**פרוייקט אמצע C2**

**אנטי-וירוס או: SAVE THE KITTENS**

בפרוייקט מגשימים מתכוננים במרץ לטקס הסיום של חניכי י"ב – בקרוב בוגרי התוכנית!

לכבוד האירוע, מעוניינים בהנהלת התוכנית להכין מצגת חגיגית ובה ברכות לבוגרים הטריים וכמובן – המון תמונות של חתלתולים!

****

בעקבות מודיעין שהתקבל מסיגל חניכת-העל ופוענח בעזרתכם, התגלתה מזימה של האקרים ערמומיים לכתוב וירוס זדוני ביותר שידביק את התמונות!

כמה מביך זה יהיה אם תמונות במצגת הסיום של תוכנית הסייבר הלאומית יהיו נגועות בוירוס!



אנא!!! עזרו במאבק מול הוירוס הנורא.

משימתכם – לכתוב תוכנת אנטי-וירוס שתזהה אילו קבצים נגועים בוירוס.

**חלק א': זיהוי קובץ נגוע בוירוס**

אתם מקבלים את הקובץ **KittenVirusSign** – זוהי חתימת הוירוס.

"קובץ נגוע" הוא קובץ אשר **מכיל את חתימת הוירוס המדויקת, במלואה, במיקום כלשהו בקובץ**.

**האנטי-וירוס שתכתבו יקבל כפרמטר קלט מהמשתמש תיקייה וחתימת וירוס** ויבדוק אם הקבצים בתיקייה נגועים בוירוס (מכילים את החתימה) או לא.

התיקייה וחתימת הוירוס **יתקבלו כפרמטרי קלט בשורת הפקודה**

(בסדר הזה! פרמטר ראשון: שם של תיקייה לסריקה. פרמטר שני: קובץ חתימת הוירוס).

**האנטי וירוס שתכתבו צריך לדעת לעבוד עם כל קובץ חתימה שינתן לו** (ז"א לא בהכרח KittenVirusSign).

**דוגמא לשורת הרצה עם העברת פרמטרh קלט בשורת הפקודה**

קובץ חתימת וירוס | תיקיה לסריקה | שם התוכנית

myAntivirus.exe D:\files D:\KittenVirusSign

ב"קבצים לעבודה על הפרוייקט" תמצאו 2 קבצים (kitten\_frog.jpg kitten\_run.jpg), שאחד נגוע בוירוס, והשני לא. כמו כן, תוכלו למצוא את חתימת הוירוס, בקובץ KittenVirusSign.

את תוצאות הבדיקה יש להדפיס למסך כפי שמפורט בדוגמת הריצה ובנוסף לשמור לקובץ AntiVirusLog.txt, בפורמט הדומה לזה שתוכלו למצוא בקובץ הדוגמה LogExample.txt המצורף למטלה.

\*יש להדפיס את התוצאות למסך ולמסמך לוג לפי סדר **אלפביתי** של שמות הקבצים.

**חלק ב': זיהוי יעיל של קובץ נגוע בוירוס באמצעות יוריסטיקה**

היוריסטיקה היא כלל חשיבה פשוט, מעין כלל אצבע המבוסס על הגיון פשוט או אינטואיציה, המציע דרך קלה ומהירה לקבלת החלטות ופתרון בעיות .

למשל – כשאומרים לכם "יש עוגיות במטבח", ואתם לא יודעים היכן הן, המקום הראשון בו תחפשו יהיה על השיש. לאחר מכן, אם לא תמצאו, תחפשו על השולחן, ואז אולי בתנור, ואז במקרר, ורק אם לא תמצאו במקומות האלו, תתחילו לחפש במקומות כמו הפריזר, המיקרוגל, מגירת הסכו"ם, הארון מתחת לכיור, וכך הלאה, עד שתמצאו את העוגיות. אתם תבחרו לחפש בסדר שכזה כי אתם רוצים למצוא את העוגיות מהר, ולכן **בוחרים בהיוריסטיקה שבה נחפש קודם כל במקומות שבהם סביר למצוא עוגיות במטבח**.

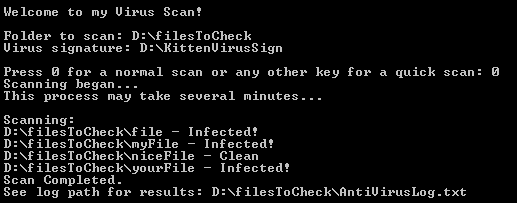
בסעיף זה עליכם להוסיף לתוכנת האנטי-וירוס שבניתם, אופציה של סריקה מהירה (Quick Scan), בהתבסס על ההיוריסטיקה הקובעת שברובם המכריע של קבצים הנגועים בוירוסים, **חתימת הוירוס נמצאת (מתחילתה ועד סופה) ב-20% הראשונים של הקובץ או ב-20% האחרונים שלו**.

