



פתרון מעבדה 2



הצפנה מעשית

טבלת Rainbow Hash Cracking (פיצוח Hash)

- עמוד 1 -

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






נושאי המעבדה

נביר את הכלים והמושגים הכרוכים בפיצוח hashes.

זמן מוערך

30 - 40 דקות

סביבת מעבדה

- VirtualBox 
- Kali Linux live 
- rtgen 
- rtsort 
- rccrack 

משימת מעבדה

התקנת מכונה וירטואלית של Kali Linux

יש ליצור מכונה וירטואלית חדשה של Kali Linux 2019.3 VM שתשמש בקורס זה.

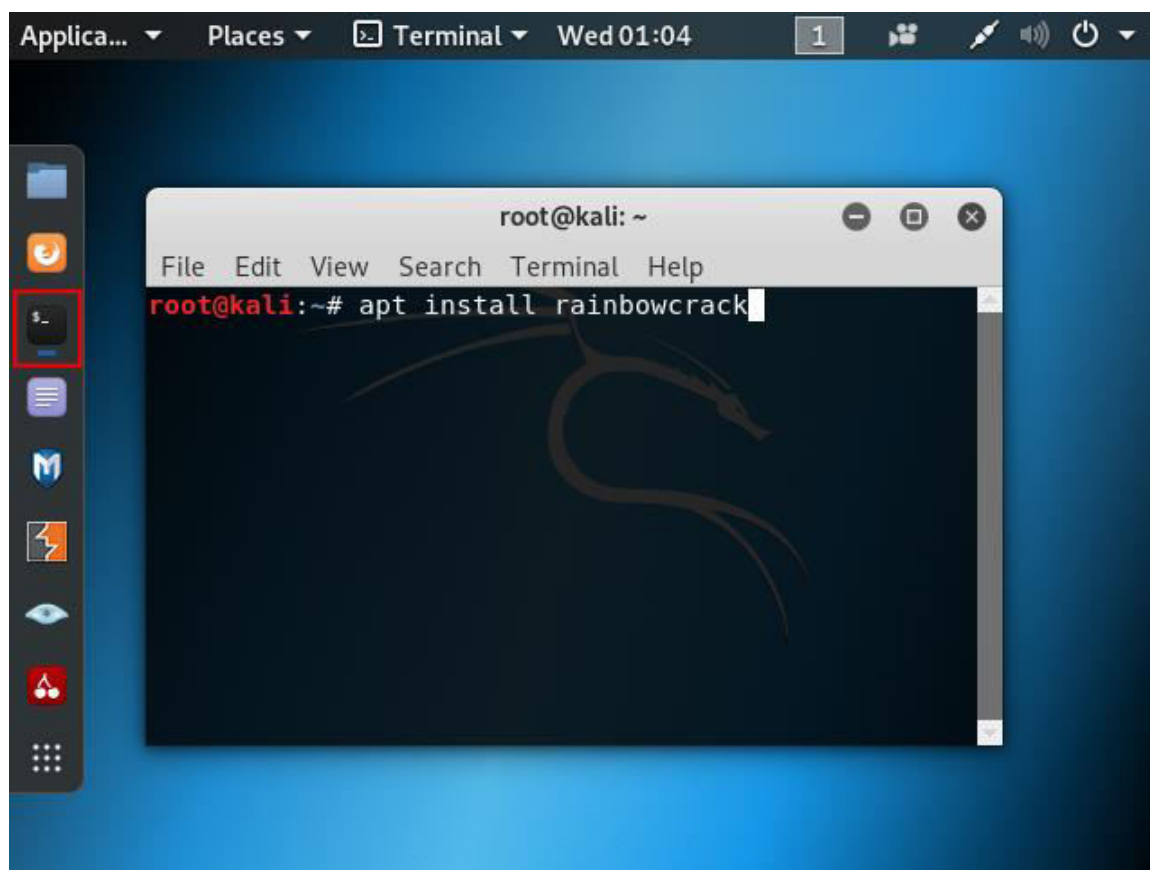
ניתן לעקוב אחר ההוראות במדריך ההתקנה של Windows 10 הממוקם במודול Installation Guide בקורס Canvas.

