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.

עבודה מול ספריות ו עבודה מול הפונקציות שלהם:-

כמו שרובנו יודעים הרבה האפליקציות בימינו משתמשים בספריות חיצוניות ידועות ובכדי להשתמש בספריות אלו אנו צריכים ללמוד את הפונקציות שלהן ולדעת איך להשתמש בפונקציות אלו

נבדק

יצור מערכת גדולה יחסית-

ההתמודדות עם יצור של מערכת גדולה וחדשנית יגזול מאתנו זמן רב שקשה לנו לצפות את עקומת הלימוד בפרויקט שכזה.

נבדק

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

ארגון הזמן , למידת הספריות האמורות וחלוקה נכונה של זמן הפיתוח יסייעו לנו להשתלט על הפרויקט תוך לקיחה של מרווחי זמן בין אירועים בלתי צפויים

יש להכניס לטבלה (בעיה / פתרון) בהתאם לדוגמאות ששלחתי (כל סעיף 6)

## 

# פתרון טכנולוגי נבחר:

## **טופולוגית הפתרון- פרישת המערכת**

נבדק

## **טכנולוגיות בשימוש**

Visual Studio Code

MongoDB Compass

Mailjet

VirusTotalAPI  
נבדק

## **שפות הפיתוח**:

**צד לקוח:**

HTML,CSS, JAVASCRIPT

השפות השימושיות ביותר לפיתוח אפליקציות וויב

**צד שרת:**

# - C

שפה עילית אשר בה ניתן לגשת לחומרה על מנת לקבל ניתונים. הייתי צריכים להשתמש בה על מנת לשלוף מידע על דפוסי רשת ואחוזי שימוש בחומרה

**בסיס נתונים:**

MongoDB

מסד ניתונים NoSQL עם ספריה ב-#C המספקת פיצ'רים לניהול נתונים

נבדק

## **תיאור הארכיטקטורה הנבחרת- הסבר בכמה מילים מדוע**

בחרתי בארכטקטורת שרת-לקוח כדי לספק מידע ללקוח שלי דרך שימוש בשרת לוקאלי עם הפיצ'רים ה-Low level של #C וזאת משום ש-JAVASCRIPT אינה יכולה לגשת לחומרה כמו #C במקביל JS מנהלת את הצגת האנפורמציה למשתמש בצורה ברורה

נבדק

## **חלוקה לתכניות ומודולים** **מחלקת MetricsFetcher:** מחלקה אחראית על שליפת אחוזי שימוש בחומרה המחלקה מכילה מתודה ראשית בשם GetMetrics מתודה זו מחזירה אחוזי שימוש במשאבים בצורת רשימה לשם שליחתם למשתמש.

**מחלקת PerformanceHub** : מחלקה המקבלת אחוזים מ-MetricsFetcher לשם שליחתם למשתמש בנוסף המחלקה מעדכנת ערכים קריטים אחרי כל מדידת אחוז שימוש כמו ממוצע שימוש וסטיית תקן של אחוזי שימוש בחלק חומרה מסויים.

**מחלקת CaptureService:** מחלקה זו שולפת פקטות מכרטיס הרשת ומעבירה אותם למנטר, המחלקה שומרת שדה של תור אשר בו יש מידע על פקטות שנשלפו. אותו תור שומר מידע על הפקטות אחרי ניטורן ושולח אותם למחלקה ששולחת אותם ללקוח לפני מחיקתם

**מחלקת PacketHub:** מחלקה אשר מקבלת את הפקטות אחרי ניטורן ושולחת אותם ללקוח, המחלקה מכילה פונקציה בשם GetPackets שצד הלקוח קורא לה באופן אוטומטי פעם אחת כל דקה.

**מחלקת Analyzer:** מחלקה שיש בה פונקציות לנטר פקוטות 5 פונקציות לשם ניטור סוגי מתקפות שונות למשל DetectSynFlood ו DetectUdpFlood אחראיות על בדיקת מתקפות דרך פקטות TCP וudp בסדר זה. במקביל DetectPingOfDeathV4/V6 הינם לבדיקת Ping of death וכל אחת מהם בודקת סוג IP אחד לחוד

**מחלקת UserController:** מחלקה שמיכילה פעולות HTTP של משתמשים כמו כניסה והרשמה וגם מכילה את פיצ'ירי בדיקת קבצים וקישורים דרך API של VirusTotal המחלקה שולפת מפתחות ה-API מקובץ appsettings.json.

