עבודת סוף בפייתון

מערכת לזיהוי וירוסים ו-Spyware

תיאור המשימה

במשימה זו תבנו מערכת Python אשר מסוגלת לזהות ולנתח קבצים חשודים בתיקייה מסוימת. התוכנה תשתמש בקריטריונים שונים כדי לקבוע אם הקובץ הוא "וירוס" או "Spyware" ותשמור את המידע בקובץ דוח. המשימה משלבת את כל הנושאים שנלמדו במהלך הקורס.

בחירת הפעולה שיש לעשות במערכת

המשתמש מתבקש לבחור אחת מהאופציות המוצעות, הנמצאות בין 1 ל-6.
(הסבר מפורט על כל אחת מהבחירות יינתן בשקפים הבאים).

בעת הכניסה הראשונה למערכת, המשתמש מועבר אוטומטית לאופציה הראשונה, מבלי צורך לבחור מתוך האופציות הקיימות.

אם המשתמש בוחר באופציה שאינה תקינה, תינתן הודעה מתאימה, והמשתמש מתבקש לבצע בחירה נוספת.

היציאה מהמערכת תתאפשר רק כאשר המשתמש בוחר באופציה השישית (6).
לפני היציאה, תוצג הודעה מתאימה על כך.

סריקה של קבצים בתיקייה מסוימת

1. התוכנית תבקש מהמשתמש להזין שם תיקייה. תשתמש בספרייה os כדי לסרוק את כל הקבצים בתיקייה זו (לא כולל תיקיות משנה הנמצאות בתיקיה זו).

תאסוף, תשמור במבנה מתאים ותציג בפורמט נוח למשתמש את הנתונים הבאים על כל אחד מהקבצים בתיקיה זו: שם הקובץ, סיומת הקובץ, גודל הקובץ (בבתים).

אם המסלול של התיקיה אינו תקין מבחינת המבנה שלו או שהתיקיה לא נמצאת, יש להציג הודעה מתאימה לכל אחת מהבעיות אשר עלו בסריקה.

זיהוי קבצים חשודים

2. התוכנית תיקח מקובץ טקסט המצורף לפרויקט זה את הרשימה של כל הסיומות החשודות ומקובץ טקסט אחר את הרשימה של השמות אשר יכולים להיות שמות של קבצים חשודים.

יש לכתוב לקובץ log חדש את הפרטים של כל הקבצים מהתיקיה אשר סרקנו בסעיף הקודם לקובץ ואשר שמם שווה לאחד מהשמות החשודים, הסוג שלהם מתאים לאחד מהסוגים החשודים או קבצים בגודל חריג (מעל 10MB) ורמת החשד (1-3 לפי כמות הקריטריונים אשר בהם עמד הקובץ מהקריטריונים אשר צוינו קודם). השם של קובץ לוג הוא: Unix time stamp + 64 Byte salt עם סיומת log.

סמן קבצים כ"בטוחים"

3. התוכנית תבקש את שם של הקובץ אשר המשתמש רוצה לסמן כקובץ "בטוח" כדי שלא יופיע שוב בסריקות עתידיות. אם קובץ זה אינו נמצא בתיקיה אשר סרקנו בסריקה האחרונה, יש להציג הודעה מתאימה על כך. אם הקובץ כן נמצא בתיקיה זו, בסריקה הבא של תיקיה זו, המערכת מתעלמת מקובץ זה. יש לחשוב על מבנה תקין לשמירת קבצים "בטוחים" במערכת.

הסטטיסטיקות של הסריקה האחרונה

4. הציגו למשתמש נתונים סטטיסטיים על הקבצים בתיקייה האחרונה אשר נסרקה:

- מספר הקבצים הכולל בתיקיה זו.
- מספר הקבצים החשודים.
- מספר הסיומות השונות אשר נמצאו בקובץ זה.
- הקובץ הגדול ביותר והקובץ הקטן ביותר בתיקייה זו.

מחיקת קבצים אשר סומנו כ"חשודים"

5. התוכנית תאפשר למשתמש למחוק את כל הקבצים שסומנו כחשודים על סמך לפחות אחד מהקריטריונים שהוזכרו בסעיפים הקודמים, מתוך התיקייה האחרונה שנסרקה.

לפני ביצוע המחיקה: יש להציג שאלה למשתמש ולוודא שהוא מאשר את המחיקה. במידה והמשתמש מאשר, יש לנסות למחוק את הקבצים.

אם קובץ אינו קיים, אין הרשאות למחיקתו, או מתרחשת בעיה אחרת בזמן המחיקה, יש להציג הודעה מתאימה למשתמש עבור כל קובץ בעייתי. למימוש הפעולה יש להשתמש במודול os לצורך בדיקת קיום הקבצים ומחיקתם. לכל קובץ אשר כן נמחק בהצלחה, יש לתת הודעה מתאימה, כולל מסלול של קובץ זה במערכת.

דרישות להגשת הפרויקט:

- חלוקת הקוד למודולים ופונקציות: יש לחלק את הקוד למודולים נפרדים ולוודא שהקוד מאורגן בצורה ברורה ומסודרת.
- הוספת הערות בקוד: יש להוסיף הערות לכל חלק בקוד, כך שיהיה ברור מה כל חלק עושה.
- תיעוד פונקציות: יש להוסיף תיעוד לכל פונקציה בקוד, כולל הסבר על מטרת הפונקציה, פרמטרים שהיא מקבלת ותוצאה שהיא מחזירה והחריגות אשר נזרקות מפונקציה זו.
- הגשה של קבצים בלבד: יש להגיש אך ורק קבצי פייתון (.py) ולא קבצים אחרים.

- עבודה קבוצתית: ניתן לעבוד על הפרויקט לבד או בזוגות בלבד.
- הגשה דרך הקלאסרום: רק אחד מחברי הקבוצה מגיש את הקבצים.
  - חבר הקבוצה השני צריך לרשום את שמו של השותף בהודעה פרטית בקלאסרום.
- קוד קריא ומסודר: יש לכתוב קוד קריא, מסודר ומובן.
- הגשה בזמן: יש להגיש את הפרויקט בזמן.
  - (לא יהיה ניתן להגיש אחרי מועד ההגשה אשר נקבע בקלאסרום)
- יש לטפל בכל החריגות אשר נזרקות בתוכנית.
- ניתן להשתמש בכל חומר אשר למדנו בקורס, כולל חומר אשר לא למדנו, אם החומר עומד בדרישות התרגיל.