جامعة الإمام عبدالرحمن بن فيصل
IMAM ABDULRAHMAN BIN FAISAL UNIVERSITY
كلية علوم الحاسب وتقنية المعلومات
College of Computer Science and Information Technology

Google Developer Student Clubs
Imam Abdulrahman Bin Faisal University

تجارب اختراق كلمات المرور - Password Cracking Experiments

لغرض التعليم FOR EDUCTIONAL PURPOSE

إعداد: عمر الغامدي

www.linkedin.com/in/omar-alghamdi7

التجربة الاولى بأستخدام اداة Hashcat

- نظام التشغيل المستخدم : Kali linux

أداة هاش كات Hashcat تستخدم لأجل اختراق كلمة المرور وتعد من أقوى الأدوات حالياً من ناحية اختراق كلمة المرور. هدف هذه الأداة تحويل الشفرة الى نص مقروء وهناك العديد من التقنيات تندرج تحت اختراق كلمة المرور ومنها:

1- القوة الغاشمة Brute force

يعد هجوم القوة الغاشمة أحد أكثر تقنيات الاختراق شيوعًا لكلمات مرور تصل إلى ثمانية أحرف. حيث يتحقق المخترق بشكل منهجي من جميع الأحرف الممكنة ، ويحسب قيمة الشفرة من مجموعة String ثم يقارنها مع شفرة كلمة المرور. يعتمد نجاح هجمات القوة الغاشمة على طول كلمة المرور. في هجوم القوة الغاشمة، يحاول المخترق كل مجموعة من الأحرف والأرقام وعلامات الترقيم لإنشاء كلمة مرور. إذا كانت كلمة المرور طويلة ، فإن هذه التقنية تستغرق وقتًا أطول من دقائق إلى عدة سنوات ، حسب النظام المستخدم وطول كلمة المرور. [5]

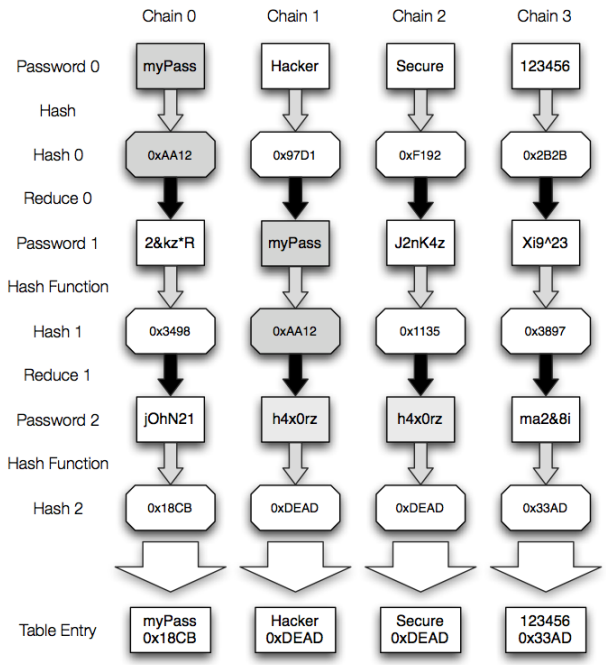
2- هجمات القاموس Dictionary Attacks

على الرغم من أنه يشبه هجوم القوة الغاشمة ، إلا أن هناك فرقًا رئيسيًا واحدًا بين التقنيتين. في هذا السيناريو، يستخدم المخترق قائمة من كلمات المرور المخزنة وتعتبر اكثر هذه كلمات المرور اكثر عرضة للاختراق (بناءً على كلمات اللغة الإنجليزية ، على سبيل المثال) بدلاً من تجربة

جميع الأحرف المحتملة واحدة تلو الأخرى. غالبًا ما تتضمن أدوات هجوم القاموس كلمات مرور معروفة وكلمات من اللغة الإنجليزية وجمل من الكتب والمزيد. [5]

