכים של הלקוח ממנו נשלחה ההודעה. | אוסף פעולות/יכולות הנדרשות ליכולת הנ"ל |
| * מחשב לקוח * Socket * מחשב שרת * טבלת DB אצל השרת | אובייקטים נחוצים |

|  |  |
| --- | --- |
| הצגת המידע באופן נגיש במחשב המנהל | שם היכולת |
| הצגת המידע באופן נגיש במחשב המנהל מאפשרת למנהל של העובדים באופן יעיל להסתכל על המידע של מחשבי העובדים ובכך לקבוע את יעילות עבודתם ואם הם עובדים כראוי או שאינם מבצעים את עבודתם כלל, ולכן חשוב להציג את המידע באופן מסודר כך שהמנהל יוכל להסתכל בנוחות ובזריזות על המידע. | מהות היכולת |
| **אצל המנהל**   * איסוף המידע מן השרת. * פענוח המידע לפי ההצפנה המוסכמת על ידי השרת והמנהל. * פענוח המידע לפי הפרוטוקול. * הצגה באופן ויזואלי על ידי GUI את נתוני ה DB בזמן אמת. | אוסף פעולות/יכולות הנדרשות ליכולת הנ"ל |
| * מחשב לקוח * Socket * מחשב שרת * מחשב מנהל * טבלת DB אצל השרת * GUI במחשב המנהל * מפתחות הצפנה | אובייקטים נחוצים |

|  |  |
| --- | --- |
| הגדרת רמת בטיחות אצל המנהל | שם היכולת |
| כאשר המנהל מתחבר לשרת לאחר ביצע תהליך Login עליו להגדיר את רמת הבטיחות שהינו רוצה בעת הפעלת המערכת אצלו, הכוונה היא שביכולתו להגביל את כמות הלקוחות שמחוברים בו זמנית לשרת ואף לתת לשרת רמת בטיחות שהשרת יפעל על ידו – רמת בטיחות תהיה כמות ההודעות שהשרת מסכים שאינן עובדות לפי הפרוטוקול שאיתו השרת מתקשר לפני שהשרת מנתק את לקוח זה. | מהות היכולת |
| **אצל המנהל**   * הצגת המידע באופן ויזואלי – GUI * התחברות ותקשורת עם השרת * הצפנת הודעות מקצה לקצה עם השרת   **אצל השרת**   * הצפנה הודעות מקצה לקצה עם המנהל * הגבלת כמות לקוחות * הגבלת כמות הודעות "בלתי חוקיות" לפי רמת בטיחות | אוסף פעולות/יכולות הנדרשות ליכולת הנ"ל |
| * Socket * מחשב שרת * מחשב מנהל * GUI במחשב המנהל * מפתחות הצפנה * אובייקטים של לקוחות בכדי שהשרת יוכל לספור לכל לקוח כמה הודעות "בלתי חוקיות" נשלחו ממנו | אובייקטים נחוצים |

# **בדיקות, לו"ז וסיכונים**

## **פירוט בדיקות שמתוכננות לפרויקט**

בפרויקט הזה אבצע מספר בדיקות כדי לוודא שהמערכת מתפקדת כפי שתוכננה. הבדיקות יתמקדו בהעברת נתונים וביכולת המעקב אחר פעולות המשתמש, תוך שמירה על יציבות המערכת. ביצוע הבדיקות הינו שלב הכרחי בפיתוח הפרויקט שבלעדיו לא ניתן להכריע אם הפרויקט עובד כראוי

**1.בדיקת העברת נתונים לשרת המרכזי**

|  |  |
| --- | --- |
| מטרה | לבדוק שהנתונים מהמחשב של העובד מועברים לשרת של המנהל באופן אמין |
| איך אבדוק | אגדיר שרת מדומה ואעקוב אחרי זרימת הנתונים ממחשבי העובדים. אשתמש בכלים לבדיקת חבילות רשת כדי לוודא שהמידע מגיע בשלמותו ובתזמון הנכון. |

**2. בדיקת עקביות הנתונים**

|  |  |
| --- | --- |
| מטרה | לוודא שהנתונים הנאספים ממחשבי העובדים משקפים את הפעולות שבוצעו במדויק. |
| איך אבדוק | אבצע פעולות מוגדרות מראש במחשב העובד, כמו פתיחת תוכנות ועבודה על מסמכים, ואשווה את הנתונים שנשלחו לשרת לאירועים בפועל. כך אוכל לראות שהמערכת עוקבת בצורה מדויקת אחר הפעולות. |

**3.בדיקת השפעה על ביצועי המערכת**

|  |  |
| --- | --- |
| מטרה | לבדוק שהמערכת לא פוגעת בביצועים של מחשבי העובדים |
| איך אבדוק | אבצע מדידת ביצועים (CPU, זיכרון) לפני התקנת המערכת ואחריה, ואשווה את התוצאות. כך אוכל לוודא שהמערכת לא מכבידה על המשאבים של המחשב ומאפשרת עבודה חלקה. |

**4. בדיקת אבטחת הנתונים**

|  |  |
| --- | --- |
| מטרה | לוודא שהתקשורת בין המנהל לשרת מוגנת. |
| איך אבדוק | אשתמש בהצפנה להעברת המידע ואבחן פרוטוקולי תקשורת מאובטחים (AES DH) על מנת לוודא שהנתונים נשארים חסויים. ומוגנים בפני האזנות של מחשבים ברשת. |

**5. בדיקת הגבלת מספר לקוחות ורמת בטיחות**

|  |  |
| --- | --- |
| מטרה | לוודא שביכולתו של המנהל להגביל כרצונו את כמות הלקוחות ולקבוע להם רמת בטיחות. |
| איך אבדוק | אחבר מנהל אל השרת ואתן מספר מאוד נמוך של לקוחות, אבדוק שכאשר מעל המספר המוגדר שהמנהל שלח של לקוחות מנסים להתחבר השרת לא יתן להם להתחבר. בנוסף אצור לקוח פיקטיבי שישלח מידע לא לפי הפרוטוקול ואבדוק אם השרת מנתק את החיבור עם לקוח |

**6. בדיקת גיבוי המידע אצל הלקוח**

|  |  |
| --- | --- |
| מטרה | לוודא שהלקוח מגבה מידע באופן אמין וביכולתו לגבה מידע בזמן אמת באופן מוגבל על ידי המנהל. |
| איך אבדוק | בזמן פעילות הלקוח אכבה את השרת ואמחוק את הנתונים שהיו שומרים עד כה אצל השרת. כאשר אדליק מחדש את השרת אבדוק אם יתקבלו נתונים שתואמים את פעילות הלקוח בזמן שהשרת היה כבוי. |

**7. בדיקת החבאתו של תוכנת הלקוח**

|  |  |
| --- | --- |
| מטרה | לוודא שהתוכנה המופעלת אצל הלקוח הינה מוסתרת מן הלקוח ואין ביכולתו לשבש את פעילותה |
| איך אבדוק | אפעיל את התוכנה אצל הלקוח ואבדוק על ידי תוכנות ופקודות שונות אם התוכנה נראית ללקוח – Wireshark, netstat, lsmod. החבאה מתוכנות ופקודות אלו ימנע מן הלקוח לשבש את פעילות התוכנה (לדוגמה - ללמוד איך התוכנית עובדת לפי הפקטות היוצאות ולחכות את התנהגות התוכנה ובכך לשבש את התוכנית). |

## **תכנון וניהול לוז**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **מספר** | **פעילות** | **תאריך יעד** | **תאריך בפועל** | **הערות** |
| **1** | הצעת רעיון פרויקט גמר | 17.10.2024 | 14.10.2024 | הצעת הפרויקט הינה פרויקט זה, לא התבצעו שינויים ברעיון הפרויקט המקורי |
| **2** | הצעה לפרויקט גמר | 30.10.2024 | 24.10.2024 | תכנון ראשוני של הפרויקט, הכלים והדרך ביצוע |
| **3** | מסמך אפיון – הגשת ביניים ראשונה | 10.11.2024 | 6.11.2024 | הגשה חלקית של אפיון הפרויקט |
| **4** | מסמך אפיון – הגשת ביניים שנייה | 20.11.2024 | 14.11.2024 | הגשה חלקית של אפיון הפרויקט |
| **5** | מסמך אפיון – הגשה סופית | 30.11.2024 | 22.11.2024 | הגשה סופית של אפיון הפרויקט המלא |
| **6** | הוכחת יכולת | 15.01.2025 | 12.01.2025 | ביצוע מעקב אחר פעולות מרכזיות ושליחה לשרת |
| **7** | ממשק גרפי | 31.01.2025 | 30.01.2025 | ממשק גרפי מלא אצל המנהל |
| **8** | פעילות מלאה של המנהל | 01.03.2025 | 27.02.2025 | המנהל יכול לעקוב אחרי העובדים ולנתר את עבודתם |
| **9** | פעילות מלאה של הלקוח | 20.03.2025 | 22.03.2025 | פיתוח מלא של קוד הלקוח כולל כל הפיצ'רים |
| **10** | סיום כתיבת הפרויקט | 31.03.2025 | 28.3.2025 | פיתוח מלא של הפרויקט ללא באגים |
| **11** | סיום בדיקות הפרויקט | 17.04.2025 | 9.04.2025 | בדיקות מלאות של הפרויקט כמו שצוין באפיון |
| **12** | תיק פרויקט | 30.04.2025 | דרוש לשנות |  |
| **13** | הגשת פרויקט גמר | --NULL-- | דרוש לשנות |  |

