חוזר מנהל מה"ט 51-4-11 – נספח מס '1 (הצעה לפרויקט גמר)

תאריך:\_\_\_\_\_\_\_\_\_\_\_

לכבוד

יחידת הפרויקטים מה"ט

**הצעה לפרויקט גמר**

יש להדפיס את כל הנתונים הנדרשים

### פרטי הסטודנטים

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| תאריך סיום  הלימודים | טלפון נייד | כתובת | ת.ז .9 ספרות | שם הסטודנט |
|  | 0526682854 |  | 315183731 | סאמר  ג'ראיסי |
|  |  |  |  |  |

שם המכללה:  **המכללה הטכנולוגית נוף** הגליל סמל המכללה: **72209**

מסלול ההכשרה: **הנדסאים**

מגמת לימוד: **תוכנה בהתמחות FS**   
מקום ביצוע הפרויקט: המכללה הטכנולוגית נוף הגליל

### פרטי המנחה האישי

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| מקום עבודה/תפקיד | תואר | טלפון נייד | כתובת | שם המנחה \* |
| מכללת נוף הגליל | Bsc/MBA | 0523203282 | יקינטון 23 חיפה | להב רון |
|  |  |  |  |  |

\* עבור מנחה אישי חדש יש לצרף קורות חיים, ניסיון מקצועי ותעודות השכלה לאישור מה"ט.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |
| חתימת הסטודנט | חתימת המנחה האישי | חתימת הגורם המקצועי מטעם מה"ט |

דרך מנחם בגין 86 תל אביב ת.ד .36049 מיקוד 67138 טלפון: 7347521-03 פקס: 7347644-03

# שם הפרויקט:

# WireTracer מערכת למעקב אחרי Packets וניטור משאבי חומרה של המחשב.

# רקע

## **תיאור ורקע כללי:** המערכת מעניקה יתרון משמעותי באבטחת מערכות, בין אם מדובר במשתמש יחיד או בקבוצת משתמשים. האבטחה מתבטאת במתן התראות על זיהוי חבילות רשת המעידות על מתקפה מקוונת נגד מכונת המשתמש, וכן בביצוע מעקב אחר אחוזי השימוש במשאבי חומרה, כגון זיכרון RAM, לצורך זיהוי והתרעה על נוכחות של וירוס מקומי במערכת

## **(נבדק)**

## **מטרות המערכת**

## בהתבסס על יכולות האבטחה המפורטות בסעיף 2.1, המערכת מציעה מנגנוני ניטור והתראה מתקדמים לזיהוי ודיווח על פעילות חריגה. באמצעות ניתוח חבילות רשת ומעקב אחר ניצול משאבי חומרה, המערכת מאפשרת איתור בזמן אמת של איומים פוטנציאליים, כגון מתקפות מקוונות או וירוסים מקומיים. התראות המערכת נועדו להבטיח למשתמשים תגובה מהירה וממוקדת, המותאמת לשמירה על תקינות המערכת ולמזעור סיכונים אפשריים.

## (נבדק)

# סקירת מצב קיים בשוק, אילו בעיות קיימות

ישנו אוסף של טכנולוגיות אשר קיימות עם אותה פונקציונליות בשוק שלושה מהם הם הנ"ל

3.1 [WireShark](https://www.wireshark.org/) האפליקציה מכילה תכונות כמו תכונת צפייה בפקטות אבל אין לה את היכולת להתריע על סכנה פוטנציאלית למחשב המשתמש דרך מתקפות אנטרנטיות כמו DDOS וPHISHING.

נבדק

3.2 [TASK MANAGER](https://learn.microsoft.com/en-us/shows/inside/task-manager) במנהל המשימות של מייקרוסופט אנו יכולים לזהות את רמת השימוש במשאבי מחשב כמו RAM CPU ודיסק קשיח מה שבעייתי במנהל המשימות זה שהוא לא מאחד זיהויי דפוסים אנטרנטים יחד עם תכונתיו הידועות, לכן הפרוייקט שלי שואף לאחד את הפונקציונליות של מנהל המשימות יחד עם זו של WIRESHARK בתוך ממשק אחד. (נבדק)

3.3 [Zeek](https://docs.zeek.org/en/master/about.html" \l "what-is-zeek) היא תוכנה לניתוח תעבורת רשת, בדומה ל-Snort ול-Wireshark המתמקדת בניטור פסיבי ותיעוד יומנים לניתוח מאוחר, כולל ניתוח HTTP ,זיהוי ומעקב. SSL עם זאת DNS, היא אינה מתאימה לניטור משאבי חומרה או זיהוי איומים מקומיים ודורשת ידע טכני מתקדם. לעומת זאת, התוכנה שלנו מציעה ממשק ידידותי, התראות מיידיות, וניתוח מותאם אישית המגן מפני איומים חיצוניים ופנימיים, תוך אספקת שכבת אבטחה הוליסטית ואפקטיבית יותר. (נבדק)

# מה הפרויקט אמור לחדש או לשפר

# הפרויקט מיועד לספק ממשק משתמש אינטואיטיבי, המאפשר לכל משתמש, ללא קשר לרמת הידע הטכני שלו, להבין ולעבד את התראות המערכת בקלות ובבהירות. הממשק עוצב בקפידה כדי להנגיש מידע קריטי בצורה ידידותית, תוך שמירה על רמה גבוהה של דיוק ואמינות. התראות המערכת יספקו מידע מפורט וזמין על איומים אפשריים, כגון וירוסים, מתקפות אינטרנטיות, או פעולות זדוניות אחרות, במטרה להעניק למשתמשים כלים אפקטיביים לזיהוי מוקדם ולתגובה מהירה. בנוסף, המערכת משלבת פתרונות חזותיים ותיאוריים המסייעים למשתמש להבין את מצב האבטחה של המערכת שלו, ומבטיחה חוויית שימוש פשוטה אך מתקדמת, שתומכת במניעת סיכונים ושיפור אבטחת המידע באופן מתמיד. (נבדק)

