

ארגון ותוכנות המחשב

תרגיל 2 - חלק י Bush

המתרגל האחראי על התרגיל: תומר צץ.

שאלותיכם במידע בעניינים מנהליים בלבד, יופנו רק אליו.

כתבו בתיבת subject: Bush 2 את"ם.

שאלות בעל-פה ייוננו על ידי כל מתרגל.

הוראות הגשה:

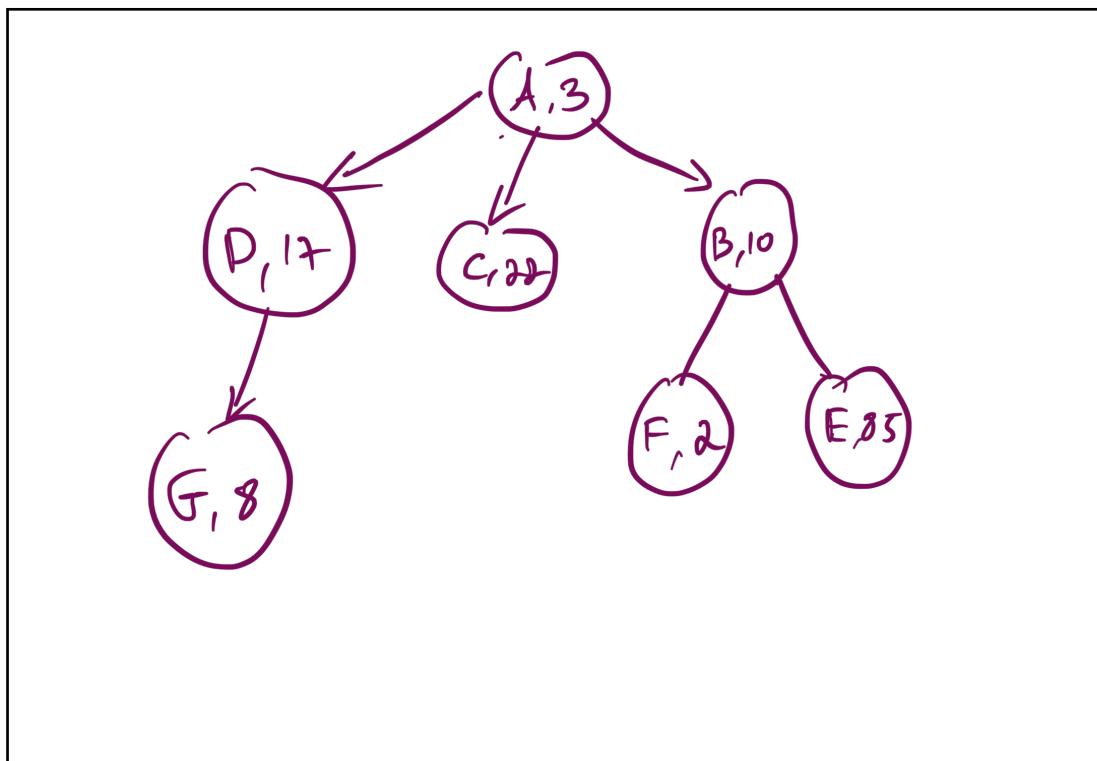
- לכל שאלה יש לרשום את התשובה במקום המועד לכך.
- יש לענות על גבי טופס התרגיל ולהגיש אותו באתר הקורס כקובץ PDF.
- על כל יום איחור או חלק ממנו, שאינו בתיום עם המתרגל האחראי על התרגיל, יורדו 5 נקודות.
- הגשתה באיחור יש לשלווה למיל של אחראי התרגיל בצירוף פרטים מלאים של המציגים (שם+ת.ז.).
- שאלות הנוגעות לתרגיל יש לשאול דרך הפיאצה בלבד.
- ההגשה בזוגות.