## **סיכונים**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **הסיכון** | **תיאור הסיכון** | **רמת סיכון** | **תיאור דרכי התמודדות** | **מה בוצע בפועל** |
| אי עמידה בלוח הזמנים | הגשה מאוחרת וחוסר עקביות בלוח זמנים המתוכנן. אי עמידה בלוח הזמנים משפיע על כל תהליך הפרויקט | קל | לדאוג לעקוב אחר הלוח זמנים. | דאגתי לעקוב אחר הלוח זמנים. |
| המידע שמועבר אינו מוצפן | המידע שמועבר מן המנהל לשרת אינו מוצפן ולכן אנשים שאינם חלק מהמערכת יכולים לפענח את ההודעות ולהשתמש בהם לטובתם | קשה | להשתמש בהצפנות שונות, הצפנה אסימפטרית להעברת המפתחות בשביל הצפנה סימטרית בשביל העברת ההודעות | השתמשתי בהצפנות בין המנהל לשרת. הסכמה על המפתחות מתבצעת בתחילת התקשורת בין השניים. |
| ממשק משתמש לא יציב ולא נוח לשימוש | ממשק המשתמש GUI אינו נוח לשימוש מה שמקשה רבות על השימוש בפרויקט מצד השרת. | בינוני | שינוי ממשק המשתמש כך שגם מי שאינו מבין את תוכן הפרויקט יוכל להבין איך להשתמש בממשק המשתמש, בדיקה כנגד אנשים חיצוניים | יצרתי ממשק משתמש שנוח לשימוש ואף נראה נוח לעין, אינו מסובך ויוצר הגיון בקרב משתמשים אפילו כשאינם מבינים בעולם המחשבים. |
| קריסת השרת | השרת נפל בשל סיבה לא ידועה כזו או אחרת | קשה | שימוש באמצעי זהירות בכדי למנוע את קריסתו של השרת (try/except), מזעור של קריסת השרת כך כאשר באמת יקרוס השרת כבר זו תהיינה בעיה חיצונית שהפרויקט לא אחראי עליה | קוד השרת ממזער את קריסתו על ידי כתיבתו כך שאם נתקל בבעיה כלשהי כזו או אחרת בזכות מנגנון try/except יתפוס את התקלה וידפיסה למסך. בנוסף הקוד הראשי של השרת מופרד מההתנהלות נגד כל לקוח בזכות threads, כלומר אם thread שמטפל בלקוח קורס, השרת ימשיך לפעול ולקבל לקוחות אחרים. |
| עומס יתר על השרת | השרת מוצף בלקוחות ומנהל מול מספר רב של לקוחות session מה שמכביד עליו ויקשה על מחשב השרת לתפקד כראוי | קשה | הגבלתם של מספר הלקוחות שיכולים להתחבר לשרת, מספר קבוע מקסימלי שיקבע מספר גג של לקוחות שיכולים בו זמנית לנהל session מול השרת | כאשר השרת מופעל, המפעיל את השרת יגדיר כמות דיפולטיבית של מקסימום לקוחות שיכולים להתחבר, לאחר מכן בעת התחברות המנהל יוכל אף הוא בעצמו להגביל את כמות הלקוחות (ההגבלה גם היא בטווח, בין 1-40 לקוחות). |
| DB של הלקוחות גדול מדי | ה DB שהשרת שומר בזמן אמת על לקוחותיו יגדל בצורה כה משמעותית מה שיכביד על השרת וביצועיו | קשה | מחיקת מידע אצל כל משתנה כאשר כמות המידע השמורה אצלו בטבלה עברה מכסה מסוימת שנקבעה מראש | במקום לשמור כל הודעה המתקבלת על ידי הלקוח כתבתי את הקוד כך שימספר כל הודעה, מה שמצד אחד חוסך כמויות גדולות של אחסון, ומצד שני חוסך גם כוח מחשוב כאשר מנסים לשלוף מידע מן DB. |
| הלקוח משנה את המערכת אצלו במחשב | הלקוח הצליח לשנות את המערכת ששולחת מידע מהמחשב אל השרת, מה שיפגע בתפקוד הפרויקט | קשה | הסתרת התוכנית כך שתעבוד מאחורי הקלעים, עבודה עם ה kernel בכדי להחביא את התוכנית. בנוסף תדאג להסתרת כל ביצועיה, שליחת המידע למחשב חיצוני גם כן הוא יוסתר על ידי התהליך. | הסתרתי את התוכנית בפני המשתמש, אין ביכולת המשתמש לבצע פעולות כנגד התוכנית משום שאין לו שום מידע עליה (הלקוח לא יכול לדעת על איזה פורט השרת מתקשר וסוג ההודעות הנשלחות אל השרת). |
| תקשורת לא אמינה | הלקוח והשרת מתקשרים באופן לא אמין, לא כל המידע שהלקוח שולח מגיע בשלמותו אל השרת | קשה | שימוש בפרוטוקול אמין TCP על מנת להבטיח שהמידע שיועבר יגיע בצורה אמינה. | השתמשתי בפרוטוקול TCP, המידע מגיע באופן אמין כאשר אין שיבושים ברשת. |
| מכונה וירטואלית אינה מקבלת מספיק משאבים מהמערכת | המשאבים שניתנו למכונה הוירטואלית עליה רץ הפרויקט לא מספיקים, ולכן מתקשה המכונה לעבוד לפי צרכי הפרויקט | בינוני | נתינה של מספיק משאבים לכל מכונה וירטואלית (RAM, CPU,NETWORK,  STORAGE) | כאשר מריצים את התוכנה אני מקצה מספיק משאבים למכונה הוירטואלית (משתנה בין מחשב למחשב, לרוב המחשבים שנבדקו בשביל ריצה מלאה צריך 2 מעבדים ו2048MB RAM) |

# **תיאור ארכיטקטורה המערכת**

## **תיאור החומרה**

בפרויקט שלי ישנם רכיבים שונים שפועלים ביחד על מנת להביא את הפרויקט לעבוד בצורה מלאה ולאפשר למנהלים שונים לעקוב אחרי עבודת עובדיהם ועל אמינות עבודתם. ראשית נגדיר את מחשבי הלקוחות, אשר מהווים את אבני היסוד של הפרויקט. הלקוחות ישלחו את המידע אל מחשב השרת, כלומר אל מחשב המנהל.

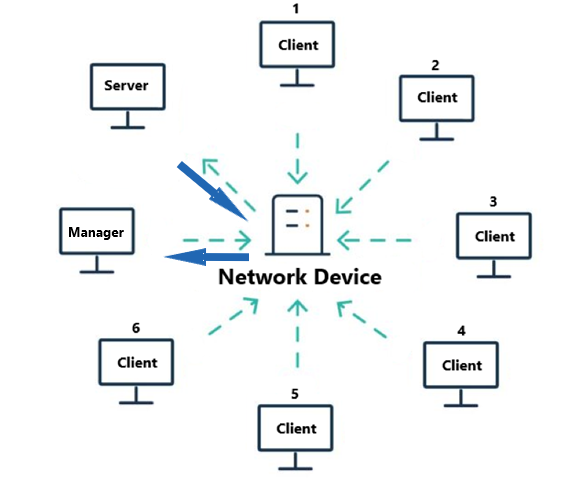
מחשב המנהל ימצא תחת אותה רשת עם מחשבי הלקוחות. המנהל יקבל את המידע מן הלקוחות דרך הרשת, המידע יועבר בצורה מוצפנת, הן בשימוש הצפנה אסימטרית להעברת המפתח והן בשימוש בהצפנה סימטרית בכדי להעביר מידע מוצפן עם המפתחות שהוחלפו בעזרת ההצפנה האסימטרית. מחשבי הלקוחות מתחברים לרשת באמצעות כרטיסי רשת המאפשרים להם לשלוח ולקבל נתונים בצורה מאובטחת.

חיבור הרשת בין הלקוח למנהל מתבצע דרך פרוטוקול TCP מאובטח, המבטיח שהנתונים יישלחו בצורה יציבה ומוגנת. מחשב השרת, שממוקם תחת אותה רשת, מקבל את המידע לפי הפרוטוקול המוסכם מהלקוחות ומעבד אותו בצורה מאובטחת. המחשב מצויד במערכת לניהול הצפנה המפענחת את המידע שהתקבל.

לאחר מכן, השרת בתקשורת עם המנהל ישלח לו בצורה מוצפנת את המידע כאשר המנהל מבקש. המנהל מציג את המידע בצורה גרפית בממשק משתמש נוח וברור, תוך שמירה על הצפנה ואבטחת המידע לאורך כל התהליך.

המנהל יכול לעקוב אחרי המידע בצורה ברורה ומסודרת. לצורך העברת המידע ברשת, ישנו גם תפקיד חשוב של רכיבי הרשת, כגון נתבים ומתגים, המוודאים שהמידע יגיע בצורה תקינה ממחשב הלקוח אל מחשב השרת והן ממחשב השרת אל מחשב המנהל ולהפך. הנתבים ומתגים אחראים על ניתוב המידע ומוודאים שהמידע יגיע ליעדו הנכון.

## **מראה גרפי של קשרי החומרה**



## **תיאור טכנולוגיות רלוונטיות**

### **שפות תכנות**

שפת תכנות C:

שפת C היא הבחירה המרכזית לפיתוח תוכנות ברמת ליבת מערכת ההפעלה. השפה מאפשרת גישה ישירה למשאבי המערכת ול-API של הליבה, מה שמעניק שליטה מלאה על תהליכים, זיכרון ורכיבי מערכת קריטיים. בעזרת C ניתן לבצע פעולות כמו עבודה עם מצביעים, ניהול זיכרון ישיר ותקשורת עם רכיבי חומרה או חלקים אחרים של המערכת.

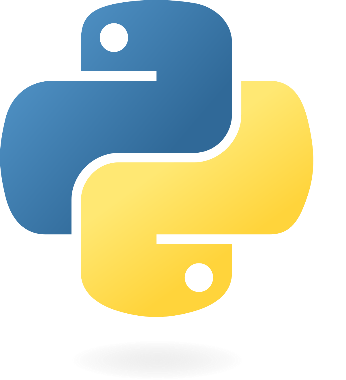
שפת תכנות Python:

Python יכולה לשמש ככלי עזר לפיתוח סביבת העבודה של הפרויקט. היא אידיאלית לאוטומציה של בדיקות, איסוף נתונים ויצירת ממשקים לתקשורת עם רכיבי המערכת. Python מצטיינת בפשטות שלה וביכולות המתקדמות שלה בטיפול ברשתות, ניתוח קבצים ולוגים, ובניהול מהיר של משימות מורכבות.

שפת תכנות SQL:

בנוסף לשפות התכנות, SQLהיא כלי מרכזי לניהול ואחסון נתונים בצורה מסודרת. היא מאפשרת ליצור מסדי נתונים, לשמור מידע, ולעבוד איתו בקלות דרך שאילתות מובנות. בעזרת SQL ניתן לארגן מידע בטבלאות עם מבנה ברור, להגדיר קשרים בין נתונים שונים, ולשלוף בדיוק את המידע הדרוש בצורה מהירה ויעילה. השפה מתאימה לניהול כמויות גדולות של נתונים ומשמשת בסיס לרוב מערכות אחסון הנתונים המודרניות.

השילוב של C, Python ו-SQL נותן לי גמישות עצומה בעבודה שלי. כל אחת מהשפות מביאה יתרונות ייחודיים, והעבודה ביניהן מאפשרת לי ליצור מערכת חזקה ומותאמת אישית. שפת C מאפשרת לי לעבוד ישירות עם המערכת, עם שליטה מלאה על הזיכרון, התהליכים והמשאבים של המחשב. אני יכול לכתוב קוד יעיל שמבצע את הפעולות הקריטיות באופן מהיר ומדויק. Python, לעומת זאת, נותנת לי דרך פשוטה ואינטואיטיבית ליצור סקריפטים שמנהלים תקשורת עם חלקי המערכת, מעבדים נתונים או מבצעים בדיקות. היכולת שלה לעבוד עם ספריות חזקות לרשתות ולעיבוד נתונים מקלה עליי לפתח חלקים מורכבים בצורה מהירה יותר. SQL

 משתלבת כדי לאפשר לי לשמור נתונים בצורה מסודרת ולשלוף אותם בקלות לפי הצורך. במקום להתעסק עם אחסון נתונים גולמיים, אני יכול להשתמש במבנה של מסדי נתונים כדי לשמור על סדר ולייעל את העבודה שלי. השילוב בין השפות האלה מאפשר לי לעבוד עם שכבת הליבה, ולאחסן את המידע בצורה מאורגנת ונגישה. כל שפה תורמת לתפקיד שונה, וביחד הן יוצרות מערכת מאוזנת תמונה שמכילה גרפיקה, עיגול, צילום מסך, לוגו

התיאור נוצר באופן אוטומטיויעילה.

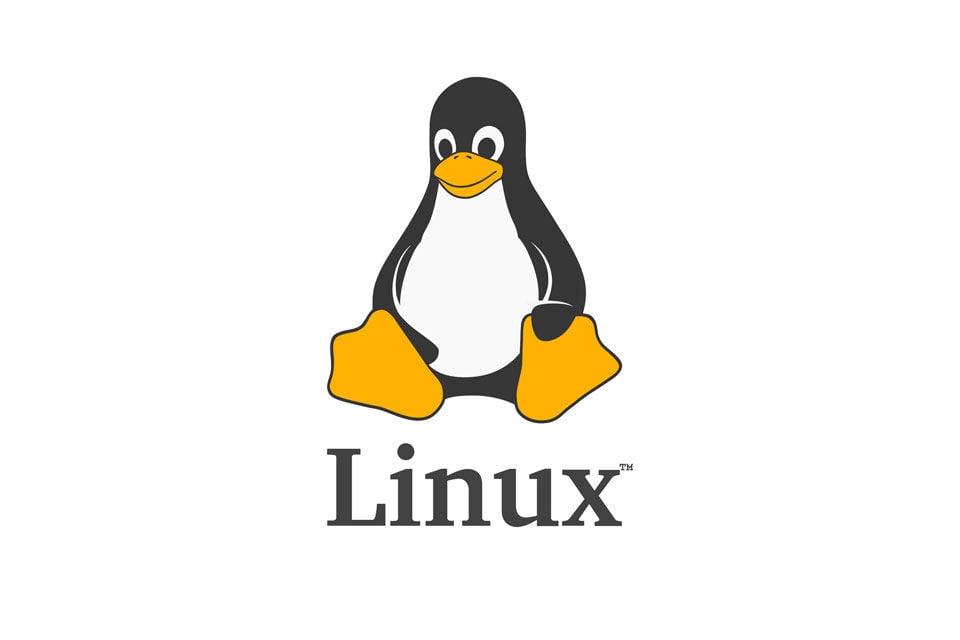
### **מערכת הפעלה**

לינוקס (Linux) היא מערכת הפעלה מבוססת קוד פתוח, כלומר, הקוד שלה זמין לציבור וניתן לשנות אותו, להפיץ אותו ולהשתמש בו ללא מגבלות מסחריות. זו אחת הסיבות לכך שלינוקס נפוצה מאוד בקרב מפתחים, חוקרי אבטחת מידע וסטודנטים שמחפשים ללמוד ולהתנסות במערכת הפעלה ברמה עמוקה.

