

הערה: לכל שאלה יש לסמן תשובה אחת (אלא אם כן צוין אחרת בשאלה עצמה).
 בכל השאלות הקוד רץ על מעבד 80x86 תחת מערכת הפעלה Linux.
 כל המספרים הנתונים בפורמט 0x... הינם בhex. שאר המספרים הינם בdecimal.

גרסא א'

חלק א': self-modifying code ו shell

1. מהם הערכים שאפשרי שידפיס הקוד הבא, משמאל לימין?

```
int i=1;

fork();   ז
i=i*2;
fork();   ז
i=i*2;
fork();   ז
i=i*2;

printf("%d\n", i);
```

- א- 8,8,8,8,8,8
- ב- 8,4,4,4,2,2,2,1
- ג- 8,8,8,8,8,8,8,8
- ד- 1,2,2,4,4,8,8,8

2. לפניך שתי תוכניות:

Program Tao

```
main()
{
    int pid;
    pid = fork();   ז
    pid = fork();   ז
    pid = fork();   ז
    tao();
}
```

Program Arnold

```
main()
{
    int pid;
    if ((pid = fork()) != 0)   ז
        if ((pid = fork()) != 0)   ז
            pid = fork();   ז
    arnold();
}
```

בהנחה שכל פעולות ה-fork() מצליחות, איזו מין הטענות הבאות נכונה?

- (א) פונקצית tao() מבוצעת ע"י 4 תהליכים, ופונקצית arnold() ע"י 3 תהליכים.
- (ב) פונקצית tao() מבוצעת ע"י 4 תהליכים, ופונקצית arnold() ע"י 4 תהליכים.
- (ג) פונקצית tao() מבוצעת ע"י 8 תהליכים, ופונקצית arnold() ע"י 4 תהליכים.
- (ד) פונקצית tao() מבוצעת ע"י 3 תהליכים, ופונקצית arnold() ע"י 8 תהליכים.

3. מה יודפס על ידי התוכנית הבאה:

```

void print(const char *str){
    system_call(4, 1, str, strlen(str));
}

void (*print_ptr)(const char *) = print;

void foo2(void){
    print("goo \n");
    return;
}

void baz(void) {
    print_ptr("foo \n");
    return;
}

int main() {
    char buf[256];
    void (*func_ptr)(void) = (void (*)(void))buf;
    memcpy(buf, foo2, ((void *) baz) - ((void *)foo2));
    func_ptr();
    return 0;
}

```

- (א) goo
- (ב) התוכנית תתרסק כי קריאה לפונקציה שלא דרך פוינטר היא לכתובת אבסולוטית
- (ג) התוכנית תתרסק כי קריאה לפונקציה שלא דרך פוינטר היא לכתובת רלטיבית
- (ד) התוכנית תתרסק כי קריאה לפונקציה דרך פוינטר היא לכתובת אבסולוטית
- (ה) התוכנית תתרסק כי קריאה לפונקציה דרך פוינטר היא לכתובת רלטיבית

חלק ג': ELF specific

שמו לב: (1) בשאלות הבאות יש להתייחס לפלט קובץ hexedit המצורף.

(2) מספרי sections מתחילים ב-0.

8. מהו הסוג של הקובץ?

- (א) ELF object file
- (ב) ELF relocatable file
- (ג) ELF executable file
- (ד) Windows word file



9. מהו ה-entry point?

- (א) 0x80800804
- (ב) 0x80800408
- (ג) 0x04088080
- (ד) 0x08048080
- (ה) 0xbff60008



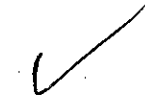
10. כמה sections יש בקובץ?

- (א) 5
- (ב) 6
- (ג) 7
- (ד) 8
- (ה) 9
- (ו) 10
- (ז) 11
- (ח) 12



11. מהו גודלו של section header יחיד?

- (א) 0x28
- (ב) 0x40
- (ג) 0x32
- (ד) 0x48
- (ה) 0x20



10 * 4 = 40
32 + 8
28

12. מהו מספר ה-section שמכיל את שמות של כל ה-sections?

- (א) 5
- (ב) 6
- (ג) 7
- (ד) 8
- (ה) 9
- (ו) 10
- (ז) 11

10



$$(40+40) = 80$$

000108

13. מהו הoffset בקובץ של ה-section מספר 2?