נבדק

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

לפי דרישות התוכנה הזו השרת צריך להיות מקומי בשל שליפת נתוני שימוש חומרה, ונתוני פקטות של המשתמש שלי. אם השרת לא היה מקומי אז שליפת הפקטות ונתוני החומרה תשלח את נתוני המכונה אשר עליה יושב השרת.  
נבדק

## ממשק המשתמש/לקוח - GUI :

**עמוד רישום כמשתמש**



נבדק

**עמוד בית (מציג פקטות)**

נבדק

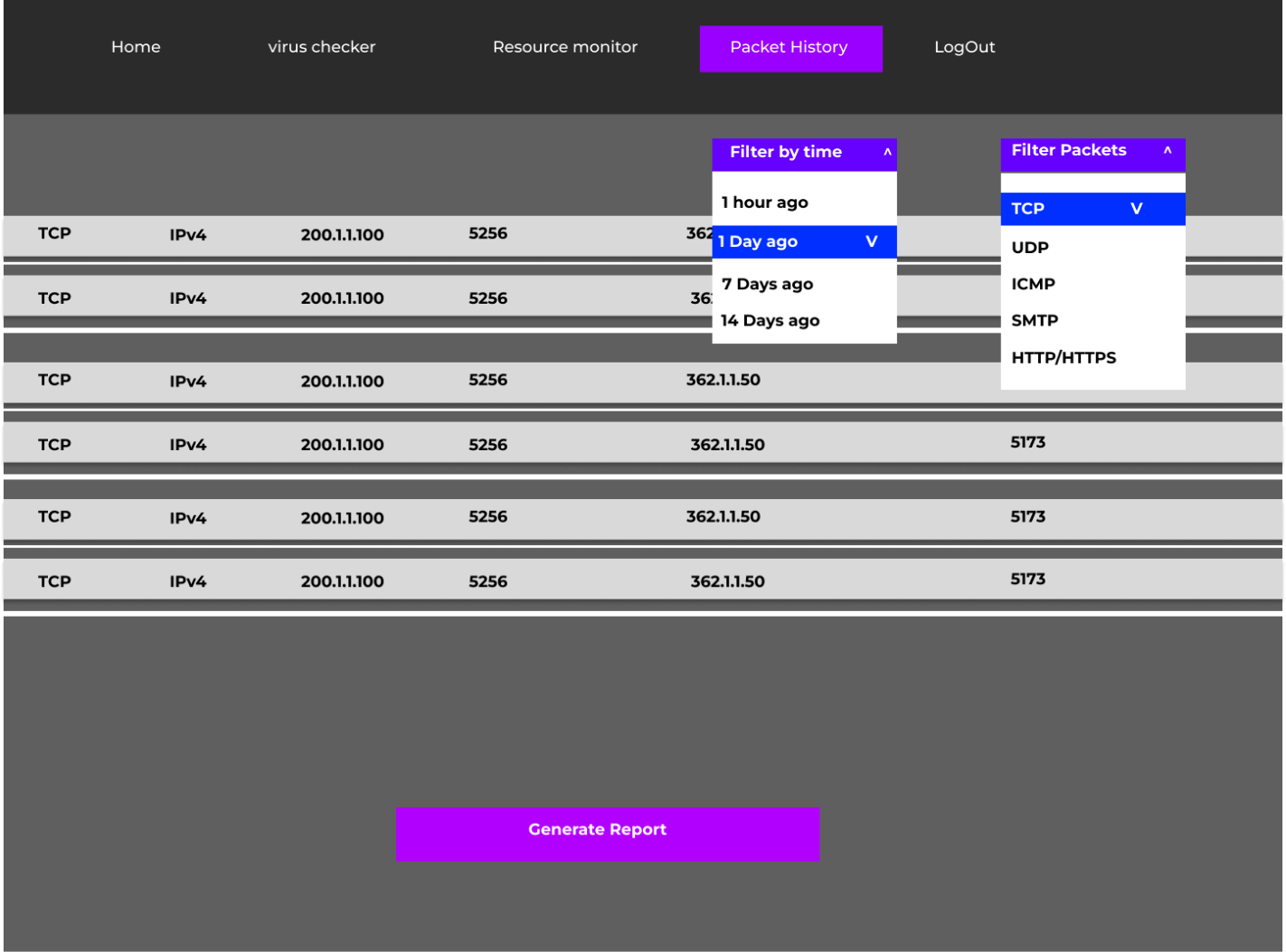