לינוקס בנויה במודל מודולרי, כך שהרכיבים שלה מחולקים לגרעין ספריות, ותוכנות מערכת. הגרעין אחראי על אינטראקציה עם החומרה, ניהול תהליכים, זיכרון ומערכות קבצים. העובדה שהקוד של הגרעין זמין מאפשרת למפתחים לחקור אותו, להבין את אופן הפעולה של המערכת, ואפילו לכתוב תוספות או שינויים כמו דרייברים.

מכיוון שלינוקס ניתנת להתאמה אישית מלאה, קל יחסית ליצור פרויקטים כמו הפרויקט שלי. ניתן לשנות את קוד הגרעין כדי להוסיף פונקציונליות או להתקין מודול קרנל KLM שמבצע פעולות מתקדמות, כמו גישה לזיכרון, ניהול תהליכים, או עקיפה של בקרות גישה. בנוסף, קהילת המפתחים של לינוקס גדולה, ויש תיעוד רב שיכול לסייע בלמידה ובהתמודדות עם אתגרים טכניים.הגמישות והנגישות של לינוקס הופכות אותה לפלטפורמה אידיאלית לפרויקטים חינוכיים ומחקריים, במיוחד בתחום אבטחת המידע והסייבר.

מכונה וירטואלית היא סביבה שמדמה מחשב עצמאי בתוך מחשב פיזי. בעזרתה ניתן להריץ מערכת הפעלה (כמו לינוקס) בתוך מערכת הפעלה אחרת, כך שיש בידנו סביבה מבודדת לחלוטין, שמנצל את המשאבים של המחשב הפיזי כמו מעבד, זיכרון ואחסון, ומחלק אותם בין מכונות וירטואליות שונות. בפרויקטים שמצריכים עבודה על פיתוח ברמה נמוכה, כמו שינוי גרעין המערכת או עבודה עם מודולים קרנל, מכונה וירטואלית חשובה מאוד. היא מאפשרת ניסוי עם הקוד בסביבה מבודדת, כך שאין חשש לשבש את מערכת ההפעלה הראשית או את המחשב הפיזי. זה גם מאפשר ביצוע בדיקות וחקירות, תוך שמירה על הסביבה האמיתית מפני נזקים אפשריים.

**תקשורת**

התקשורת בפרויקט זה היא חלק מרכזי ומהותי בהצלחתו. המטרה היא לאפשר העברת מידע בין המערכת שבה רץ הקוד לבין מחשב אחר בצורה יעילה, אמינה ובטוחה. התקשורת מהווה את הגשר בין המידע שנאסף לבין היכולת לנתח ולהשתמש בו, ולכן תכנון נכון של מנגנון זה הוא חיוני. בפרויקט מתוכנן שימוש בפרוטוקול TCP (Transmission Control Protocol) לצורך התקשורת.

TCP נבחר בשל היתרונות המשמעותיים שלו באמינות ובניהול מסרים. זהו פרוטוקול שמבטיח שכל המידע הנשלח מגיע ליעדו בדיוק כפי שנשלח, ובסדר הנכון. אמינות זו קריטית במיוחד במערכת שמטרתה להעביר נתונים מדויקים. TCP פועל באמצעות יצירת חיבור מבוקר בין שני מחשבים, תהליך המתחיל ב"לחיצת יד משולשת" (Three-Way Handshake) שמבטיחה ששני הצדדים מוכנים לתקשורת. תהליך זה מאפשר גם התמודדות עם בעיות כמו אובדן נתונים או הפרעות בתקשורת, כיוון שהפרוטוקול כולל מנגנוני תיקון וידוא.

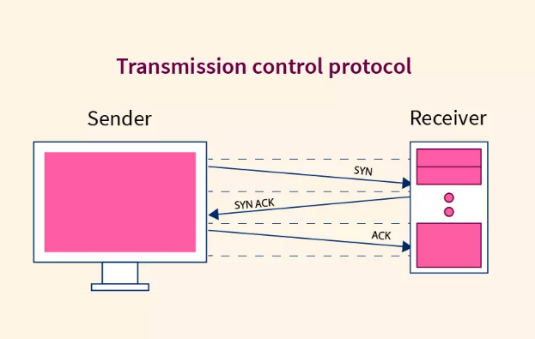
מרכיב חשוב נוסף בתקשורת בפרויקט הוא שימוש בנתונים מוצפנים. הצפנה היא כלי מרכזי להבטחת אבטחת המידע שנשלח, ובמיוחד כאשר מדובר בתקשורת שעשויה לכלול מידע רגיש או קריטי. ההצפנה מגנה על הנתונים מפני גישה לא מורשית, כך שגם אם צד שלישי מצליח ליירט את התקשורת, הוא לא יוכל לפענח את המידע שנשלח.

בעת תכנון הפרויקט, יינתן דגש לשילוב מנגנוני הצפנה חזקים, כמו שימוש באלגוריתמים סטנדרטיים כגון AES ו DH, כדי להבטיח רמת אבטחה גבוהה. הנתונים המוצפנים יישלחו במסגרת חיבור ה-TCP, כך שנוכל ליהנות גם מאמינות הפרוטוקול וגם מהגנה על המידע.

שילוב הצפנה בתקשורת מבטיח שהמערכת לא רק פועלת ביעילות אלא גם משמרת את אבטחת המידע. האיזון בין אמינות, יעילות ובטיחות הוא קריטי להצלחת הפרויקט, והתכנון המוקפד של התקשורת נועד להשיג מטרה זו בצורה מיטבית.

הפרויקט מתוכנן לפעול בתוך רשת מקומית. רשת מקומית היא מערכת תקשורת המחברת מספר מחשבים ומכשירים אחרים בתוך שטח גיאוגרפי מוגבל, כמו בית, משרד או מוסד חינוכי. ה-LAN מתאפיינת במהירות תקשורת גבוהה יחסית וביכולת לשלוט ברשת באופן ישיר, מה שהופך אותה לפתרון אידיאלי לפרויקט זה.

הבחירה לפעול בתוך רשת LAN נובעת ממספר סיבות: ראשית, העבודה ברשת מקומית מפחיתה את התלות באינטרנט החיצוני, מה שמאפשר גישה מהירה ואמינה יותר בין המחשבים ברשת. שנית, LAN מספקת רמה מסוימת של פרטיות, שכן התקשורת נשארת בתוך הרשת הפנימית ואינה נחשפת לרשתות חיצוניות שעלולות להיות פגיעות יותר להתקפות. בפרויקט זה, התקשורת תתבצע רק בין מחשבים הנמצאים באותה רשת מקומית, מה שמבטיח יעילות וביצועים מיטביים. הגבלה זו גם מפשטת את תהליך ההגדרה והניהול של התקשורת, כיוון שאין צורך להתמודד עם מורכבויות כמו ניתוב דרך כתובות IP חיצוניות או פתיחת פורטים בנתב. חשוב לציין כי בעוד שה-LAN מספקת יתרונות רבים מבחינת מהירות ואמינות, היא גם מציבה מגבלות – הפרויקט לא יוכל לתקשר עם מחשבים מחוץ לרשת המקומית. עם זאת, מגבלה זו היא חלק מהתכנון ומטרתה להבטיח פשטות, אבטחה ושליטה טובה יותר על המערכת.



### **תחומי עניין**

הפרויקט עוסק במגוון תחומי עניין טכנולוגיים המשלבים ידע תאורטי עם יישום מעשי. להלן תחומי העניין המרכזיים בפרויקט:

רשתות מחשבים ותקשורת נתונים

תכנון מנגנוני התקשורת בפרויקט נעשה תוך שימוש בפרוטוקול TCP, שמספק אמינות וניהול מסרים יעיל. נושא זה כולל הבנה מעמיקה של ניהול חיבורים, טיפול בהפרעות ושמירה על תקשורת תקינה בין רכיבי המערכת.

אבטחת מידע והצפנה

אחד ההיבטים המרכזיים בפרויקט הוא הגנה על הנתונים המועברים בזמן אמת באמצעות הצפנה. שילוב אלגוריתמים חזקים כמו AES ו DH מבטיח הגנה מפני גישה לא מורשית ושמירה על פרטיות המידע, גם אם הוא מיירט על ידי צד שלישי.

מערכות הפעלה וניהול משאבים

פיתוח מודול ליבה בלינוקס מחייב ידע מתקדם במבנה מערכת ההפעלה וניהול משאבים. התחום עוסק בשימוש יעיל במנגנונים כמו קריאות מערכת, ניהול זיכרון ותיאום בין תהליכים בזמן אמת.

תכנות ושפות מחשב

הפרויקט עושה שימוש בשפות כמו C, המאפשרות גישה ישירה למשאבים ושיפור ביצועים. תחום זה כולל כתיבת קוד ברמת ליבה תוך תשומת לב לאופטימיזציה ופתרון בעיות בזמן ריצה.

תכנון מערכות מורכבות

הפרויקט משלב בין מספר תחומי טכנולוגיה, מה שמחייב תכנון מקיף וחשיבה אסטרטגית. המערכת מתוכננת כך שתהיה יעילה, מאובטחת וקלה לתפעול, תוך שילוב פתרונות יצירתיים לאתגרים הנדסיים. תצוגת נתונים בזמן אמת

אחד ההיבטים החשובים בפרויקט הוא הצגת הנתונים הנאספים באופן גרפי ברור ואינטואיטיבי בזמן אמת, מבלי לשמור את המידע לאחר הריצה. המידע מוצג בממשק משתמש ידידותי, שמאפשר ניטור והבנה מיידיים של פעולת המערכת. תחום זה כולל שימוש בטכנולוגיות גרפיות ותכנון חוויית משתמש, תוך התחשבות על גמישות והתאמה למשתמשים.

תחומי העניין הללו מאפשרים ליצור פרויקט עשיר ומאתגר, שמחבר בין ידע טכנולוגי מתקדם לבין יישומים מעשיים בתחום מערכות ההפעלה, אבטחת המידע והנדסת התוכנה.