- 0x8a (א)
- 0x8b (ב)
- 0x8c (ג)
- 0x8d (ד)
- 0x8e (ה)



14. מהן שם ה-section שמספרו 2?

- .smale (א)
- .kontsevich (ב)
- .zelmanov (ג)
- .tao (ד)
- .bss (ה)
- .text (ו)



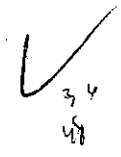
15. כמה program headers יש בקובץ?

- 2 (א)
- 4 (ב)
- 8 (ג)
- 9 (ד)
- 10 (ה)



16. מהו ה-offset בקובץ של תחילת טבלת program headers?

- 52 (א)
- 26 (ב)
- 13 (ג)
- 0x040880a0 (ד)
- 0x040880b0 (ה)
- 0xa0 (ו)
- 0xb0 (ז)

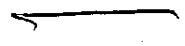


0x458

17. ידוע כי strtab מתחילה ב- offset 0x2e8 ו-symtab ב offset 0x458 מתחילת הקובץ. מהו הערך של 'ooo' symbol?

0x2e8

- 0x0804808a (א)
- 0x0804808b (ב)
- 0x0804808c (ג)
- 0x0804808d (ד)
- 0x0804808e (ה)
- 0x0804808f (ו)



18. באיזה section נמצא ה-string "The Netwide Assembler..."?

- .comment (א)
- .data (ב)
- .bss (ג)
- .strtab (ד)
- .shstrtab (ה)