**עמוד אבטחת קבצים**

נבדק

עמוד אבטחת קישורים



נבדק

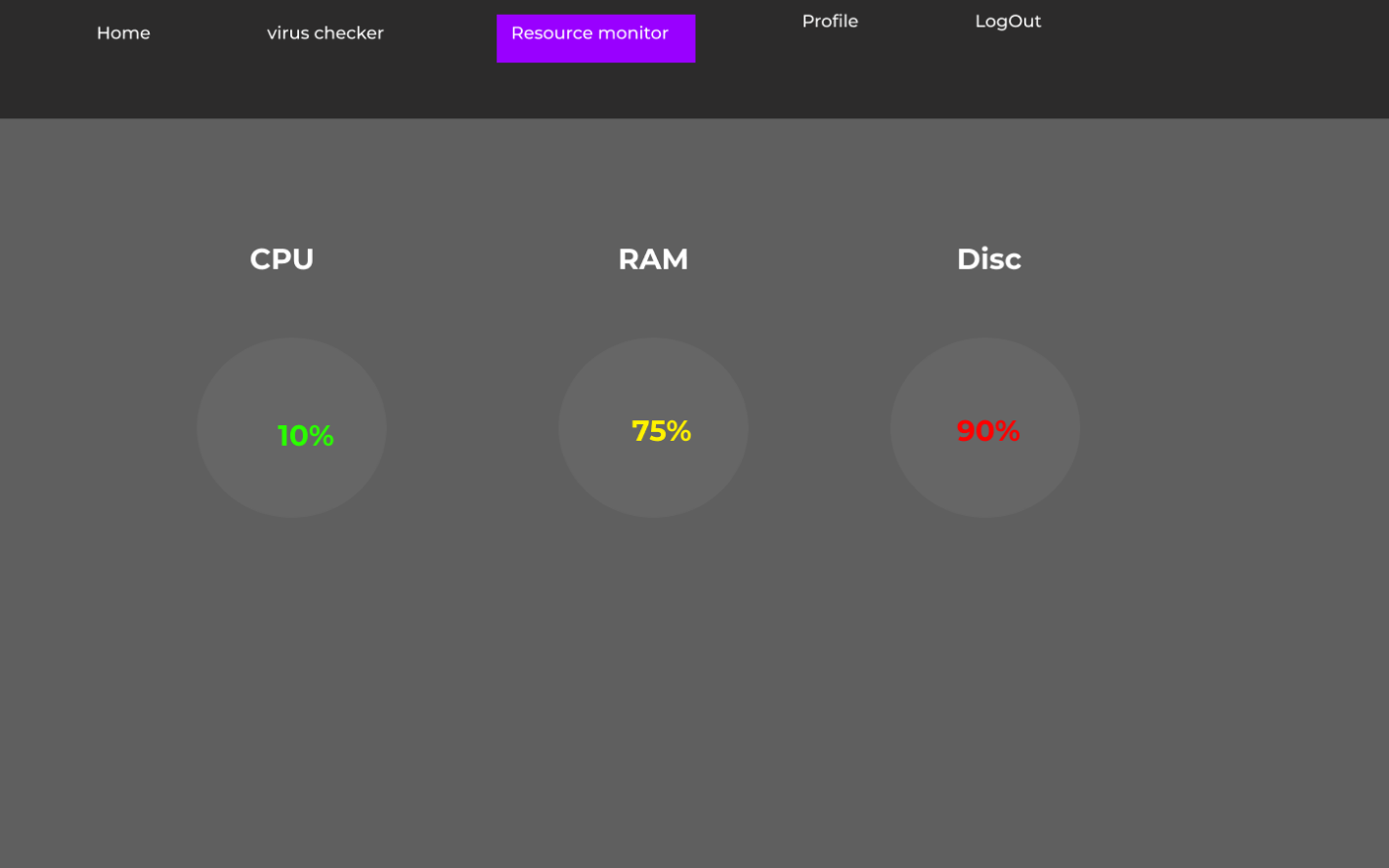
**ממשק דוחות**

נבדק

**ממשק דוחות (יצירת דו"ח)**

נבדק

**עמוד רמת שימוש במשאבי מחשב**



נבדק

## **ממשקים למערכות אחרות/ API**:

**Mailjet API:** API לשם שליחת מיילים למשתמשים בעת שימוש יתר בחומרה, דפוסים זדוניים ו קבצים\קישורים בעייתיים ישלחו התרעות למשתמש.

