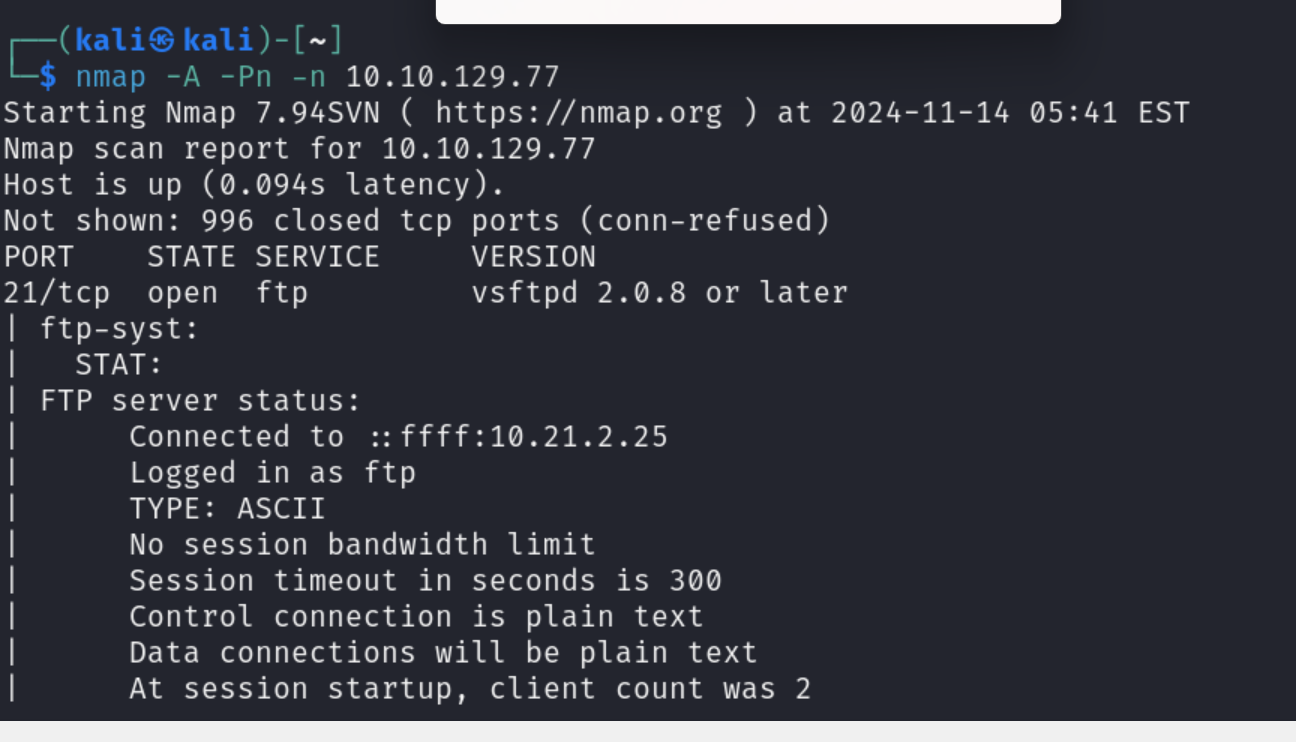
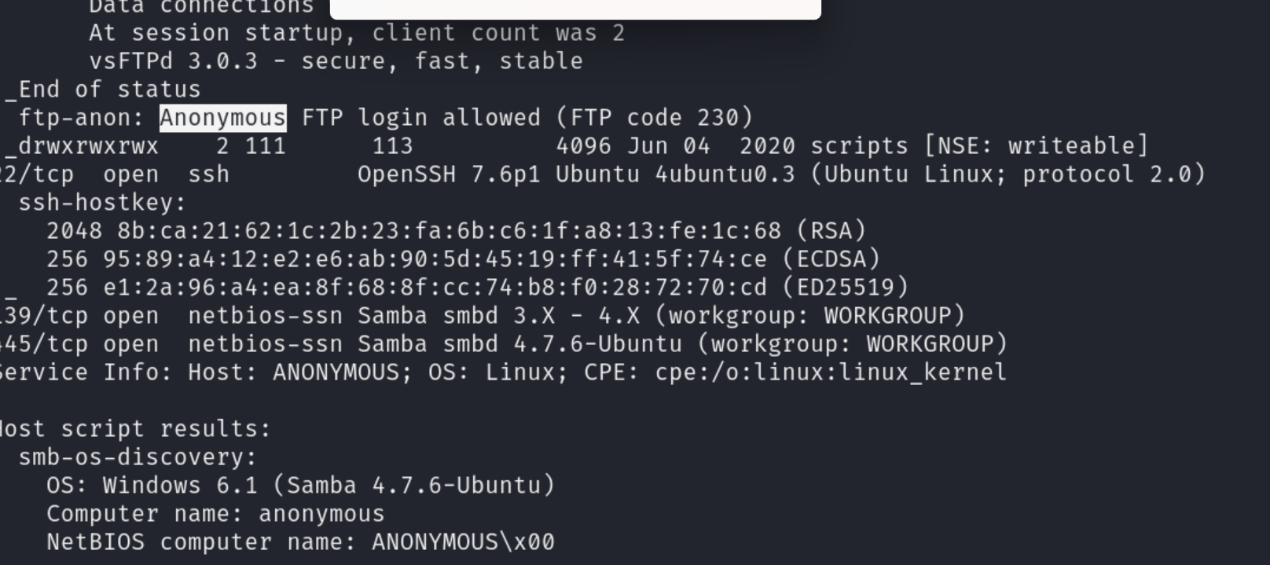
**'דוח pt**