00000000	7F 45 4C 46	01 01 01 00	00 00 00 00	00 00 00 00	00 00 00 00	.ELF.....
00000010	02 00 03 00	01 00 00 00	80 80 04 08	34 00 00 004.	
00000020	08 01 00 00	00 00 00 00	34 00 20 00	02 00 28 004.(.	
00000030	0C 00 09 00	01 00 00 00	00 00 00 00	00 80 04 08	
00000040	00 80 04 08	90 00 00 00	90 00 00 00	05 00 00 00	
00000050	00 10 00 00	01 00 00 00	90 00 00 00	90 90 04 08	
00000060	90 90 04 08	00 00 00 00	00 00 00 00	06 00 00 00	
00000070	00 10 00 00	00 00 00 00	00 00 00 00	00 00 00 00	
00000080	B8 01 00 00	00 BB 00 00	00 00 CD 80	01 02 03 04	
00000090	00 54 68 65	20 4E 65 74	77 69 64 65	20 41 73 73	The Netwide Ass	
000000A0	65 6D 62 6C	65 72 20 30	2E 39 38 2E	33 39 00 00	embler 0.98.39..	
000000B0	2E 73 79 6D	74 61 62 00	2E 73 74 72	74 61 62 00	.symtab..strtab.	
000000C0	2E 73 68 73	74 72 74 61	62 00 2E 74	65 78 74 00	.shstrtab..text.	
000000D0	2E 7A 65 6C	6D 61 6E 6F	76 00 2E 6B	6F 6E 74 73	.zelmanov..konts	
000000E0	65 76 69 63	68 00 2E 73	6D 61 6C 65	00 2E 74 61	evich..smale..ta	
000000F0	6F 00 2E 64	61 74 61 00	2E 62 73 73	00 2E 63 6F	o..data..bss..co	
00000100	6D 6D 65 6E	74 00 00 00	00 00 00 00	00 00 00 00	mmment.....	
00000110	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	
00000120	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	
00000130	1B 00 00 00	01 00 00 00	06 00 00 00	80 80 04 08	
00000140	80 00 00 00	0C 00 00 00	00 00 00 00	00 00 00 00	
00000150	10 00 00 00	00 00 00 00	21 00 00 00	01 00 00 00!	
00000160	02 00 00 00	8C 80 04 08	8C 00 00 00	01 00 00 00	
00000170	00 00 00 00	00 00 00 00	01 00 00 00	00 00 00 00	
00000180	2B 00 00 00	01 00 00 00	02 00 00 00	8D 80 04 08	+.....	
00000190	8D 00 00 00	01 00 00 00	00 00 00 00	00 00 00 00	
000001A0	01 00 00 00	00 00 00 00	37 00 00 00	01 00 00 007.....	
000001B0	02 00 00 00	8E 80 04 08	8E 00 00 00	01 00 00 00	
000001C0	00 00 00 00	00 00 00 00	01 00 00 00	00 00 00 00	
000001D0	3E 00 00 00	01 00 00 00	02 00 00 00	8F 80 04 08	>.....	
000001E0	8F 00 00 00	01 00 00 00	00 00 00 00	00 00 00 00	
000001F0	01 00 00 00	00 00 00 00	43 00 00 00	01 00 00 00C.....	
00000200	03 00 00 00	90 90 04 08	90 00 00 00	00 00 00 00	
00000210	00 00 00 00	00 00 00 00	04 00 00 00	00 00 00 00	
00000220	49 00 00 00	08 00 00 00	01 00 00 00	90 90 04 08	I.....	
00000230	90 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	
00000240	01 00 00 00	00 00 00 00	4E 00 00 00	01 00 00 00N.....	
00000250	00 00 00 00	00 00 00 00	90 00 00 00	1F 00 00 00	
00000260	00 00 00 00	00 00 00 00	01 00 00 00	00 00 00 00	
00000270	11 00 00 00	03 00 00 00	00 00 00 00	00 00 00 00	
00000280	AF 00 00 00	57 00 00 00	00 00 00 00	00 00 00 00W.....	
00000290	01 00 00 00	00 00 00 00	01 00 00 00	02 00 00 00	
000002A0	00 00 00 00	00 00 00 00	E8 02 00 00	70 01 00 00P.....	
000002B0	0B 00 00 00	13 00 00 00	04 00 00 00	10 00 00 00	
000002C0	09 00 00 00	03 00 00 00	00 00 00 00	00 00 00 00	
000002D0	58 04 00 00	42 00 00 00	00 00 00 00	00 00 00 00	X...B.....	
000002E0	01 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	
000002F0	00 00 00 00	00 00 00 00	00 00 00 00	80 80 04 08	
00000300	00 00 00 00	03 00 01 00	00 00 00 00	8C 80 04 08	
00000310	00 00 00 00	03 00 02 00	00 00 00 00	8D 80 04 08	
00000320	00 00 00 00	03 00 03 00	00 00 00 00	8E 80 04 08	
00000330	00 00 00 00	03 00 04 00	00 00 00 00	8F 80 04 08	
00000340	00 00 00 00	03 00 05 00	00 00 00 00	90 90 04 08	
00000350	00 00 00 00	03 00 06 00	00 00 00 00	90 90 04 08	
00000360	00 00 00 00	03 00 07 00	00 00 00 00	00 00 00 00	
00000370	00 00 00 00	03 00 08 00	00 00 00 00	00 00 00 00	
00000380	00 00 00 00	03 00 09 00	00 00 00 00	00 00 00 00	
00000390	00 00 00 00	03 00 0A 00	00 00 00 00	00 00 00 00	
000003A0	00 00 00 00	03 00 0B 00	01 00 00 00	00 00 00 00	
000003B0	00 00 00 00	04 00 F1 FF	05 00 00 00	0D 00 00 00	
000003C0	00 00 00 00	00 00 F1 FF	0E 00 00 00	90 90 04 08	
000003D0	00 00 00 00	00 00 06 00	15 00 00 00	8C 80 04 08	
000003E0	00 00 00 00	00 00 02 00	17 00 00 00	8D 80 04 08	
000003F0	00 00 00 00	00 00 03 00	1A 00 00 00	8E 80 04 08	
00000400	00 00 00 00	00 00 04 00	1E 00 00 00	8F 80 04 08	
00000410	00 00 00 00	00 00 05 00	23 00 00 00	80 80 04 08#.....	
00000420	00 00 00 00	10 00 01 00	2A 00 00 00	90 90 04 08*.....	
00000430	00 00 00 00	10 00 F1 FF	36 00 00 00	90 90 04 086.....	
00000440	00 00 00 00	10 00 F1 FF	3D 00 00 00	90 90 04 08=.....	
00000450	00 00 00 00	10 00 F1 FF	00 62 2E 73	00 6D 65 64b.s.med	

57 bytes
16
80
21
17.
37
16.7 = 68P
64
32 R
20
1612
1C
28
30
P
48 2,
32.

strtab 26 = 1818 18