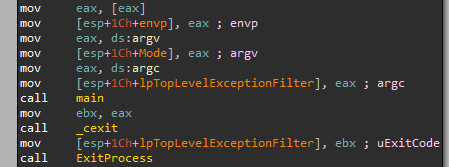
Reverse HW 2

**Goblin**

תחילה, כאשר ניגשנו לקובץ ניסינו להבין איפה מתחיל הmain. ניסינו להסתכל על המחרוזות בתכנית, אך לא הצלחנו באופן מובהק להבין מהן איזו פונקציה היא הmain, ולכן בסופו של דבר הסקנו איזה פונקציה היא הmain לפי קריאה של הstart. חיפשנו את הפונקציה שמקבלת את envp, argv, argc, ובעזרת מידע נוסף מהIDA הגענו לפונקציה הנכונה:



לאחר מכן, הסתכלנו על תחילת הריצה של main. תחילה, היא קוראת לפונקציה שלא ממש משפיעה על הלוגיקה של התכנית. לאחר מכן, main קוראת לפונקציה שבהמשך נתנו לה את השם PrepareMaze.

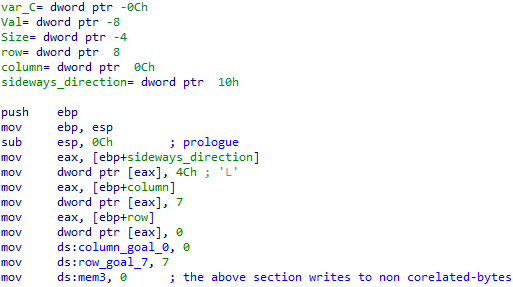
הפונקציה PrepareMaze: ניתן לראות כי הפונקציה כותבת לרצף של 64 בתים בזכרון.  
אחרי בחינה מעמיקה, הגענו למסקנה שמה שהיא כותבת לזכרון נראה ככה:

A picture containing blue, electric blue, pattern, majorelle blue

Description automatically generated

תחילה חשבנו שהרצף הזה מייצג את המפתח שאנחנו מחפשים, ושבמהלך ריצת התכנית מתמלאים "הערכים הנכונים" . לקראת סוף הניתוח של הקובץ, הבנו שמדובר במבוך.

בנוסף, על ידי התבוננות בחלק הבא של הפונקציה:



הגענו למסקנה שהפונקציה מקבלת כפרמטרים שני מצביעים ל-int ומצביע ל-char. בהמשך הבנו את מטרת הפרמטרים הללו – בעזרתם הפונקציה מאתחלת את המיקום ההתחלתי שלנו במבוך (שורה ועמודה) ואת הכיוון ההתחלתי שבו אנו זזים (בתמונה זהו התו ‘L’).

הפונקציה מאתחלת (בלי קשר לפרמטרים) את מיקום המטרה במבוך, ואת מונה הדגלים.

בכך סיימנו את ניתוח הפונקציה PrepareMaze.

המשך main:

בתחילת main, מאותחלים שני משתנים. הסקנו שתפקידיהם הם של counter ו-limit של לולאה, וכעת הגענו לניתוח תוכן הלולאה.

הלולאה רצה עד 7 פעמים. איטרציה של הלולאה נראית כך:

תחילה, קוראים לפונקציה שמאוחר יותר קראנו לה GetCommand. נפרט על ניתוחה כעת:

GetCommand:

הפונקציה מקבלת שני פרמטרים – char\*, int\*.

ה-char\* משמש לאחסון ה-command שניתן על ידי המשתמש. ה-int\* משמש לאחסון מספר.

הפונקציה קולטת תו מהמשתמש ושומרת אותו בפרמטר ה-char\*. אחרי כן, יש קריאה לפונקציה נוספת. בהתחלה לא כל כך הבנו מה הפונקציה הנוספת עושה, אך כן הבנו שהיא לא משפיעה על הלוגיקה של התכנית(מאוחר יותר גילינו שהיא מקודדת את המפתח בהתאם למהלכים במבוך).

לאחר קליטת תו מהמשתמש ב-GetCommand – ראינו כי אם התו אינו ‘C’ או ‘D’ או ‘U’ – ריצת התכנית מסתיימת.  
אם התו הוא ‘C’, אז קוראים תו נומרי שמתורגם למספר בין 0(כולל) ל-9(כולל).

המשך הלולאה ב-main: יש שני מסלולים בלולאה, וההחלטה לאיזה מסלול לגשת נקבעת על פי התו שנקלט ב-GetCommand.

