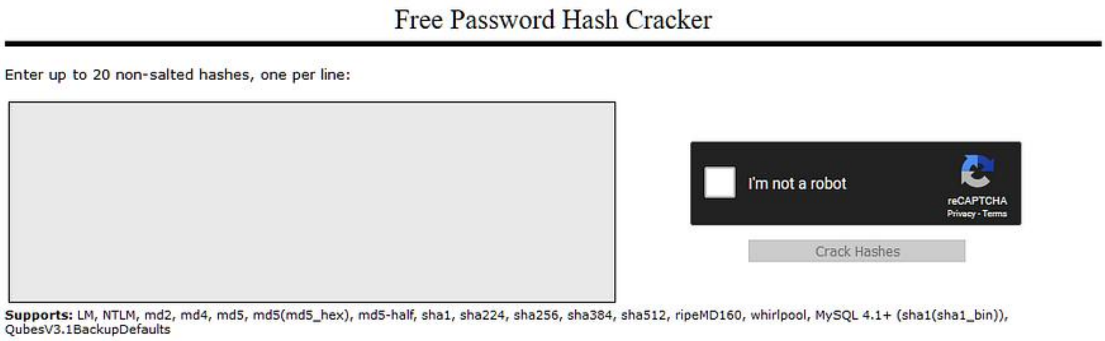
Task 7 : Cryptographic Failures (Supporting Material 2)

We saw how to query an SQLite database for sensitive data in the previous task. We found a collection of password hashes, one for each user. In this task, we will briefly cover how to crack these.

When it comes to hash cracking, Kali comes pre-installed with various tools. If you know how to use these, then feel free to do so; however, they are outwith the scope of this material.

Instead, we will be using the online tool: `Crackstation`. This website is extremely good at cracking weak password hashes. For more complicated hashes, we would need more sophisticated tools; however, all of the crackable password hashes used in today's challenge are weak MD5 hashes, which Crackstation should handle very nicely.

When we navigate to the website, we are met with the following interface:

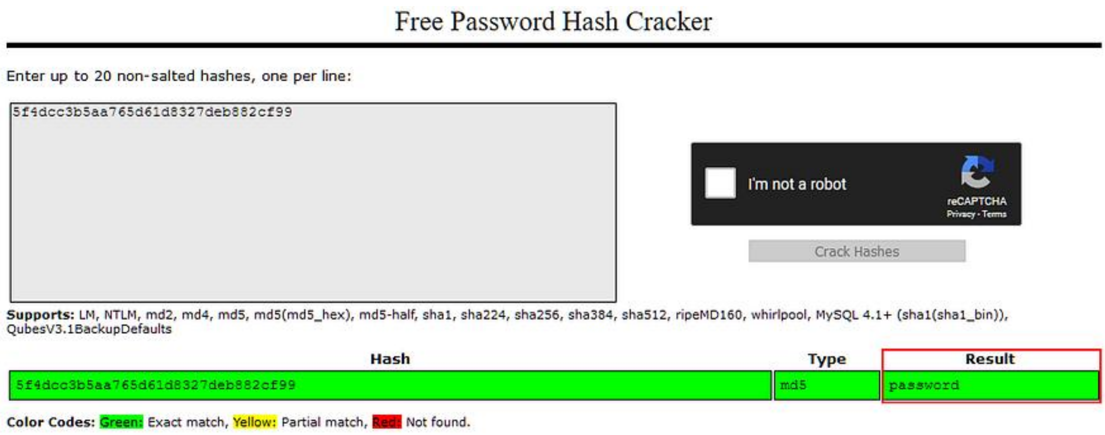


Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Let's try pasting the password hash for Joy Paulson, which we found in the previous task (`5f4dcc3b5aa765d61d8327deb882cf99`). We solve the Captcha, then click the "Crack Hashes" button:



Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

```
5f4dcc3b5aa765d61d8327deb882cf99
```

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
5f4dcc3b5aa765d61d8327deb882cf99	md5	password

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

We see that the hash was successfully broken, and the user's password was "password". How secure!

It's worth noting that Crackstation works using a massive wordlist. If the password is not in the wordlist, then Crackstation will not be able to break the hash.

The challenge is guided, so if Crackstation fails to break a hash in today's box, you can assume that the hash has been specifically designed not to be crackable.

Answer the questions below :

1. Read the supporting material about cracking hashes.

A. No answer needed