**Virus Total API:** API שנותן יכולת למשתמשים לבדוק קבצים וקישורים זדוניים ה-API מחזיר תוצאות בדיקת קובץ\קישור ותוכנה שלי משתמשת בהם לשלוח התרעה מתאימה למשתמשים בה.

נבדק

## **שימוש בחבילות תוכנה**:

**PacketDotnet:** ספריה שנותנת לי את הגישה למחלקות שעוזרות לי לשלוף מידע על פקטה

**SharpPcap:** הספריה שעוזרת לשלוף את הפקטות מכרטיס הרשת

**QuestPDF:** ספריה שנותנת לי את היכולת להכין תבניות טפסים שאותם אני שולח דרך המייל

**BCrypt.Net:** ספריה אחראית על הצפנת מידע כגון סיסמאות משתמשים. הספריה מסתמכת על אלגורתמי Hashing לעשות זאת

**MongoDB.Driver:** ספריה שנותנת לי את היכולת לגשת לחלק מהפונקציונאליות של MongoDB

**MongoDB.Driver.Core:** החלק המשלים של MongoDB.Driver שנותנת לי גישה לעוד פונקציונאליות במסד הנתונים

נבדק

# שימוש במבני נתונים וארגון קבצים

## נא פרט את מבני הנתונים.



נבדק

## 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**

נבדק

## **Data flow**

**Context Diagram**



נבדק

**DFD0**

****

נבדק

**DFD1 for P2 – threat Identifications**



נבדק

**DFD1 for P3 – Hardware Threats Identifications.**

****

נבדק

**DFD 1 for P4 – Files Threats Identifications**

****

נבדק

מילונים

מילון ישויות:

|  |  |  |
| --- | --- | --- |
| קוד | שם | תיאור |
| E1 | **משתמש** | **המשתמש שיכול לבצע פעולות במערכת** |
| E2 | Virus total API | **API הנותן את היכולת למשתמש לבדוק אם קובץ מסוים הוא זדוני או לא** |
| E3 | Mailjet API | **API העוזר בשליחת דוחות לדיווח פקטות זדוניים, שימוש יתר, או קובץ זדוני** |

מילון תהליכים:

|  |  |  |
| --- | --- | --- |
| קוד | שם | תיאור |
| P1 | **ניהול משתמשים** | **תהליך המנהל פעולות הכניסה והרישום של משתמשים** |
| P2 | **ניטור וזיהוי איומים** | **פעולה העוזרת לנטר פקטות** |
| P2.1 | **לוכד וניטור פקטות** | **פעולה שלוכדת פקטות ושולחת אותם למנטר לפני החזרתם למשתמש** |
| P2.2 | **שליחת ד"וח** | **פעולה ששולחת ד"וח של תוצאת ניטורי פקטות למייל משתמש** |
| P3 | **ניהול נתוני שימוש במשאבים** | **מנהל התראות לפעולת בדיקת אחוזי שימוש בחומרה.** |
| P3.1 | **מאזין שימוש חומרה** | **מאזין וחשב אחוז השימוש בקומפוננטים של החומרה** |
| P3.2 | **שליחת ד"וח** | **מנהל שליחת דוחות של תוצאות אחוזי שימוש בחומרה** |
| P4 | **בדיקת קבצים** | **מנהל בדיקת קבצים שלמשתמש יש חשש שהם זדוניים** |
| P4.1 | **זיהי קבצים** | **תהליך שמקבל קבצים ושולח אותם ל-API של Virus total לשם בדיקת רמת סכנתו של הקובץ** |
| P4.2 | **שליחת ד"וח** | **תהליך ששולח דוחות המדווחות על סכנת קובץ אשר נבדק דרך שימוש בתהליך מס' 4.1** |

