Crack The Hash (John and Ripper)

Hash

- احنا طبعا درسنا ال keys وال encryption وعرفنا انه بيتفك عادي هتعمل ايه بقي لو قولتلك ان الhash ده مبيتفكش؟
- يعني ايه hash؟ الهاش عباره عن اني انا بغير شكل الكلمه بخليه شكل تاني عباره عن حروف ورموز مفهومه
  test => 098f6bcd4621d373cade4e832627b4f6
- يعني مثلا ده شكل كلمة test لما احولها ل hash
- وخلي بالك ان الهاش ده مبيتفكش هو بيتخمن
- مبدأيا عاوز افهمك حاجه ان مثلا اي موقع او اي حاجه ليها database وبيخزنو باسوردات العملاء مثلا بيخزنوها علي شكل hash
- يعني مثلا موقع زي فيسبوك لما انت تعمل اكونت عليه الباسورد اللي انت عملته بيتحول لhash وبيتخزن فالdatabase كا نوع من الحمايه من الهاكرز وبرضو من مطورين الشركه نعم؟ مطورين الشركه؟ اقولك اه فيسبوك مثلا شركه عملاقه وفيها مبرمجين كتير جدا فا انا ايه ضمني ان حد ممكن يسرب بيانات او يعرف باسورد حد معين
- الhash بقي فيه منه انواع وكل نوع بيتخلف علي حسب الطول

أنواع الهاش

ID	نوع الهاش	الطول (عدد الحروف)	ملاحظات
1	MD5	32 characters	قديم وسهل الكراك دلوقتي
2	SHA-1	40 characters	أضعف من SHA2 وأمانه مش قوي
3	SHA-256	64 characters	من عيلة SHA2 — أمان عالي
4	SHA-512	128 characters	أطول وأقوى — من عيلة SHA2
5	NTLM	32 characters	مايكروسوفت — زي MD5 شوية
6	bcrypt	60 characters	يستخدم Salt والفيسبوك بيستخدمه — صعب يتكراك
7	DES	13 characters	قديم جدًا ومفيش حد بيستخدمه
8	LM Hash	32 characters	خاص بمايكروسوفت وبيتخزن Uppercase
9	SHA-3 (256)	64 characters	أحدث من SHA2

Crack the Hash

- طيب حلو جدا انا دلوقتي عاوز اكسر الهاش ده اقولك ان احنا مش هنكسره احنا هنخمنه ولو خمنا صح هتعرف تكسره يعني مش الهاش هتعرف تكسره
- في ادوات معينه بتكون فيها مجموعه كبيره جدا من الكلمات وفيها الhash بتاعها فا انت لما تيجي تكراك هاش بتقارن الهاش اللي انت اديتهولها باللي عندها ولو مطابق للهاش اللي عندها بتديك الكلمه نفسها
- بس احنا بقي بنستخدم wordlist فيها بقي كلمات اكتر زي rockyou ودي فيها اكتر من 14 مليون كلمه
- عشان اعمل كراك علي الهاش في طرق كتير ممكن استخدم ادوات زي hashcat - john and ripper او مواقع زي crackstation.net بس احنا هنا هنستخدم john and ripper

John and Ripper

- طيب عشان استخدم التول اول حاجه هنزلها مع اني هيا كده كده بتكون موجوده عالكالي بس لو مش موجوده اكتب الكوماند ده

```
apt install john
```

- وبعد كده ننزل wordlist زي rockyou مثلا وبعد كده نحط الهاش اللي عاوزينه ف فايل
- وبعد كده نبدأ نعمل كراك عن طريق الكوماند ده

```
<john <--wordlist=wordlist-name> <hash-file
john --wordlist=rockyou.txt hash.txt
```

Salt

- طبعا الdevelopers لقو ان الhackers بيعرفو يكسرو الهاش فا قالو احنا هنحط salt علي الهاش يعني بالظبط زي ماترجمت هنحط ملح عالهاش
- الsalt عباره عن رموز او حروف او ارقام معينه كده بحطها فأول الهاش عشان تميزه وعشان تصعب عملية الcracking

الفكرة

لما بتعمل هاش لباسورد زي `123456`
هايديك نفس النتيجة لأي حد كاتب نفس الباسورد.

```
SHA256(123456) = e10adc3949ba59abbe56e057f20f883e
```

يعني لو 100 يوزر عاملين نفس الباسورد ← الهاش بتاعهم هيبقى نفس الرقم
ودي مصيبة لإن أي حد معاه **rainbow table** هيعرفها بسهولة.

الحل = Salt

بنضيف كلمة زيادة عشوائية (salt) مع الباسورد
عشان نغير نتيجة الهاش
مثال:

- الباسورد: `123456`
- الـ salt: `@A9!`
- **النتيجة:**
- كل يوزر حتى لو باسورده زي زميله، هيطلعله هاش مختلف
- مفيش rainbow table تقدر تجيب الباسورد بسهولة

أنظمة بتستخدم Salt أوتوماتيك

- **bcrypt** 2a$12rkEdwk/IIRmZPFUnVXCOPOYBaYrmQrCgwj3Ia Sf5IXvXOvK8/43ju
  يعني بص عنا اول ماتشوف الـ$ دي مثلا تعرف ان دي bycrypt
- **scrypt**
- **argon2**

أنظمة محتاجة تضيف Salt يدوي

- **MD5**
- **SHA1**

- SHA256

ليه نستخدم Salt؟

- يمنع إن 2 يوزر عندهم نفس الباسورد يطلعوا نفس الهاش
- يحمي من rainbow table attacks
- يصعّب أي محاولة كراك