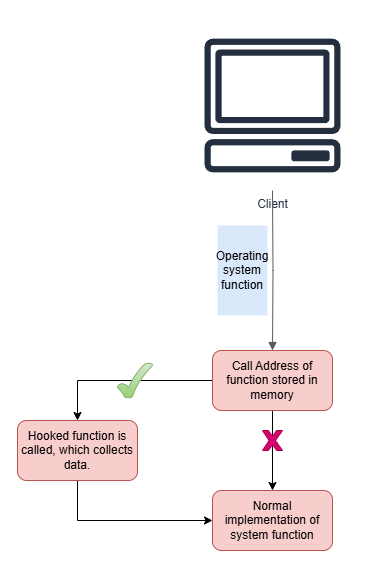
## **תיאור זרימת המידע במערכת**

### **האזנה שקטה על מחשב המשתמש**

תיאור הגרף:

גרף זה מציג את היכולת "האזנה שקטה על מחשב המשתמש". יכולת זו יכולה אך ורק לבוא לידי ביטוי על ידי שיתוף פעולה עם מערכת ההפעלה. ההאזנה השקטה מתבצעת באפשרות החבאת מידע מן המשתמש, שדבר זה אפשרי אך ורק בעזרת קוד מערכת הפעלה. דרך נגישה לעשות זאת מבלי לשנות את קוד מערכת ההפעלה עצמה (פעולה אפשרית, אך דורשת מכל מחשב שרוצה להריץ את פרויקט זה לשנות קוד במערכת ההפעלה שלו. כלומר פעולה ארוכה ולא יעילה, וגם מסוכנת אשר מדובר פה במערכת הפעלה, שהיא התוכנית הכי רגישה על המחשב, וכל שינוי מיותר בה יכול לגרור לסיכונים לכלל התנהלות המערכת) הינה על ידי השתמשות ב Kernel loadable module במערכת הפעלה לינוקס. לינוקס כמערכת הפעלה מאפשרת להוסיף אליה קוד אף תוך כדי זמן ריצה (מפה מגיעים המילים loadable module), הוספת אותו קוד הינו כלי חזק אשר התוכנית רצה בזיכרון של מערכת ההפעלה ובעלת גישה לנתונים רבים שאינם נגישים מהמשתמש. כפי שאפשר לראות בגרף, אפליקציות המשתמש יכולות רק לתקשר עם הקרנל, אך לא בעלות שינוי שלו. הוספת מודול משלנו למערכת הפעלה מאפשר לנו לשנות את הדרך ואת המידע שאליו אפליקציות המשתמש חשופות אליו.

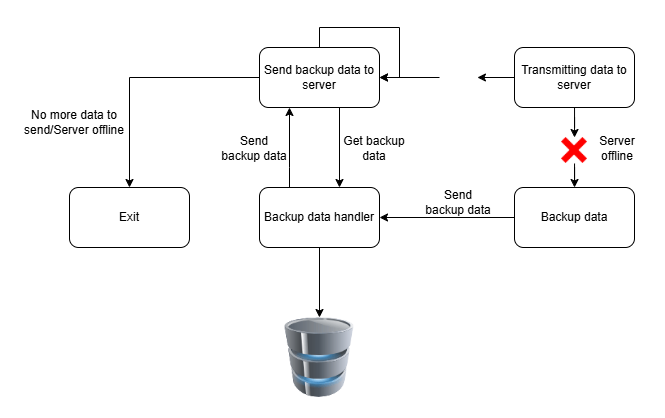
### **איסוף מידע בזמן אמת מן מחשב המשתמש**



תיאור הגרף:

גרף זה מציג את היכולת "איסוף מידע" במחשבי המשתמשים. איסוף המידע מתבצע באמצעות מונח הנקרא Hooking, מונח זה הינו תהליך שבו אנו יוצרים ניתוב מחדש של תהליך זרימת הקוד ולמעשה מנתבים אותו דרך פונקציות שלנו שבעזרתן נוכל להחליט לבצע האזנה בסתר על המידע המועבר במערכת הפעלה כחלק מקריאת הפונקציות. כמו שניתן לראות גם לאחר שינוי הפעולה בכדי שנוכל להאזין, הפעולה המרכזית עדיין נקראת, כלומר לא התבצעה פגיעה בפעולת מערכת, אלא רק האזנה מאחורי הקלעים.

### **גיבוי נתונים אצל המשתמש בעת שרת כבוי**

Check Mark Icon Green PNG Transparent Background, Free Download #45000 -  FreeIconsPNG

תיאור הגרף:

גרף זה מציג את היכולת "גיבוי נתונים" במחשבי המשתמשים. כאשר הלקוח מנסה לשלוח הודעה אל השרת והשרת איננו זמין (או כלשהי בעיה אחרת בשליחת ההודעה), הלקוח יגבה את המידע אצלו במחשב על ידי שימוש בממשק שיודע להתנהל כנגד מאגר הנתונים. כאשר הלקוח כן מצליח לתקשר עם השרת הוא יוודא כי אין מידע ששמור במאגר גיבוי המידע, ולכן ינסה לרוקנו כל פעם שיש חיבור מוצלח עם השרת.

### **שליחת מידע המשתמש אל המנהל**

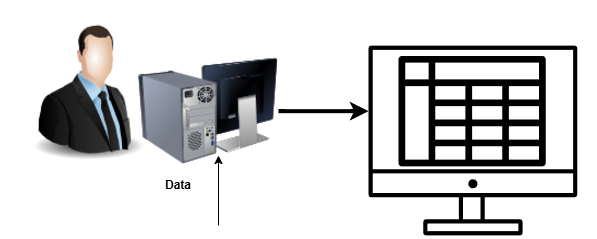
תמונה שמכילה צילום מסך, תרשים, עיצוב

תוכן שנוצר על-ידי בינה מלאכותית עשוי להיות שגוי.

תיאור הגרף:

גרף זה מציג את היכולת "שליחת מידע מהמשתמשים אל המנהל". השליחה מתבצעת על ידי איסוף המידע מהמחשבים של העובדים והעברתו דרך רכיבי אינטרנט. כל עובד מחובר דרך הרשת לרכיב אינטרנט, אשר מרכז את המידע מכל תחנות העבודה. לאחר מכן, המידע נשלח ישירות למחשב של השרת, שם הנתונים נאספים ועוברים עיבוד לצורך ניתוח או הפקת דוחות, לאחר מכן נשלח למנהל. פעולה זו מאפשרת לארגון לרכז את המידע במקום אחד ולהבטיח שהמנהל מקבל גישה למידע חיוני בזמן אמת.

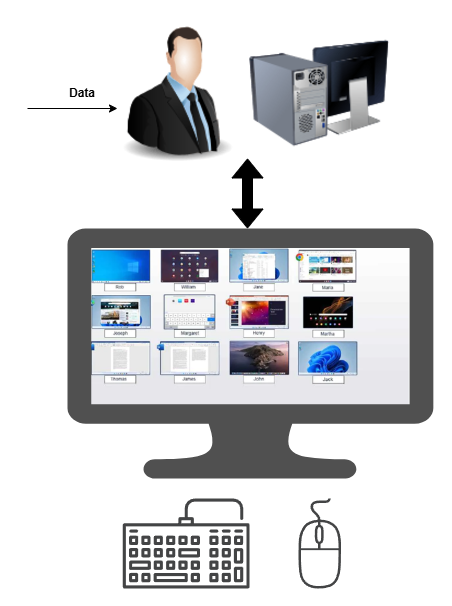
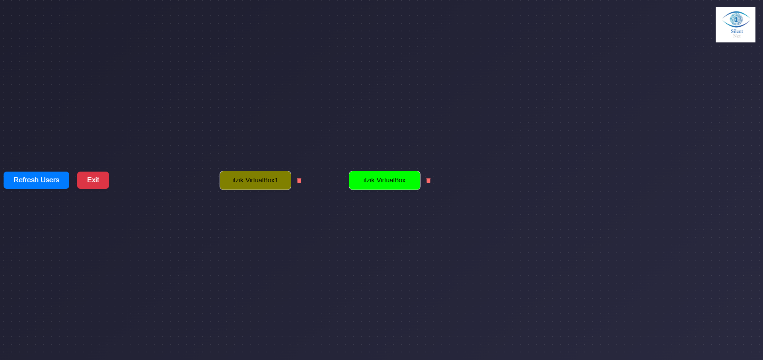
### **איסוף המידע במחשב השרת ל DB**



תיאור הגרף:

גרף זה מציג את היכולת "איסוף המידע במחשב השרת ל DB". איסוף המידע מתבצע על ידי שליחת נתונים מהמחשבים המקומיים של העובדים אל השרת, שם הוא שומר את המידע בצורה מסודרת בתוך DB, ה DB יפריד בין המידע שהוא מקבל מהמשתמשים, וכך יוכל המנהל להבחין בין סוגי המידע שנשלחים אליו. תהליך זה מתחיל באיסוף הנתונים, מהתוכנות או מהפעילות של המשתמשים במחשבים שלהם. הנתונים מועברים דרך רכיב אינטרנט באופן מאובטח, ולאחר מכן מגיעים לשרת המרכזי, שם הם עוברים עיבוד ראשוני ונשמרים בטבלאות מסודרות בבסיס הנתונים. תהליך זה מאפשר לארגון לנהל כמויות גדולות של מידע בצורה יעילה, להבטיח אחסון מאובטח של הנתונים, ולספק גישה מהירה לצורך ניתוח, קבלת החלטות או שיפור תהליכים עסקיים.

### **הצגת המידע באופן נגיש במחשב המנהל**



תיאור הגרף:

גרף זה מציג את היכולת "הצגת המידע באופן נגיש במחשב המנהל". תהליך זה מתאר את הדרך שבה הנתונים שנשמרו בשרת מוצגים בצורה נוחה וקלילה למשתמשים. המידע שנשמר בבסיס הנתונים במחשב השרת ונשלח אל המנהל אשר מציג בצורה מאורגנת על מסך, למשל כטבלה או גרף, כך שמנהלים יכולים לגשת אליו בקלות, להבין אותו בצורה מהירה ולבצע עיבודים נוספים אם נדרש. הנתונים המוצגים יכולים להיות תוצאות של חיפושים, דוחות או מידע אקטואלי הנוגע לפעילות המשתמש. הגישה למידע נעשית באמצעות מחשבים או מכשירים המחוברים לרשת, והמחשב המרכזי בשרת אחראי על שליחת המידע בצורה מסודרת, נגישה ובצורת המאפשרת למנהלים להבין את הנתונים במהירות וביעילות.

### Check Mark Icon Green PNG Transparent Background, Free Download #45000 - FreeIconsPNGCheck Mark Icon Green PNG Transparent Background, Free Download #45000 - FreeIconsPNGCheck Mark Icon Green PNG Transparent Background, Free Download #45000 - FreeIconsPNGCheck Mark Icon Green PNG Transparent Background, Free Download #45000 - FreeIconsPNG**הגדרת רמת בטיחות אצל המנהל**

תיאור הגרף:

גרף זה מציג את היכולת "הגדרת רמת בטיחות אצל המנהל". הגרף מתאר איך המנהל יכול להגדיר אצל השרת עד כמה לקוחות הוא מרשה ומכך השרת מגביל את כמות הלקוחות המחוברים אליו בו זמנית. בשל קושי ההמחשה בגרף, לא היה ניתן להמחיש את רמת הבטיחות שהמנהל יכול להגדיר, אך גם היא פרמטר שהמנהל מעביר לשרת בו הוא מחליט על כמות ההודעות הלא חוקיות שהשרת מרשה לכל לקוח ברצף. כפי שניתן לראות בגרף המנהל החליט כי כמות מקסימלית של לקוחות תהייה 4, ולכן רק ארבעה מחשבים הצליחו להתחבר אל השרת, בעוד השניים האחרים לא יכולים להתחבר לשרת ולא מקיימים session עימו.

### **ניסוח וניתוח של הבעיה האלגוריתמית**

הבעיה האלגוריתמית המרכזית בפרויקט שלי היא ניהול יעיל של אחסון הודעות, כך שלא תיגרם הצפה של המערכת במספר רב מדי של הודעות. הבעיה מתעוררת כאשר אין בקרה על כמות ההודעות, מה שעלול להוביל לשימוש מוגזם במשאבי מערכת כגון זיכרון או דיסק, ולגרום לקריסות או האטה משמעותית של התוכנה. דוגמה לכך היא כאשר הודעות נאגרות בקובץ במהירות גבוהה מהיכולת של המערכת לעבד ולמחוק אותן, וכתוצאה מכך גודל הקובץ תופס נפח רב ויוצר עומס.

### **אלגוריתמים קיימים לפתרון הבעיה**

הפתרון הנפוץ לבעיה זו הוא שימוש במבנה נתונים מעגלי (Circular Buffer), שבו האחסון מתנהל בצורה מעגלית: כאשר מגיעים לסוף המקום הפנוי, המצביע חוזר להתחלה ומתחיל לדרוס נתונים ישנים. כך, נשמרת שליטה על כמות הנתונים המאוחסנים, והמערכת לא מתמלאת ללא הגבלה.