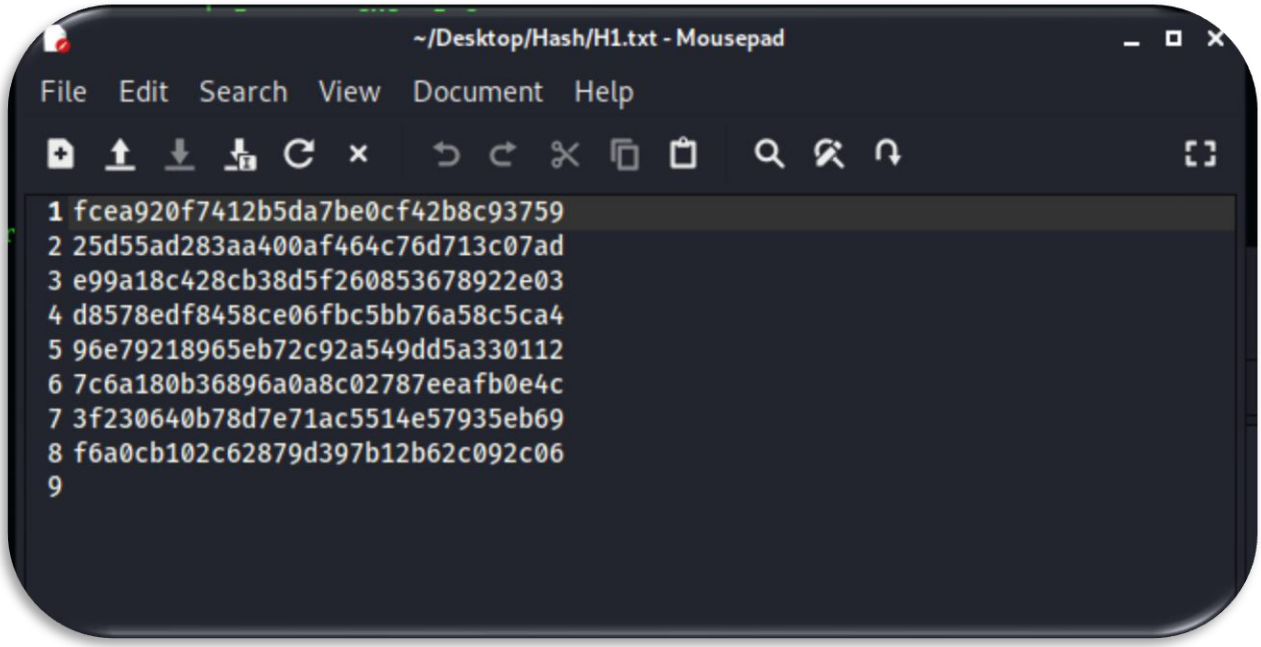
3- هجمات طاولة قوس قزح Rainbow Table Attacks

جدول قوس قزح هو جدول مُجمَّع مسبقًا يُستخدم لاستعادة التجزئة. كل جدول قوس قزح مخصص لطول محدد لكلمة مرور تحتوي على مجموعة محددة جيدًا من الأحرف. تهدف هذه التقنية إلى تقليل وقت التخمين ولكنها تقتصر على كلمات المرور التي لا تزيد عن تسعة أحرف والتجزئة بدون تشفير "Salt" لكلمة المرور. [5]