מילון מאגרי מידע

|  |  |  |  |
| --- | --- | --- | --- |
| קוד | שם מאגר | שם הטבלה | שדות הטבלה |
| D1 | **מאגר נתוני משתמש** | **User** | UserId  Name  Email  Password  DateOfBirth |
| D2 | **מאגר פקטות חריגות** | **PacketHistory** | Packet\_ID  Packet\_Type  Source\_IP  Destination\_IP  Source\_Port  Source\_MAC  Destination\_MAC  Direction  IP\_Version  AppLayerData  Danger\_Level  Header\_Length Total\_Length  User\_ID  Packet\_Check\_Time  Description |
| D3 | **מאגר נתוני שימוש** | **ResourceAnomallyHistory** | Anomally\_ID  Device\_ID  BreachedPercentage  TimeStamp |
| D4 | **מאגר פרטי קבצים זדוניים** | **VirusCheckerHistory** | File\_Name  CheckID  IsHarmful  User\_ID  Check\_Time |

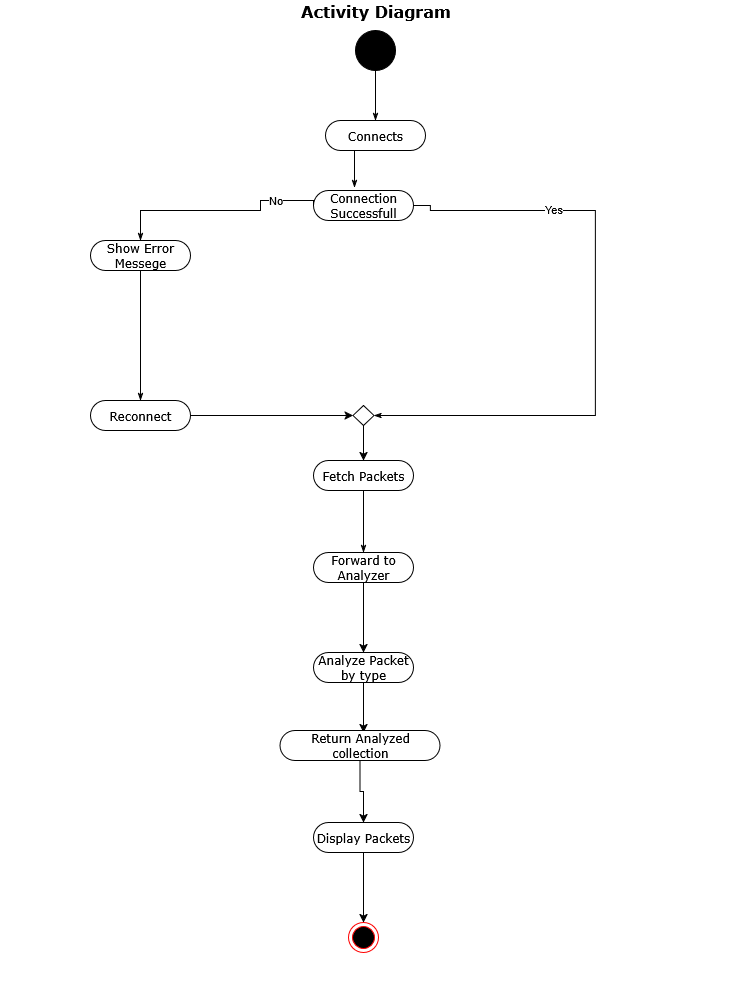
**מילון זרימות מידע**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **קוד** | **שם הזרימה** | **מקור** | **יעד** | **שדות זרימה** |
| F1 | פרטי רישום | 1E | 1P | \*Email  \*Password  Date of Birth  Name |
| F2 | נתוני משתמש | 1P | 1D | \*Email  \*Password  Date of Birth  Name |
| F3 | נתוני אימות משתמש | 1D | 1P | Email  Password |
| F4 | אימות מייל | 1P | 1E | Email  Encrypted password,  Date of birth |
| F5 | נתוני רשת או\ו משאבים | 2P | 2D | משאבים  AvgPercentage  רשת  Packet\_Type  Source\_IP  Destination\_IP  Source\_Port  Destination\_Port  Source\_MAC  Destination\_MAC  Direction  IP\_Version  App\_Layer\_Data  Danger\_Level  Header\_Length  Total\_Length  Packet\_Check\_Time  Description |
| F6 | נתוני ניטור דפוסים | 2D | 2P | Packet\_Type  Source\_IP  Destination\_IP  Source\_Port  Destination\_Port  Source\_MAC  Destination\_MAC  Direction  IP\_Version  App\_Layer\_Data  Danger\_Level  Header\_Length  Total\_Length  Packet\_Check\_Time  Description |
| F7 | פרטי בקשת ניטור שימוש במשאבים | 1E | 3P | Email |
| F8 | פרטי התראת מייל | P3 | E2 | Packet\_Type  Source\_IP  Destination\_IP  Source\_Port  Destination\_Port  Source\_MAC  Destination\_MAC  Direction  IP\_Version  App\_Layer\_Data  Danger\_Level  Header\_Length  Total\_Length  Packet\_Check\_Time  Description |
| F9 | נתוני שימוש יתר במשאבים | 3P | 3D | Email |
| F10 | נתוני שימוש לדוחות וגרפים | 3D | 3P | Packet\_Type  Source\_IP  Destination\_IP  Source\_Port  Destination\_Port  Source\_MAC  Destination\_MAC  Direction  IP\_Version  App\_Layer\_Data  Danger\_Level  Header\_Length  Total\_Length  Packet\_Check\_Time  Description |
| F11 | נתוני קובץ לבדיקה | 1E | 4P | File bytes,  Email |
| F12 | נתוני קובץ לבדיקה | 4P | E3 | File Bytes |
| F13 | נתוני תוצאות בדיקה | 3E | 4P | Anti-Virus-Name  Is malicious |