שאלה 1 (45 נק') – שגרות:

נעה המ"מ שמעה כי היא הולכת לקבל מוחזר עתודאים. נעה לא יודעת מה עושים העתודאים בזמןם בחופשי אז היא החיליטה לרשום להם תוכנית באסמבלי לשעות הפנא. לפניכם מקטע הנתונים שנועה כתבה:

1	.section .data	16	E: .long 85
2	A: .long 3	17	.quad 0
3	.quad B	18	F: .long 2
4	.quad C	19	.quad 0
5	.quad D	20	G: .long 8
6	.quad 0	21	.quad 0
7	B: .long 10	22	
8	.quad E		
9	.quad F		
10	.quad 0		
11	C: .long 22		
12	.quad 0		
13	D: .long 17		
14	.quad G		
15	.quad 0		

- א. ציירו את הגרף המתkeletal מפירוש מקטע הנתונים (מומלץ להסתכל בתרגיל 3 תרגיל 1 ולהזכיר כיצד מפרשים את הדיזכרון כרשימה מקושרת). בכל צומת בגרף צינו את התווית המתאימה לו בלבד (אין צורך לציין ערכים נוספים) (3 נקודות)



הסמלת ספייר, שבאה לעזור לנויה, חשבה איך לשעשע את העתודאים הצעירים. לצורך כך, היא כתבה את הפונקציה הפשוטה `func` וקוד שמשתמש בא:

```

23   .section .text
24   .global _satart
25   _start:
26       mov $17, %esi
27       mov $A, %rdi
28       call func
29       movq $1, %rdi
30       sub %rax, %rdi
31       movq $60, %rax
32       syscall
33
34   func:
35       push %rbp
36       movq %rsp, %rbp
37       cmpl %esi, (%rdi)
38       jne next
39       mov $1, %rax
40       jmp end
41
42   next:
43       mov $0, %r10
44   test:
45       cmpq $0, 4(%rdi,%r10,8)
46       je fail
47       push %rdi
48       push %r10
49       mov 4(%rdi,%r10,8), %rdi
50       call func
51       pop %r10
52       pop %rdi
53       cmpq $0, %rax
54       jne finish
55       inc %r10
56       jmp test
57
58   finish:
59       mov $1, %rax
60       jmp end
61
62   fail:
63       mov $0, %rax
64   end:
65       leave
66       ret
67

```

ב. נתון שבתחילת התוכנית ערך של `rsp` הוא `X`. כאשר `X` הוא מספר הקסדצימלי. מה הוא הערך המקסימלי ומה הערך המינימלי ש-`rsp` יכול לארוך ריצת התוכנית? הבינו את התוצאה באמצעות נוסחה שהמספרים בה הם בסיס הקסדצימלי (בטאו את התשובה באמצעות `X`). (7 נקודות)

$$X - 40 \leq 2 \times \text{rsp} \leq X$$



ג. רשמו מה יהיה פלט הפונקציה עבור קטע הקוד הנוכחי (5 נקודות).

ד. המירו את הפונקציה לשפת C על ידי כך שתשלימו את המקומות החסרים בקוד. היעזרו בהגדרת `struct` שנתונה לכם (10 נקודות):

```

typedef struct _Node{
    int data;
    struct _Node** sons;
}Node;

```

הערות:

1. מבנה `struct` בזיכרון אליו היו היחסים מקרים את הקוד היה שונה מהצורה שבו הוא מופיע בקטע `data` לעיל. הסיבה טוביה לכך בברורה הבאה.
2. הניחו שהכוונה ב`**Node` היא שרשימת המצביעים לבנים נמצאת בתוך `struct` ומוצגת כמערך באורך לא קבוע (ולכן גם `struct` בגודל לא קבוע). דבר זה אינו חוקי בשפת C. של שפת C תופס מקום קבוע בזיכרון. לשם התרגיל אנחנו מיחים משוח חריג, שניתן להשיג ובזכות העובדה שאנו כותבים באסמבלי)
3. מותר להשלים יותר ממילה אחת בכל קו אך לא יותר מפקודה אחת!

```

bool func ( Node *root, int x){
    if (root->data == X)
        return True;
    Node *son = root->sons;
    while(son != null) {
        if (func(son, x))
            return True;
        son += 1.
    }
    return False;
}

```

הערה: בסעיפים הבאים יש כל מיני שינויים בקוד. כל שינוי מתקיים רק בסעיף בו מופיע. זאת אומרת שהסעיפים לא תלויים אחד בשני.

