

תרגול למבחן במערכות הפעלה:

שאלה 1:

1. צור תיקייה בשם **Work** בכונן הראשי C.
2. בתוך התיקייה **Work**, צור תיקיית משנה בשם **Reports**.
3. בתוך **Reports**, צור קובץ ריק בשם **summary.doc**.
4. כתוב פקודה המציגה 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 מוחקות 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 סיומת **.exe**. כיצד תוכל לבדוק אם הקובץ אכן בפורמט PE מבלי להפעיל אותו? ציין שיטות או מאפיינים שניתן לבדוק.
2. נתון לך קובץ מסוג **.dll**. באילו כלים או פקודות תוכל להשתמש כדי לבדוק:
א. אילו שמות פונקציות הקובץ מייצא (export)?
ב. אילו שמות ספריות הקובץ מייבא (import)?

שאלה 3:

1. בעזרת **Task Manager**, בחר תהליך עם שימוש חריג בזיכרון. ציין:

- את שם התהליך
- את PID שלו
- האם הוא שייך למשתמש או למערכת
- האם קיימים לו תהליכים צאצאים (Child Processes)

צרך צילום מסך של כל סעיף: חלון התהליך, פרטי ה-PID, ותרשים העץ אם קיים.

שאלה 4:

בכלי Process Explorer, בחר תהליך כלשהו.
כיצד תוכל לזהות את תהליך האב (Parent Process) של התהליך הנבחר?

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

שאלה 5:

כתוב סקריפט batch שמבצע את הצעדים הבאים:

1. הסקריפט יבקש מהמשתמש להזין שם של תיקייה (Path או שם יחסי).
2. אם התיקייה לא קיימת, תוצג הודעת שגיאה מתאימה, והסקריפט יסתיים מיד.
3. אם התיקייה קיימת, הסקריפט יבקש מהמשתמש להזין שם של 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 קיים- יש לתת הודעה מתאימה והסקריפט יסתיים מיד.

שאלה 6:

1. הסבר בקצרה:
מהו TCPView ומה היתרון בשימוש בו על פני פקודות סטנדרטיות כמו netstat?
2. הפעל את TCPView במערכת Windows.
 - ציין שלושה תהליכים שמחזיקים חיבורים פעילים (Established).
 - עבור כל תהליך, פרט:
 - א. את שם התהליך
 - ב. את כתובת ה-IP והפורט של היעד
 - ג. את מצב החיבור
 - צרך צילום מסך הממחיש כל אחד מהתהליכים שנבחרו.