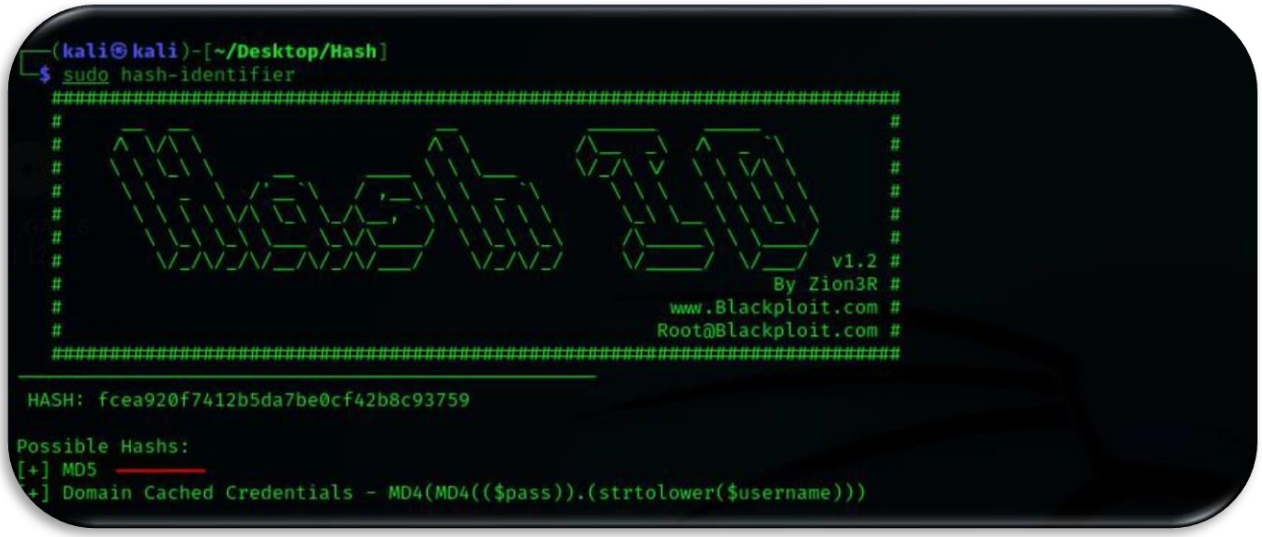
التجربة الاولى (تطبيقاً):

- ملف يحتوي على شفرات



- أداة تستخدم لتحديد نوع الشفره

Hash-identifier



- نوع الشفره MD5=0

- نوع الهجوم Straight = 0

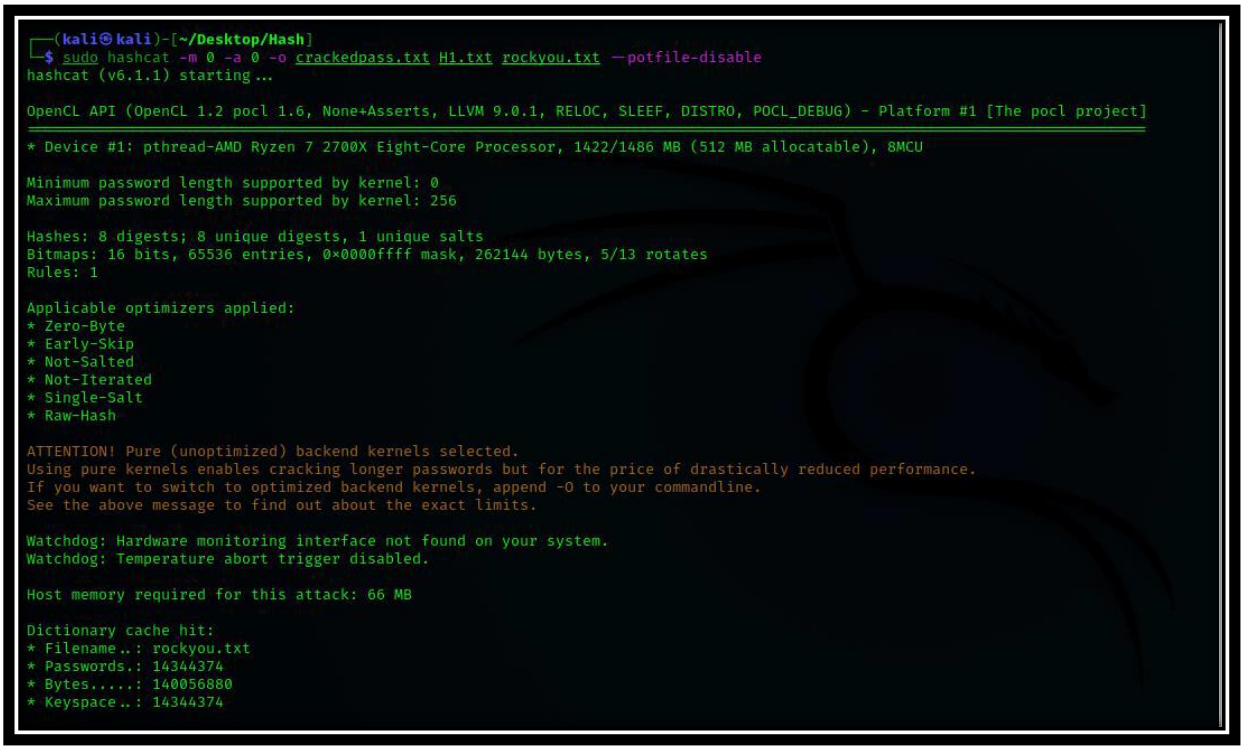
- الامر المستخدم لأداء اختراق كلمة المرور :

```
sudo hashcat -m 0 -a 0 -o crackedpass.txt H1.txt rockyou.txt --potfile-disable
```

