

**פתרון למכונתLame שלHTB**

מאת דניאל גובני



# הקדמה

פלטפורמת HTB , הינה פלטפורמת אימונים ל-PT מתחילים וחובבים, שרוצים לחזק את ידע שלהם,

ולאתגר את עצמם. באמצעות אותם אתגרים, אנחנו היום נעבור על מכונת Lame מבוססת מערכת

הפעלה לינוקס, את תהליך פריצה נבצע, בעזרת Kali שלנו , וכמובן המון הגיון, למידה עצמית, ומחקר

מכונה הזאות ספציפית נחשבת, רמה קלה ומצריכה ידע בסיסי, בתפעול פריימוורק של , Metasploit.

שמכיל המון כלים, אנחנו נתעסק עם כלי , msfconsole שמכיל לא מעט אקספלויטים ופאיילודים

מכל סוגים , כעת נתחבר ל-VPN שלנו שהורדנו תחילה ב-HTB ונפעיל את מכונת Lame

ונקבל את כתובת **IP** : 10.10.10.3

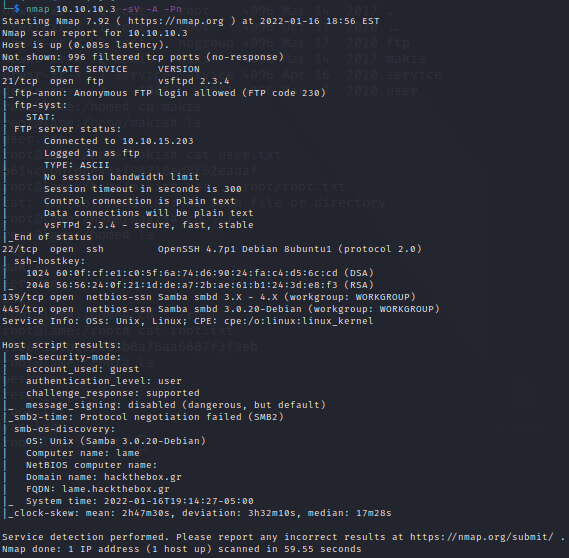


נתחיל בסריקת פורטים בסיסית נתחיל לחפש שירותים פגיעים :

sudo nmap 10.10.10.3 -sV -Pn -A -sC

בואו נחקור את שירותים, ונחפש משהו פגיע, במטרה לחדור למערכת, ולהשיג את דגלים

שלנו !



לאלו שכבר סרקו כמה מכונות, יזההו ישר שיש פה , שירות – FTP פגיע, להרצת קוד

נוכל לברר גם בעצמנו אם שירות פגיע, בגוגל אני לפני גוגל מנסה, את searchsploit –

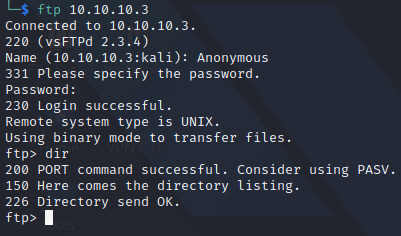
כלי נהדר שעוזר לנו לחפש אקספלוטים שכבר מותקנים , לנו על Kali , כמו כן בואו נתעמק ,

בכל סריקה למקרה נקודת כניסה שלנו לא תהיה FTP לפני שאנחנו מתחילים בשלב השגת גישה

למערכת נתחיל בהבנה שלה מה היא מריצה איזה שירותים נוכל להתחבר דיפולטיבי איזה נוכל לפרוץ

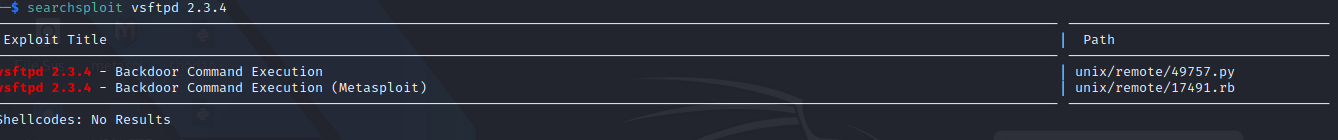
ועוד...

