

אפיון פרויקט

הגנת סייבר

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

**שם מנחה: אופיר שביט**

**נושא הפרויקט: פלטפורמת תצפית שקטה על פעילות עובדים בחברה**

תמונה שמכילה טקסט, לוגו, גופן, גרפיקה

התיאור נוצר באופן אוטומטי**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.
  + 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 תהליך 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.

תמונה שמכילה טקסט, לוגו, גופן, גרפיקה

התיאור נוצר באופן אוטומטי

**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 פעולותיי 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.

**תמונה שמכילה טקסט, צילום מסך, גופן, מספר

התיאור נוצר באופן אוטומטי**





תמונה שמכילה טקסט, לוגו, גופן, גרפיקה

התיאור נוצר באופן אוטומטי**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 תהליכי user mode, 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. מעבר לכך על הפרויקט להשתמש בסוגי הצפנות שונים בכדי להעביר את המידע בצורה מאובטחת לצד השרת. המערכת איננה עוסקת באבטחה של מערכות הפעלה (כמו שצוין AntiVirus), שמירת סיסמאות בתוך DB ועוד...



* תמונה שמכילה טקסט, לוגו, גופן, גרפיקה

  התיאור נוצר באופן אוטומטי**פירוט תיאור המערכת (אפיון)**

**תיאור מפורט של המערכת**

* + המערכת הינה מערכת האזנה שקטה על מחשבים במערכת הפעלה לינוקס. היא תהייה אחראית על האזנה למתודות שונות במערכת ההפעלה והסתרה שלה בתוך מערכת ההפעלה כך שלאחד העובדים בחברה שאין לו הרשאות גבוהות על אותו מחשב לא יוכל בכלל לדעת שהתוכנית נמצאת לו על המחשב, וגם אם כן מודע לכך לא תהייה באפשרותו כלל למחיקה של התוכנה והפסקת עבודתה. בזכות האזנה של המערכת למחשב העובד היא תוכל לשלוח מידע על פעילות המחשב, וכך המנהל של העובד ידע אם העובד שלו מבצע את עבודתו כראוי. המידע ישלח למחשב של המנהל, שם הוא יוכל להסתכל על המידע של כל עובד בנפרד באופן מסודר, ובכך יוכל באופן יעיל לתצפת על עובדיו מבלי שיצטרך להתאמץ ולבזבז זמן וכסף מיותר על עובדיו, המערכת מייעלת את העבודה של המנהל.

****

**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, הנתונים יכללו בתוכם – מקשי מקלדת, לחיצות עכבר, צילומי מסך, שמע ועוד... 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.

תמונה שמכילה טקסט, לוגו, גופן, גרפיקה

התיאור נוצר באופן אוטומטי**פירוט יכולות המערכת**

1.האזנה שקטה על מחשב המשתמש.

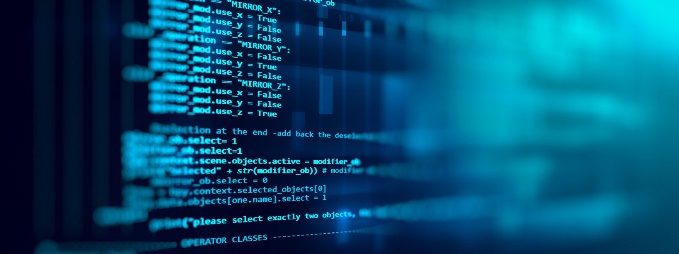
2.איסוף מידע בזמן אמת מן מחשב המשתמש.

3.שליחת מידע של מחשב המשתמש אל מחשב השרת.

4.איסוף המידע במחשב השרת אל תוך DB.