בחרתי לתקוף את החדר Anonymous ב try hack me-

ראשית עשיתי ***recon*** ע"י הכלי nmap השתמשתי בפקודה ובפלגים הבאים :

**nmap -A -Pn -n 10.10.129.77**

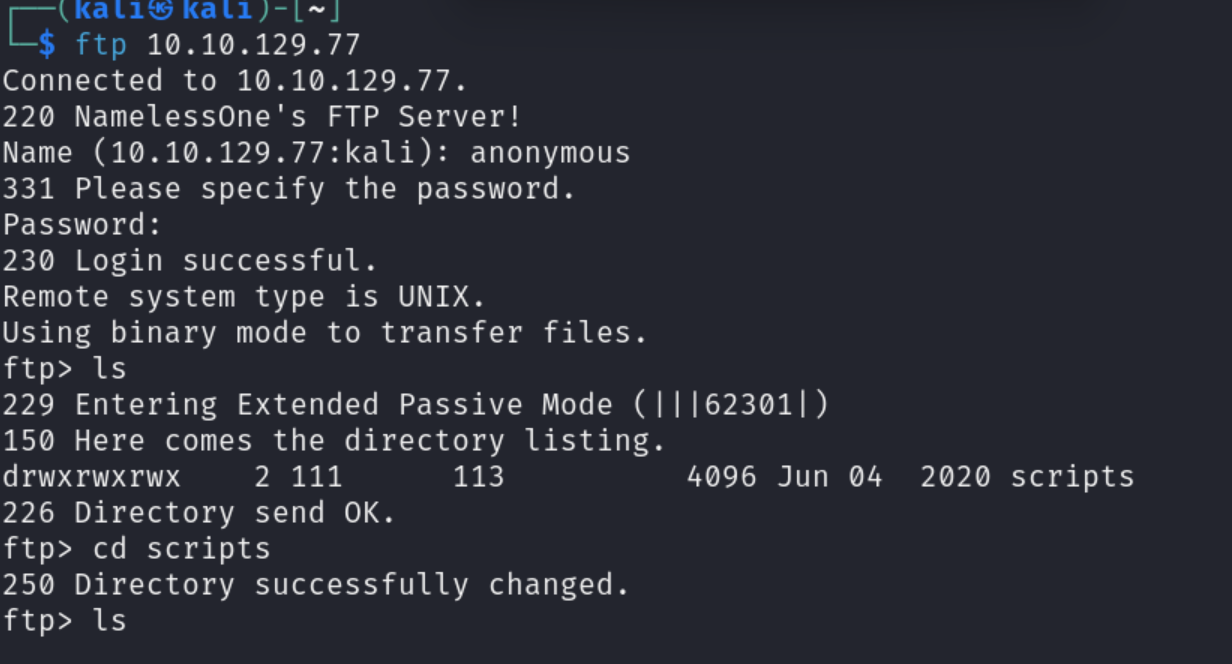




מצאתי 4 פורטים פתוחים ומצאתי את ה ***vulnerability***  שלהם החלטתי ללכת על

פורט 21 שזה פרוטוקול שמאפשר העברת קבצים ברשת ושאפשר להתחבר ל ftp בצורה אנונומית בלי סיסמא . ראיתי את הגירסה שהיא פגיעה vsftpd 2.0.8