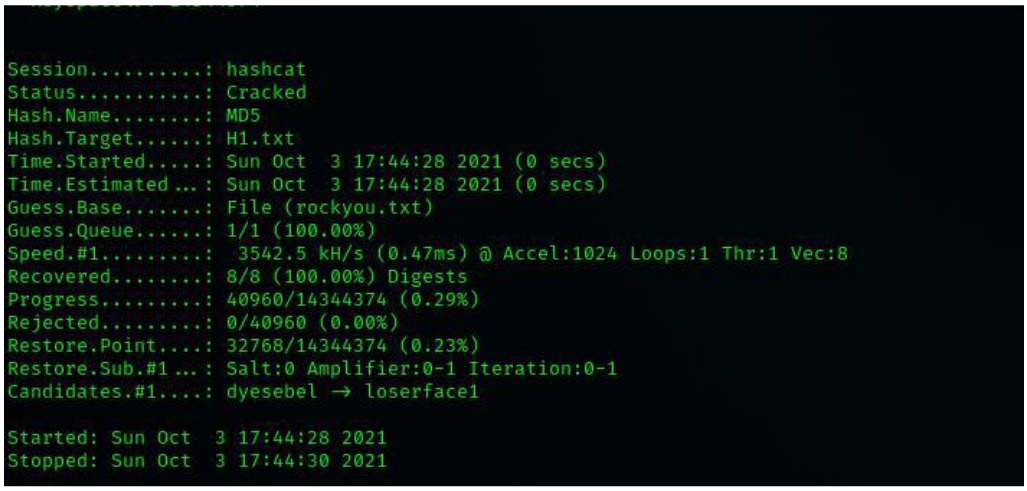
نوع الشفره -m

نوع الهجوم -a

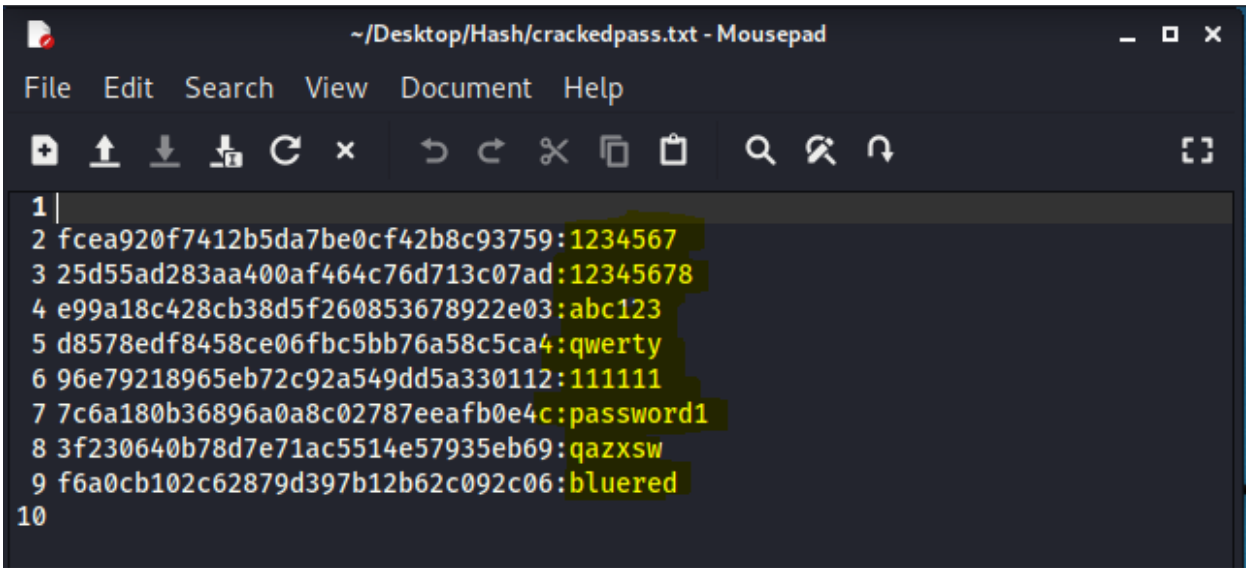
لاختراق الشفره اكثر من مره --potfile-disable



- معلومات عن اختراق الشفره



- تمت عملية اختراق كلمة المرور



التجربة الثانيه بأستخدام أداة Hydra

- نظام التشغيل المستخدم : Kali linux

أداة Hydra تستخدم لأجل تخمين كلمة المرور و اسم المستخدم على المواقع من خلال خدمات كثيرة. راح نستخدم خدمة SMTP (Simple mail transfer protocol) في هذي التجربة وهي خدمة لنقل البريد الالكتروني وتستخدم خوادم البريد لإرسال رسائل البريد واستلامها.

- الامر المستخدم في هذه التجربة :

```
sudo hydra smtp.gmail.com smtp -l tintrey00@gmail.com -P rockyou.txt -s 465 -S -v -V
```

