

تحدي الاسبوع 5

للتعامل مع تحدي كسر كلمات المرور الضعيفة المشفرة بخوارزمية MD5، سأقوم بالخطوات التالية:

1. تحليل الملف واستخراج التجزئات:

- سأبدأ بفتح الملف الذي يحتوي على كلمات المرور المشفرة بخوارزمية MD5. سأقوم باستخراج كل التجزئات (hashes) الموجودة في الملف.

2. اختيار الأدوات المناسبة لكسر كلمات المرور:

- سأختار أداة مناسبة لكسر التجزئات. هناك عدة أدوات قوية يمكن استخدامها، من بينها:

- John the Ripper: أداة مفتوحة المصدر تُستخدم لكسر كلمات المرور باستخدام قواميس وكسر التجزئات.

- Hashcat: أداة قوية تدعم كسر العديد من خوارزميات التشفير، بما في ذلك MD5.

3. إعداد هجوم القوة الغاشمة أو القاموس:

- هجوم القاموس:

- سأقوم بتجهيز قائمة بكلمات المرور المحتملة (dictionary) لاستخدامها في هجوم القاموس. هذه القائمة قد تحتوي على كلمات مرور شائعة الاستخدام.

- هجوم القوة الغاشمة (Brute Force):

- إذا لم أتمكن من كسر بعض التجزئات باستخدام القاموس، سأقوم بتجربة هجوم القوة الغاشمة الذي يجرب كل الاحتمالات الممكنة لكلمات المرور حتى يتمكن من العثور على الكلمة الصحيحة.

4. تنفيذ عملية كسر كلمات المرور:

- سأستخدم John the Ripper لتطبيق هجوم القاموس على التجزئات المستخرجة. سأقوم بتشغيل الأداة باستخدام الأمر التالي:

```
Bash Copy code
john
--wordlist=<path_to_wordlist>
<path_to_hash_file>
```

- إذا لم أتمكن من كسر جميع التجزئات باستخدام القاموس، سأقوم بتجربة Hashcat مع هجوم القوة الغاشمة:

```
Bash Copy code
hashcat -a 0 -m 0
<path_to_hash_file>
<path_to_wordlist>
```

- سأتابع العملية وأراقب النتائج لمعرفة كلمات المرور التي تمكنت من كسرها.

5. تحليل النتائج:

- سأقوم بتحليل كلمات المرور التي تمكنت من كسرها وتوثيق النقاط المشتركة بين كلمات المرور الضعيفة، مثل الطول القصير أو عدم احتواءها على رموز وأرقام.

- سأقارن بين النتائج وكلمات المرور التي لم أتمكن من كسرها لتحديد مدى قوة كل منها