Day 17 – Simulate Password Cracking (Ethically)

Step 1:

Open Password List; choose 3-5 passwords for experiment

Step 2:

Convert Passwords to Hashes (to Simulate Stolen Hashes)

Use an online SHA-1 generator like this:

https://emn178.github.io/online-tools/sha1.html

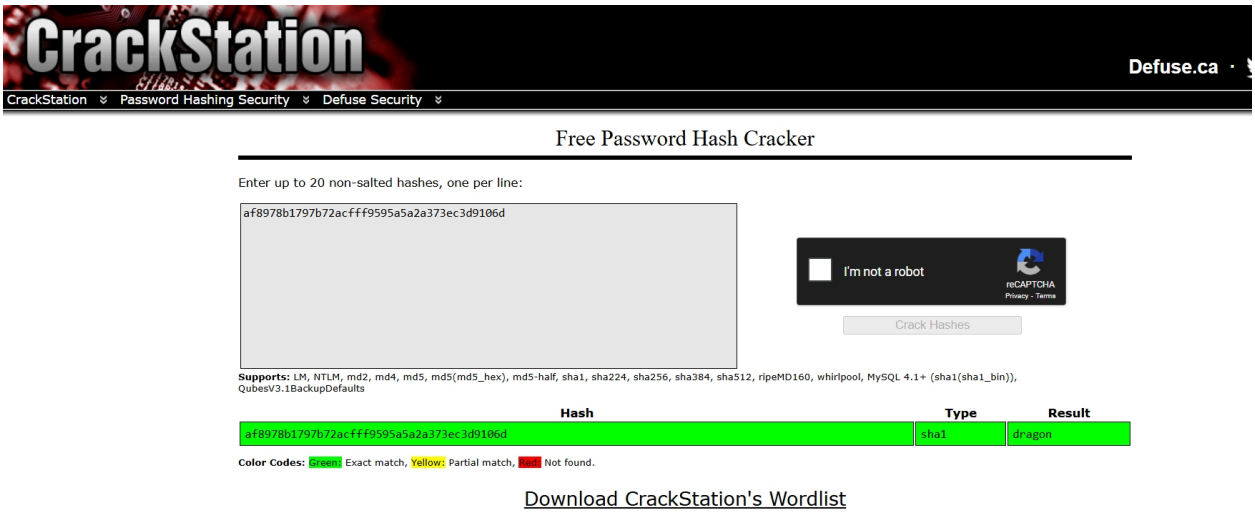
Password → Hashes

dragon → af8978b1797b72acfff9595a5a2a373ec3d9106d
1q2w3e4r → 48efc4851e15940af5d477d3c0ce99211a70a3be
sunshine → 8d6e34f987851aa599257d3831a1af040886842f
654321 → dd5fef9c1c1da1394d6d34b248c51be2ad740840
master → 4f26aeafdb2367620a393c973eddbe8f8b846ebd

Step 3:

Simulate Cracking with CrackStation

https://crackstation.net/



very common passwords get cracked instantly

Results from CrackStation:

I pasted the hashes into CrackStation.net and almost all of them were instantly cracked. This proves how weak and common passwords are easy targets for attackers.

What I Learned:

- Common passwords are extremely easy to crack.
- Hashes alone don’t make passwords secure — if the password is weak, it's still vulnerable.
- Passwords should be long, random, and ideally stored with added security measures (like salting).

Takeaway:

Even without hacking skills, anyone can use publicly available tools to simulate password cracking. It’s a strong reminder to use **strong, unique passwords** for every account.