מעבדת סייבר - הגנה
מטלת תכנות Process Monitor חלק ראשון

במטלה זו נפתח כלי שינטר לנו את התהליכים הרצים במערכת, וידווח על שינויים שיכולים להיות קריטיים עבורנו כאנשי SOC. בדומה לכלי Zenoss שהכרנו - המנטר לנו שירותים.

את הכלי נפתח בשפת פייתון, ומצורפים לכם חומרי לימוד על השפה. ההמלצה שלנו היא לצפות בסרטון המעביר את בסיס השפה, להכיר את השימוש במבני הנתונים שלה (כלול בסרטון), ולאחר מכן לתכנן את התרגיל. בשלב זה, נבנה את מצב המוניטור.

<u>מצב מוניטור</u> – עבור X זמן שהמשתמש קובע, התוכנית דוגמת כל X זמן את כל התהליכים הרצים במחשב, ומציגה האם נצפה שינוי מהדגימה הקודמת. כלומר האם יש process שכבר אינו רץ, או האם יש process חדש שרץ במערכת. על כל שינוי שהתקיים יש להתריע למשתמש בממשק.

במצב זה נכתוב ל2 קבצי לוג שונים:
processList – לקובץ זה נדפיס את דגימות הפרוססים שכרגע רצים (בכל פעם את הדגימה האחרונה). בכל פעם קובץ זה יתמלא בכל דגימה שלנו, וישמור את כל הדגימות שעשינו במהלך מצב המוניטור לפי זמן.
Status_Log.txt – קובץ לוג זה הוא למטרת מעקב. נדפיס לקובץ כל שינוי שהוצג לנו במצב המוניטור. לדוגמה process חדש שנוצר, process שהפסיק לעבוד וכו'. במילים אחרות: כל מה שהודפס לממשק המשתמש בטרמינל במצב המוניטור יודפס ללוג זה.

<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>

הגשה:

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.

פייתון:

במטלה זו נעשה שימוש בפייתון 2.7 שתוכלו להוריד מהלינק הבא:

https://www.python.org/ftp/python/2.7.13/python-2.7.13.msi

בלינוקס הוא מותקן כבר מראש.

כמו כן אנחנו ממליצים להשתמש בPycharm כIDE (גירסת הcommunity היא חינמית כקוד פתוח). הוא הכי נוח, ומאפשר גם להוריד ספריות ישירות מהממשק שלו.

https://www.jetbrains.com/pycharm/download

סרטון מעולה לבסיס שצריך לפייתון בפחות משעה:

https://www.youtube.com/watch?v=N4mEzFDjqtA

דוגמאות לsyntax שונים בפייתון שיוכלו לעזור לכם:

https://www.tutorialspoint.com/python/index.htm

בהצלחה!