התחברתי לftp ע"י הפקודה **ftp 10.10.129.77**



רשמתי את השם משתמש : Anonymous וכאן בעצם התחברתי ftp

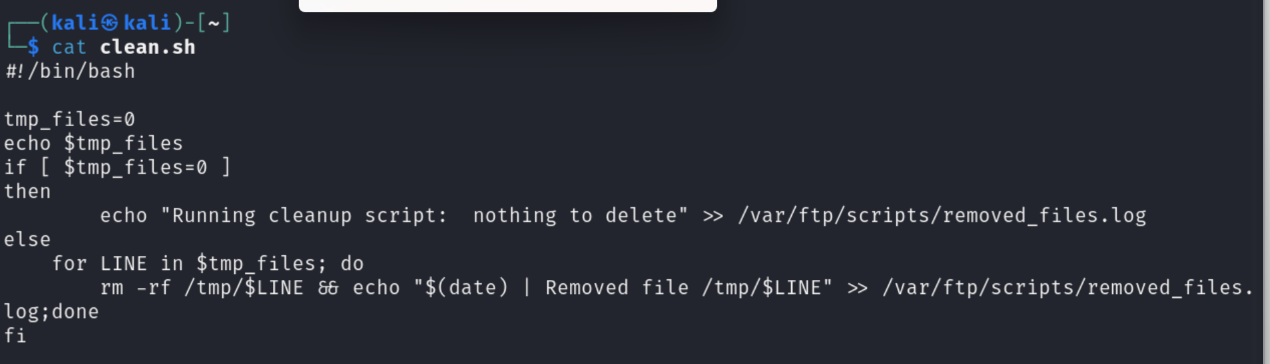
כאן אני בעצם עושה ***exploit***

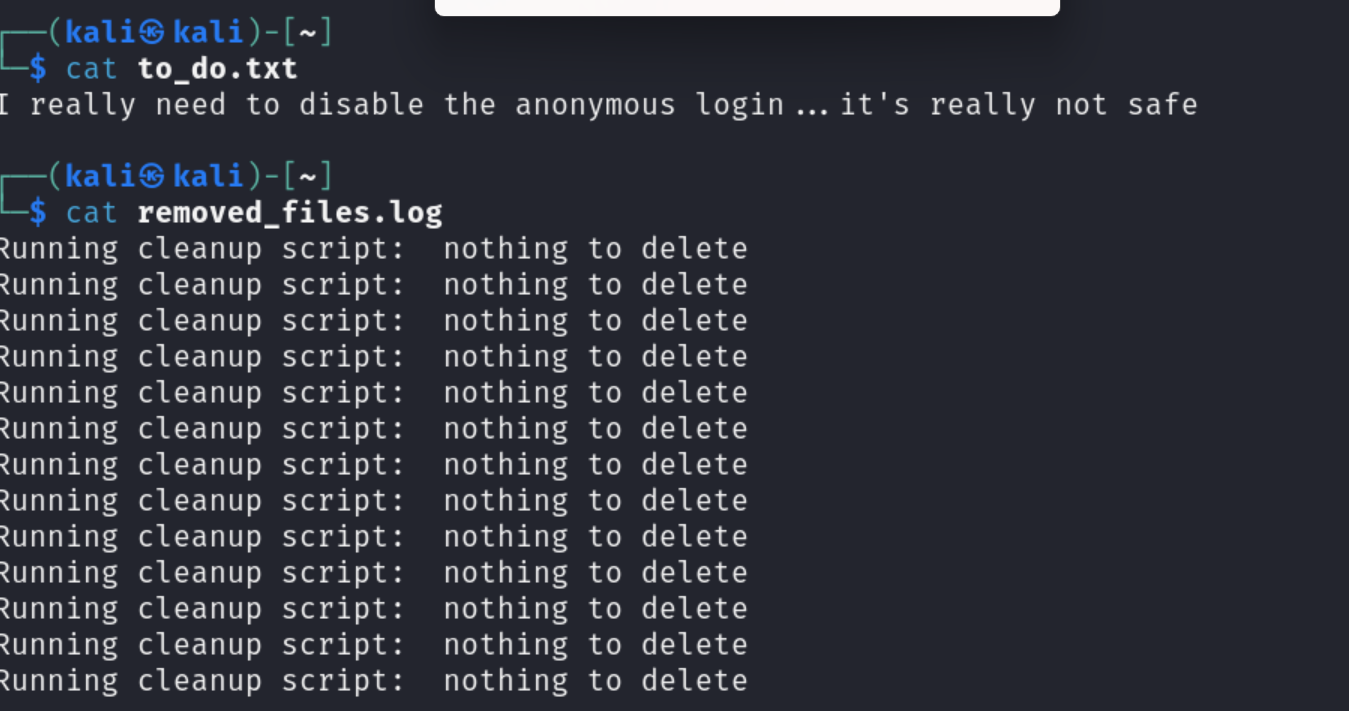
ומשם נכנסתי לתיקייה ובתוכה ראיתי 3 קבצים אז קודם כל הורדתי אותם אליי ע"י הפקודה:

