**פתב"ס ק"פ**

**מבוא**

אתם חניכים בכיתה, יושבים ומחכים שהמערך יתחיל.

פתאום האור נכבה, ואתם מתחילים לשמוע מנגינה מוכרת.

טו טו טו דו. הו יאאא הייי יאאאא.

שיר הפתיחה של קים פוסיבול מתנגן!

האור נפתח, ואתם רואים את לינוי ומיכאל (קים פוסיבול ורון סטופבל).

הם מתחילים לספר לכם שמישהו פרץ למתקן. לא ברור מי זה, אבל הוא השתלט על המצלמות, על ה-FOOD TRUCK ועל ציוד האבטחה. ממה שנודע לנו הוא מארגון הטרור המפורסם - **חיסור**, ולא ידוע עדיין מה רצונו.

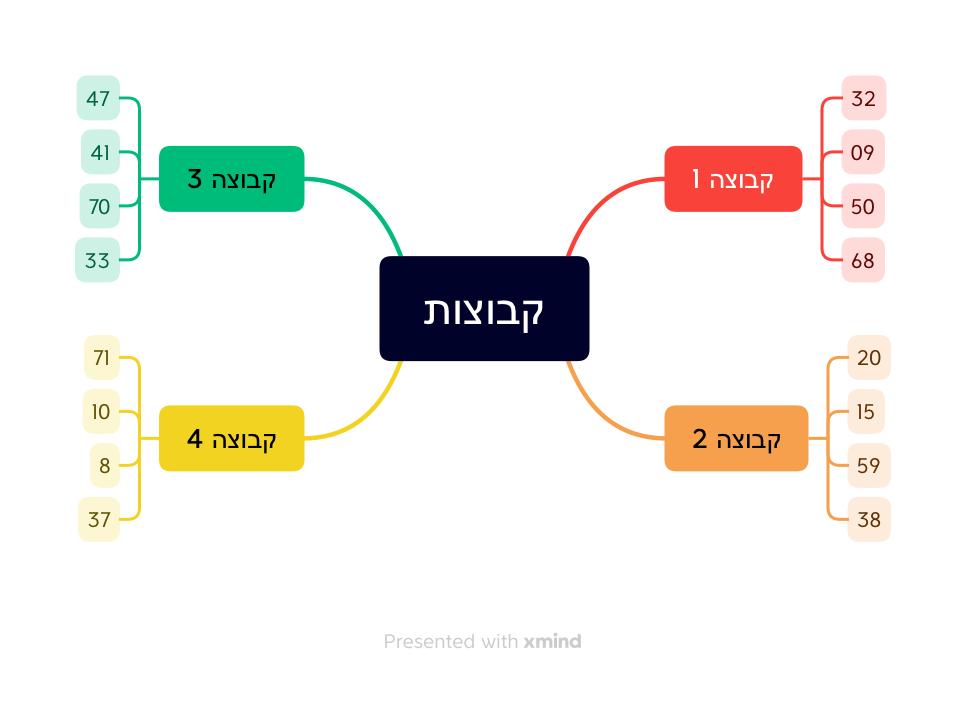
אנחנו צריכים את עזרכתם למצוא את הפורץ.

מזל שבשביל המשימה, יש לכם את האתר של קים פוסיבול לעזרה!

~לינק בלינק ;)~

לפני שתגשו למשימה, תריצו את הקובץ המצורף מבלי להתסכל על התוכן שלו.

קבוצות:



**פתב"ס**

שלב 0:

להריץ את הקובץ חובה שנתנו.

שלב 1:

נכנסים לאתר של קים פוסיבול ורואים הרבה מידע על נוולים. אחרי כמה זמן מבינים שאין שום דבר מעניין באתר ומתחילים לחקור. כשנסניף את התעבורה, נראה פקטות HTTPS מוצפנות שנראות מעניינות. נלך לאתר, ושם נראה את הפקטה המופענחת.

ב-data שלה, יש את השיר של ק"פ ובתוכו הוא מכיל לינק לאתר של השלב הבא:

שלב 2:

נכניסים לאתר, אשר מוריד לנו אוטומטית קובץ. נבחן את הקובץ ונראה שהוא ללא סיומת. נוכל לעשות אחד משני דברים:

א. להריץ את פקודת ה-Linux file על הקובץ ולגלות שזה קובץ זיפ.

