מעבדת סייבר - הגנה
מטלת תכנות Process Monitor חלק שני

בהמשך למטלה הקודמת, נרצה להוסיף את המצב הבא:

<u>מצב ידני</u> – במצב זה נרצה להשתמש בקובץ processList על מנת לטעון 2 דגימות מטווחי זמן שונים ולבצע השוואה. התכנית תקבל תאריך ושעה ל2 אירועים, תטען מהקובץ את 2 הדגימות, ותציג שינויים בדומה למצב הmonitor (תהליך חדש שנוצר בדגימה העדכנית יותר, תהליך שכבר אינו רץ בדגימה העדכנית יותר וכו'). אפשר להסתמך על קירוב השעות, כלומר אם אין דגימה מטווח הזמן המדויק, אז לעגל בהתאם לרצונכם.

בנוסף, נרצה לייצר ממשק משתמש:
<u>UI</u> – כדי לאפשר למשתמש לנווט בנוחות בין המצבים, צרו תפריט UI לכלי. לא חובה GUI, אפשר גם תפריט command line.

<u>דגשים חשובים:</u>
- מזכירים שאנחנו בקורס הגנת סייבר. ולכן אנחנו שמים דגש רב על הגנת הכלי שלנו. עצם המטרה של הכלי, ברור לנו שהאקרים ירצו לחבל לנו בפעולתו כדי להקשות עלינו. בזמן ריצת הכלי אנחנו כותבים ל2 קבצים וסומכים על המידע שבהם. נסו לחשוב כיצד לבדוק ולהקשות על האקר לחבל לנו בקבצים אלה ולשנותם. במידה והצליח, התריעו על כך למשתמש כדי שיזהה את הפעולה.

- אנחנו משאירים לכם את הדרך למימוש הכלי כרצונכם. עם זאת, אנחנו שמים דגש על מודולריות התוכנה. כתבו את הכלי בצורה מודולרית ומסודרת וחישבו איך אתם מחלקים אותו למחלקות מתאימות, כך שאם נבקש מחר להוסיף/להוריד מאפיינים בתוכנית, לא תאלצו לשנות את רוב הקוד שלה.

- הכלי מיועד להיות cross platform – כלומר לרוץ גם על מערכת ההפעלה Windows וגם על מערכת ההפעלה Linux. אנא השתמשו בלינוקס בהפצת Ubuntu.

- הכלי מיועד לבדיקה עבור שרת בודד ולא עבור רשת, כלומר הכלי ינטר את התהליכים הרצים על אותו מחשב המריץ את התוכנה.

- *<u>אתם מוזמנים להרחיב את התכנית עם כל דבר מיוחד ומעניין שלדעתכם יכול להוסיף לה.</u>*
  <u>(דברים מעניינים ויצירתיים הם כיוון טוב לבונוס).</u>

<u>הגשה:</u>
נא להגיש את המטלה בקובץ rar/zip עם שם מלא.
יש לצרף בהגשה מסמך word המפרט על המבנה של התוכנית שלכם, ספריות שעשיתם בהן שימוש ולאיזו מטרה, פירוט על המחלקות ומבני הנתונים שהשתמשתם בהם, דרכים להתגונן מפני האקרים (כפי שציינו בדגשים), וכל דבר מיוחד שהוספתם.

בהצלחה!