1) get clean.sh 2) get removed\_files.log 3) get to\_do.txt

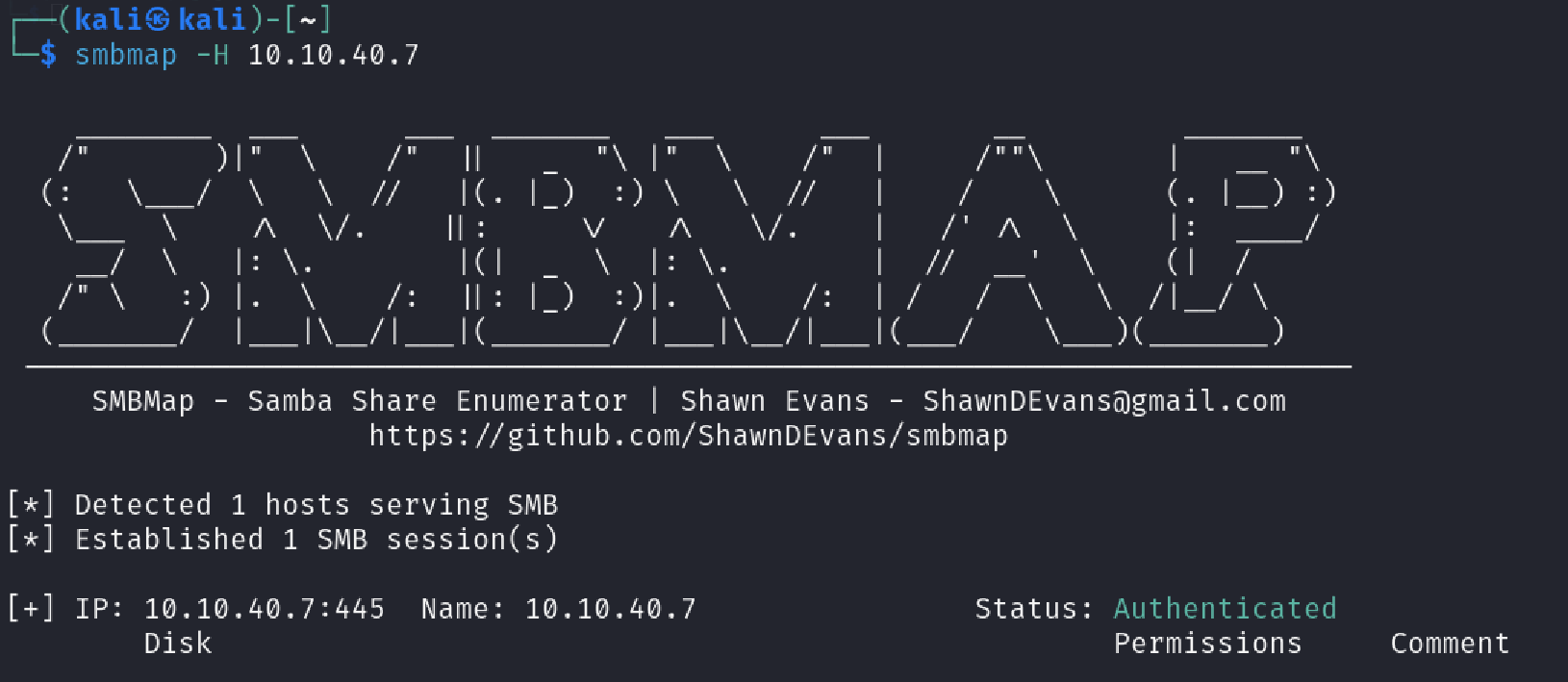
אחר הרצתי אותם כדי לראות מה כל אחד עושה :