5.הצגת המידע באופן נגיש במחשב השרת.

|  |  |
| --- | --- |
| 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 ב user-mode * 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 |

תמונה שמכילה טקסט, לוגו, גופן, גרפיקה

התיאור נוצר באופן אוטומטי



|  |  |
| --- | --- |
| 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 באופן מוצפן   **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 |

תמונה שמכילה טקסט, לוגו, גופן, גרפיקה

התיאור נוצר באופן אוטומטי



|  |  |
| --- | --- |
| 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 על ידי פענוח המידע המוצפן. * 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 |

תמונה שמכילה טקסט, לוגו, גופן, גרפיקה

התיאור נוצר באופן אוטומטי



|  |  |
| --- | --- |
| הצגת המידע באופן נגיש במחשב השרת | שם היכולת |
| הצגת המידע באופן נגיש במחשב השרת 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 השרת**   * איסוף המידע מן הלקוח על ידי פענוח המידע המוצפן. * פענוח המידע לפי הפרוטוקול * הכנסה ל DB את הערכים של הלקוח ממנו נשלחה ההודעה * הצגה באופן ויזואלי על ידי GUI את נתוני ה DB בזמן אמת | אוסף פעולות/יכולות הנדרשות ליכולת הנ"ל |
| * מחשב לקוח * Socket * מחשב שרת * טבלת DB אצל השרת * GUI במחשב השרת | אובייקטים נחוצים |

 תמונה שמכילה טקסט, לוגו, גופן, גרפיקה

התיאור נוצר באופן אוטומטי

תמונה שמכילה טקסט, לוגו, גופן, גרפיקה

התיאור נוצר באופן אוטומטי

* **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 כ"מנהל" 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. |

תמונה שמכילה טקסט, לוגו, גופן, גרפיקה

התיאור נוצר באופן אוטומטי**4. בדיקת אבטחת הנתונים**

|  |  |
| --- | --- |
| מטרה | לוודא שהנתונים המועברים לשרת מוגנים ולא חשופים לגורמים חיצוניים. |
| איך אבדוק | אשתמש בהצפנה להעברת המידע ואבחן פרוטוקולי תקשורת מאובטחים (AES RSA) על מנת לוודא שהנתונים נשארים חסויים.  אני מתכנן לבצע כל בדיקה עם רישום מפורט של התוצאות, כך אוכל להבין איפה יש צורך בשיפור ולהציג את הממצאים כחלק מהפרויקט החינוכי. |





**תכנון וניהול לוז – להמיר לטבלאות ולפרט יותר**

**שלב 2: תכנות**

* + להתמקד בעיקר בכתיבת הקוד. להתחיל לקודד את התכונות שתכננתי, ולעבוד על כל הפונקציות המרכזיות.לזהות את התכונות שאני רוצה לכלול בפרויקט שלי ואכין מתווה ראשוני.
  + להקדיש זמן למידה וכתיבה של קוד בצורה מסודרת כדי להבטיח שהוא יציב וניתן להרחבה.
  + לבצע ניסויים על ה-hooks ולזהות אילו מהם נחוצים עבור הפרויקט
  + לבצע תיקונים ושיפורים בקוד לאחר הבדיקות והניסויים.

**שלב 1: תכנון והכנות**

* + ללמוד על הטכנולוגיות והכלים השונים שיכולים להיות שימושיים.
  + לזהות את התכונות שאני רוצה לכלול בפרויקט שלי ואכין מתווה ראשוני.
  + לתכנן את הקוד באופן כללי, להגדיר את הפונקציות העיקריות ולבנות את המבנה הכללי של הקוד.

תמונה שמכילה טקסט, לוגו, גופן, גרפיקה

התיאור נוצר באופן אוטומטי

**שלב 3: תיעוד וסיכום**

* + לתעד את הקוד ואת הצעדים שביצעתי, כולל הסברים על הפונקציות והיכן הן נמצאות בקוד.להקדיש זמן למידה וכתיבה של קוד בצורה מסודרת כדי להבטיח שהוא יציב וניתן להרחבה.
  + להכין מדריך למשתמש שיסביר כיצד להפעיל את התוכנה ואילו דרישות יש למערכת.
  + לכתוב סיכום של הפרויקט, כולל אתגרים שהיו בדרך, פתרונות שנמצאו ולמידה מהתהליך.

**ניהול סיכונים**