קיימות גישות שונות לניהול Circular Buffer: למשל, שימוש בשני מצביעים (ראש ו-זנב), ניהול מונה הודעות, ובדיקת מצבי מלא/ריק. אפשר גם להגדיר מדיניות כמו דריסת הודעות ישנות אוטומטית או חסימת כתיבה כאשר אין מקום חדש עד שהתפנה מקום. לכל גישה יתרונות וחסרונות — דריסת נתונים ישנים מתאימה כאשר חשוב לשמור על זרימה רציפה, ואילו חסימה מתאימה כאשר לא רוצים לאבד מידע כלל.

### **סקירת הפיתרון הנבחר**

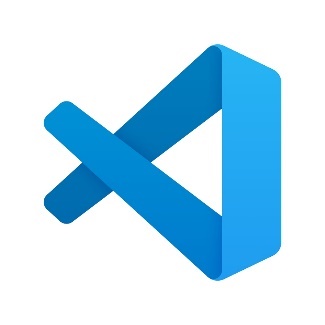
הפתרון שבחרתי — Circular Buffer בקובץ עם דריסה אוטומטית — מאפשר שמירה על ביצועים גבוהים ללא צורך בתחזוקה מורכבת. באמצעות ניהול פשוט של מצביעי קריאה וכתיבה, אני יכול לוודא שהקובץ לעולם לא יגדל מעבר לגבול מוגדר, וכך למנוע קריסה או האטת המערכת. בחרתי לא להשתמש בגישות אחרות כמו רשימות מקושרות או מבני תור מתוחכמים, כיוון שהן מוסיפות מורכבות מיותרת ואינן מתאימות לצורך הבסיסי של שליטה קלה וגמישה בגודל הנתונים. התממשקות עם קובץ שמתנהג כמקום אחסון מעגלי מביאה עימה את היכולת לאחסן בצורה יעילה ללא שימוש בפקודות שונות של מערכת ההפעלה הקשורות לקבצים. מימוש בצורה נכונה של אלגוריתם זה מייעל את הליכי הפרויקט ואף מבטיח על כמות מוגדרת מראש של מידע שלא תלך לאיבוד כאשר השרת לא פעיל אך הלקוח מבצע את עבודתו. מוטב לציין כי בפרויקט יש לשמור בתוך הקובץ עצמו את שני המצביעים של הקובץ, אשר יש להתחשב במקרה כאשר מחשב הלקוח קורס ויש מידע בתוך קובץ הגיבוי, לכן לאחר כל קריאה/כתיבה נעדכן את מצביעים אלו בסוף הקובץ.

### **הפנייה למקור רלוונטי**

[מהו באפר מעגלי](https://en.wikipedia.org/wiki/Circular_buffer)

## **תיאור סביבת הפיתוח**

תמונה שמכילה גרפיקה, עיצוב גרפי, לוגו, צילום מסך

התיאור נוצר באופן אוטומטיהסביבה בה אני עובד דורשת שימוש במכונה וירטואלית, משום שעלי להפעיל גרסה מסוימת של מערכת לינוקס, שהיא חשובה להרצת הקוד שלי. באמצעות מכונה וירטואלית, אני יכול ליצור סביבה מבודדת שמתפקדת בצורה עצמאית ומסייעת לי לבצע ניסויים ובדיקות בצורה בטוחה ומבוקרת. במכונה הווירטואלית אני מריץ גרסה מסוימת של לינוקס שיכולה להשתנות לפי הצורך, מבלי להשפיע על מערכת ההפעלה הראשית שלי. אני משתמש בכלים כמו VirtualBox או VMware כדי להקים ולהפעיל את הסביבה הווירטואלית הזו. לצורך פיתוח הקוד, אני משתמש בשני עורכי טקסט עיקריים: VIM ו-VSCode.VIM הוא עורך טקסט מאוד פופולרי ונוח למי שמכיר את הפקודות וזקוק לכלים בסיסיים, ומאפשר לי לכתוב קוד בצורה מהירה ויעילה, במיוחד בסביבת לינוקס. הוא קל, גמיש ומאפשר עבודה מהירה עם קבצים ללא צורך בממשק גרפי. מצד שני, אני משתמש גם ב-VSCode, שהוא עורך מודרני ומתקדם יותר, המציע אינטגרציה עם כלים נוספים כמו ניהול גרסאות, דיבאגינג, ותוספים רבים שמקליקים את העבודה עם קוד. בנוסף, אני משתמש ב-Git ו-GitHub לניהול גרסאות הקוד שלי. Git הוא כלי לניהול גרסאות שמאפשר לי לעקוב אחרי השינויים בקוד, לשמור על גרסאות קוד שונות ולשלוט בצורה יעילה בהתפתחויות הקוד לאורך הזמן. GitHub הוא שירות מבית Git שמאפשר לי לשתף את הקוד, לעבוד בצוות ולגבות את הקוד שלי. כלים אלו חשובים במיוחד כשיש צורך לעקוב אחרי שינויים רבים בקוד ולשתף את העבודה עם אחרים. כחלק מהתהליך, אני גם עושה שימוש ב-Wireshark כדי לנתח את התקשורת בין רכיבי המערכת. Wireshark הוא כלי מצוין לתפיסת וניתוח תעבורת רשת, אשר מאפשר לי לראות את זרימת המידע בין השרתים והלקוחות, ולוודא שאין בעיות בתקשורת או בשימוש בכתובת IP. זה חשוב במיוחד לבדיקת האינטראקציות וההעברות נתונים, כדי לוודא שהקוד עובד בצורה תקינה. לסיכום, אני עושה שימוש בסביבה מאוד עשירה שמספקת לי את כל הכלים הנדרשים לפיתוח, בדיקות, וניהול הקוד שלי. מכונה וירטואלית מספקת לי את הגמישות, עורכי הטקסט מאפשרים עבודה נוחה ומהירה, Git ו-GitHub חשובים לניהול הגרסאות, ו-Wireshark מאפשר ניתוח ופתרון בעיות בתקשורת. כלים אלו יחד יוצרים סביבה עוצמתית ומסודרת לפיתוח מתקדם.

## **תיאור פרוטוקול התקשורת**

החשיבות של פרוטוקול תקשורת בפרויקט שלי היא מכרעת, שכן הוא מבצע את התיאום וההבנה בין כל הרכיבים במערכת. פרוטוקול תקשורת מספק את הכללים וההנחות שדרכם רכיבי המערכת יכולים להבין אחד את השני ולהעביר מידע בצורה מסודרת וברורה. אם הפרוטוקול מוגדר בצורה טובה, הוא הופך את התקשורת לפשוטה יותר ומובנת לכל הצדדים המעורבים, ללא צורך בהבנה עמוקה של כל רכיב בנפרד. פרוטוקול טוב יכול להגדיר כיצד נשלחים ומתקבלים נתונים, אילו פורמטים נתמכים, איך להתמודד עם טעויות או חיבורים לא יציבים, ואיך ניתן לזהות את הנתונים בצורה אפקטיבית. הוא מספק מנגנונים של סנכרון ותקשורת בין תהליכים או רכיבים שונים במערכת, ומבצע את כל התיאומים הנדרשים כדי להבטיח שהנתונים יגיעו בשלמותם ובזמן. פרוטוקול ברור ומובנה מסייע במניעת טעויות בתקשורת, ומונע תקלות שעלולות להיגרם כאשר אין הבנה משותפת לגבי הציפיות בין הצדדים. יתר על כן, פרוטוקול תקשורת מגדיר את ההתנהגות של המערכת והופך את הפרויקט לנגיש יותר מבחינת פיתוח ותחזוקה.

מבנה הפרוטוקול תקשורת בו אשתמש בפרויקט הינו במבנה הבא:

1. אורך הודעה (כארבעה תווים שמהווים מספר)

2. סוג הפעולה שהתבצעה (המתודה שנקראה/איזה פעולה המשתמש ביצע)

3. המידע הקשור לאותה פעולה (פרמטרים)

התו המפריד להודעות יהיה הבית ‘\x1f’ (בזכות היותו בית שלא נמצא באף הודעה בין חלקי הפרויקט השונים, לכן לא יתערבב עם חלקי הודעה שונים). חשוב להתייחס לכך שאם התו המפריד יהיה חלק מהחלק השני של ההודעה, תיווצרנה בעיה בפרוטוקול, לכן נימנע מלשלוח הודעה שכוללת בחלק השני שלה את התו הנ"ל. לא תהיינה בעיה שהתו יופיע כחלק מהחלק השלישי של ההודעה, אשר ברגע שנמצא התו המפריד הראשון, שם נדע לבצע את ההפרדה בין חלקי ההודעה. כאשר יהיה שימוש בתו המפריד בחלק השלישי של ההודעה דבר זה יהיה בכדי לבצע הפרדה בין הפרמטרים של פקודה זו.

### **דוגמה להודעות:**

CIE\x1f480006 (שימוש באינפוט של חומרה)

CPO\x1fchrome.exe0014 (פתיחת תהליך).

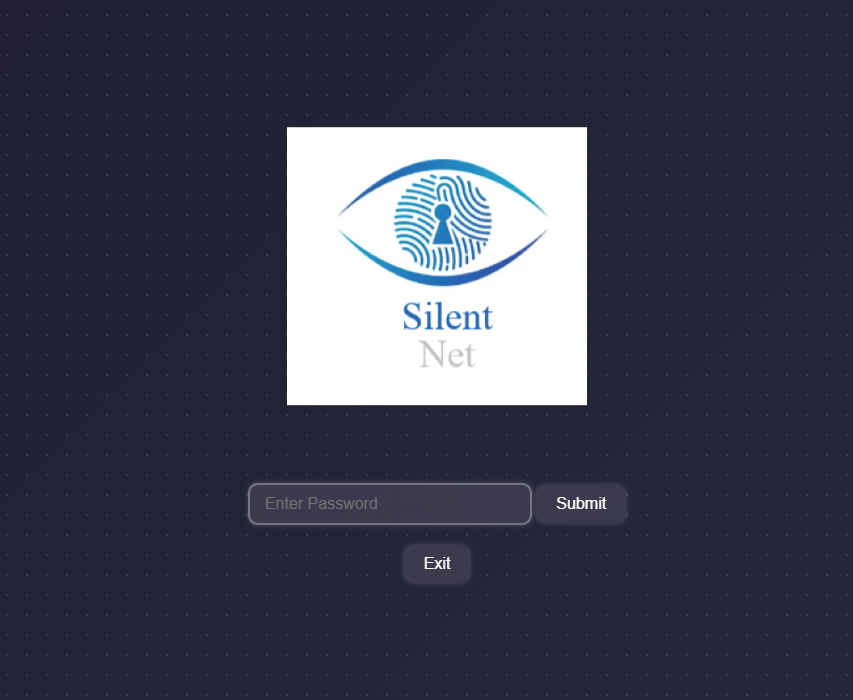
ועוד...