1) cat to\_do.txt 2) cat removed\_files.log 3) cat clean.sh

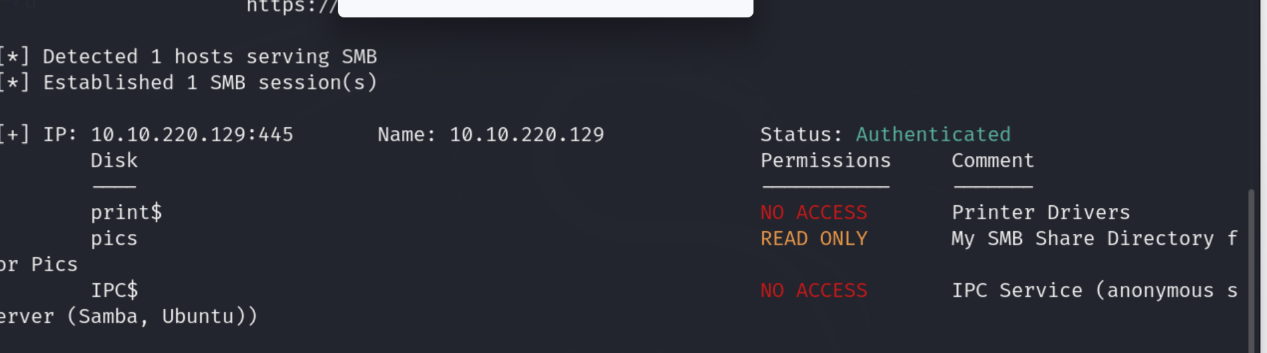




אחר כך נכנסתי ל smbmap -H 10.10.129.77 כאן רציתי לבדוק אם יש שיתופים על המחשב הזה וראיתי שזה **pics**



ושיניתי את הייפי כי זה השתנה לי בגלל שנגמר הזמן במכונה



בקובץ cat to\_do.txt ראיתי שרשם שזה לא בטוח וצריך להסיר את זה.

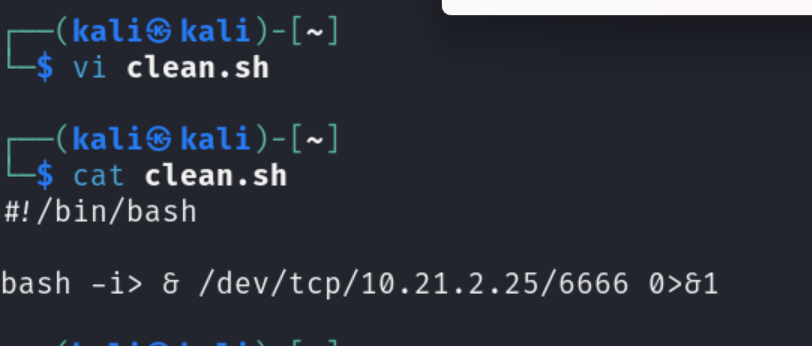
בקובץ cat removed\_files.log אני רואה שמריץ סקריפטים וניראה שאין מה למחוק.ובקובץ cat clean.sh יש סקריפט שרץ כל זמן מסוים ורשום var ftp script אני צריכה למצוא לו מעטפת הפוכה ושם חיפשתי על פייתון ואת זה אני מעתיקה ושמה בקובץ חדש פתחתי נוטפד והדבקתי שם שיניתי את אייפי של המכונה שלי ופורט 1234 אחר העתקתי אותו ל nano clean.sh