אז האם נשים לב אנחנו יכולים להתחבר לשירות FTP באמצעות אנונימוס (שם משתמש וסיסמה ברירת מחדל בהמון FTPים) אז ננסה ואם נסייר בשרת FTP ניראה שאין כאן כלום שיעזור לנו ☹



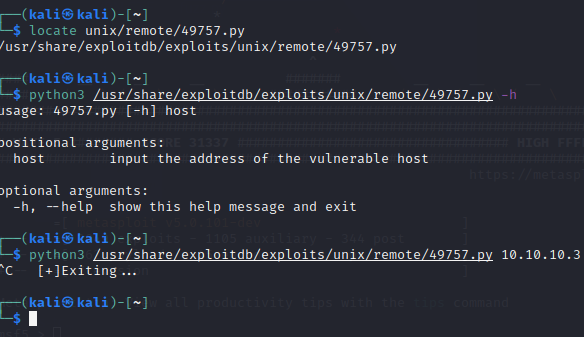
אבל הגרסה פגיעה כמו שאמרנו בהתחלה אז אני יחפש את גרסה,

של FTP הפגיע וניראה שיש לנו כמה אקספלויטיים :



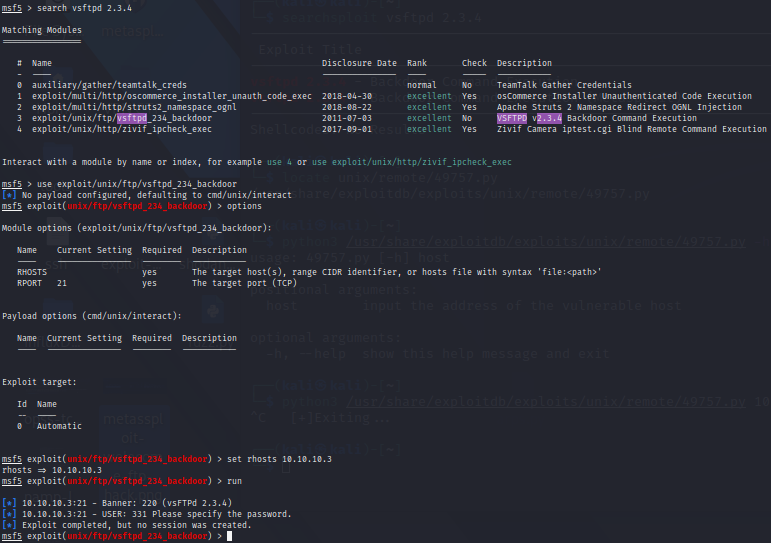
ניתן ליראות שקיים לנו במכונה שתי אקספלויטים אחת מקושר למטאספליוט ואחד מ exploit-db-

אני ינסה תחילה את exploit-db וניראה שהוא דורש רק HOST הכוונה לכתובת אייפי נעביר לו ונחכה



לאחר כמה דקות לא קיבלתי תגובה משרת ומשהו וזה לא עבד אז הלכתי למטאספלויט וחימשתי אותו

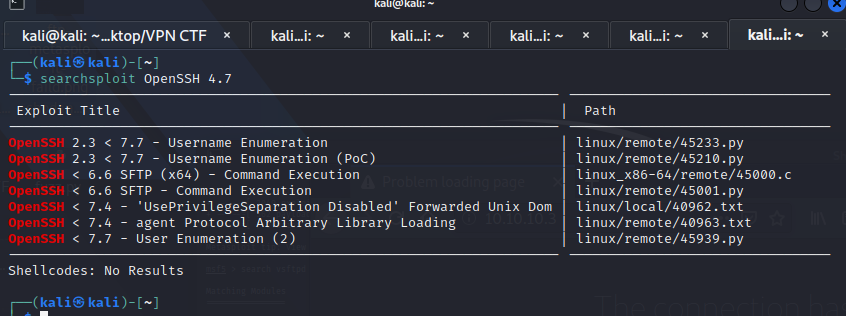
ונסתי שוב :