### **טבלת הודעות פרוטוקול**

|  |  |  |  |
| --- | --- | --- | --- |
| שם ההודעה | מבנה שדות ההודעה | נשלח מ-/אל- | תיאור |
| CAU | תעודת זהות כרטיס רשת (MAC) ולאחר מכן שם הוסט (hostname) | לקוח אל שרת | הודעה הנשלחת כל תחילת תקשורת בין לקוח לשרת |
| CPO | שם תהליך | לקוח אל שרת | שם תהליך שנפתח על ידי הלקוח |
| CCU | מספרי ליבה ואחוזי שימוש בה מופרדים עם תו ההפרדה בין כל ליבה. לאחר הליבה האחרונה יופיע גם השעה בה נמדדו נתונים אלו –  0,56\x1f1,98,datetime | לקוח אל שרת | אחוזי שימוש בכל ליבה במעבד של המחשב |
| COT | קטגוריה של סוג אפליקציה | לקוח אל שרת | אפליקציות אליהן הלקוח מתקשר ברשת |
| CIE | מספר | לקוח אל שרת | קלט מכל חומרה המתקבל במחשב הלקוח מתקבל כקוד, אותו קוד נשלח לשרת |
| MME | אין (חוץ מסוג ההודעה ואורכה) | מנהל אל שרת | המנהל מודיע אל השרת על סיום החיבור ביניהם |
| MST | כמות לקוחות מקסימלית ולאחר מכן רמת בטיחות | מנהל אל שרת | לאחר התחברות המנהל אל השרת הוא ישלח לו את ההגדרות הרצויות למנהל – כמות לקוחות מקסימלית המחוברים לשרת ורמת בטיחות של השרת כנגד כל לקוח |
| MGC | אין (חוץ מסוג ההודעה ואורכה) | מנהל אל שרת | המנהל מבקש מן השרת את הנתונים הכלליים על הלקוחות המחוברים |
| MGD | שם הלקוח | מנהל אל שרת | המנהל מבקש את שלל הנתונים על לקוח ספציפי |
| MDG | שם הלקוח | מנהל אל שרת | המנהל שולח לשרת שם של לקוח שהוא רוצה למחוק את הנתונים שלו מהשרת |
| MCC | אין (חוץ מסוג ההודעה ואורכה) | מנהל אל שרת | המנהל בודק אם השרת פתוח לתקשורת, אחרת המנהל לא יהיה שימוש במערכת של המנהל |
| MCN | השם הנוכחי של הלקוח והשם החדש של הלקוח | מנהל אל שרת | המנהל מבקש להחליף שם של לקוח |
| MIH | אין (חוץ מסוג ההודעה ואורכה) | שרת אל מנהל | השרת מעדכן את המנהל כי עדכון השם לא חוקי |
| MCH | אין (חוץ מסוג ההודעה ואורכה) | שרת אל מנהל | השרת מעדכן את המנהל כי עדכון השם הצליח |
| MMP | אין (חוץ מסוג ההודעה ואורכה) | מנהל אל שרת | המנהל מעדכן את השרת שהוא הולך לשלוח לו את הסיסמה |
| MIC | אין (חוץ מסוג ההודעה ואורכה) | שרת אל מנהל | השרת מעדכן את המנהל שהסיסמה ששלח לא נכונה |
| MVC | אין (חוץ מסוג ההודעה ואורכה) | שרת אל מנהל | השרת מעדכן את המנהל שהסיסמה ששלח תקפה והחיבור יוצא לפועל |
| MAC | אין (חוץ מסוג ההודעה ואורכה) | שרת אל מנהל | השרת מעדכן את המנהל כי קיים כבר מנהל מחובר לשרת ועל כך לא ייתן לעוד מנהל להתחבר |
| EXH | ערכי DH – יכול להיות גם g/p וגם המפתח הציבורי | שרת/מנהל אל מנהל/שרת | החלפת מפתחות שמתחרשת בתחילת התקשורת בין השרת למנהל |

## **תיאור מסכי המערכת**

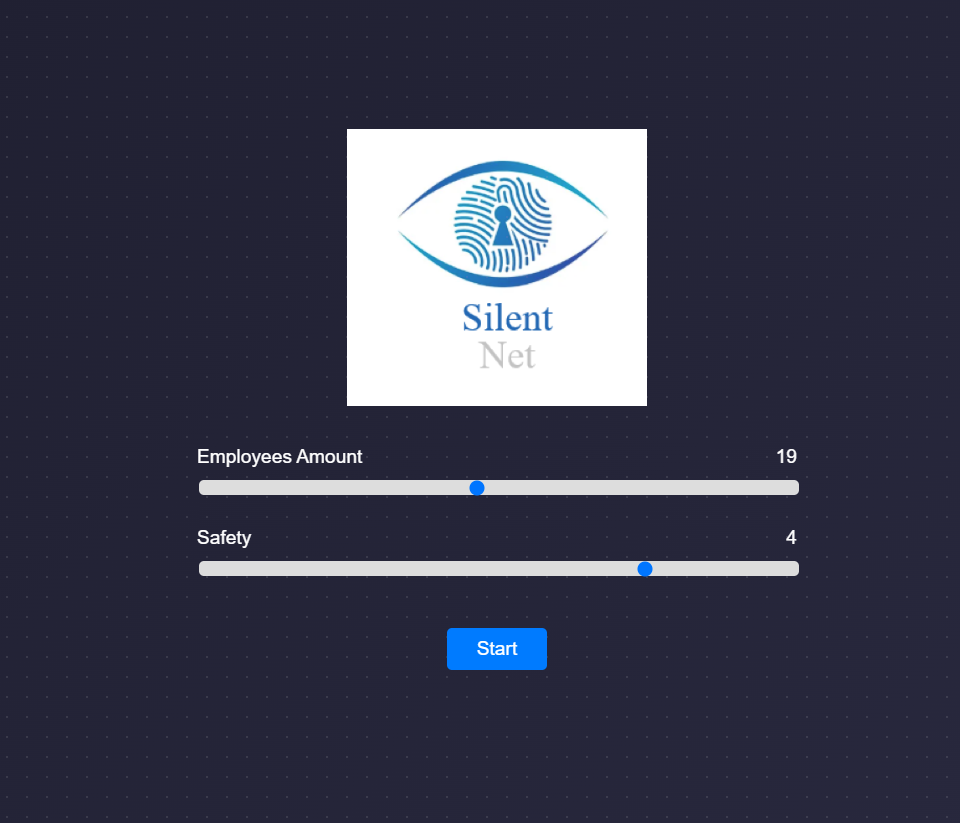
### **מסך פתיחה**



מהות מסך:

מסך זה הינו המסך הראשון ביותר שיופיע במחשב המנהל כאשר הוא פותח את התוכנית. מסך זה הינו מסך פתיחה, כלומר מחכה לקלט המשתמש על מנת להמשיך הלאה. כפי שאפשר לראות במסך זהו בעצם הלוגו של המערכת "Silent Net". במסך זה על המנהל להכניס סיסמה שידועה לו מראש, במידה והסיסמה נכונה ימשיך למסך הבא. במידה והסיסמה לא נכונה יופיע לו הודעה על כך ולא ימשיך למסך הבא. (במידה וכבר מחובר מנהל אחר, המנהל יופנה למסך הטעינה).

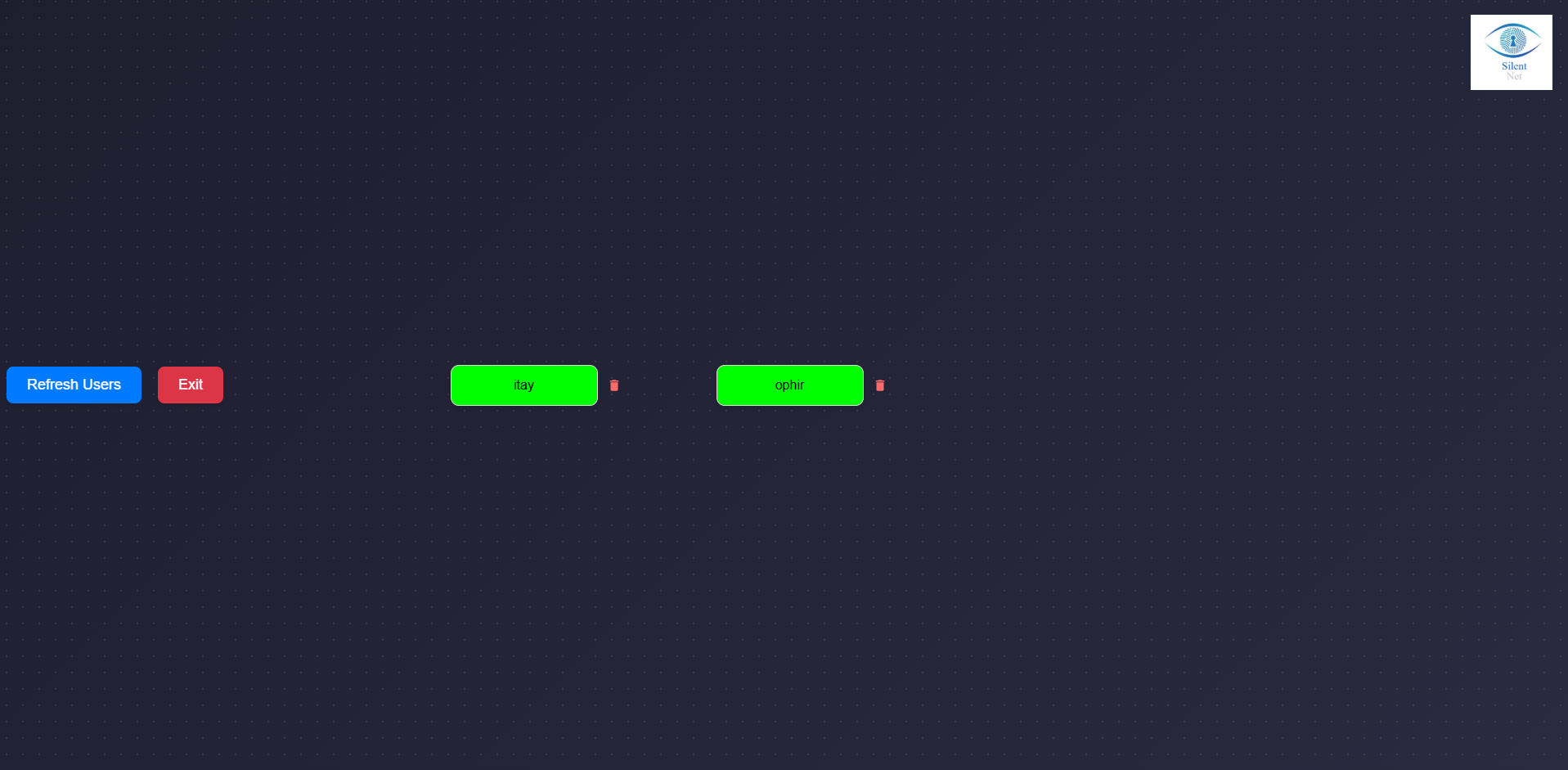
### **מסך הגדרות**



מהות מסך:

מסך זה הינו המסך השני אשר מוצג במחשב המנהל, מסך זה מבקש מן המנהל עצמו להכניס באופן ידני את ההגדרות הראשוניות ביותר לתוך הפרויקט. אחת מן ההגדרות (הראשונה) מבקשת את הכמות המקסימלית של לקוחות שיכולים להתחבר למחשב השרת. הגדרה זאתי מונעת מן מחשב השרת לקרוס בעת עומס, בנוסף על כך מונעת התקפה ידועה בשם DDOS/DOS בה מתחברים כמויות גדולות של לקוחות אל מחשב השרת במטרה להפיל אותו בשל עומס. ההגדרה השנייה קובעת את כמות הבטיחות של הפרויקט, כלומר הכוונה היותר מדויקת היא כמה מחשב השרת משאיר קשר עם מחשב מסוים, עד שהוא מנתק אותו בשל היות אותו קשר עם מחשב שמטרותיו זדוניות. רמת הבטיחות היא בסופו של דבר כמה מחשב השרת משאיר קשר עם מחשב לקוח לאחר שמחשב הלקוח שוב ושוב שלח מידע שלא ניתן לפיענוח ולא עומד בפרוטוקול. אם מחשב לקוח שולח באופן עקבי מידע לא אמין, רמת הבטיחות תקבע מתי כבר להפסיק להאמין לאותו לקוח ולנתק את הקשר איתו.

### **מסך ראשי**



מהות מסך:

מסך זה הינו המסך השלישי אשר מוצג במחשב המנהל, מסך זה מראה בזמן אמת את המחשבים המחוברים כרגע למחשב השרת ואשר מנהלים איתו קישור. אותם מחשבים שולחים מידע אל מחשב השרת. שמות המחשבים בדוגמה זו הינם שמות של משתמשים אמיתיים, אך בעת חיבור ראשוני שם המחשב יהיה כשם ה hostname (אשר אין שם אחר שייצג את מחשב זה והוא קריא).