שימוש בטבלת Rainbow כדי לפצח Hash

יש לפצח את ה-hash הנתון באמצעות התקפת טבלת rainbow.

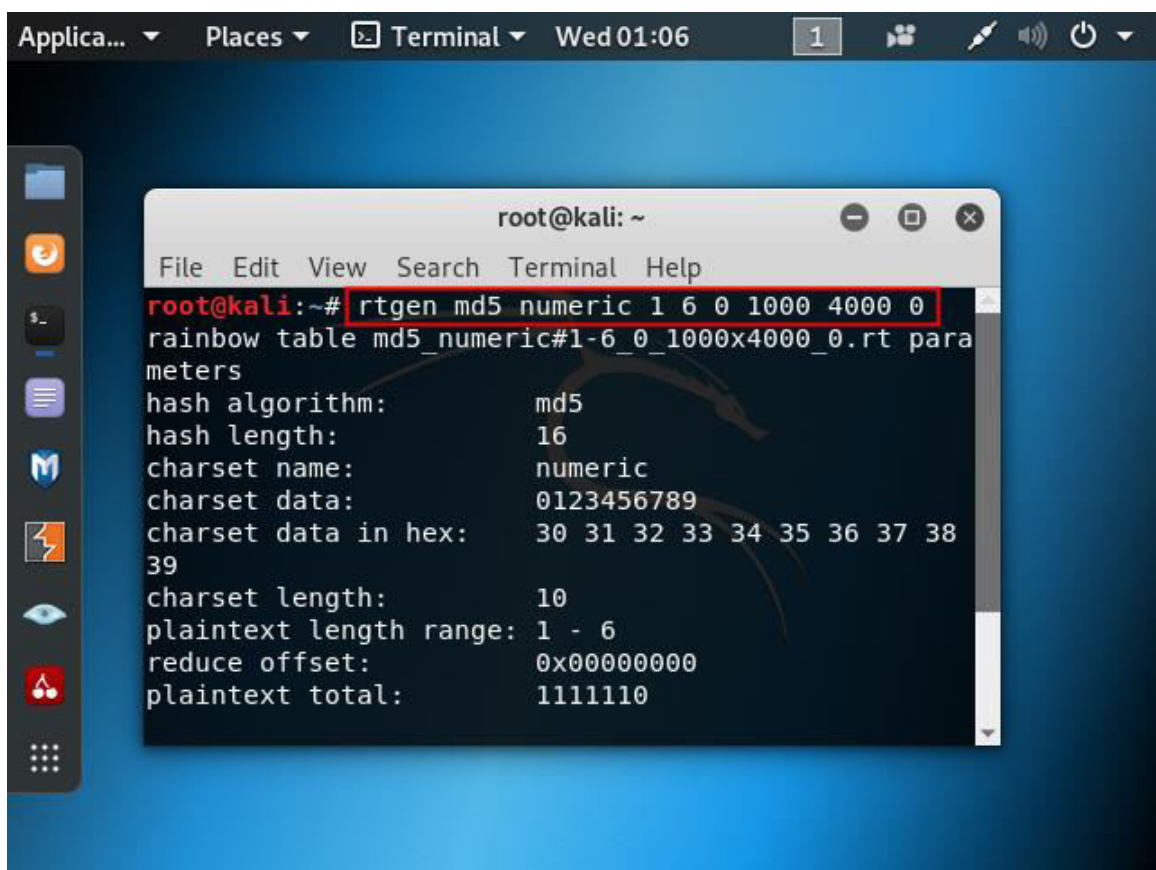
74765968c67007219b197f4d9aafb4e2

1 יש להתקין *rainbowcrack* באמצעות הפקודה: **apt install rainbowcrack**

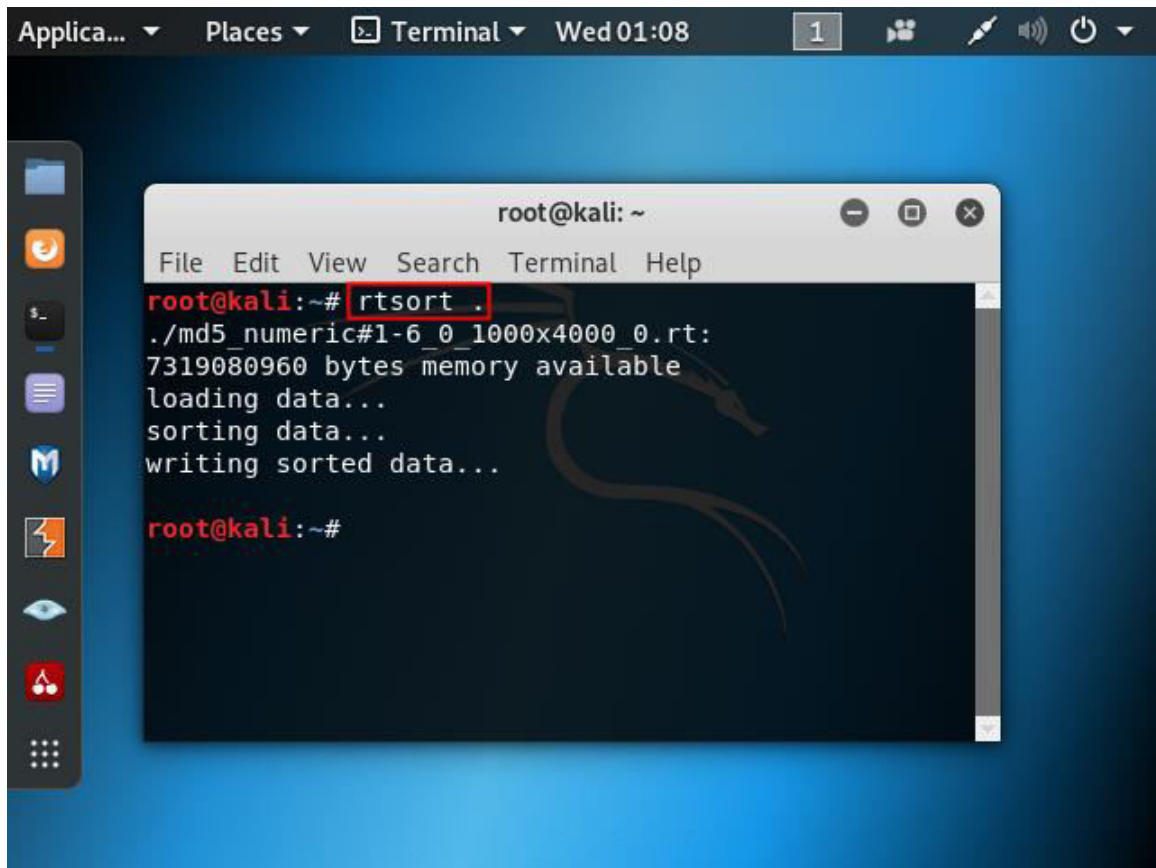


יש ליצור טבלת rainbow של md5 עם שישה מספרים באמצעות מבנה הפקודה הבא: **rtgen md5 numeric 1 6 0 1000 4000 0**

- rtgen - התכנית הבינארית המשמשת ליצירת טבלת rainbow.
- md5 - סוג ה-hash.
- numeric - מערך התווים שיש להשתמש בו, שבמקרה שלנו הוא מספרים.
- 1 - האורך המינימלי של הסיסמה.
- 6 - האורך המקסימלי של הסיסמה.
- 0 - פונקציית הרדוקציה החישובית הממפה ערכי hash לערכי טקסט רגיל.
- 1000 - אורך השרשרת שתיווצר.
- 4000 - מספר השרשראות שיווצרו.
- 0 - לכמה קבצים תחולק טבלת ה-rainbow (במקרה שלנו, 1).