ושוב נכשל נסתי מספר פעמיים וכשלון חוזר על עצמו עם מספר כלים שונים אז הגיע הזמן לשנות גישה

משהו שאתם חייבים לזכור תמיד אנחנו חייבים להיות בעלי ראש "פתוח" לנסות דברים אחרים העיקר מה שלא הרבה מבינים הוא ניסוי וטעייה ואם משהו לא מצליח בפעם העשירית שום דבר לא ישתנה בפעם העשרים וכנראה יש לו סיבה והגיע הזמן לבצע חישוב מסלול מחדש אבל **לעולם** לא לזנוח נקודות תקיפה פוטנציאליות ייתכן שמקרה הזה הותקן - [Patch](https://he.wikipedia.org/wiki/%D7%98%D7%9C%D7%90%D7%99_%D7%AA%D7%95%D7%9B%D7%A0%D7%94) אז נחזור לסריקה שלנו ונסתכל שיש לנו גם

שירות SSH פגיע אבל פגיעות כאן נמוכה ולא משמעותית :



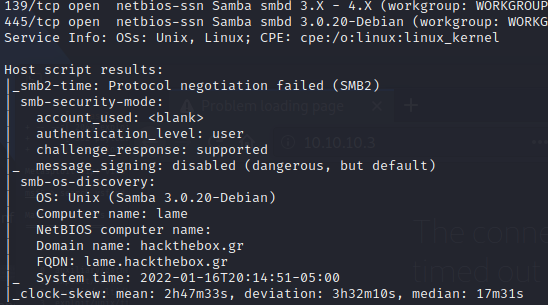
היא תוכל לעזור לנו בלדעת איזה משתמשים

קיימים במכונה את פגיעות הזאות נשים בצד למקרה שנמצא סיסמה במערכת ננסה למחזר אותה

בשירות – SSH ואם לא נוכל להתחבר ל-ROOT נוכל לקבל באמצעות פגיעות את כל משתמשים על מכונה

ולבדוק אולי סיסמה שייכת להם אז כרגע אין לי עניין ה-SSH אולי נחזור אליו בהמשך

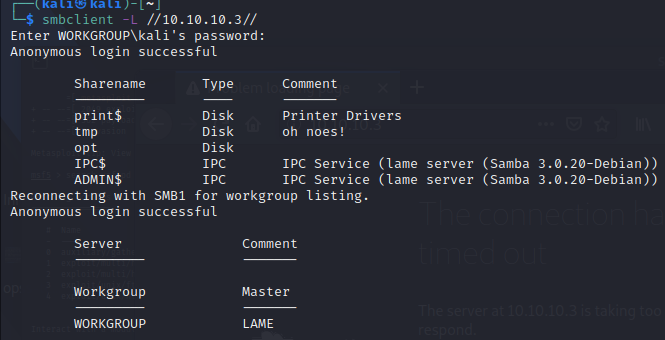
אז נמשיך וניראה שיש לנו גם שירות [SMB](https://he.wikipedia.org/wiki/SMB_(%D7%A4%D7%A8%D7%95%D7%98%D7%95%D7%A7%D7%95%D7%9C)) זה ניראה מעניין אם נסתכל על תוצאות של -Nmap



מגניב נראה שהרשאות כאן לוקות בחסר וקיבלנו את גרסה מדויקת : Samba 3.0.20

ננסה תחילה להתחבר באמצעות smbclient סיסמה נכניס ריקה ונראה שיש לנו גישה

לכמה תיקיות בשרת SMB אז נבדוק מה יש בתוכם :