ב. להסתכל על הקובץ ב-hex workshop ולראות שזה מתחיל ונגמר ב-pk. לבדוק בויקיפדיה/מקור אחר ומשם להבין שזה קובץ זיפ.

לאחר מכן, נשנה את הסיומת zip לקובץ ונראה שקיבלנו קובץ zip.

שלב 3:

נחלץ את ה-zip ונראה בתוכו קובץ טקסט, עם נתיב לכונן הרשתי s. כשנפתח את הנתיב ב-file explorer, נראה תיקייה המכילה כל מיני תמונות (בניהם מימז איכותיים) ומסמכים. נעבור עליהם כי אנחנו אנשים מסורים לעבודתנו, אבל לא נראה דבר מעניין.

חשד: קובץ מוחבא.

נתחיל לחקור את התיקייה הנתונה, ונגלה שאכן יש תיקייה מוסתרת בתוך התיקייה. נפתח אותה, ונראה שהיא מכילה קובץ אחד - תמונה.

נפתח את התמונה ולא נראה משהו רלוונטי. עם זאת, מה שכן מעניין הוא גודל התמונה, אשר הוא לא קטן.

נלך ל-hex workshop המוכר והאהוב, ונראה שהתמונה מכילה מידע נוסף. נראה שוב pk וקובץ exe. נעתיק את הבתים שלא מתארים את התמונה, ונפתח אותם קובץ בפני עצמו (או שנעשה unzip לתמונה באמצעות לינוקס), ונראה שקיבלנו **עוד zip**.

שלב 4:

נחלץ את ה-exe שמופיע בתוך ה-zip ונריץ אותו.

שלב 4.1:

לראות שיש סטרינג שבודקים מולו ושהשסטרינג שנבדק הוא קלט מהמשתמש בטרמינל. צריך להבין איך להכניס את הסטרינג כקלט (דורש לשים מרכאות מסביב) ואז עוברים לשלב 4.2

שלב 4.2:

אפשר לראות שיש אלגוריתם שעושה שחלוף בין החצי הראשון לשני בסטרינג ואז עושה קסור של כל אות עם תו קבוע. אפשר לעשות את השלבים הפוך על הסטרינג המוצפן ולקבל את הסיסמא הנכונה.

שלב 5:

נראה שהמחרוזת שנקבל משלב 4 היא לא קריאה.

חשד: המחרוזת מוצפנת.

ננסה את דרך ההצפנה XOR שהופיעה בשלב הקודם. נחפש אחר המפתח ואז נראה שרשום בכיתה בענק מסוגלות וגם במשפט שהופיע בסוף שלב 4. נעשה XOR mesugaloot ונקבל את המשימה הבאה.

שלב 6:

כפי שהיה רשום לנו במשימה, נשלח ping לכתובת הרשומה. נקבל ping בחזרה ולא נבין מה הלאה.

נסניף את התעבורה ב-wireshark ונראה בפקטות ICMP, padding שנראה מוזר. נראה שהוא מכיל '=' ותווים באנגלית, ונבין שהוא מוצפן ב-base64. נפענח אותו ונקבל את השלב הבא.

שלב 7:

הטקסט שפיענחנו בשלב הקודם אמר לנו לחפש קובץ מפה. בעזרת הפקודה tree הם ימצאו כמה קבצים שמכילים את המילה map, אבל רק אחד מהם יהיה הנכון. ניתן לדעת מי הנכון לפי כך שבנתיב לקובץ מפה הנכון יהיה רשום this is the right path. כשהם יפתחו את הקובץ יהיה להם רשום לזכור מספר כלשהו ולגשת אלינו.

שלב 8:

מקבלים תמונה של מפה, ומבינים שצריך למצוא את החדר X. נזכרים במספר שהיה רשום לזכור, ומבינים שזה המספר של החדר. הולכים לשם ושם יהיה משהו שהחבאנו. משם חוזרים לכיתה הרגילה וניצחון!