ויצרתי מאזין : 1234 nc -nvlp

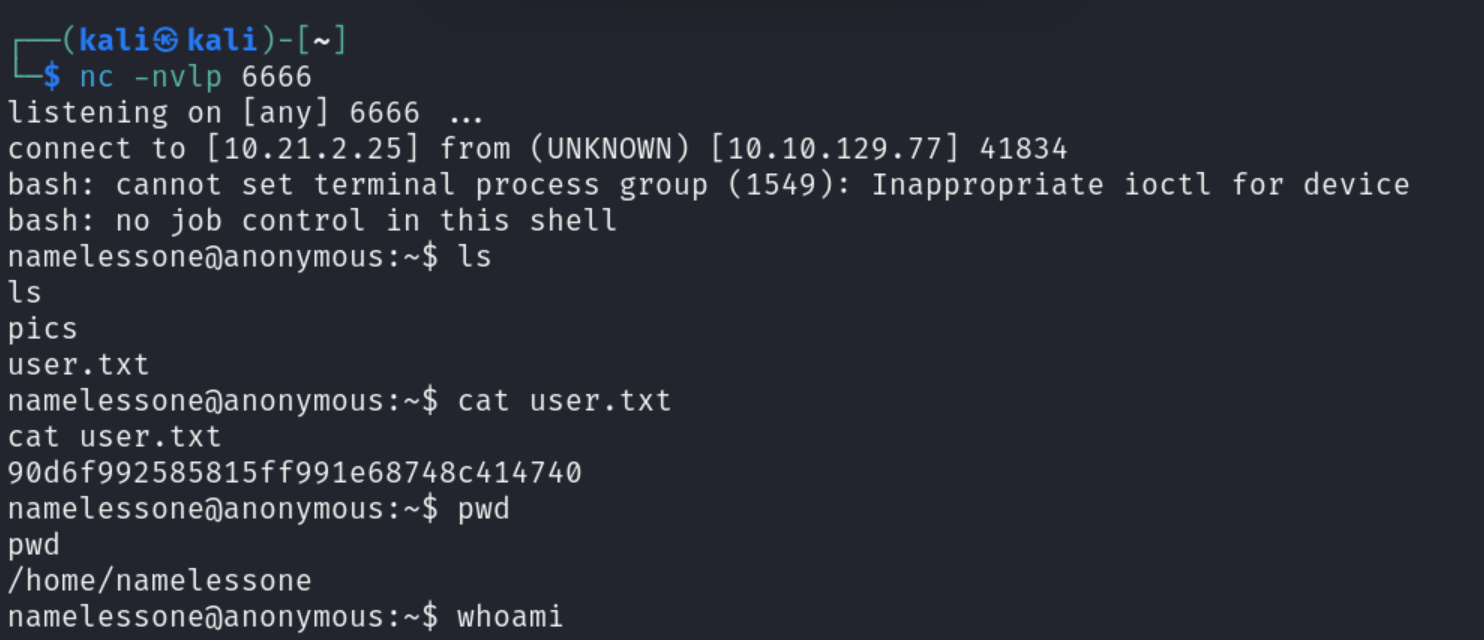
חזרתי חזרה ftp העליתי את הקובץ put clean.sh ורשמתי ls וראיתי שהקובץ נשאר באותו הגודל .ולא יצר לי מאזין....

ניסיתי לבדוק קישוריות עשיתי ping 10.10.129.77 והיה קישוריות ועדיין לא הצליח

אז עשיתי שינוי בקובץ clean.sh ורשמתי הפעם



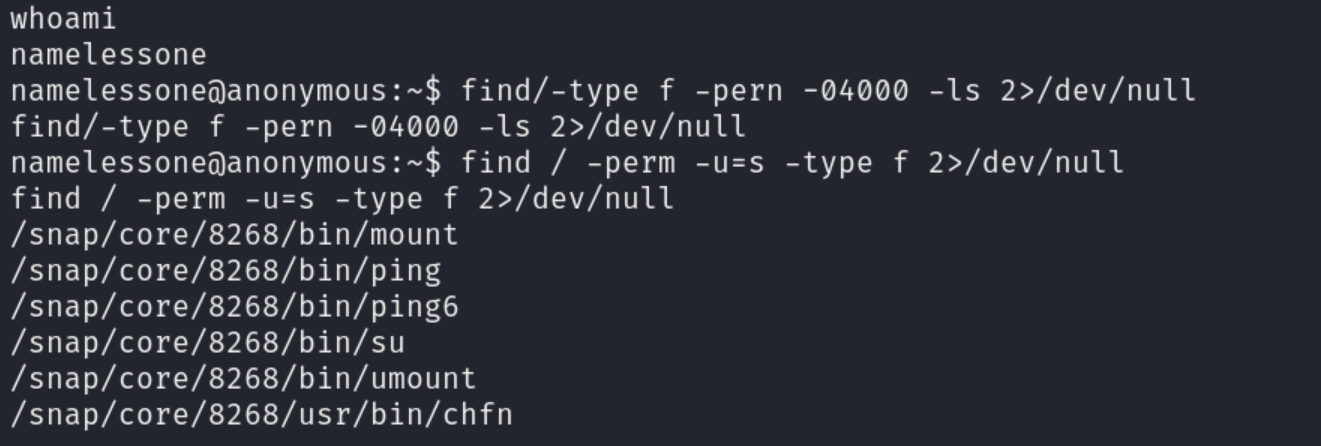
אז בעצם אני רוצה ליצור shell ואני רוצה שיתחבר מרחוק וכל השגיאות יעביר ל <& ולפורט פנוי 6666 ועכשיו אני יצור את המאזין עם הפורט הזה.