ה. ציליל המ"כית מאמינה שהכל צריך להיות אחיד ומסודר. היא מחליטה לחת את מקטע הנתונים של נועה ולשנות בכל struct את הוגו longoa בquad. כמוום מקטע הנתונים ישתנה כך:

```

1 .section .data
2 A: .quad 3
3 .quad B
4 .quad C
5 .quad D
6 .quad 0
7 B: .quad 10
8 .quad E
9 .quad F
10 .quad 0

```

ובאופן דומה כל שאר האותיות יחליפו את הנתון הראשוני במקומם בquad. רשמו את השינויים שצריכים להיוות בקוד על מנת שייעבוד בצורה תקינה עם מקטע הנתונים החדש

(5 נקודות)

4(.rdi,%r198) 8(.rdi,%r198) -45,49
cmpd fldq cmpl empq, 37 47
esi fildq rsi -2 rlnd

- ו). יוגב הסמ"צ אוחב לעזר לנועה ולכן החליט לשנות את מבנה הנתונים באופן הבא:

```
13    D: .long 17
14          .quad A
15          .quad 0
```

- מה יהיה פלט התוכנית? יש לסמן תשובה מבין התשובות הבאות ולנמק במשפט אחד: (5 נקודות)

 - a. התוכנית תסתה ופלט הפונקציה יהיה 1
 - b. **הtright**. התוכנית תסתה ופלט הפונקציה יהיה 0
 - c. התוכנית תכנס לוולאה אונסופית
 - d. התוכנית תקרוס במהלך ריצה
 - e. התוכנית כל לא תבנה

$$rdi = 1 - rax = 1 - 1 = 0$$

בימוק: גן, פארק נטוי, כביש 1, קריית מוצקין, א-ק'ם, 1-ק'ם.

- ז. הקוד הגיע למב"סית ובגלאן קוצר הזמן שלא היא החלטה לקצר את הקוד. לפניכם מספר שינויים שהמבחן סית הצעעה. עליכם לכתוב עבור כל אחת מההצעות האם נכונות השגרה תיפגע (האם יש קלט עבורו השגרה לאחר השינוי שוניה מהשגרה לפני השינוי). הסבירו בקיצור את תשובה! (10 נקודות)

- b. מחיקת הפקודה pop בשורה 51

בנוסף ל-3 נספחים
לכטם מושגנו
ב-15 כטבב (טבב, טבב, טבב)

- הוספה פקודה push %rdi אחרי test בשורה 44.

הסופת פקודה push %rdi בshorta 44

- d. הוספה הפוקדה push %rdi אחרי test בשורה 44, הוספה הפוקודה: mov (%rsp), %rdi לפני המען בשורה 56.

rdi nc %i :.rsp 6 c, -r.e. & as pce ale
q1ap pla rdi -s r1B ues rd lpius pen' id
o1e rdi -n pheu' po >s jefail "s 46 >re
: jop eur

שאלה 2 (30 נק') – קריאות מערכת:

ג'ואי מרגיש מתוכסל מכך שחבריו חושבים שהוא פחות חכם מהם. לכן, הוא מחליט להרשים אותם בעצרת כתיבת קוד באסמבלי. הקוד שג'ואי מתכוון לכתוב קוד שיקרא קלט מהמשתמש שבו הוא יתאר אילו מאכלים הוא מעוניין לקבל והקוד יחזיר לו מה ג'ואי מוכן לתת לו.

- א. לפניים מקטע הנתונים שגואי כתוב מבלי ערכי הנתונים עצם:

```
.section .data
msg1: .ascii ???????
msg2: .ascii ???????
msg1_len: .quad _msg2 - msg1
msg2_len: .quad _msg1_len - msg2
all_msg_len: .quad _msg1_len - msg1
```

ג'ואי לא יודע עדין אילו מחרוזות הוא יכתוב. עליים להשלים את המיקומות הריקים שקשורים לארci המחרוזות כך שמשתנה `len`_msg1 יהיה האורך של `msg1`, ב-`len2` `msg2` יהיה האורך של `msg2` ובמשתנה `len_all` יהיה שווה לסכום אורךי המחרוזות `msg1` `msg2` ו-`msg3`. שימו לב עליים לעשות זאת בצורה כזו שהארוכים יהיו נכונים בעת ריצת התוכנית ללא קשר לאילו מחרוזות ג'ואי יאותחל ערכיהם של `msg1` ו- `msg2`.

