"הוירוס"

הרעיון של הוירוס הוא שהוא נמצא במחשב אחד ואח"כ מתפשט לעוד מחשבים בטווחי זמן קבועים.

ה"וירוס" מחולק לשני חלקים. לשרת ולקוח. הלקוח הוא החלק שמוטמע אצל הקורבן והשרת נמצא בתוקף.

החלטנו שאין צורך לעטוף את הוירוס בshellcode היות וזה לא החלק החיוני לpoc, אנו מנסים רק למצוא את התקשורת שהוא יוצר, ולא את ההכנסה שלו למחשבים.

מה קורה אצל הלקוח?

1. הלקוח יוצר תקשורת (סוקט עם השרת).
2. יוצר רשימה של כל הקבצים בdirectory הנוכחי.
3. הוא שולח את הרשימה לשרת ומחכה להודעה עם שם הקובץ הרצוי.
4. לאחר הגעת ההודעה, נשלח גודל הקובץ ותכולתו.

מה קורה אצל השרת?

1. השרת נענה לסוקט הלקוח.
2. השרת מקבל את רשימת הקבצים מהלקוח ושולח את שם הקובץ הרצוי.
3. הוא מקבל מהשרת את הקובץ הרצוי ואת גודלו.