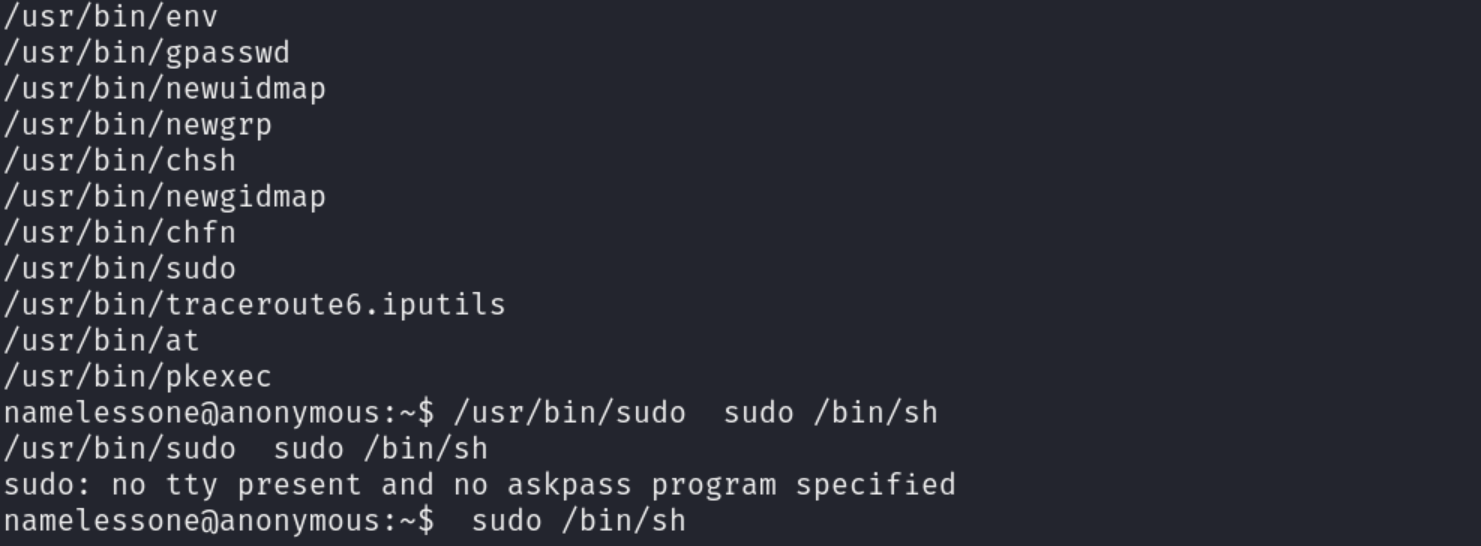


כאן אני רוצה להשתמש ב***pylod***

ועשיו אני רוצה להעלות הרשאות וראיתי את הקובץ של user.txt

רציתי לבדוק איפה נמצא הקבצים של root ןכאן זה נמצא הפקודה הראשונה לא צלחה לי ניסיתי פקודה אחרת דומה וזה כן נתן לי .