| F14 | נתוני קבצים זדוניים | 4P | 4D | Name,  Date,  Result,  userId |
| F15 | נתוני תוצאות בדיקה | 4P | 1E | Name,  Date,  Result, |
| F16 | פרטי ברשה לבדיקות תעבורה ומשאבים | 1E | 2P | Session id |
| F17 | פרטי קבצים זדוניים | 4D | 4P | Name,  Date,  Result |
| **נתוני זרימות ל-2P** | | | | |
| F1 | נתוני בקשת ניטור לדקה | 1E | 2.1P | Session id |
| F2 | נתוני פקטות חריגות | 2.1P | 2D | Source\_IP  Destination\_IP  Source\_Port  Destination\_Port  Source\_MAC  Destination\_MAC  Direction  IP\_Version  App\_Layer\_Data  Danger\_Level  Header\_Length  Total\_Length  Packet\_Check\_Time  Description |
| F3 | תוצאות ניטור ל-Frontend | 2.1P | 1E | Source\_IP  Destination\_IP  Source\_Port  Destination\_Port  Source\_MAC  Destination\_MAC  Direction  IP\_Version  App\_Layer\_Data  Danger\_Level  Header\_Length  Total\_Length  Packet\_Check\_Time  Description |
| F4 | נתוני פקטות זדוניים | 2D | 2.2P | Source\_IP  Destination\_IP  Source\_Port  Destination\_Port  Source\_MAC  Destination\_MAC  Direction  IP\_Version  App\_Layer\_Data  Danger\_Level  Header\_Length  Total\_Length  Packet\_Check\_Time  Description |
| F5 | פרטי הודעת מייל | 2.2P | 2E | Email  +  Source\_IP  Destination\_IP  Source\_Port  Destination\_Port  Source\_MAC  Destination\_MAC  Direction  IP\_Version  App\_Layer\_Data  Danger\_Level  Header\_Length  Total\_Length  Packet\_Check\_Time  Description |
| F6 | נתוני פקטות זדוניים | 2.2P | 2D | - |
| **נתוני זרימות ל-3P** | | | | |
| F1 | נתוני בדיקת אחוזי שימוש | 1E | 3.1P | Session id |
| F2 | ממוצעי שימוש חומרה | 3.1P | D3 | AvgCpuUsage AvgRamUsage AvgDiskUsage |
| F3 | אחוזי שימוש חומרה | 3.1P | 1E | cpuUsage,  ramUsage,  diskUsage |
| F4 | נתוני שימוש יתר לתיעוד | P3.1 | D3 | AvgUsage  DeviceName  Standard Deviation |
| F5 | דוח שימוש חריג | P3.2 | E2 | DeviceName  AvgUsagePercentage  UsagePercentage  StandardDeviation |
| F6 | דוח שימוש יתר | P3.2 | D3 | AvgUsagePercentage  DeviceName  StandardDeviation |
| 7F | נתוני שימוש לצורך דוח | 3D | 3.2P | AvgPercentage DeviceName  StandardDeviation |
| **נתוני זרימות ל-4P** | | | | |
| F1 | נתוני קובץ לבדיקה | 1E | 4.1P | File bytes,  Email |
| F2 | נתוני קובץ כסיביות | 4.1P | 3E | File bytes |
| F3 | תוצאת בדיקה | 3E | 4.1P | MaliciousFlagNumber,  OkFlagNumber |
| F4 | תוצאות בדיקה של קובץ זדוני | 4.1P | 4D | FileName  Date of Check  Num\_Of\_Detections,  Num\_Of\_Evasions |
| F5 | פרטי קבצים שנשמרו | 4D | 4.2P | UserId |
| F6 | נתוני מייל לדיווח | 4.2P | 2E | Email,  FileName,  Date of Check,  Num\_Of\_Detections,  Num\_Of\_Evasions |

