# פתרון מעבדה 1

CYBER SCHOOL

## SearchSploit


כל הזכויות שמורות © סייבר סקול בע"מ, אילנות 7, כרמיאל | 077-7781383

CYBER SCHOOL

## נושאי המעבדה

דרך ההצגה של כל הניצולים הזמינים וכיצד להוריד אותם באמצעות SearchSploit דרך CLI.

## זמן מוערך

15-30 דקות

## סביבת מעבדה

- סביבה וכלים
  - VirtualBox
    - Kali Linux
- SearchSploit


כל הזכויות שמורות © סייבר סקול בע"מ, אילנות 7, כרמיאל | 077-7781383

# משימת מעבדה: עבודה עם SearchSploit

יש להשתמש ב-SearchSploit כדי למצוא ולהוריד ניצולים עבור שירותי OpenSSH ו-Apache.

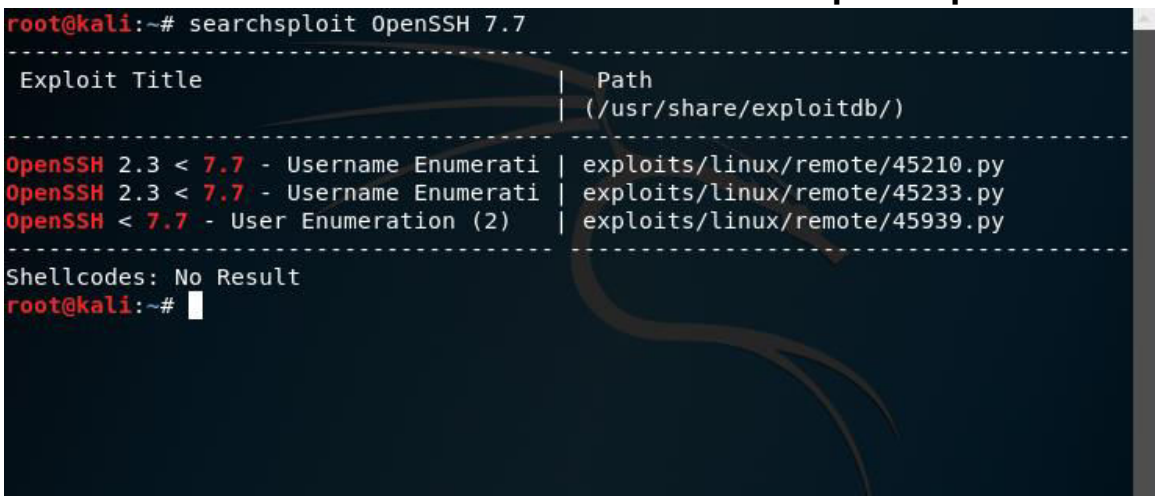
1. יש לוודא שהמכונות הווירטואליות Kali ו-pfSense פועלות.
2. במחשב Kali, יש להשתמש ב-SearchSploit כדי לחפש נקודות תורפה ב-OpenSSH 7.7.

פתרון :

יש להתחיל הפעלת מסוף על ידי לחיצה על הסמל המודגש בצילום המסך למטה.

כדי לחפש נקודות תורפה באמצעות **SearchSploit**, יש להריץ את הפקודה:

**searchsploit OpenSSH 7.7**





כל הזכויות שמורות © סייבר סקול בע"מ, אילנות 7, כרמיאל | 077-7781383

יש שלוש נקודות תורפה פוטנציאליות שאפשר לנצל.

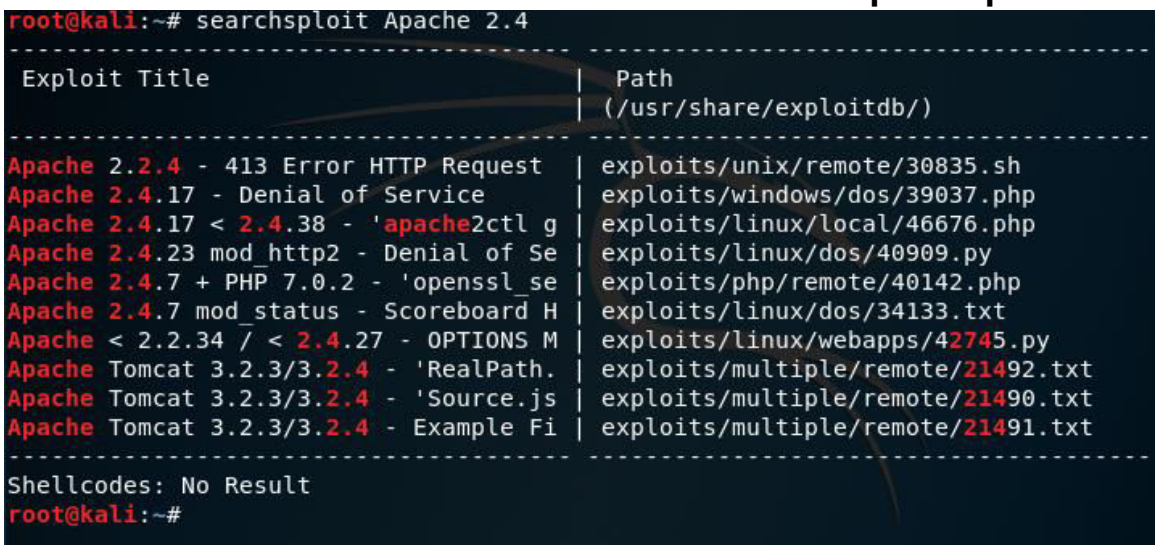
יש לשים לב כמה נקודות תורפה פוטנציאליות אפשר לנצל.

