**שאלות חזרה ל-x86\_64**

1. **הראה בקוד אסמבלי 2 דרכים לדאוג לכך שכל גישה מסוג**

**MOV RAX,FS:[RBX]**

**יהיה גישה להיסט RBX בחצי העליון של הכתובות הקנוניות?**

**תשובה:**

**1.**

**MOV EAX,0**

**MOV EDX,0FFFF8000h**

**MOV ECX, 100h**

**WRMSR**

**2.**

**MOV RAX, 0FFFF800000000000h**

**WRFSBASE RAX**

1. **בזמן שרץ הקוד של גרעין מערכת ההפעלה הרצה ב- long mode,**

**ערך ה-CS=16. שיטת המימוש של המעבר בקריאת מערכת היא ע"י פסיקת התוכנה INT 2Eh. הכתובת הלינארית של נקודת הכניסה לסדרן קריאות המערכת הוא 0FFFFFFFF0000EA10h.**

**מה אתה יכול להגיד על כניסות ההמרה Descriptor Tables במערכת?**

**תשובה:**

**CS=10000b 🡺 TI=0, CPL=00, Index = 10 = 2**

* **GDTR[2] : DPL=00, L=1, C=0, P=1**

**IDT[2eh] = IDT[46] : STYPE=01111, DPL=11, P=1**

**Target Selector: 16, Target Offset: 0FFFFFFFF0000EA10h**

1. **נניח שמתבצעת הגישה הבאה:**

**MOV RBX,0FFFF80000A04F0E0h**

**MOV [RBX],RAX**

**איזה כניסות באיזה טבלאות דפים מערבות בהמרה של הכתובת הלינארית לכתובת פיזית, בשלושת הגדלים האפשריים של דפים?**

**מהו ההיסט בתוך הדף, בשלושת המקרים?**

**תשובה:**

**הכתובת הלינארית של הגישה היא:**

**0FFFF80000A04F0E0h**

**16 הביטים העליונים חסרי משמעות.**

**מה שנותר הוא**

**80000A04F0E0h =**

**100000000000000000001010000001001111000011100000b=**

**דפי 4k:**

**100000000-000000000-001010000-001001111-000011100000**

**256 - 0 - 40 – 79 – 224**

**לפיכך מעורבים:**

**PML4[256]**

**PDP[0]**

**PD[40]**

**PT[79]**

**Offset in page = 224**

**דפי 2M:**

**100000000-000000000-000101000-0001001111000011100000**

**256 – 0 – 40 - 323808**

**לפיכך מעורבים:**

**PML4[256]**

**PDP[0]**

**PD[40]**

**Offset in page = 323808**

**דפי 1GB:**

**100000000-000000000-0001010000001001111000011100000**

**256 – 0 – 168095968**

**לפיכך מעורבים:**

**PML4[256]**

**PDP[0]**

**Offset in page = 168095968**

**נניח שבדוגמא האחרונה, מדובר בדפים 4k והמיקומים הפיזיים של הטבלאות המערבות הן:**

**PML4 – 8192**

**PDP – 32768**

**PD- 65536**

**PT – 131072**

**מה אתה יכול להסיק מכך?**

**תשובה:**

**CR3.PML4TBA = 8192/4096 = 2**

**PML4[256].PDPBA = 32768/4096 = 8**

**PDP[0].PDBA = 65536/4096 = 16**

**PD[40].PTBA = 131072/4096 = 32**

**אם ידוע שהכתובת הפיזית שהמעבד ניגש אליה מתחילה ב-168095968, מה אפשר לומר על הכניסות בטבלאות בשלושת האפשריות של הגדלים של הדפדוף?**

**דף 4k:**

**PT[79].PPBA = (168095968- 224)/4096 = 168095744/4096 =**

**41039**

**דף 2M:**

**PD[40].PPBA =**

**(168095968 – 323808)/4096 = 167772160/2097152 = 80**

**דף :1GB**

**PDP[0].PPBA = (168095968 -168095968)/** **1073741824 =**

**0/1073741824 = 0**