- ב. לפני ביצוע קריית מערכת מתבצעים גיבויים של ערכים מסוימים בתוכנית. נרצה להבדיל בין האחריות של מערכת המעבד ואחריות של קוד המשתמש. ביצוע גיבויים אלו.

ה- מה באחריות קוד המשפט לగבות?

b. מה באחריות מערכת ההפעלת לగבות? (באים להזכיר `rflags`, `rip` ו-`cs` ועוד.)

c. מה באחריות המעבד לגבי הכתובת `rip` ?
הכתובת `rip` נמצאת בפונקציית `main` .
הכתובת `rip` נמצאת בפונקציית `func` .
הכתובת `rip` נמצאת בפונקציית `main` .
הכתובת `rip` נמצאת בפונקציית `func` .

ג. ג'ואי רצתה לחסוך בזיכרון והחליטה שבסמך למשתמש ב**syscall** sys_read ישרota לפונקציות sys_write ו sys_writer שמערכת הפעלה ממסמת (ביצע את הפקדה **call sys_write**). האם קרייה ישירה צזו תעבוד? אם כן הסבירו לג'ואי מה נדרש לעשות כדי שההעיבוד והאם יש בכך סיכון. אם לא,

רשמו באיזה אחד משלבי התוכנית (המפלט, ריצה, טעינה, קישור וכו') יקרה הכישלון ומדובר.

לעומת ה-`write` שקיים ב-`sys_write`, ה-`write` שב-`syscall` מושך אליו מalloc.

ד. חברת טובה של ג'ואי, פיבי, טוענת שאין בכלל צורך בשתי פקודות `return` שונות. ואמרה לג'ואי לבטל חלוטין את פקודת `ret` ולהשתמש רק ב-`ret`. האם הצעה של פיבי טובה וישראל?

לכ. פקודה `ret` מוחזקת ב-`RAX` → `RIP` → 3. פ'. פ' → `RFLAGS1` → `RAX` → `ret` → `sys`

ה. רוא שמע על הקוד שג'ואי כותב לו ורצה להצטרף לחגיגת. הוא נסע לננס מערכות הפעלה השנתית וביקש אישור להויסיף קריית מערכת חדשה `sys_pivot`. קריית המערכת זו תיצור 3 תיקיות עם השם "pivot1", "pivot2", "pivot3" (הרשאות התקיימה לא משנהות). האם הקוד של רוא (שיקרא על ידי `entry_syscall` כמו כל קריית מערכת) צריך להמשיך לשומר על קונבנציות `system`? נמקו.

לכ. פ' → `ret` → `CALL` → `sys_pivot` → `3` → `C`

ו. הסבירו מה על רוא לעשות/להויסיף/לשנות לקוד מערכת הפעלה על מנת שהקרייה שלו תעבור (רף לפि מה שלמדתם בקורס)

התפקיד נקבע ב-`sys_pivot`. ק'ם קולג'ן
א? ז' → `CALL` → `sys_pivot` → `3` → `C` → `ret`

ז. גונטר, מנהל בית הקפה, שמע על כל המשחקים במערכת הפעלה שהחברים עושים וביקש מהם לכתב עבורי גם קריית מערכת חדשה. הוא מעוניין בקריית מערכת בשם `order_coffee`. היא תקבל בתוקן קלט את הארגומנטים הבאים: סוג קפה (מספר שלם), גודל ה怆 (תו), לקחת או לשבת (`bool`), חט או קר (`bool`), שם המזמין (מחוזת), האמלהויסיף מאפה (`bool`), האם התשלום באשראי או במזמין (`bool`).
ומחזירה את מספר הזמןה בתור פלט.
אם ניתן להויסיף קריית מערכת שכזו? נמקו.

