מעבדת סייבר - הגנה  
מטלת תכנות Process Monitor

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.  
  
לכלי שלנו יהיו כמה מצבים:  
  
מצב מוניטור – עבור X זמן שהמשתמש קובע, התוכנית דוגמת כל X זמן את כל התהליכים הרצים במחשב, ומציגה האם נצפה שינוי מהדגימה הקודמת.   
שינויים שנרצה להתריע עליהם:  
1) האם יש פרוסס חדש שנוצר בדגימה האחרונה שלנו?  
2) האם יש פרוסס חדש שכבר אינו רץ בדגימה האחרונה שלנו אל מול הדגימה הקודמת?  
3) האם יש פרוסס שבבמוצע מנצל יותר RAM מהרגיל? (בצעו ממוצע כלשהו לבחירתכם על שימוש הRAM לתהליך ספציפי והציגו האם יש שינוי משמעותי בניצול הRAM). כמובן שבגלל שמדובר בממוצע, התרעות מסוג זה נרצה להציג על פני טווח של מספר דגימות ולא בין כל 2 דגימות.  
4) האם נוצר לתהליך כלשהו תהליך בן (child process)? לעיתים היווצרות של תהליך בן יכולה להיות פעולה זדונית (נתקל בזה במהלך הקורס). התריעו על תהליך בן חדש שנוצר, וציינו מי האבא.  
  
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.   
  
מצב ידני – 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.  
  
UI – כדי לאפשר למשתמש לנווט בנוחות בין המצבים, צרו תפריט UI לכלי. לא חובה GUI, אפשר גם תפריט command line.   
  
דגשים חשובים:  
- 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.

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

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!