אז לאחר שתחברנו קיבלנו רשימה של תיקיות לפנינו אנחנו ננסה לגלוש לשתי תקיות

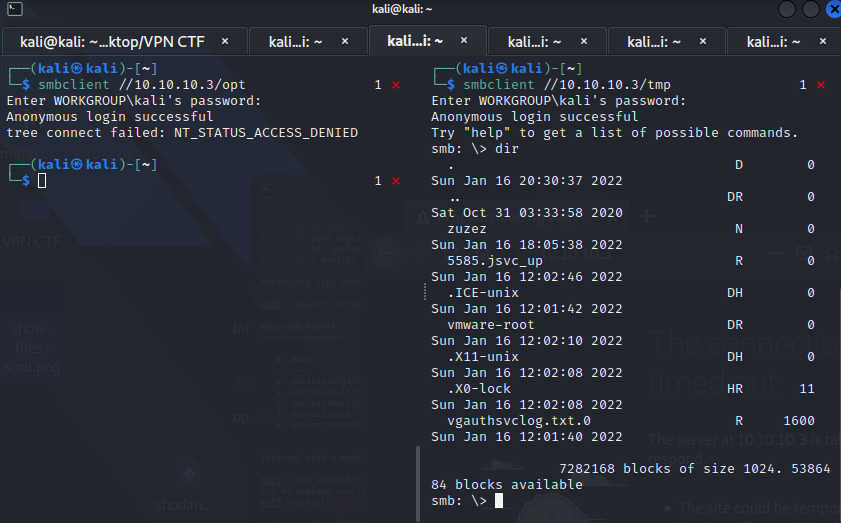
שאנחנו רואים שיש לנו כישה אליהם וננסה להבין מה יש שם אולי משהו שיעזור

לנו ואם לא אולי גרסא פיגעה מי יודע ?

ניראה בתיקיות tmp,opt אין שום דב מעניין עברתי כל כל קבצים ולתקייה אחת אחן לנו גישה והגיע

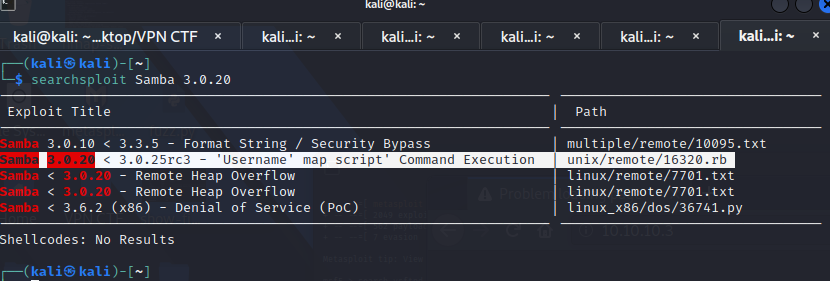
הזמן לחפש פגיעות לשירות SMB שלנו שמכיל את גרסאת – Samba 3.0.20

ניתן ליראות בצד ימין את תקיית tmp ומצד שמאל את תקייה שאין לנו גישה אליה opt



נוכל גם לראות שיש לנו פגיעות הרצת קוד לגרסא שלנו במטאספלויט אני ינסה לברר קצת

על חולשה בגוגל ונגלה שהיא מאוד ידוע וישנה [(2007-2447-CVE)](http://cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2007-2447)



נפתח את מטאספלויט ונתחיל בחימוש שלנו אם לא יעבוד נעבור לאקספלויטים הבאים כמו

שאתם רואים קיימות לנו מספר אקספלוטים שנוכל להתשמש בהם כעת יש כאלו אוהבים לקרוא

לזה ([POC](https://he.wikipedia.org/wiki/%D7%94%D7%95%D7%9B%D7%97%D7%AA_%D7%94%D7%99%D7%AA%D7%9B%D7%A0%D7%95%D7%AA)) כי אנחנו בעצם מוכחים היתכנות של פגיעות פוטנציאלית חדל קישוקושים ונחזור

לעבודה שלנו ! אנחנו צריכים לחפש את פיגעות במטאספלויט פקודות מסודות כאן :