נבדק

# תיאור המרכיב האלגוריתמי – חישובי

**Activity Diagram:   
Packet Capture and Analysis – Real Time Flow**





לפרק את אחד מה types ולעשות את התרשים עליו. לדוגמה tcp Packet Analysis

## **איסוף מידע וניתוחים סטטיסטיים (אנליטיקות)**

באפליקציה זו איסוף נתונים על מנת להעיר על אנומאליות הוא עיקר ישנו אוסף של מקרים שבהן ניתן לאסוף נתונים על מנת שדיווחינו למשתמש יהיו מדויקים יותר אותם נתונים נמצאים בטבלה הנ"ל (לסדר את הניסוח הוא לא ברור)

לרדת לרזולוציה טכנית כיצד מבוצע ניתוח הנתונים ואיסוף הנתונים על הפקטות.

כותרות אחידות

|  |  |
| --- | --- |
| **סוג מידע** | **למה הוא חשוב** |
| אחסון ממוצעי שימוש במשאבי מחשב. | הנני מאחסן את הנתונים הללו לשם זיהוי אנומאליות בשימוש משאבים אותם ממוצעים גם מאוחסנים עם סטיית תקן לשם דיווח מדויק יותר על שימוש יתר |
| נתוני בדיקת קבצים | על מנת לתת גישה למשתמש לראות את היסטורית הקבצים אשר הוא בדק אנו שומרים את שם הקובץ, תאריך ביצוע המשתמש לבדיקה, ואת תוצאת הבדיקה במסדי הנתונים |
| נתוני דפוסים חשודים | נתוני דפוסים חשודים נשמרים במסד נתונים לשם גישה להיסטורית הפקטות ולשם זיהוי "פטרנים" חשודים |
| נתוני משתמש | נתוני משתמש כמו מייל סיסמא מוצפנת נשמרים במסד הנתונים משום שהתכנה מספקת את היכולת לאוסף של משתמשים להשתמש בה אותה תכנה צריכה לספק את היכולת לצור יותר מפרופיל אחד |

# תיאור/התייחסות לנושאי אבטחת מידע

אצלנו הפריטים הרגישים ביותר הם פרטי המשתמש בעיקר סיסמאות הפרופילים שהמשתמשים יצרו. בשל הצפנת הסיסמאות השתמשנו בספריית BCrypt.Net בצד השרת לשם ביצוע Hashing לסיסמאות אלו (ניסוח – לא מבינים מה קוראים)

# משאבים הנדרשים לפרויקט:

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

|  |  |
| --- | --- |
| **שעות** | **מטרה** |
| 50 | איסוף מידע ולימדה על ספריות |
| 150 | תכנות צד לקוח client |
| 150 | תכנות שרת server |
| 100 | בדיקות עבודת שירותי התוכנה |