3 יש להשתמש ב-SearchSploit כדי לחפש נקודות תורפה ב-שירות Apache 2.4 ולשים לב כמה נקודות תורפה פוטנציאליות יש ב-Apache 2.4.

פתרון :

כדי לחפש נקודות תורפה באמצעות SearchSploit, יש להריץ את הפקודה:

**searchsploit Apache 2.4**



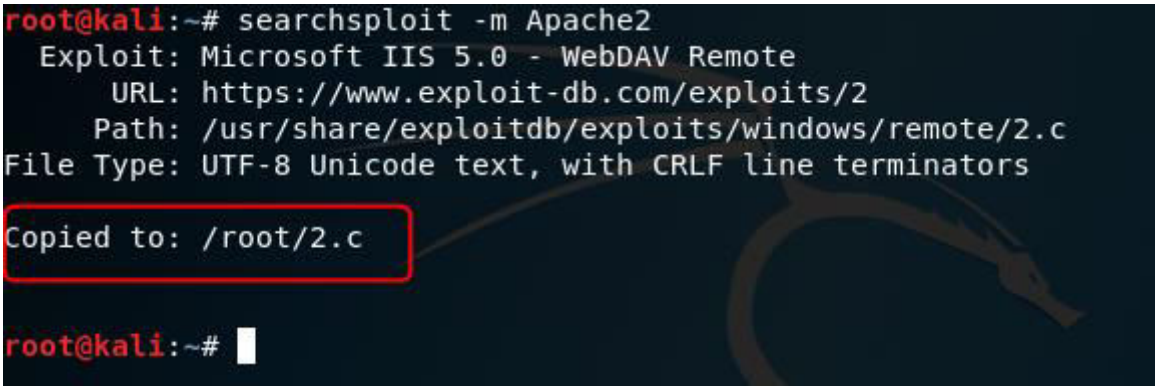

ניתן לנצל שש נקודות תורפה אפשריות.יש שלוש נקודות תורפה פוטנציאליות שאפשר לנצל.


כל הזכויות שמורות © סייבר סקול בע"מ, אילנות 7, כרמיאל | 077-7781383

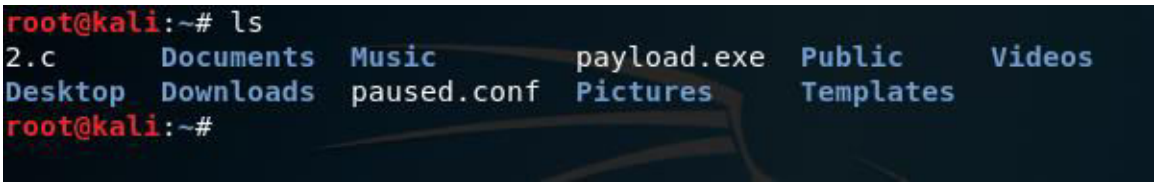
4 יש להשתמש ב-**SearchSploit** כדי העתיק את הסקריפט של Apache ולאמת שהקובץ קיים לאחר ההורדה.

## פתרון :

כדי להוריד את הסקריפט, יש להריץ את הפקודה את **searchsploit -m Apache2**




כדי לוודא שהקובץ הורד, יש להריץ את הפקודה **ls** בספרייה שאליה הוא הועתק, או פשוט **ls** בספרייה הנוכחית: **/ls/root/Desktop**





כל הזכויות שמורות © סייבר סקול בע"מ, אילנות 7, כרמיאל | 077-7781383

# רמזים

**משימת מעבדה**

- מריצים את SearchSploit דרך המסוף.
- יש לשקול להשתמש במדריך העזרה של SearchSploit כדי ללמוד איך להעתיק את הניצול.


כל הזכויות שמורות © סייבר סקול בע"מ, אילנות 7, כרמיאל | 077-7781383