# דרישות מערכת ופונקציונאליות (לעשות סעיף 5)

## דרישות מערכת פיתוח המערכת ידרוש שימוש ב-VISUAL STUDIO בנוסף ל-API של VIRUS TOTAL וגם ניתוח פקטות המרמיזות על מתקפות אנטרנטיות על המשתמש

## דרישות פונקציונאליות

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **NFR** | **FR** | **דרישות ותיאור** | **מספר מזהה** | **קטגוריה / מודול** |
|  | **V** | המערכת תאפשר רישום ראשוני עם אימות כתובת מייל | 1.1 | רישום וכניסה למערכת |
|  | **V** | בעת כניסה למערכת, המשתמש יצטרך להזין שם משתמש וסיסמה | 1.2 |  |
|  | **V** | למערכת תהיה אפשרות לאיפוס סיסמה דרך כתובת המייל של המשתמש | 1.3 |  |
|  | **V** | המערכת תבצע ניטור בזמן אמת של תעבורות רשת ותזהה דפוסים חריגים | 2.1 | ניטור חבילות רשת |
|  | **V** | המערכת תשלח התראה מיידית במקרה של מתקפוות כמו DDOS או PHISHING | 2.2 |  |
|  | **V** | למערכת תהיה אפשרות לייצא דוחות מפורטים על פעילות רשת | 2.3 |  |
|  | **V** | המערכת תעקוב אחרי ניצול CPU, RAM ודיסק קשיח ותתריע על שימוש חריג | 3.1 | ניטור משאבי חומרה |
|  | **V** | ניתן יהיה להציג גרפים על שימוש במשאבי חומרה לאורך זמן | 3.2 |  |
|  | **V** | המערכת תשלח התראות ברורות במקרה של זיהוי דפוסים חשודים או איומים | 4.1 | התראות בזמן אמת |
|  | **V** | ההתראות יכללו מידע על סוג האיום, מקורו, והמלצות לפעולה | 4.2 |  |
| **V** |  | המערכת תכלול ממשק משתמש ברור ואינטואיטיבי, שיתאים למשתמשים לא טכניים | 5.1 | ממשק משתמש |
| **V** |  | התצוגה תציג נתוני רשת ומשאבים בצורה גרפית וברורה | 5.2 |  |

רשימת דרישות המשתמש מהמערכת, מהן הפעולות בהן נדרשת המערכת לתמוך.

# בעיות צפויות במהלך הפיתוח ופתרונות: (תפעוליות, טכנולוגיות, עומס ועוד)

## תיאור הבעיות- הללו כפועל יוצא של דרישות המשתמש מהתוכנה.

## פתרונות אפשריים. (נא ציין פתרונות אפשריים וחלופות ארכיטקטוניות)

# פתרון טכנולוגי נבחר:

## טופולוגית הפתרון- כלומר: פרישת המערכת , היכן יתבצע יישום המערכת deployment

## טכנולוגיות בשימוש (איזה ומדוע בכמה מילים)

## שפות הפיתוח: (איזה שפות ומדוע בכמה מילים)

## תיאור הארכיטקטורה הנבחרת- הסבר בכמה מילים מדוע

## חלוקה לתכניות ומודולים

## סביבת השרת (מקומי, וירטואלי, ענן, שירות אירוח)

## ממשק המשתמש/לקוח - GUI :

## ממשקים למערכות אחרות/ API:

## שימוש בחבילות תוכנה:

# שימוש במבני נתונים וארגון קבצים

## נא פרט את מבני הנתונים.



## נא פרט את שיטת האחסון (מאגר, קבצים ובאיזה טכנולוגיה)

## נא ציין מנגנוני התאוששות מנפילה\קריסה\תמיכה בטראנזקציות.

# תרשימי מערכת מרכזיים

## Use Case

## Sequence Diagram

## Data flow

# תיאור המרכיב האלגוריתמי – חישובי

## איזו בעיה בא הפרוייקט לפתור, ואיך יפתור?

## איסוף מידע וניתוחים סטטיסטיים (אנליטיקות)

# תיאור/התייחסות לנושאי אבטחת מידע

# משאבים הנדרשים לפרויקט:

## מספר שעות המוקדש לפרויקט, חלוקת עבודה בין חברי הצוות

## ציוד נדרש

## תוכנות נדרשות

## ידע חדש שנדרש ללמוד לצורך ביצוע הפרויקט

## ספרות ומקורות מידע

# תכנית עבודה ושלבים למימוש הפרויקט

# תכנון הבדיקות שיבוצעו

## נא פרט בטבלה ,בדיקות תהליכיות ברמת משתמש בהן נדרשת המערכת לעמוד

(Full flow)

|  |  |
| --- | --- |
| תיאור הבדיקה | התנהגות צפויה |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

## נא פרט בטבלה, מס מייצג של בדיקות יחידה למודולים המרכזיים בהן נדרשת המערכת לעמוד unit test)):

|  |  |
| --- | --- |
| תיאור הבדיקה | התנהגות צפויה |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

# )version control בקרת גרסאות)

|  |  |
| --- | --- |
|  |  |
|  |  |
| חתימת הסטודנט | חתימת המנחה האישי |

### הערות ראש המגמה במכללה

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

### אישור ראש המגמה

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |
| שם | חתימה | תאריך |

### הערות הגורם המקצועי מטעם מה"ט

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

### אישור הגורם המקצועי מטעם מה"ט

שם: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ חתימה: \_\_\_\_\_\_\_\_\_\_\_\_ תאריך:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_