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

## 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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **מספר מזהה** | **דרישה ותיאור** | | **FR** | **NFR** |
| 1 | **רישום וכניסה למערכת ובטיחות צד משתמש** | |  |  |
| 1.1 | המערכת תאפשר רישום ראשוני עם אימות כתובת מייל (נבדק) | | V |  |
| 1.2 | למערכת תהיה אפשרות לאיפוס סיסמה דרך כתובת המייל של המשתמש נבדק | | V |  |
| 1.3 | נתונים רגישים של משתמש, כגון סיסמה, יעברו הצפנה באמצעות אלגוריתם Hashing מתקדם מסוג **BCrypt** נבדק | | V |  |
| 1.4 | אימות בקשות HTTP של המשתמש יתבצע באמצעות **JWT** (JSON Web Token), אשר נשלח למשתמש בעת התחברות למערכת נבדק | | V |  |
| 2 | **ניטורי מערכת** |  | |  |
| 2.1 | המערכת תבצע ניטור בזמן אמת של תעבורות רשת ותזהה דפוסים חריגים כמו דפוסי TCP/SYC במספר גדול שמציגים סיכוי למתקפת DDOS נבדק | | V |  |
| 2.2 | המערכת תשלח התראה מיידית במקרה של מתקפות כמו DDOS או PHISHING נבדק | | V |  |
| 2.3 | המערכת תעקוב אחרי ניצול CPU, RAM ודיסק קשיח ותתריע על שימוש חריג נבדק | | V |  |
| 3 | **התראות בזמן אמת** |  | |  |
| 3.1 | המערכת תספק התראות ברורות במקרה של זיהוי דפוסים חשודים המעידים על מתקפות סייבר או איומים מקומיים, כגון וירוס המתחזה לקובץ תקין. בנוסף, המערכת תאתר שימוש יתר במשאבי החומרה ותתריע על כך בזמן אמת נבדק | | V |  |
| 3.2 | ההתראות יכללו מידע על סוג האיום, מקורו, והמלצות לפעולה נבדק | | V |  |
| .33 | פונקציונאליות ההתראה בזמן אמת תנוהל ע"י API של שקעים (SOCKETS) שגם יהיה חלק מתהליך ניטור דפוסי אינטרנט. | | V |  |
| 4 | **ממשק משתמש** | |  |  |
| 4.1 | התצוגה תציג נתוני רשת ומשאבים בצורה גרפית וברורה. ניתוני הרשת יוצגו ע"י תיבות טקסט המכילות את סוג הפקטה, זמן הגעתה, צבע התיבה יראה את רמת סיכון פקטה (אדום, צהוב, ירוק) נבדק | | V |  |
| 4.2 | ניצול משאבי המחשב יוצג באמצעות תרשים מעגלי פתוח, בו יוצגו אחוזי השימוש במשאבים השונים. צבע המעגל יתאים לרמת השימוש, לדוגמה: ירוק לניצול נמוך, צהוב לניצול בינוני, ואדום לניצול גבוה. נבדק | | V |  |
| 4.3 | הנתונים עבור כל דפוס שנשלח מהשרת יוצגו בתוך כרטיסיה, ויכללו את הפרטים הבאים:   1. סוג פקטה כגון TCP\UDP... 2. מקור ויעד הפקטה (כתובת IP) 3. תיאור קצר על סוג הפקטה נבדק | |  | V |
| 5 | **דוחות וגרפים** | |  |  |
| 5.1 | המערכת תייצא דוחות מפורטים הכוללים:   * פעילות רשת: תעבורת רשת לפי IP, סוג פרוטוקול (TCP/UDP), וזיהוי איומים. * משאבי חומרה: ניצול RAM, CPU, ודיסק קשיח לאורך זמן. נבדק | | V |  |
| 5.2 | המערכת תשלח מיילים לשם התראת המשתמש על דפוסים מסוכנים במידה שהמשתמש היה רחוק מהמחשב. מיילים אלו יכללו תיאור קצר על פקטה מסוכנת ואיך בדרך כלל היא משומשת ע"י גורמים זדוניים  נבדק | |  | V |
| 5.3 | המשתמש יכול לסנן את התצוגה בממשק כך שתציג את כל סוגי הפקטות או פקטות מסוג מסוים בלבד, בהתאם להעדפתו נבדק | |  | V |
| 5.4 | ניתן יהיה להציג גרפים על שימוש במשאבי חומרה לאורך זמן נבדק | |  | V |
| 6 | **בינה בטחונית-Security Intelligence** | |  |  |
| 6.1 | המערכת תזהה מתקפת DDoS באמצעות ניתוח וספירה של פקטות TCP/SYN נבדק | | V |  |
| 6.2 | המערכת מסוגלת לזהות מתקפות מסוג IP Spoofing על ידי השוואה בין כתובת ה-IP לכתובת ה-MAC של הגורם המזוהה כמחופש. נבדק | | V |  |
| 6.3 | המערכת מבצעת בדיקה של גודל כל פקטה על מנת להתריע בפני המשתמש על מתקפות כמו **Ping of Death**. פקטות חריגות הן בדרך כלל בגודל העולה על 65,535 בתים. נבדק | | V |  |
| 6.4 | המערכת מזהה מתקפת Smurf באמצעות בדיקת פקטות ICMP המופנות לכתובת השידור (BROADCAST ADDRESS). בכתובת ברירת המחדל מדובר ב-255, אך בתצורות רשת הכוללות Subnetting, כתובת השידור עשויה להשתנות בהתאם לטווח הכתובות של תת-הרשת. נבדק | | V |  |
| 6.5 | המערכת מסוגלת לזהות מתקפות מסוג Land Attack על ידי בדיקה של כתובת ה-IP המקורית והכתובת היעד. אם שתי הכתובות זהות, המערכת תתריע בפני המשתמש נבדק | | V |  |

