

תרגול ל מבחן במערכות הפעלה:

שאלה 1:

1. צור תיקייה בשם **Work** בכונן הראשי C.
2. בתוך התיקייה **Work**, צור תיקייה משנה בשם **Reports**.
3. בתוך **Reports**, צור קובץ ריק בשם **summary.doc**.
4. כתוב פקודה המציג את תוכן התיקייה **C:\Work\Reports**, כולל פרטי תאריך, גודל וסוג.
5. כיצד ניתן לדעת אם פריט בתוצאה של הפקודה **dir** הוא קובץ או תיקייה? הסבר בקצרה.
6. כתוב פקודות אשר יוצרות העתק של הקובץ **summary.doc** בשם **final.doc** ואז מוחקתו את הקובץ המקורי.
7. כתוב פקודה אשר מכניסה את השורה:
This is the final report
לקובץ חדש בשם **note.txt** בתיקייה **C:\Work\Reports**

שאלה 2:

1. ניתן לך קובץ חשוד עם הסיומת **.exe**.
כיצד תוכל לבדוק אם הקובץ אכן בפורמט PE מבלי להפעיל אותו?
ציין שיטות או מאפיינים שנייתן לבדוק.
2. נתנו לך קובץ מסווג **.dll**.
באיו כלים או פקודות תוכל להשתמש כדי לבדוק:
 - א. אילו שמות פונקציות הקובץ מיצא (**export**)?
 - ב. אילו שמות ספריות הקובץ מיבא (**import**)?

שאלה 3:

1. בעדרת **Task Manager**, בחר תחילה עם שימוש חריג בזיכרון.
ציין:
 - את שם התהיליך
 - את PID שלו
 - האם הוא שיר למשתמש או למערכת
 - האם קיימים לו תהליכי צאצאים (**Child Processeses**)

צրף צילום מסך של כל סעיף: חלון התהיליך, פרטי ה-**PID**, ותרשים העז אם קיימ.

שאלה 4:

בכלי **Process Explorer**, בחר תהיליך כלשהו.
יכיזד תוכל לזרהות את תהיליך האב (**Parent Process**) של התהיליך הנבחר?

- אילו שודות או עמודות יש להפעיל כדי לראות מידע זה?
- האם ניתן לראות את הקשר גם במבנה העז? הסבר.

שאלה 5:

כתבו סקריפט **batch** שמבצע את הצעדים הבאים:

1. הסקריפט יבקש מהמשתמש להזין שם של **תיקייה (Path או שם ייחודי)**.
2. אם התיקייה לא קיימת, תוצג הודעה שגיאה מתאימה, והסקריפט יסת祢ם מיד.
3. אם התיקייה קיימת, הסקריפט יבקש מהמשתמש להזין שם קובץ לבדיקה.
4. אם הקובץ נמצא – הסקריפט יבקש שם חדש לקובץ, ואז יעתיק את הקובץ לתיקייה שממוקמת מדרגה אחת מעל לתיקייה המקורית, בשם החדש שהוזן.
5. אם לא קיימ – יש לתת הודעה מתאימה והסקריפט יסת祢ם מיד.

שאלה 6:

1. הסבר בקצרה:
מהו netstat ומה היתרונו בשימוש בו על פני פקודות סטנדרטיות כמו **TCPView**?
2. הפעיל את **TCPView** במערכת Windows.

- ציין שלושה תהיליכים שמחזיקים חיבורים פעילים (**Established**).
- עברו כל תהיליך, פרטי:
 - את **שם התהיליך**
 - את **כתובת ה-IP** וה포רט של היעד
 - את **מצב החיבור**
- צרף צילום מסך הממחיש כל אחד מהטהיליכים שנבחרו.