השתמשו בהיוריסטיקה לבניית האופציה לסריקה מהירה, המאפשרת לסרוק את כל הקבצים בזמן קצר יותר מאשר הבדיקה המלאה שכתבתם בסעיף א'. כאשר אתם מגלים את הוירוס ב-20% הראשונים או האחרונים, ציינו זאת בהדפסה למסך ובקובץ הלוג (דוגמה ניתן לראות ב- LogExampleQuick.txt)

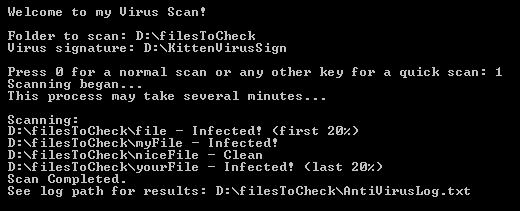
**שימו לב:** תוצאות הסריקה צריכות להיות זהות לחלוטין! זאת אומרת אם קובץ כלשהו נמצא נגוע בסריקה הרגילה, הוא צריך להתגלות כנגוע גם בסריקה המהירה (ולהיפך).

**דוגמאות ריצה**

**סריקה רגילה:**



**סריקה מהירה:**

****

**דגשים**

* כתבו ממשק נח למשתמש! כולל בחירה בין אופציה לסריקה מהירה או רגילה, וכל דבר אחר שאתם חושבים שיקל וינעים את חווית המשתמש (User Experience).
* בחנו מקרוב את קבצי הלוג שקיבלתם – LogExampleQuick.txt ו- LogExample.txt. עליכם לכתוב קובץ לוג מפורט ונח למשתמש להבנה! כולל מהי התיקייה שנסרקת, איזו אופציית סריקה נבחרה, ובמידה ונבחרה האופציה לסריקה מהירה – האם הוירוס נמצא (מתחילתו ועד סופו) ב-20% הראשונים או האחרונים של הקובץ.
* יש ליצור את קובץ הלוג באותו המיקום בו נמצאים הקבצים.
* כדאי **לתכנן** את כל תוכנית האנטי-וירוס, בעיקר חלוקה לפונקציות, **לפני תחילת העבודה**. כדאי שתהיה רק פונקציה אחת שבאמת סורקת קובץ. חשבו על חתימת הפונקציה!
* מומלץ לכתוב את הסריקה הרגילה, לבדוק אותה לעומק, ורק אז להתקדם לכתיבת הסריקה המהירה. שימו לב שבתכנון נכון, לאחר שסיימתם לכתוב את הקוד של הסריקה הרגילה, לא תידרש עוד עבודה רבה.
* **אל תחכו לרגע האחרון בשביל להתחיל לבדוק את הקוד**. באמת. אל!
* מומלץ לאשר את התכנון ולהיעזר במדריכים לפני תחילת כתיבת הקוד.
* במידה ועולים קשיים, התייעצו עם גוגל, חברים, אחים בוגרים וכמובן המדריך.
* על מנת שהבדיקה האוטומטית תעבוד, **בגישה לקבצים ותיקיות אתם מתבקשים להשתמש בסלאש "/" ולא בסלאש אחורי "\"**. בווינדוס ניתן להשתמש בשני הסוגים (גם מעורבבים) אך במערכת הבדיקות יש שימוש בסלאש בלבד.
* התאמה נוספת למערכת הבדיקה האוטומטית – **הדפיסו את התוצאות למסך וללוג לפי סדר אלפביתי של שמות הקבצים**.

**דגשים להגשה במערכת הבדיקות האוטומטית**

* גם אם בקובץ הפרוייקט יבאתם את dirent.h באמצעות מרכאות כך: "include "dirent.h#, לפני ההגשה במערכת הבדיקות האוטומטית יש לשנות לשימוש בסוגריים משולשים כך:   
  <include <dirent.h#
  + [סרטון הסבר להוספת הספרייה dirent.h](https://drive.google.com/file/d/1FTWWo9HA7h9AsIr-LoHcONW0XeOaBTWt/view?usp=sharing)
* בנתיבי הקבצים במערכת האוטומטית יש להשתמש ב-slash (/) **ולא** ב-backslash (\).

**בדיקת התוכנה**

חשבו כיצד לבדוק את תקינות הקוד.

אנחנו סיפקנו לכם שני קבצים בלבד לבדיקה – האם זה מספיק על מנת לבדוק את תקינות התוכנה כולה – כולל הסריקה המהירה? (רמז: **לא**).

**התוכנות שתגישו ייבדקו על מגוון קבצים** (לא רק שניים), ולכן – בדקו מראש את התוכנה לעומק ובאופן יסודי. לשם כך, **מומלץ ליצור קבצי בדיקה נוספים**, שיתמודדו עם מגוון תרחישים אפשריים (קובץ נגוע בהתחלה / בסוף / באמצע, קובץ קטן מדי מכדי להכיל את חתימת הוירוס, קובץ שהוא בעצמו חתימת הוירוס, ועוד?).

**בונוס**

הקובץ Infected הוא קובץ נגוע וכן חברת האנטי-וירוס שמגשימים עובדת איתה מצאה שחתימת הוירוס בקובץ זה נמצאת החל מבית מס' 11 של הקובץ עד בית מס' 42 (כולל).

כתבו תוכנית אשר מקבלת נתיב של הקובץ הנגוע, מס' בית ראשון ומס' בית אחרון של חתימת הוירוס בקובץ, ומייצרת קובץ בינארי הדומה לקובץ KittenVirusSign - המכיל אך ורק את חתימת הוירוס.

\* קרדיט לתמונות במסמך זה: www.warrenphotographic.co.uk

**בהצלחה!**