צריך להיות עד 300 שעות לאחד

## **ציוד נדרש**

החומרה הנדרשת עבור הפרויקט :-

* ווינדוז 10 או 11
* מעבד עובד ברמת intel core i3

נבדק

## **תוכנות נדרשות**

Visual Studio Code

Dotnet cli

Nodejs

MongoDB Shell

MongoDB Compass

MongoDB Server

PostMan  
נבדק

## **ידע חדש שנדרש ללמוד לצורך ביצוע הפרויקט**

* Sockets
* מבנה דפוס אינטרנטי
* MailjetAPI
* VirusTotalAPI

## **ספרות ומקורות מידע**

* PacketDotNet: https://github.com/dotpcap/packetnet
* SharpPcap:https://github.com/dotpcap/sharppcap
* Mailjet: https://dev.mailjet.com/content/guides

# תכנית עבודה ושלבים למימוש הפרויקט

|  |  |  |
| --- | --- | --- |
| 1. | קבלת החלטה על נושא הפרויקט והתנעה ראשונית | 12.2024 |
| 2. | כתיבת הצעה/ניתוח פרויקט וממשקים | 12.9.2025 |
| 3. | Code Review 1 + מסירת ספרי פרויקט | 12.9.2025 |
| 4. | Code Review 2 – ועדה פנימית (מועד הגנה?) | 15.10.2025 |

נבדק

הכותרות צריכות להיות אחידות

# תכנון הבדיקות שיבוצעו

|  |  |
| --- | --- |
| **תיאור הבדיקה** | **התנהגות צפויה** |
| הכנסת פרטי רישום עם מייל תקין וסיסמה חוקית | השרת מחזיר קוד ,HTTP 200 OK  המשתמש נוסף למסד הנתונים בהצלחה |
| הכנסת פרטי רישום עם סיסמה לא תקינה (לא עומדת ב־REGEX) | השרת מחזיר קוד HTTP 400עם הודעת שגיאה על תקינות הסיסמה |
| בדיקת תגובה לשרת להכנסת נתוני משתמש שכבר קיים | השרת צפוי להחזיר 400 בקשה לא תקינה כי המשתמש אשר הוקלד כבר נמצא |
| המשתמש מזין קישור זדוני בשדה ולוחץ על הכפתור "Check Url" | מתקבל מייל אוטומטי למשתמש עם דוח סריקה מפורט: שם הדומיין, תאריך ושעה, מספר מנועים שסימנו כ-malicious, מספר מנועים שסימנו כ-harmless/undetected והמלצה לבדוק שוב את המקור, מוצגת גם הודעה בממשק שהקישור מסוכן |
| המשתמש מזין קישור תקין בשדה ולוחץ על הכפתור "Check Url" | מתקבל מייל אוטומטי למשתמש עם דוח סריקה שמציג 0 מנועים זדוניים, מספר מנועים harmless/undetected והודעה שהקישור בטוח, בממשק מוצגת הודעה שהקישור בטוח |
| המשתמש מזין קישור חשוד בשדה ולוחץ על הכפתור "Check Url" | מתקבל מייל עם דוח סריקה שמציין את מספר המנועים שסימנו כ-Suspicious, מוצגת גם הודעה בממשק שהקישור חשוד |
| המשתמש מעלה קובץ זדוני דרך "File Checker" | מתקבלת הודעה שהקובץ מסוכן כולל מספר מנועים שזיהו אותו, ונשלח דוח PDF למייל |
| ברקע: מתבצע ניטור פקטות רשת, מזוהה דפוס התקפה (למשל TCP FLOOD) | הפקטות החשודות מסומנות כחשודות/זדוניות, ומתווספות לדוח פקטות חשודות, ונשלח דוח PDF למייל |
| ברקע: מתבצע ניטור חומרה, מזוהה שימוש חריג ב- (CPU,DISC,RAM) | נוצר דוח PDF עם נתוני השימוש החריגים ונשלח למייל המשתמש |
| ברקע: מתקבלות פקטות חדשות מהשרת (SignalR) | הרשימה מתעדכנת אוטומטית ומוצגות הפקטות החדשות |
| המשתמש לוחץ על כפתור סינון ובוחר "TCP" | ברשימה מוצגות רק פקטות מסוג "TCP" |
| המשתמש לוחץ על פקטה מסויימת ברשימה | נפתח חלון פרטים עם מידע על הפקטה שנבחרה |
| המשתמש משנה משנה את הסינון כאשר יש פקטה מסומנת | בחירת הפקטה מתאפסת (החלון נסגר) |

נבדק

|  |  |
| --- | --- |
| ??????? |  |
|  |  |
| 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:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_