**Password Attacks**

**Haveibeenpwned.com**

* Check if you’ve been pwned

**Password cracking**

* Dictionary attacks
  + Using most common words
* Brute force
  + Every possible combination
* Hybrid attack
  + Using the above in conjunction with human psychology

**Hashcat**

* A tool for cracking
* Once password hashes are stolen, an attack can be started
* Identify which hashing algorithm has been used
* E.g., dictionary attack – can hash all dictionary items and compare to stolen hashes

Crackstation.net

Strong Password:

Hash 🡪 Salt 🡪 Iterate 🡪 Encrypt

Operating System Passwords

* No protection against someone with physical access
* Can be bypassed by booting device using another operating system and examining the files
  + Live CD or take HD out and connect to different machine
* Password doesn’t even need to be cracked
  + The hash can actually just be replaced

Password recovery tools are a great example of this

YubiKey

* 2FA

Whole Disk Encryption is how you mitigate this