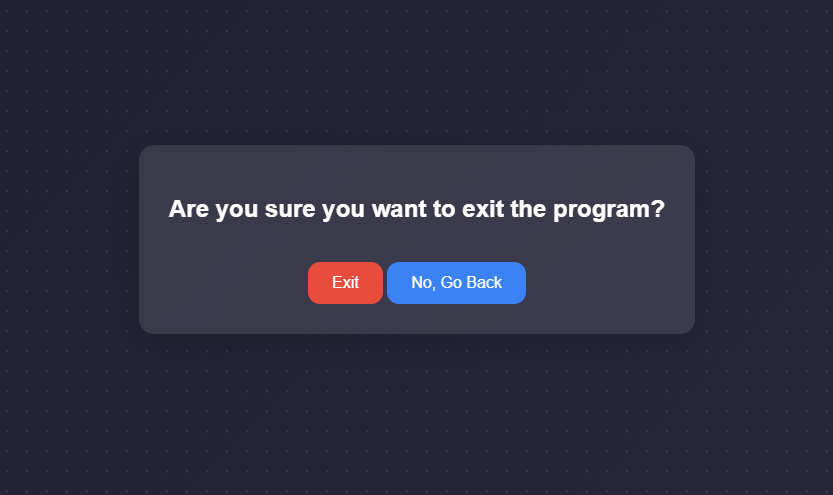
### **מסך אישי**



מהות מסך:

מסך זה הינו המסך הרביעי אשר מוצג במחשב המנהל. מסך זה מראה בזמן אמת את המידע אשר מתקבל מן אותו מחשב בעל כתובת מסוימת. ניתן להגיע למסך זה על ידי לחיצה על אחד השמות הקיימים במסך הראשי. ניתן לראות במסך את הנתונים השונים כמו תהליכים שנפתחו במחשב הלקוח, שימוש בליבות השונות, כמות מילים ממוצעת לדקה, זמנים בהם הלקוח לא היה פעיל, וסוגי IP אליהם פנה הלקוח

### **מסך יציאה**



מהות מסך

תמונה שמכילה טקסט, צילום מסך, לוגו, עיצוב

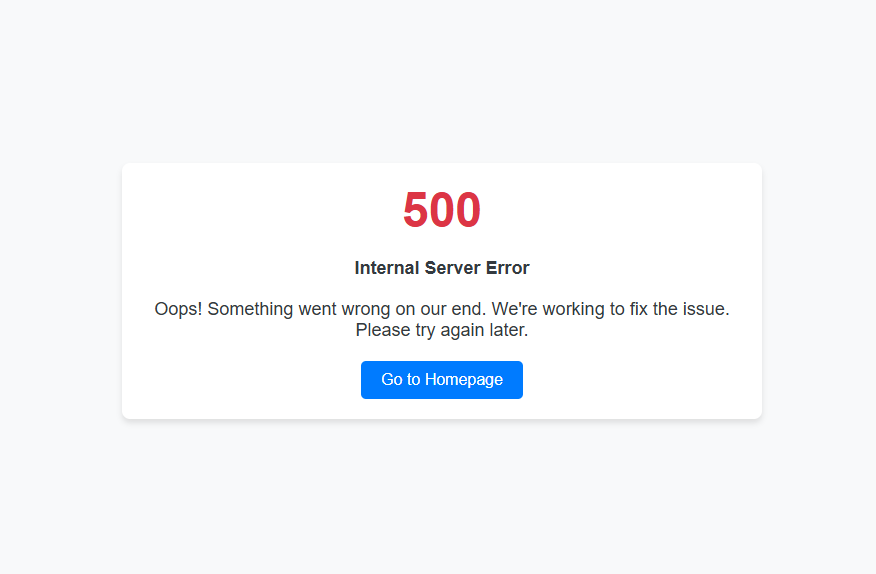
תוכן שנוצר על-ידי בינה מלאכותית עשוי להיות שגוי.מסך יציאה, זהו המסך שיופיע למנהל לאחר שהמנהל רוצה לסגור את התוכנית. המסך בא לוודא שהמנהל לא רצה לצאת בטעות מן המערכת, ולכן שואל אותו שוב אם ברצונו לסגור ולצאת מן המערכת.

### **מסך טעינה**

מהות מסך:

מסך זה יופיע כאשר אבד החיבור עם השרת, ולכן המנהל יופנה למסך זה בו הוא יכול לנסות להתחבר אל השרת כאשר ירצה, אם החיבור יצליח המנהל יופנה למסך ההגדרות, אם לא, יישאר במסך זה.

### **מסך שגיאה**



מהות מסך:

מסך שגיאה, מופיע כאשר מתרחשת שגיאה אצל הקוד של התוכנית של המנהל. המסך מוביל למסך הבית שהוא מסך הטעינה.

### תמונה שמכילה טקסט, כרטיס ביקור, צילום מסך, גופן תוכן שנוצר על-ידי בינה מלאכותית עשוי להיות שגוי.**מסך 404**

מהות מסך:

כאשר המנהל ינסה לשנות את ה URL לכתובת לא חוקית (בתוך התוכנית), יופנה אל המנהל העמוד הזה שמוביל גם כן הוא אל מסך הבית – מסך הטעינה.

### **דיאגרמת מסכים**

תמונה שמכילה צילום מסך, טקסט, תרשים, עיצוב

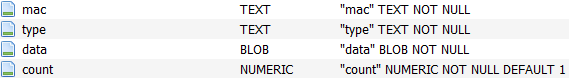
תוכן שנוצר על-ידי בינה מלאכותית עשוי להיות שגוי.

## **תיאור מבני נתונים**

הפרויקט עוסק בשלל מבני נתונים שונים, המרכזיים ביניהם בהם עושה שימוש הם שתי טבלאות מרכזיות כמסד נתונים (בצד השרת) ובקובץ מרכזי (בצד הלקוח).

**צד שרת – מסד נתונים server\_db**

טבלה ראשונה - logs

תמונה שמכילה טקסט, צילום מסך, מספר, גופן

תוכן שנוצר על-ידי בינה מלאכותית עשוי להיות שגוי.המידע שנשלח מהמחשב יכול לכלול נתונים שונים, קלט מחומרה, שמות תהליכים, ערכי CPU ועוד... כל מחשב שולח את המידע האחרון שנשלח, והמערכת בצד השרת מעדכנת באופן רציף בטבלה הראשונה. במערכת שלי, כל כתובת MAC משמשת כמפתח (key), וערך המפתח הוא המידע שנשלח מהמחשב הלקוח. המידע יכול להיות טקסטואלי (כמו שם תהליך), מספרי (כמו קוד של קלט מחומרה), או בייטים (כמו תו מפריד). כל עדכון מידע ממחשב ספציפי מעדכן את המספר של כמות הפעמים של אותו מידע. דוגמה למידע מתוך logs והגדרתו (אין מפתח בטבלה זו) -

השדות לפי התמונה משמאל: כתובת מאק הינו שדה מסוג טקסט וכך גם שדה סוג ההודעה, שדה המידע עצמו הוא שדה המוגדר כ BLOB – מידע בינארי. השדה האחרון הינו שדה שמונה את כמות הפעמים של ההודעה הנוכחית, וכמובן יהיה שדה מסוג מספר.

טבלה שנייה – uid

תמונה שמכילה טקסט, צילום מסך, גופן, קו

תוכן שנוצר על-ידי בינה מלאכותית עשוי להיות שגוי.כל תקשורת בין לקוח לשרת מתחילה כאשר הלקוח שולח לשרת את שם ה hostname של המחשב וכתובת ה MAC של כרטיס רשת. מידע זה עוזר לשרת להבדיל בין הלקוחות השונים שמחוברים אליו. מידע זה נכתב בטבלה נפרדת בה רק שני הנתונים הללו שמורים, כתובת MAC ושם המחשב (שניהם מסוג טקסט). המידע נשמר בטבלה נפרדת בשביל הפרדה לוגית ובשל שוני ערכי הנתונים שצריך לשמור. הצורך בשמירת שם המחשב הוא בכדי שכאשר המנהל מבקש את רשימת המחשבים המחוברים הוא יוכל להסתכל עליהם לפי שמות ואף גם לשנות אותם לשמות אחרים, דבר שיקל עליו מאשר להסתכל על כל מחשב ככתובת ה MAC שלו. דוגמה למידע מתוך uid והגדרתו (השדות מוגדרים כ UNIQUE מה שמכריח את התוכנית לא להכניס את אותו MAC או hostname פעמיים – בדומה למפתחות) –



**צד לקוח – קובץ לגיבוי מידע**

בצד הלקוח, מיושם מנגנון גיבוי מקומי המיועד לשמירה זמנית של נתונים אשר לא עלה בידם להישלח אל השרת הייעודי עקב תקלות שרת או הפרעות בתקשורת הרשת. מנגנון זה ממומש באמצעות קובץ גיבוי בעל מבנה מעגלי (Ring Buffer) וגודל אחסון מוגדרת מראש.

בעת אירוע הדורש גיבוי, הלקוח מבצע העתקה מדויקת של המידע המיועד לשליחה אל קובץ זה, תוך שמירה על פורמט הנתונים המקורי כפי שהוא מוגדר בפרוטוקול התקשורת עם השרת. עם חידוש התקשורת התקינה עם השרת, הלקוח יוזם תהליך של שליחת הנתונים השמורים בקובץ הגיבוי אל השרת. מאחר וגודלו של קובץ הגיבוי הינו קבוע ומוגבל, מנגנון הדריסה המחזורית הינו חלק בלתי נפרד מפעולתו.

עם התמלאות הקובץ, נתונים חדשים יכתבו על גבי הנתונים הוותיקים ביותר, ובכך יאפשרו המשך פעולה רציפה של מנגנון הגיבוי גם תחת עומס נתונים מתמשך. השימוש בקובץ גיבוי בעל גודל קבוע הינו דרישה פונדמנטלית של הפרויקט. החלטה זו נובעת מן הצורך לצמצם את ההשפעה על משאבי המחשוב של הלקוח, ובפרט זיכרון ומשאבי דיסק.

באמצעות הגבלת גודל הקובץ, מתאפשרת פעולה יציבה וצפויה של מנגנון הגיבוי ברקע, באופן שקוף למשתמש הקצה וללא פגיעה בביצועי המערכת הכוללים. חשוב להדגיש כי המידע המאוחסן בקובץ הגיבוי משקף באופן ישיר את מבנה הנתונים המוגדר בפרוטוקול התקשורת בין הלקוח לשרת.

הקובץ אינו מבצע כל שינוי או עיבוד של המידע, ותפקידו היחיד הוא שימור זמני של נתונים טקסטואליים או בינאריים המיועדים לשליחה עתידית. ארכיטקטורה זו מבטיחה נאמנות לנתונים המקוריים ומפשטת את תהליך השחזור והשליחה מחדש בעת חידוש הקישוריות עם השרת.

## **סקירת חולשות ואיומים**

בפרויקט זה העוסק במגוון נושאים מעולם הסייבר אחד הנושאים שצריך לקחת בחשבון הוא ייצור קוד בטוח אשר יודע להתגונן נגד מתקפות שונות בכדי להבטיח ריצה חלקה ומלאה של הפרויקט ללא הפרעות ומבלי חשש לחדירה לנתונים פרטיים. הפרויקט נמנע מאיומים שונים ומתגונן בפני חולשות בנושאים השונים ובדרכים הבאות –

שכבת האפליקציה

Web

בפרויקט קיימת עבודה עם Web לצורך הצגה נוחה של GUI לצד המנהל. בכדי להימנע ממתקפות שונות הפרויקט נמנע מלתת למנהל (אשר הוא הרכיב היחידי בפרויקט בעל GUI) גישה להכנסת קלט כצורת טקסט (בכדי להימנע ממתקפות דומות למתקפה XSS – מתקפה ידועה שמנצלת את העובדה שאתרים לא בודקים או מנקים נכון קלט של משתמש, ומאפשרים להכניס קוד ישירות לדף(.