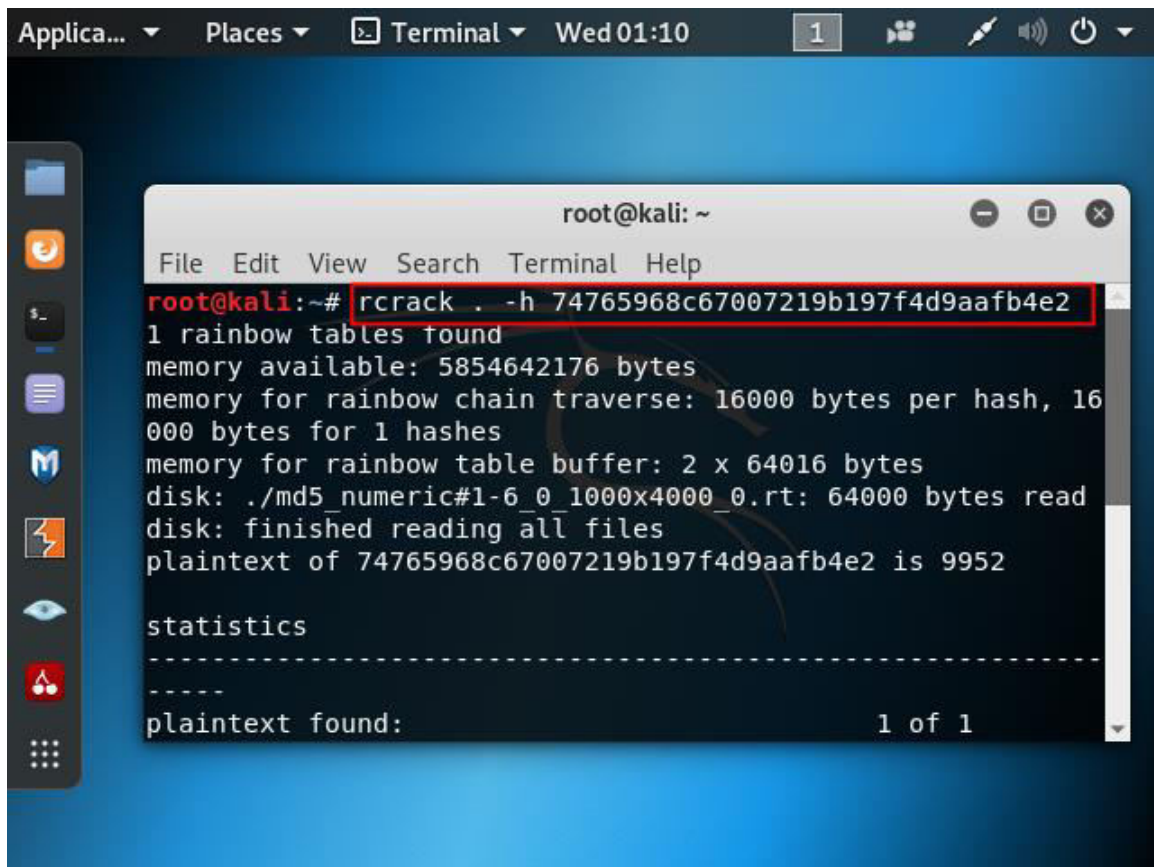


3 יש למיין את טבלת ה-rainbow בעזרת הפקודה .rtsort.



```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# .rtsort .  
./md5_numeric#1-6_0_1000x4000_0.rt:  
7319080960 bytes memory available  
loading data...  
sorting data...  
writing sorted data...  
root@kali:~#
```

4 יש לפצח את ה-hash בעזרת הכלי **rcrack**.
הערה: כדי להעתיק את ה-hash ל-VM Kali Linux, יש להשתמש ב-shared clipboard המוצג במדריך ההתקנה של Kali Linux.



```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# rcrack . -h 74765968c67007219b197f4d9aafb4e2  
1 rainbow tables found  
memory available: 5854642176 bytes  
memory for rainbow chain traverse: 16000 bytes per hash, 16000 bytes for 1 hashes  
memory for rainbow table buffer: 2 x 64016 bytes  
disk: ./md5_numeric#1-6_0_1000x4000_0.rt: 64000 bytes read  
disk: finished reading all files  
plaintext of 74765968c67007219b197f4d9aafb4e2 is 9952  
  
statistics  
-----  
-----  
plaintext found: 1 of 1
```

פתרון:

כדי לפצח את ה-hash, יש להריץ את הפקודה הבאה בחלון הפקודות:

```
rcrack . -h [hash]
```

התוצאה אמורה להיות **9952**.