לכ. פ' → `CALL` → `sys_order_coffee` → `3` → `C`
(`CALL` → `sys_order_coffee` → `3` → `C`)
א? ז' → `CALL` → `sys_order_coffee` → `3` → `C`
א? ז' → `CALL` → `sys_order_coffee` → `3` → `C`
א? ז' → `CALL` → `sys_order_coffee` → `3` → `C`

שאלה 3 (25 נק') – רמות הרשאה ואוגר הדגלים:

א. הפוקודה `pushfd` דוחفت את הערך של אוגר הדגלים למחסנית. והפקודה `popfd` מוציאת את אוגר הדגלים מהמחסנית. הסבירו כיצד באמצעות שילוב של שתי פקודות אלו ניתן להציג את הדגלים OF ו-CF. שימו לב במיידת ואחד הדגלים כבר דלוק יש להשאירו דלוק כלומר, בסיום התהילה על שני הדגלים להיות דלוקים. אין לשנות את שאר הביטים בריגיסטר הדגלים. בנוסף, אין לשנות אף רגיסטר שהוא לא `rip, rip, rsp, rflags` (גם לא באופן זמני).

הערה: במידה ובדקתם את עצמכם באמצעות דיבאג'ר וראיתם שנדריך גם דגל TF זה בסדר תלמודו

<p>pushf</p> <p>org ox801 (%rsp)</p> <p>popfq</p>	<p>במהר מודיע הוא נדלק תוך כדי דיבוג.</p> <p>(א3) כארום 0 OF (א3) כארום 11</p> <p>מ'1א או מ' ox801 יוכן רנק ox801 יוכן רנק.</p> <p>א3) שמעה מ' זכר נרכך.</p>
---	--

RFlags NC NZC OV
לפניהם נסמן ב-RCF
הטבות הנקודות נסמן ב-RSF

ב. הול' התחמנית רוצה לאפשר לעצמה גישה ישירה אל התקני הקולט פلت ללא צורך בקריאות מערכות. איזה שינוי באוגר הדגלים יכול לעזור להול' במטרתה?

הערה: לא צריך לצין פקודה ספציפית, רק להגיד מה צריך לעשות ברמה התיאורטית

לנ"ט יתק"ג. נס"ע, ס"כ מוג' הילע, ככ' רשותן הרכזתי.

ג. הול' מחלוקת לנוסות את התעלול מסעיף א' רק שבמקום לשנות את CF וOF היא רוצה לשנות את IOPL. להפתעתה, היא לא מצליחה לשנות את הביטים הללו. הסבירו מה ההיגיון בכך שהוא לא מצליח לשנות את IOPL? תתייחסו לצורך בקיאות מערכת.

ד. הoli לא מתייחסת ומנסה לgesת לעיה באופן אחר. היא תכתוב עצמה קרי'ת מערכת שתיעזר לה. הקרי'ה תאפשר לכל משתמש לקרוא לה ולאחר שהיא תסתה'ם המשתמש יוכל לgesת ישירות להתקני הקלט פלט ללא צורך בקרי'ת מערכת. הסבירו מה על הoli לעשות בקרי'ת מערכת שהיא כומרת על מנת שהתקוריות שללה מצלמים

מערכת שאינה כותבת על מנת שהתוכנית שולח תאייה.

הערה: הסעיפים הבאים קשורים לפסיקות מומלץ לענות עליהם לאחר תרגול 6.

ה. וויל החבר המבולבל של הווי מתלבט כיצד ניתן לחסום פסיקות תוכנה لكن הוא שואל את הווי.
אילו מבין התשובות הבאות על הווי לענות לו? יש לסמן את האפשרות הנכונה.

1. כיבוי דגל IF באוגר הדגלים
2. הדלקת דגל IF באוגר הדגלים
3. שינוי CPL ל00
4. לא ניתן לחסום פסיקות תוכנה.

ו. כתעת נתון שוויל הצליח להגיע למצב שבו CPL שווה ל-0. וויל מעוניין לחסום פסיקות חומרה שאין מועברות דרך כניסה NMI. כיצד הוא יכול לעשות זאת? (5 נקודות)

1. כיבוי דגל IF באוגר הדגלים
2. הדלקת דגל IF באוגר הדגלים
3. עליו לחבר את הפסיקות לכנית NMI ואז לכבות את דגל IF
4. לא ניתן לחסום פסיקות חומרה ולכן לא יצליח.