*-Process Monitor*

***(מצורפים בתיקייה הקוד וכל קבצי הטקסט הרלוונטיים***)

ה- Process Monitor הוא כלי שמנטר את התהליכים הרצים במערכת ומדווח על שינויים שהתבצעו, אם תהליך שרץ נסגר או נוספו תהליכים חדשים.

בתוכנית ישנן שימוש בספריות הבאות:

* psutil – ספריה המספקת ממשק לאחזור מידע על כל התהליכים הפועלים ושימוש במערכת (CPU, זיכרון, דיסקים, רשת, משתמשים) באמצעות python.
* Time
* Datetime
* base64- ספריה ב- python שמאפשרת להצפין ולפענח מידע באמצעות הקידוד base64 שהיא שיטת קידוד נתונים המייצגת נתונים בינאריים בפורמט טקסטואלי.
* os- מספק דרך ניידת לשימוש במערכת ההפעלה התלויה בפונקציונליות. במטלה, מאפשר גישה לקבציי הטקסט ולמחיקה.
* Platform- גישה לנתונים מזהים של הפלטפורמה הבסיסית. במטלה, מאפשר להגדיר תנאים על מנת שיוכל לעבוד עם מ"ה windows או Linux (בודק איזו מ"ה קיימת ובהתאם מפעיל את הפקודה המתאימה).

על מנת להפעיל את התוכנית הראשית יש להזדהות ע"י שם משתמש וסיסמא. במידה ואחד משדות הזדהות שגוי, לאחר 3 ניסיונות התוכנית מסתיימת.

(שם משתמש: Admin, סיסמא: Pr00ce55M0n!70R)

בנוסף, על מנת להתגונן מפני האקרים הקבצים מוצפנים ורק למי שיש את "המפתח" יכול לראות את הפיענוח שלהם, כלומר להבין שזה לפי base64.

על מנת לאפשר למשתמש לנווט בנוחות בין המצבים, ישנו תפריט UI לכלי.

בתוכנית הראשית ישנן ארבע אפשרויות:

1. יצירת הקבצים המוצפנים (processList ו- Status\_Log).

(ראשית יש את MonitorEncode אשר מקבלת משתנה X שמייצג את הזמן המנוחה (sleep) בין דגימה לדגימה. הפונקציה יוצרת את הקבצים המוצפנים (processList ו- Status\_Log). השתמשתי במבנה נתונים dictionary , כאשר המפתח הוא ה-pid (כיוון שהוא ייחודי לכל תהליך) והערך הוא מחרוזת של שם התהליך, סטאטוס וזמן. השתמשתי בכתיבה לקובץ על מנת ליצור את הקובץ ולצרף אליו כל פעם את התהליכים שרצים).

1. יצירת פיענוח של הקבצים המוצפנים.

(לאחר מכן יש את MonitorDecode שנועד לפענח את הקבצים שיצרנו. גם כאן יש שימוש בכתיבה לקובץ. בנוסף יש קריאה מהקובץ המוצפן ל-list וכל שורה הוא מפענח וכותב את הפענוח לקובץ חדש).

1. מצב מנוהל (ידני)- שימוש בקובץ processList על מנת לטעון 2 דגימות מטווחי זמן שונים ולבצע השוואה. התכנית תקבל תאריך ושעה לשני אירועים, תטען מהקובץ את 2 הדגימות, ותציג שינויים בדומה למצב הmonitor-. אם לא קיימת דגימה מטווח הזמן המדויק, זה מוציא דגימה מהזמן הבא הקרוב ביותר.
2. מחיקת כל הקבצים שנוצרו.
3. יציאה מהתוכנית.

* הכלי הינו cross platform – תומך גם במערכת ההפעלה Windows וגם במערכת ההפעלה Linux.
* יש לגרור את קבצי הטקסט לתוך התוכנית על מנת לראות את ה- UI בצורה מלאה.