# 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 :

**עמוד רישום כמשתמש**



נבדק

**עמוד בית (מציג פקטות)**

נבדק

**עמוד אבטחת קבצים**

נבדק

עמוד אבטחת קישורים



נבדק

**ממשק דוחות**

****

נבדק

**ממשק דוחות (יצירת דו"ח)**

****

נבדק

**עמוד רמת שימוש במשאבי מחשב**



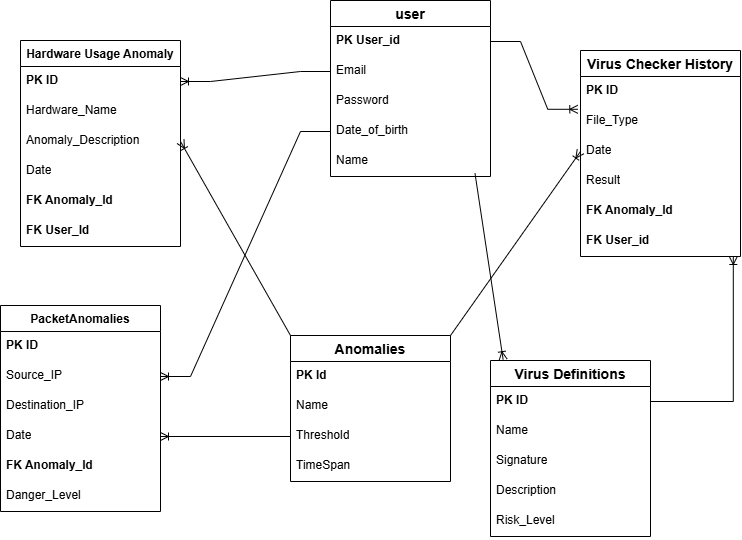
נבדק

## ממשקים למערכות אחרות/ API:

## שימוש בחבילות תוכנה:

# שימוש במבני נתונים וארגון קבצים

## נא פרט את מבני הנתונים.





Hardware Usage – צריך להוסיף תאריך ולתעד רק את האנומליה לשנות את שם הטבלה ל HardwareUsageAnmaly יש לתעד את החומרה שיש בה אנומליה ואת התאריך ותאור האנומליה.

יש לעבור על הממשקים ולראות שהמידע שמופיע בממשקים או שנלקח ממסד הנתונים או מה API מה שנלקח ממסד הנתונים צריך להיות ב ERD.

ב ERD לציין רק את שמות השדות ואם זה PK או FK לא צריך לציין את סוג השדה.

במסד הנתונים יש לתעד רק את האנומליות אחרת אם תתעד כל פקטה מסד הנתונים יתנפח מהר מאוד.

יש להכיל מסד נתונים של וירוסים – אולי כדאי לבדוק במאגר מסויים – שב איתי בשישי על ה ERD.

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

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

# תרשימי מערכת מרכזיים

## Use Case

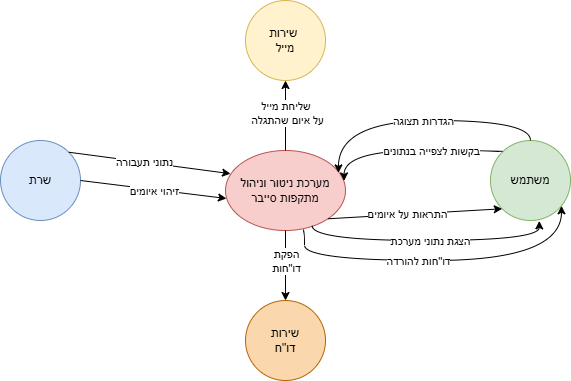


\* נבדק.

## Sequence Diagram

## Data flow

Context Diagram



ב context מופרט מידי !!!!

# 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:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_