מסלול א' – אם התו שנקלט אינו ‘C’:

נקראת הפונקציה שמאוחר יותר קראנו לה MoveRow. נפרט עליה כעת.

הפונקציה MoveRow: מקבלת int\*, int, char.

בעזרת הפרמטרים המספריים, הפונקציה מחשבת את המיקום הנוכחי במבוך ובודקת שאין במיקום זה את התו ‘X’ או ‘.’(נקודה). אחרת התכנית מסתיימת.  
אחר כך, בהתאם להאם התו הוא ‘U’ או ‘D’, משנים את ערך הארגומנט הראשון לפי התו שנמצא במיקום הנוכחי.  
בשלב זה של הניתוח, עדיין חשבנו שהמבוך הוא מפתח, אך התחלנו לפקפק בכך, כי הייתה לנו הרגשה ש-U ו-D מציינים Up או Down בהתאמה, לפי הצורה שבה משנים את הארגומנט הראשון (מספר שורה).

לאחר שינוי הארגומנט הראשון, קוראים איתו לפונקציה אחרת, שקראנו לה PathBlockCheck. פונקציה זו בודקת שהמיקום החדש הוא בתחומי הלוח ושהמיקום החדש אינו מיקום של תו ‘X’. אחרת התכנית מסתיימת.

עברנו כעת למסלול האחר בלולאה ב-main. מסלול זה מתרחש אם התו שנקלט מהמשתמש הוא ‘C’. במסלול זה נקראת פונקציה חדשה, שקראנו לה מאוחר יותר MoveInSidewayDirection.  
הפונקציה MoveInSidewayDirection: מקבלת ארבעה פרמטרים – int\*, int\*, char\*, int.

מאוחר יותר הבנו שהפרמטרים מהווים את מספר השורה, מספר העמודה, כיוון התזוזה, ומספר הצעדים.

הפונקציה קוראת לעצמה באופן רקורסיבי כמספר הצעדים. בכל צעד רקורסיבי, היא בודקת את כיוון התנועה ולפיו היא משנה את מספר העמודה. אם הגענו לקצה המבוך, אז משנים את מספר השורה ואת הכיוון. בנוסף, אם עוברים במשבצת שבה התו ‘F’, מקדמים את מונה הדגלים.

בשלב זה התמונה התבהרה לנו, והבנו כי מדובר במבוך ולא במפתח, וכי R\L\D\U הם כיווני תנועה. בנוסף, הבנו כי C והמספר מסמלים צעדים \ התקדמות.

מכאן, חזרנו אחורה, התחלנו לתת שמות למשתנים\לפונקציות, ולפענח את חוקי המשחק. בנוסף, סיימנו לפענח את הלולאה ב-main, שבודקת בסופה האם הגענו למשבצת הסיום, והאם אספנו שני דגלים.

חוקי המשחק שהבנו הם:

* אנחנו נמצאים בתוך מבוך 8x8, מתחילים במשבצת [0,7], וכיוון התנועה הוא שמאלה.
* יש במשחק עד שבעה מהלכים.
* בכל שלב, נותנים אחת משלוש פקודות :

1. U
2. D
3. C + Number

אם הפקודה היא U או D : מסתכלים על התו במיקום הנוכחי במבוך. עולים או יורדים מספר שורות כמספר התו.

אם הפקודה היא C + Number, אז מתקדמים לפי כיוון התנועה הנוכחי, כ-Number צעדים. במידה ומתקדמים מעבר לגבולות הלוח, אז משנים את כיוון התנועה, ועולים שורה במקום להתקדם לצדדים. לאחר עליית השורה ממשיכים להתקדם את יתרת הצעדים. תוך כדי ההתקדמות, בודקים האם עברנו במשבצת שיש בה דגל 'F', ומקדמים את מונה הדגלים בהתאם.

* כאשר מגיעים למשבצת [7,0], בודקים האם אספנו שני דגלים ואם כן, מודפס מפתח ההצפנה הסופר סודי. 😊

בהתחלה, חשבנו שצריך לעצור בכל משבצת שיש בה F אם אנחנו רוצים לאסוף את הדגל, ומספר המהלכים לא הספיק לנו תחת המגבלות הללו. לכן שינינו את קובץ הריצה כך שיהיו לנו יותר מהלכים.

בהבסת המשחק (לאחר ששינינו את הקובץ) התקבל לנו המפתח הבא:



המפתח שקיבלנו היה נראה לנו משונה, ולכן חזרנו אחורה והבחנו שאפשר לאסוף דגלים במהלך תנועה. פתרנו את המבוך בשבעה צעדים, וקיבלנו את המפתח הבא:

A black background with white text

Description automatically generated with low confidence

ההבדל בין המפתחות השונים שקיבלנו נובע מכך שהמפתח נוצר על בסיס הפקודות שאנחנו מכניסים.