בנוסף, מתקפה ידועה נוספת היא כאשר האתר אינו בודק כראוי ואוכף את הגישה לקבצים שונים, כלומר המשתמש יכול לפי ה URL לשנות אותו ולהגיע לקבצים שלא היו בכוונת כותב השרת ציבוריים. הפרויקט נמנע ממתקפה כזאת על ידי שהוא נותן גישה אך ורק ל URLים ספציפיים, ואם השם המבוקש לא נמצא בהם שגיאה 404 תופיע למנהל.

אומנם הפרויקט נמנע מלתת גישה לקלט טקסט מן המשתמש ב GUI אך כן יש מקרים בודדים בהם קיים שימוש והם כאשר המנהל מתבקש להכניס סיסמה בכדי להיכנס למערכת וכאשר המנהל רוצה להחליף שם לאחד המחשבים המחוברים. הסכנה פה היא מתקפת - sql injection טכניקת תקיפה שבה תוקף מזריק פקודות SQL זדוניות לשדה קלט במטרה לשנות את שאילתת המסד נתונים ולבצע פעולות לא מורשות.

כאשר מכניסים סיסמה אין אפשרות לבצע מתקפה אשר בצד השרת בשלב זה עוד לא ניגשים אל מסד הנתונים. אך כאשר מחליפים שם ניתן לבצע מתקפה ולפגוע במסד הנתונים, אך הפרויקט נמנע ממתקפה זו על ידי בדיקת תווים מיוחדים בשמות שניתנו, אם המנהל נתן שם עם תווים אלו שיכולים לבצע פגיעה, הפרויקט לא ישלח את השם אל השרת.

תהליך login – צד לקוח וצד שרת

צד שרת:

כחלק מהליך ה login המנהל צריך לשלוח סיסמה שרק היא ידועה למנהלים, כלומר לא כל אדם יכול להשיג את הנתונים שהשרת מספק למנהלים, אלא רק מי שיודע את הסיסמה איתה השרת התחיל.

צד לקוח:

כחלק מהליך ה login הלקוח צריך לשלוח את הנתונים שיעזרו לשרת לזהות את לקוח זה – כתובת ה MAC של כרטיס הרשת וה - hostname של המחשב.

שני תהליכי login אלו קריטיים אשר מנהל/לקוח שלא יבצע אותם כמו שצריך לא ימשיך ב session עם השרת, כלומר לא ניתן לשלוח הודעות לשרת שמדמות הודעות שנשלחות באמצע session ולהשיג מידע/לשלוח מידע (שישמר בשרת) מבלי לבצע את התהליך ההתחלתי. הדבר מונע התחזות לאנשים.

הצפנה

כמו שצוין בחלק הקודם, המנהל שולח סיסמה אל השרת בתחילת ה session כחלק מתהליך ה login שלו. כמצופה, לא ניתן לשלוח סיסמה מבלי להצפין אותה אחרת האזנה פשוטה על ידי מתקפה MITM (Man in the middle – מחשב שמאזין למידע הנשלח בין שני מחשבים אחרים מבלי ידיעתם) יכולה לגרום להפצת הסיסמה ואנשים שהם לא המנהל יוכלו להשיג את המידע ולמחוק אותו!

בפרויקט נעשה שימוש בהצפנה שמתנהלת בין המנהל לשרת (עוד לפני שליחת הסיסמה). ההצפנה מונעת מכל מחשב שמאזין להבין את המידע הנשלח בין מחשב המנהל למחשב השרת ולא יהיה לו תועלת מכך. סוגי ההצפנות ופרוטוקולים שהפרויקט משתמש בהם הן:

DH (Diffie Hellman) – פרוטוקול להחלפת מפתחות ידוע שמסתמך על קושי פתרון בעיית הדיסקרט לוגריתם (Discrete Logarithm Problem), הפרוטוקול מאפשר לשני אנשים להגיע למפתח פרטי על ערוץ ציבורי (כך שאם מישהו מאזין לתקשורת הוא אינו יכול להגיע למפתח הפרטי). הפרויקט משתמש במספרים גדולים וחזקים שיקחו זמן רב בשביל מחשב מאזין לפענח בכדי להגיע למפתח הפרטי.

לאחר ששני הצדדים בעלי המפתח הפרטי ניתן כעת להשתמש בהצפנה המידע עם אותו מפתח פרטי שמשותף רק לשניהם. בשלב הזה הפרויקט משתמש בהצפנה סימטרית AES (מצב CBC) – אלגוריתם להצפנה סימטרית שפועל במצב שרשור בלוקים (Cipher Block Chaining) כדי לשפר את האבטחה על ידי קישור כל בלוק מוצפן לבלוק הקודם, הצפנה חזקה שמקשה על מי שינסה להאזין לתעבורה.

חשוב לציין כי יש חשיבות גדולה לשימוש ב TCP עם מצב CBC בהצפנה AES, אשר מכיוון שההצפנה הינה הצפנת בלוקים, כל בלוק מסתמך על הבלוק הקודם כחלק מההצפנה, ולכן גם הקידוד יעבוד באותה צורה, כלומר עם בלוק אחד הולך לאיבוד או אפילו רק חלק ממנו, דבר שמאוד יתכן בפרוטוקולים כמו UDP, לא יהיה ניתן לפענח את המסרים מהצד השני.

DOS/DDOS

אחת המתקפות הקלות לביצוע אך האפקטיביות מבניהן. ההתקפה מסתמכת ישירות על כך שמשאבים של מחשב אינם אינסופיים, ולכן אם רכיב אחד מקבל כמות עצומה של משימות בבת אחת הוא ככל הנראה יקרוס/לא יתפקד כמצופה. הפרויקט נמנע ממתקפה זו בכמה דרכים שונות:

* הגבלת כמות הלקוחות אצל השרת, השרת פשוט לא ייצור session עם לקוחות כאשר כבר קיימים כמות לקוחות מחוברים ככמות שהמנהל הגביל את השרת. בנוסף המנהל יכול גם כן להגביל את השרת לכמות בעצמה מוגבלת של לקוחות (המנהל לא יכול לתת מעל 40 לקוחות, כמות גדולה אך מעליה השרת מתקשה בביצוע פעילותו).
* הגבלת כמות המנהלים שיכולים להיות מחוברים לשרת בו זמנית. בפרויקט רק מנהל אחד יכול לנהל session עם השרת (אפילו שהמנהל מקבל יחס עליון – גם אם כמות הלקוחות הגיעה לכמות הלקוחות המקסימלית המנהל עדיין יכול להתחבר).
* הגדרת רמת בטיחות ללקוחות. המנהל יכול להגדיר לשרת את רמת הבטיחות שהוא רוצה כאשר הוא מחובר לשרת, רמת הבטיחות היא מקושרת ישירות לכמות ההודעות שהשרת לא יכול לפענח שמגיעה מן לקוחות, לאחר כמות ההודעות האלו שמגיעה ברצף השרת סוגר את ה session עם הלקוח. הגדרה זו מונעת מלקוח שכן התחבר כראוי לשרת לבצע מתקפת DOS על השרת.

שכבת התעבורה – פרוטוקול TCP

TCP מספק חיבור אמין (reliable) בין שני צדדים באמצעות מנגנון של לחיצת יד משולשת (Three-Way Handshake). במהלך לחיצת היד, שני הצדדים מאמתים אחד את השני ומסכימים על פרמטרים בסיסיים של החיבור. התהליך מבטיח שהחיבור נוצר בכוונה תחילה ולא נוצר בטעות או בהתקפת זיוף פשוטה (כגון IP spoofing). בנוסף, TCP כולל מנגנוני בקרת שגיאות - לכל מקטע (segment) נוסף Checksum — מספר שמייצג את תוכן המקטע.

כשמקבלים מקטע, בודקים אם החישוב מתאים. אם יש טעות, המקטע נזרק והצד השולח ישלח אותו שוב, סידור מנות - לפעמים מנות מגיעות בסדר שונה מזה שבו הן נשלחו (בגלל רשתות). TCP נותן לכל מקטע מספר סידורי (Sequence Number), וכשהצד המקבל מקבל מנות, הוא מסדר אותן לפי המספרים כדי לשחזר את הנתונים בדיוק כמו שנשלחו, ובקרת זרימה - TCP מוודא שהשולח לא יציף את המקבל ביותר מדי נתונים.

לשם כך המקבל מודיע לשולח כמה מקום פנוי יש לו בזיכרון (בחלון שנקרא Window Size). כך, השולח מתאים את קצב השליחה למה שהמקבל מסוגל לקלוט ולעבד, שמגינים על שלמות הנתונים ומקטינים סיכון לפגיעות כתוצאה מהעברת נתונים חלקית או שגויה.

Timing attack

סוג של תקיפת צד-ערוץ שבה התוקף מנתח את הזמן שלוקח למערכת לבצע פעולות שונות, כדי לגלות מידע סודי כמו סיסמאות, מתקפה זו מסתמכת על ההתנהגות הטבעית של המחשב בביצוע פעולות שונות. אם צד אחד יודע את הדרך בה מתבצעת פעולה מסוימת הוא יכול למדוד זמנים כמה זמן לוקח לכל קלט להחזיר תשובה מהשרת.

הדרך שבה השרת בודק אם הסיסמה נכונה היא על ידי השוואת אות אות, ברגע שאות לא טועמת את האות בסיסמה השמורה, הוא מסיים את הבדיקה ומחזיר FALSE, עם ידע זה, הצד המתקיף יכול לנסות סטרינגים שונים ולראות מה לוקח לשרת יותר זמן להגיב, ולפי זה הוא יכול לדעת אם הוא בכיוון לסיסמה הנכונה לא.

ניתן לבצע מתקפה זו אם המנהל בטעות השאיר את המחשב שלו פתוח ועובד השיג גישה למחשב המנהל (בהסתמך שהתוכנית סגורה כאשר המנהל לא על המחשב, אם המנהל לא סוגר את התוכנית כשהוא לא על המחשב ועובדים יכולים להשיג גישה למחשב שלו זה כבר מעבר לתחום הפרויקט), העובד יכול לנסות לשלוח סיסמאות שונות בדף פתיחה אל השרת ולראות מה לוקח יותר זמן.

הפתרון לבעיה זו הוא דווקא פשוט למימוש בצד השרת – לאחר כל פעם שהשרת מאמת סיסמה שנשלחה אליו הוא מחכה למשך זמן רנדומלי (עד לשנייה) ורק לאחר מכן מגיב בחזרה לצד השני. ביצוע פעולה זו גורם לכך שאין באפשרות הצד השני לעולם לדעת אם הסיסמה מקיימת בתוכה חלק מתוך הסיסמה האמיתית ובכך לא יקבל רמזים לגבי הסיסמה האמיתית.

קשיים:

Timeout- על סוקט קרנלי, היה קושי בלמצוא את הפקודה שמאפשרת לעשות זאת.

ביצוע פעולות blocking עם interrupt context היה תוקע את כל המערכת וכל המערכת מפסיקה לעבוד.

חיפוש פעולות שנקראות על ידי הקרנל.

פתרונות:

-בהתחלה הפיתרון היה להריץ תהליכון שבודק, לאחר מכן אחרי חיפוש מעמיק מצאתי פקודה קרנלית שנותנת לבצע timeout שליחת וקבלת הודעות.

-לאחר קריאת ספר מצאתי מבנה נתונים שפותח תהליכונים מאחרי הקלעים ומתזמן אותם ב process context לפי סדר – workqueue.

-הרבה פעולות של הקרנל שעליהם אני מבצע הוקים דורשות חיפוש ב source code, לכן הורדתי את ה source code על המחשב שלי וכל פעם שאני צריך למצוא פקודה אני מחפש שם.