בס''ד

**מטלה מעבדת הגנה**

**Process Monitor**

הדר אלון 205749211

הסבר על הספריות:

**Psutil –**

ספריה זו תומכת בwindows ובlinux כאחד.

השתמשתי בספריה זו על מנת לקבל את כל התהליכים שרצים. השתמשתי בה בעיקר במוניטור והשתמשתי בפונקצית process\_iter() שבמחלקה process המציגה את כל הפרוססים ברגע הנתון.

**WatchDog –**

ספריה זו תומכת בwindows ובlinux כאחד.

השתמשתי בספריה זו על מנת לספק שירותים של watch service על מנת להגן על הקבצים על ידי כך שבכל פעם שנעשית מחיקה, יצירה או העברה של קובץ – מתקבלת התראה על כך ובכך נדע האם מישהו עשה שימוש בקבצים שלי מבלי ידיעתי.

במכוון לא רציתי שאקבל התראה על כתיבה לתוך הקובץ מכיוון שלא אוכל לדעת מתי אני ערכתי את הקובץ ומתי מישהו מבחוץ ערך אותו ולכן בכל פעם דגמתי את מועד השינוי האחרון ובכל קריאה או כתיבה לקובץ דאגתי לבדוק שלא נעשתה איזושהי כתיבה או קריאה לקובץ(על ידי מישהו חיצוני) בזמן שונה מהזמן דגימה האחרון ששמרתי קודם לכן.

**Stat –**

ספריה זו תומכת בwindows ובlinux כאחד.

השתמשתי בספריה זו על מנת להפוך את הקבצים שלי לReadOnly בין כל דגימה כך שבתחילת דגימה ביטלתי את ההגבלה ובסיומה הגבלתי שוב.

אמנם מי שרוצה לחבל באמת בקבצים יוכל להוריד במאפיינים את ההגבלה אך עדיין קיימת האפשרות ולו הקטנה ביותר שהוא ישכח או לא יספיק לערוך ולשנות את מה שרצה לפני שהקובץ חזר להיות ReadOnly .

דרכים להתגוננות:

הדרכים להתגוננות שהשתמשתי בהם הם ReadOnly , LastModified , והתראות על יצירה מחיקה והעברה של הקבצים.

כל זאת מעלה התראה על ידי כתיבת הפעולה בconsole .

דרכים נוספות שחשבתי להשתמש בהן ולא מצאתי דרך :

* להפוך את הקבצים לhidden
* לייצר לקבצים גישה רק על ידי סיסמא
* והצפנה של הקבצים

הסבר על המחלקות:

**Files\_Handler –**

מחלקה זו תפקידה להגדיר את הפעולות שהמערכת תעשה כאשר יתבצעו שינויים לא רצויים בקבצים המתועדים של המוניטור.

המחלקה יורשת מהמחלקה PatternMatchingEventHandler אשר שייכת לספריה WatchDog אשר פירטתי עליה קודם ובספריה Time .

**Monitor –**

המחלקה הראשית .

במחלקה זו כל הפרוייקט מתבצע.

היא כותבת וקוראת לתוך קובץ נוכחי(ProcessList ) שבו נתעד ונוסיף בכל פעם את התהליכים המתבצעים במערכת.

תוך כדי כך היא בכל דגימה מכניסה לתוך List את התהליכים האחרונים שלה אשר אותם היא משווה לתהליכים הבאיםהנוכחים.

לאחר מכן מתבצעת דגימה נוספת על התהליכים הנוכחים ומתבצעת השוואה בין התהליכים הנוכחים לבין התהליכים שנמצאים בList שהגדרנו קודם לכן.

כל התהליכים שהשתנו (התווספו או נמחקו) נרשמים לתוך הקובץ החדש(Status\_Log ) אשר מתעד את כל התהליכים שעברו שינוי.