**Giant**

תחילה, בדומה ל-Goblin, הסקנו איזו פונקציה היא ה-main. ראינו כי הmain מכילה 4 קריאות לפונקציות. הראשונה אינה משפיעה על הלוגיקה של התכנית ואחריה 3 קריאות לפונקציות שאינן קשורות אחת לשנייה. כל פונקציה קולטת קלט מסוים, אשר בהינתן הקלט הנכון היא מדפיסה חלק ממשפט התוצאה.

פונקציה 1:

פונקציה זו מקבל ארבעה קלטי char מהמשתמש, ומחברת אותם לint אחד בצורה הבאה:

בנוסף, היא מגדירה פונקציה נוספת בתור ה-UnhandledExceptionFilter.

לאחר מכן מבצעים חיסור בין המילה "NLUL" לקלט הנוצר וקוראים באמצעות printf מכתובת זו. לאחר מכן יש בדיקה על התוכן של dword\_408020 ואם הוא לא 0 יש הדפסה של תחילת המשפט כתלות בקלט.

הפונקציה אשר מגדירים בתור ה-filter, כותבת nops לטקסט ושמה 1 בכתובת dword\_408020. לכן היינו רוצים שהיא תיקרא ונקבל את תחילת המשפט.

לשם כך, ניתן את הקלט "NULL" מה שיגרום לחיסור להיות 0 ויגרורnull pointer dereference, ה-filter יקרא והמשפט יודפס.

פונקציה 2:

הפונקציה מאתחלת מערך של int על ה-stack, מוסיפה פרמטרים וקוראת לפונקציה רקורסיבית. לאחר מכן, היא עוברת בלולאה ולפי ערכי המספרים בכתובת המערך מדפיסה את המשך משפט התוצאה. השאלה הייתה מה הפונקציה הרקורסיבית עושה ומה הקלט הדרוש בשלב זה?

שמנו לב שבתחילת הפונקציה הרקורסיבית בודקים האם הפרמטר השני קטן מהפרמטר השלישי, ואם כן מחשבים את האמצע ביניהם. חישוב זה הזכיר לנו אלגוריתמים כמו  
binary search או merge sort. לאחר מכן קוראים 5 בתים ב-Hexa מהמשתמש, משנים את הרשאות הגישה ל-text בכתובת 0x4019BF שיהיו Read, Write, Execute, וכותבים לשם את הקלט. בהסתכלות לכתובת זו אנו רואים שיש 6 פקודות nop רצופות. בנוסף, שמנו לב שחישוב זה קורה רק בקריאה הראשונה לפונקציה ולא בקריאות רקורסיביות חוזרות.

לאחר מכן מכינים את הארגומנטים וקוראים לפונקציה הרקורסיבית שוב. מכינים שוב את הפרמטרים אך אין קריאה נוספת. הארגומנטים הוכנו באופן הבא:

Recursion(arg0, arg4, average of arg4 and arg8, argC+1)

ובפעם שבה אין קריאה, ויש פקודות nop במקום, הכנת הארגומנטים נראית כך:

(arg0, average of arg4 and arg8 + 1, arg8, argC+1)

בשלב זה הבנו שככל הנראה מדובר ב-merge sort ולכן חסרה הקריאה הרקורסיבית הנוספת.

חישבנו את המרחק הרלטיבי שיש לקפוץ מפקודת ה-nop השישית בעת קריאה רקורסיבית ל-MergeSort. שמנו לב כי קידוד של פקודת call מתחיל ב-E8 ואז 4 בתים של offset:

ולכן הקלט לפונקציה על מנת לבצע את הקריאה היה: E8 CA FE FF FF

שמתורגם ל-call MergeSort בזמן ריצה.

לאחר השלמת הפונקציה MergeSort ריצת פונקציה 2 נותנת את המשך משפט הפלט.

