תרגיל בית שב"כ נועם כהן:

בשלב הראשון עלינו למצוא את פונקציית הmain.
כמו שלמדנו, נרד כמה שיותר לסוף הקוד, והmain אמור להיות לפני הexitcode.
כמו כן, בד"כ לפני הקריאה של הmain נראה במפורש push של 3 ערכים:

```
loc_4015B1:
call    sub_4048D6
mov     edi, eax
call    sub_4048D0
mov     esi, eax
call    sub_404514
push    eax
push    dword ptr [edi]
push    dword ptr [esi]
call    sub_4012D0
add     esp, 0Ch
mov     esi, eax
call    sub_40473B
test    al, al
jnz     short loc_4015E2

push    esi             ; uExitCode
call    sub_404864
```

אנו רואים באלגוריתם הראשון לפני הקריאה ל sub_4012D0 דחיפה של 3 ערכים.
בנוסף, הפונקציה מופיע ממש קצת לפני הexitcode.
ניכנס לפונקציה הנ"ל:

```
; Attributes: bp-based frame fuzzy-sp

sub_4012D0 proc near

FileInformation= byte ptr -4F4h
var_4E8= dword ptr -4E8h
var_4E4= dword ptr -4E4h
Dst= byte ptr -4D0h
var_3C8= byte ptr -3C8h

push    ebp
mov     ebp, esp
and     esp, 0FFFFFFF8h
sub     esp, 4F4h
lea     eax, [esp+4F4h+Dst]
push    esi
push    104h
push    0
push    eax
call    sub_4020D0
add     esp, 0Ch
lea     eax, [esp+4F8h+Dst]
push    104h            ; nSize
push    eax             ; lpDst
push    offset Src      ; "%PROGRAMFILES%\\meseeker inc"
call    ds:ExpandEnvironmentStringsA
lea     eax, [esp+4F8h+FileInformation]
push    eax             ; lpFileInformation
push    0               ; fInfoLevelId
lea     eax, [esp+500h+Dst]
push    eax             ; lpFileName
call    ds:GetFileAttributesExA
test    eax, eax
jz      short loc 401381
```

והגענו לmain. נשנה את שם הפונקציה לmain:

```
push    eax             ; envp
push    dword ptr [edi] ; argv
push    dword ptr [esi] ; argc
call    main
```

נרד קצת למטה:

```
push    offset unk_416458
call    sub_4012A0
add     esp, 8
```

```
unk_416458      db  25h ; %
                db  73h ; s
```

כפי שאנו יכולים לראות, בפקודה push offset unk_416458 אנו יכולים לראות %s-
ז"א שמדובר במחרוזת.
מטעמי נוחות, נעבור ל x32dbg, נגיע לmain, ונרד לאזור הקוד בו מופיע הs%:

```
shabakfirst.00BD1360
 lea ecx,dword ptr ss:[esp+130] ; ecx:EntryPoint
 call shabakfirst.BD1390
 lea eax,dword ptr ss:[esp+130]
 push eax
 push shabakfirst.BE6458 ; BE6458:"%s"
 call shabakfirst.BD12A0
 add esp,8
```

נשים בשורה הראשונה label ונקרא לו jump_here. אנו עושים זאת כיוון שאנו מניחים שכאן מתבצעת ההדפסה של מה שאנחנו רוצים.

```
00BD1360 <shabakfirst.jump_here>
 lea ecx,dword ptr ss:[esp+130] ; ecx:EntryPoint
 call shabakfirst.BD1390
 lea eax,dword ptr ss:[esp+130]
 push eax
 push shabakfirst.BE6458 ; BE6458:"%s"
 call shabakfirst.BD12A0
 add esp,8
```

בעת ניגש לפקודה text eax, eax :

```
test eax,eax
je shabakfirst.BD1381
```

ונשנה אותה לפקודה jmp jump_here:

```
jmp <shabakfirst.jump_here>
```

נשים breakpoint בתחילת ובסוף הקוד ונריץ:

```
shabakfirst.00BD12D0
push ebp
mov ebp,esp
and esp,FFFFFFF8
sub esp,4F4
lea eax,dword ptr ss:[esp+24]
push esi ; esi:EntryPoint
push 104
push 0
push eax
call shabakfirst.BD20D0
add esp,C
lea eax,dword ptr ss:[esp+28]
push 104
push eax
push shabakfirst.BE91B0 ; BE91B0:"%PROGRAMFILES%\\meseeker inc"
call dword ptr ds:[<&ExpandEnvironmentStringsA>]
lea eax,dword ptr ss:[esp+4]
push eax
push 0
lea eax,dword ptr ss:[esp+30]
push eax
call dword ptr ds:[<&GetFileAttributesExA>]
test eax,eax
je shabakfirst.BD1381
```

הגענו לפקודה test eax, eax (ששינינו אותה ועכשיו היא jmp jump_here)
עכשיו נמשיך ונראה שזה יקפוץ לlabel ששמנו:

```
00BD1360 <shabakfirst.jump_here>
lea ecx,dword ptr ss:[esp+130] ; ecx:EntryPoint
call shabakfirst.BD1390
lea eax,dword ptr ss:[esp+130]
push eax
push shabakfirst.BE6458 ; BE6458:"%s"
call shabakfirst.BD12A0
add esp,8
```

נמשיך עד אחרי פקודת הcall האחרונה:

```
00BD1360 <shabakfirst.jump_here>
lea ecx,dword ptr ss:[esp+130] ; ecx:EntryPoint
call shabakfirst.BD1390
lea eax,dword ptr ss:[esp+130]
push eax
push shabakfirst.BE6458 ; BE6458:"%s"
call shabakfirst.BD12A0
add esp,8
```

ויצאה לנו התשובה הבאה:

```
 *-------------------------------------------------------------*
/                                                               \
|                                                               |
|                                                               |
|   Great Job!                                                  |
|   Your password is:                                           |
|                                                               |
|   Never_Clean_DNA_Vials_With_Your_Spit                        |
|                                                               |
|                                                               |
|                                                               |
|                                                               |
\                                                               /
 *-------------------------------------------------------------*
```

סיימנו את התרגיל 😊 !