**מטלה 2 מעבדת סייבר הגנה**

**מגישים:**

**בר גניש 313174583**

**נור 206610966**

**לכלי שלנו 2 מצבים:  
מצב מוניטור – המשתמש בוחר כל כמה זמן הוא רוצה שהכלי יבדוק אילו סרוויסים רצים במערכת ובודק אילו שינויים חלו בין הדגימה הנוכחית לאחרונה,  
סרוויסים שעבדו והפסיקו לעבוד והפוך ומתריע למשתמש על כל שינוי, נוסף לכך הכלי רושם את כל הסרוויסים שרצים לקובץ serviceList עם תאריך ושעה ואת השינויים הוא שומר בקובץ לוג ששמו status\_log.**

**מצב ידני – הכלי מקבל 2 תאריכים ולוקח מהstatus\_log את הנתונים על שני התאריכים הנ"ל ומשווה ביניהם, מה שעובד בתאריך הנוכחי והפסיק לעבוד בתאריך הישן יוצג בתור תהליך חדש שהתחיל לעבוד ומה שלא עובד כרגע אך עבד בתאריך הישן יוצג בתור סרוויס שהפסיק לעבוד, המצב הזה לא רושם לשום קובץ לוג אך מדפיס כמובן למשתמש את ההבדלים.**

**הספריות שבהן השתמשנו הן:**

**Os- לצורך הרצת פקודות מערכת מפייטון**

**Platform- לצורך זיהוי המערכת הפעלה שלנו**

**Time- לצורך הפעלת טרד ש"מרדים" את הכלי כל כמה שניות שהמשתמש בחר למען מצב המוניטור**

**Subprocess- לצורך הפעלת פקודות מערכת ברקע וללא פלט**

**בקובץ הראשי שמריצים run.py יש לנו רק מחלקה אחת אך מלא פונקציות:**

**Main- הmenu שמריץ את הכלי**

**Dif- בודק מה ההבדל בין 2 קבצים למען כתיבה בstatus\_log את השינויים במצב מוניטור**

**Difmanual- בודק מה ההבדל בין 2 תאריכים בstatus\_log למען השוואה במצב ידני**

**Findlast- שומר קובץ חדש שבו הדגימה האחרונה מהservicelist**

**Delete- מוחק את ה+ים שמופיעים כשרואים את הסרוויסים הרצים בווינדוס**

**remove\_spaces- מוחק את הרווחים שאנו מקבלים כשאנו מקבלים משום מה בwindows במצב מוניטור**

**Findpos- מוצא תאריך מסויים מהservicelist ושומר אותו בקובץ חדש, נעזרים בזה במצב הידני**

**Check\_files- בודק שלא שינו את הקבצים שלנו ואם שינו הוא מתריע למשתמש ויוצא מהתוכנית**

**Update\_duc1- מעדכן את גיבוי הserviceList לאחר ששינינו אותו**

**Update\_duc2- מעדכן את גיבוי הstatus\_log לאחר ששינינו אותו**

**ישנם קבצי עזר dontrun.sh שהוא הקובץ שמטפל במוניטור בלינוקס(כך ניסיון להעביר אותו לפייטון קרס אפילו השארנו את הניסיונות בהערות)**

**ישנו עוד קובץ codes.py שהוא קובץ שמריץ הdontrun.sh כל הפונקציות שיש בו יש גם ב.run.py**

**דרך ההתגוננות שלנו מפני האקרים היא לשמור את כל תוכן הקבצים בכלי וכל הזמן לבדוק שאין שינוי, כמובן שכשאנחנו משנים את הקבצים אנחנו מעדכנים את התוכן.**

**יש לנו באג בהגנת הקבצים אז כרגע ביטלנו את ההגנה, (תמיד זה מתריע על שינוי למרות שאין שום שינוי של התוקף) מתנצלים על הבאגים בכל זאת פרויקט ראשון גדול שלנו בפייטון☺**