-l> تسجيل الدخول

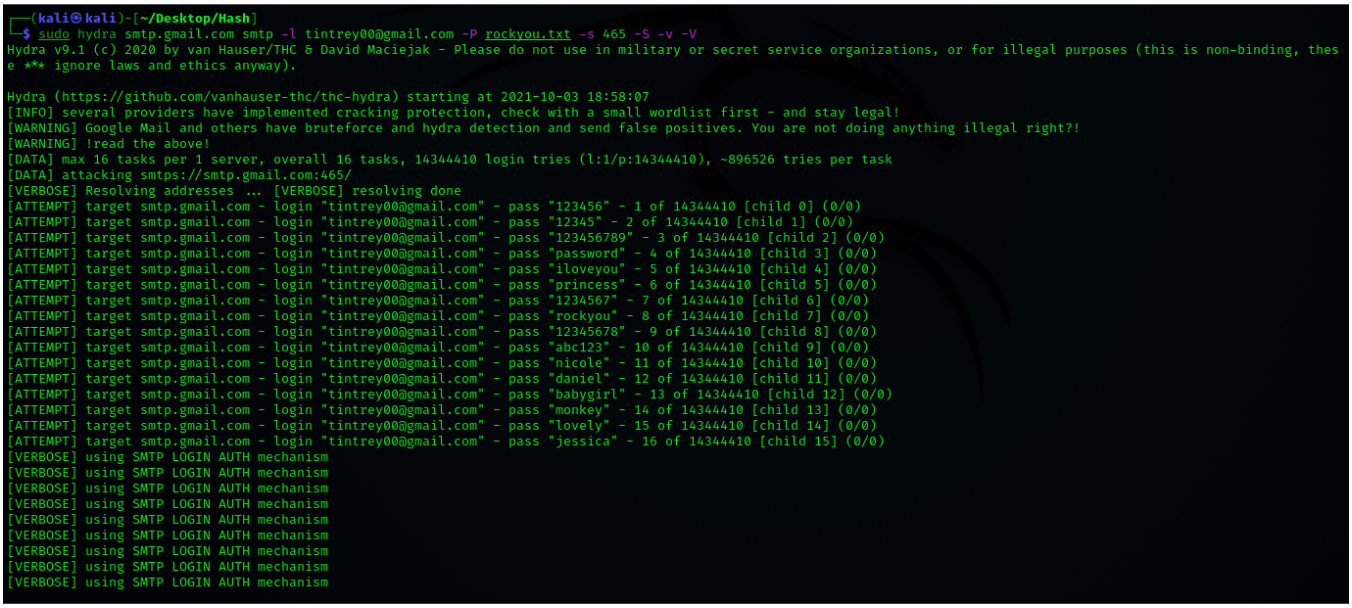
-P> مقارنة مع قائمة الكلمات rockyou.txt

-s> رقم المنفذ

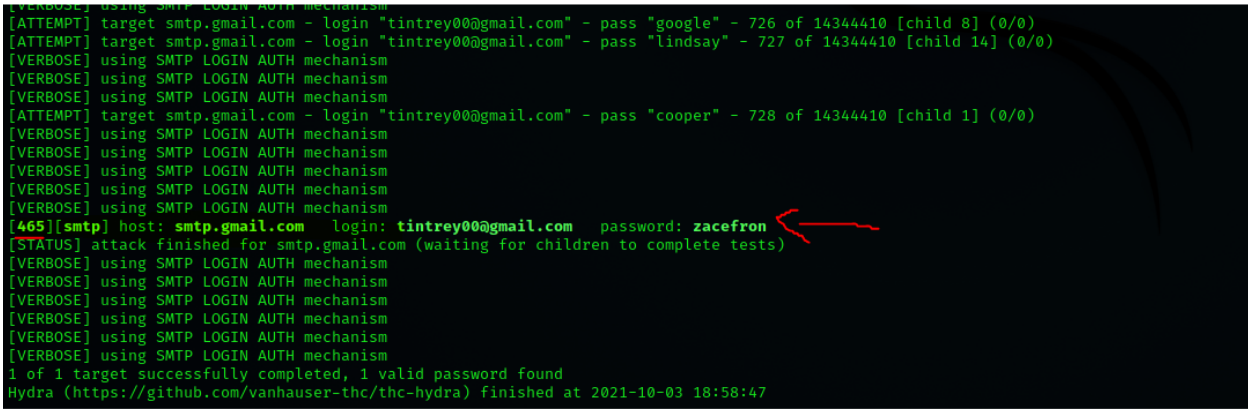
-S إجراء اتصال SSL

-v -V اظهار جميع المعلومات المهمة لتسجيل الدخول + كلمة المرور لكل محاولة

- توضح الصور أدناه عملية الاختراق بعد تنفيذ الأمر المذكور أعلاه.



- تم اختراق كلمة المرور وهي : zacefron



المصادر:

[1] Hashcat.net. 2021. hashcat - advanced password recovery. [online] Available at: <https://hashcat.net/hashcat/> [Accessed 3 October 2021].

[2] GitHub - hashcat/hashcat: World's fastest and most advanced password recovery utility. (2021). Retrieved 3 October 2021, from https://github.com/hashcat/hashcat. [Accessed 3 October 2021].

[3] Team, A., Team, A., Team, A., & Team, A. (2005). Examples of Kali Linux Hydra Tool - All About Testing. Retrieved 3 October 2021, from https://allabouttesting.org/examples-of-kali-linux-hydra-tool/ [Accessed 3 October 2021].

[4] (2021). Retrieved 3 October 2021, from https://www.kali.org/tools/hydra/ [Accessed 3 October 2021].

[5] Versions, F., Software, A., Suites, I., Suites, M., Reviews, M. and Managers, P., 2022. *The Different Types of Password Cracking Techniques - Best Reviews*. [online] Password Managers Reviews. Available at: <https://password-managers.bestreviews.net/the-different-types-of-password-cracking-techniques/> [Accessed 25 January 2022].