שאלה 1

א. לא נכון, הקריאה לקריאת המערכת הנכונה מתבצעת לפי העברת מס' הקריאה בפונ' הwrapper. התחילית "sys_" הינה קונבנציה בלבד.

ב. לא נכון, פונקציית מעטפת הינה פונקציה "רגילה" לחלוטין ולכן יכולה לקבל כל מספר של ארגומנטים.

ג. נכון, ניתן להעביר עד 6 פרמטרים באופן ישיר דרך הרגיסטרים, אך ניתן להעביר פרמטרים נוספים דרך המחסנית.

ד. לא נכון, הפקודה int 0x80 היא פקודת אסמבלי והקומפיילר יודע להתייחס אליה ככזאת לפי תווית __asm__ שאומרת לו שמתחיל קוד אסמבלי.

שאלה 2

א. נרצה להפריד בין user mode לkernel mode כדי שנוכל להגביל את המשתמש ממשחק באיזורים ויכולות רגישות של המערכת. לכן ע"י int אנו מוציאים את האפשרות מידי המשתמש לעבור לkernel mode, לעומת call/ret שיכולות להיקרא ע"י המשתמש.

ב. בגלל שאיננו יודעים את מספר הפרמטרים מראש בעת כתיבת הפונקציה, נרצה להעביר את מספר הפרמטרים לפונקציה. הפרמטר השמאלי ביותר יכנס אחרון למחסנית ולכן הוא יהיה הפרמטר האחרון במחסנית, כך שיופיע במקום קבוע ביחס לesp ואפשר יהיה תמיד למצוא אותו. כך על ידי פרמטר זה נוכל להעביר מידע נוסף על מספר הפרמטרים שמועברים.

ג. מספר הפרמטרים שפונקצית printf חושבת שמועברים אליה משפיע רק על הקריאה מהמחסנית, לכן אם הועברו מעט מידי פרמטרים היא יתייחס לכתובות עמוקות יותר כפרמטרים למרות שהנן זבל מבחינתה

ד. לא נרצה שהמשתמש יוכל לשלוח בלוק של מידע ששייך לאזור הקרנל בזכרון ובכך לגרום לקרנל לבצע בעקיפין פעולות שנאסרו מלכתחילה על המשתמש. נבדק גם אורך הבלוק כדי שגם כתובות ב"שולי" אזור המשתמש לא יוכלו להיות מועברים ובכך לחרוג.

שאלה 3

א. ראשית מריצים את main ובכך נוצר התהליך הראשון.
לאחר מיכן נכנסים לmyfork שמבצע fork. התהליך הבן מקבל כערך החזרה 0 ולכן לא יכנס לתוך התנאי וכתוצאה מכך לא יקרה לfork נוסף.
התהליך המקורי יקבל את מספר התהליך החדש (הבן) ולכן יכנס לתנאי ויקרא רקורסיבית לmyfork שתקרא לfork וחוזר חלילה.

הכניסה הרקוסיבית תתבצע 43 פעמים ולכן ביחד עם התהליך המקורי יווצרו בסה"כ 44 תהליכים.

ב. קיימים שני פלטים אפשריים:
   a. 0 ואז 1: לאחר הfork התהליך המקורי ממשיך לwait ומחכה לבן שלו שיסיים את הריצה. תהליך הבן לא יכנס לתנאי וידפיס 0.
   אחר כך יגדיל את value ל1 ויחזיר אותו. כעת יקבל האב את ערך זה ויצא מהwait (בעל ערך 1) ויתקדם וידפיס 1, ולבסוף יצא.
   b. יודפס 10: במידה והfork יכשל לא יהיו לתהליך המקורי בנים ולכן יוחזר לתוך value הערך ECHILD ששוה ל10 ולכן לאחר WEXITSTATUS ישארו רק 8 הביטים התחתונים, כלומר הערך 10. מיד לאחר מיכן ימשיך התהליך להדפסה של "10" ויצא.

כלומר הפלטים האפשריים הם "10" או "01".