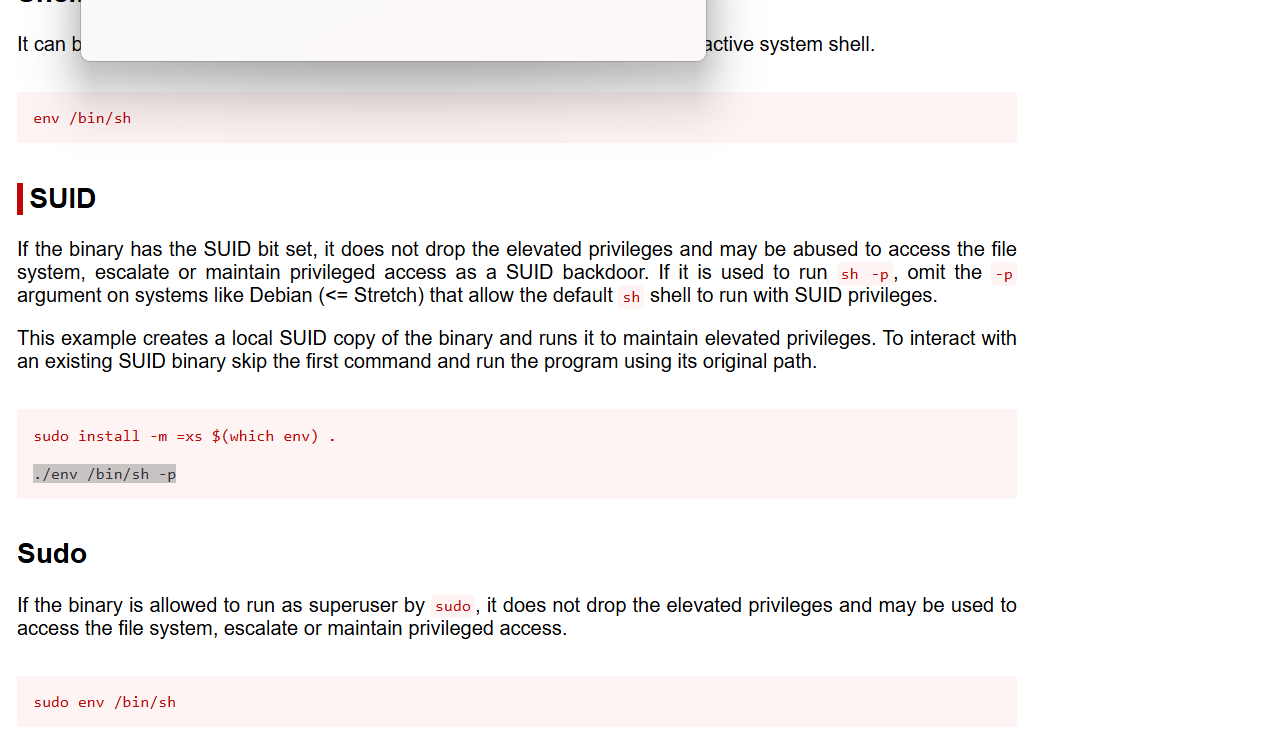




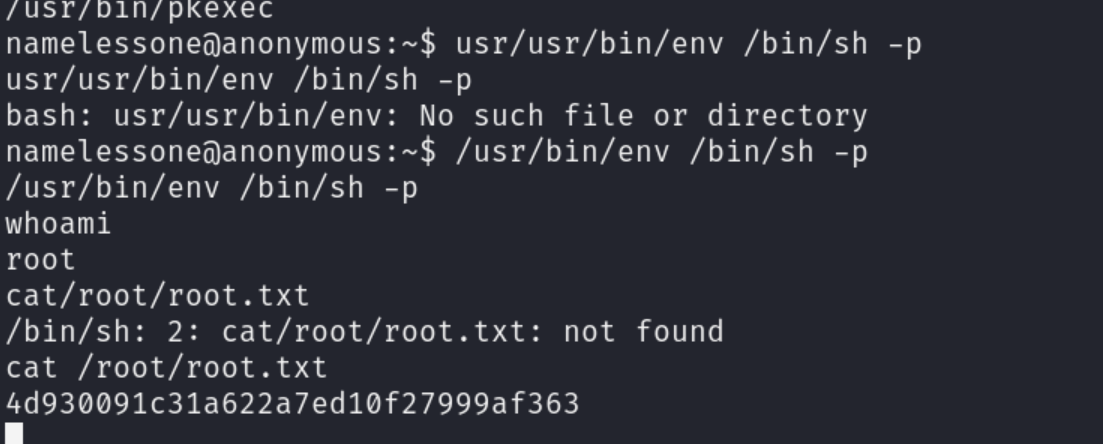
העתקתי את הקובץ ונכנסתי לאתר gtpobins

שם הוא נתן לי כל מיני קונפיגורציות להשתלטות על המערכת רשמתי env ו אז suid

ןמצאתי את הפקודה אבל זה עדיין לא נתן לי הרשאות של רות



וניסיתי כל מיני פקודות עד שעשיתי את הפקודה הזאת : /usr/bin/env /bin/sh -p



וכאן בעצם הצלחתי ועשיתי את ה internal

**והפכתי להיות root** וראיתי את הקובץ של root