פונקציה 3:

בפונקציה זו ישנם סה"כ ארבעה קלטים אשר לא קשורים זה לזה, וכל אחד מהם נבדק בנפרד. הקלטים הם מספר ב-HEXA ושלושה מספרים נוספים. נתאר את הבדיקות על כל קלט:

קלט 1: HEXA

הפונקציה מתחילה בלקבל 4 בתים ב-HEXA מהמשתמש. לאחר מכן היא בודקת האם המספר שלילי. אם כן, היא עושה לו neg (על ידי חישוב (0 – num)) ושומרת בזכרון. ניתן לפרש זאת כפעולת ערך מוחלט. אולם, בסוף הפונקציה אנו צריכים שהמספר יהיה שלילי. אנחנו פתרנו זאת בשתי דרכים שונות:

1. מציאת מספר x כך ש 0-x עדיין מקודד למספר שלילי. מספר זה הוא 0x80000000.
2. מכיוון שמספר זה אינו משפיע על הקלט המודפס, גישה נוספת הייתה לשנות את קובץ ה-exe כך שהבדיקה האחרונה תבדוק שהמספר חיובי במקום שלילי, ולכן כל מספר אחר, לדוגמה 10, יעבור את הבדיקה.

קלט 2: int

כל הבדיקות על הקלט הזה הוא שה-byte הראשון שלו הינו EC. המספר 236 יעבוד במקרה זה. חשוב לציין שגם בהדפסת הפלט מסתכלים רק על הבייט הראשון של קלט זה ולכן המספר המדויק לא משנה כל עוד ה-byte הראשון יהיה כמו שרשום לעיל.

קלט 3: int

ההגבלות על מספר זה הן שהוא יהיה גם קטן מאפס וגם שלאחר שנוריד ממנו 1 ונעשה test עם עצמו הפקודה jle לא תקפוץ.

על מנת שהפקודה jle תקפוץ צריך ש ZF=1 או ש OF!=SF, בנוסף ידוע שTest מכבה את OF.

ולכן סה"כ אנחנו צריכים שהמספר שיתקבל יהיה חיובי. לכן נשתמש במספר השלילי הקטן ביותר, מה שיגרום ל-integer underflow ויהפוך את המספר לחיובי, כלומר המספר הינו 0x80000000.

קלט 4: int

היינו צריכים לתת קלט אשר יפתור את המשוואה *, זוהי משוואה ריבועית פשוטה והקלט אשר פותר אותה הינו .*

*כלומר, לאחר הכנסת הקלט,  
   
(כאשר =* 0x80000000*),  
קיבלנו את המשך משפט התוצאה.*

*סיכום:*

*סה"כ היו לנו 3 פונקציות. כל אחת מקבלת קלט משלה, פולטת חלק ממשפט התוצאה ואינה קשורה לפונקציות האחרות. עבור הקלט*

*NULL E8 CA FE FF FF 80000000 236 -2147483648 -70   
(שצבועים לפי הפונקציה הרלוונטית) קיבלנו את הפלט C:\Users\User1\Pictures\Screenshot_63.png*

*וסיימנו עם giant.*

**Wizard**

כמו בgoblin ו-giant, גם בwizard מצאנו את הmain והתעלמנו מהפונקציה הראשונה שנקראת ממנה.

בשונה משני הקבצים הקודמים, שמנו לב שבהרצת הקובץ מודפס pattern של מגן דוד עם סימני שאלה אדומים בנקודת מפגש.

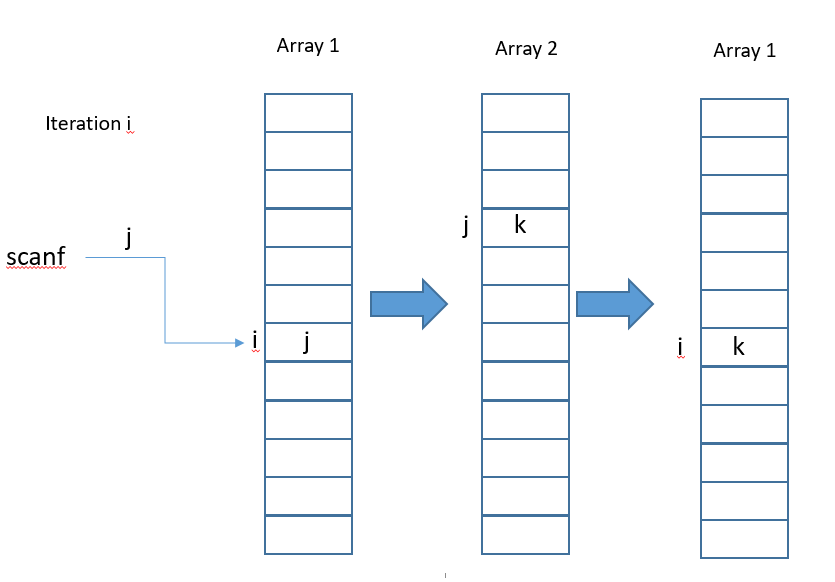
קוד זה מחולק לשתי פונקציות שאינן קשורות זו לזו:

StarOfDavidPuzzle:

בתחילת הפונקציה הראשונה מאתחלים 12 בתים על המחסנית במספרים 1-12 בסדר כלשהו, לצורך ההסבר נקרא לו מערך 1. בנוסף מאתחלים באפסים 12 בתים נוספים במקום אחר על המחסנית, לצורך ההסבר נקרא לו מערך 2.

החלק הבא בפונקציה הכיל לולאות רבות והדפסות רבות, ללא הסתכלות מעמיקה, הנחנו כי זהו קטע הקוד אשר מדפיס את מגן הדוד עם הסימנים האדומים.

בשביל להבין איפה אנחנו צריכים לעשות אינטרקציה עם הקוד, חיפשנו איפה scanf נקראת בפונקציה. לאחר חקירה, הבנו כי scanf נקראת בלולאה 12 פעמים, כאשר כל קריאה עובדת בצורה הבאה:



כאשר j הוא מספר בין 0 ל11 ויש בדיקה שמוודאת שלא השתמשנו באותו אינדקס פעמיים.

בשלב זה הבנו שבגלל שיש 12 סימני שאלה אדומים, לכן ככל הנראה כל איבר במערך מייצג סימן שאלה.

לאחר מכן ראינו בניתוח שסוכמים 6 רביעיות ושישיה אחת וכדי לעבור את השלב צריך שהסכום שלהם יהיה 26 כל פעם. הדבר הראשון שעשינו היה לבדוק מיהם הרביעיות והשישיה. על ידי הכנסת פרמוטציה אקראית בתור קלט, יכולנו למפות את הקלטים לסימני השאלה וגילינו שהרביעיות הן הנקודות שנמצאות על צלעות המשולשים במגן דוד, ושהשישיה היא קצוות המגן.

כתבנו script בפייתון אשר עובר על כל הפרמוטציות האפשריות עד שהוא מוצא פתרון שדואג שסכום הרביעיות והשישיה יהיה 26, ואז התאמנו את הקלט כדי שלכל אינדקס יכנס המספר שאנחנו רוצים. למשל, רצינו שהמספר העליון בכוכב יהיה 1, ולכן המספר הראשון שהכנסנו הוא 2, כי במקום השני במערך 2 יש את הספרה 1, וכך הלאה.

לבסוף הבנו שהחלק השני של הפונקציה הוא הדפסת הפתרון,

פונקציה 2:

לפונקציה 2 יש שני חלקים, החלק הראשון הוא החלק בו מצפים לקבל קלט שהוא מחרוזת עם ירידת שורה.

לאחר מכן, מורידים מכל האיברים במחרוזת 'A', עושים פעולה על המחרוזת ומוסיפים לכל האיברים 'A'. לאחר מכן משווים את המחרוזת הסופית למחרוזת נתונה, ובמידה והן שוות כותבים את כתובת של הפונקציה על המחסנית לאחר המחרוזת שהכנסנו. לבסוף מעתיקים את ה29 הבתים הראשונים של מחרוזת הקלט למקום כלשהו בזיכרון ומוסיפים לזיכרון במקום הdword\_409024 1.

הפעולה שעושים על המחרוזת: לאחר חקירה של הפעולה הכללה חקירה סטטית ודינמית, גילינו שעושים למחרוזת Xor ציקלי לכל שני איברים סמוכים, כאשר לאחרון עושים Xor עם הראשון. נשים לב שעבור האיבר האחרון ה-Xor הוא עבור הערך החדש ולכן

מכיוון שresult ידוע, אפשר לקבל את מחרוזת הקלט במקום ה28. ואז בלולאה:

מכיוון שresult ידוע, אפשר לקבל את מחרוזת הקלט במקום הi.

בעזרת script פייתון מצאנו את כל המחרוזת והצלחנו לעבור את הבדיקה.

כעת היינו רוצים לחזור על הפונקציה, כי כאשר עדכנו את ערך dword\_409024, הפונקציה עוברת לbranch אחר אשר מדפיס את שארית הפלט, לבסוף משחזר את כתובת החזרה המקורית ואת הebp, ויוצא כמו שצריך. לשם כך, הוספנו למחרוזת הקלט ריפוד של 16 0, (זה יכול היה להיות כמעט כל ערך) וכעת, בגלל שהמחרוזת מגיעה עד סוף הframe, הכתיבה לאחר המחרוזת דורסת את כתובת החזרה והפונקציה אכן תיקרא שנית. קיבלנו את שארית משפט הפלט וסיימנו את wizard.

