Weak Passwords

Weak Passwords make it easy for unauthorized individuals or automated programs to guess or crack which poses serious security risks as they can be easily exploited through various attack methods such as brute force and dictionary attacks

TODO - this could be less wordy - see the QA guidance I just posted in Discord Following that process,

1. *service has weak password*
2. *attacker guesses password through brute force or dictionary attack*
3. *attacker gets access to the service*
4. *because attacker got access to a service, the weak password was bad "The service was found configured with a weak password. Weak passwords can be guessed by attackers through various means, such as bruteforce or dictionary attacks, providing unauthorized access to the service."*

Weak passwords present a significant security vulnerability for services. When a service is configured with easily guessable passwords, it becomes susceptible to exploitation by attackers. These attackers can employ techniques such as brute force or dictionary attacks to guess the password. As a result, unauthorized access can be gained, compromising the security of the service and potentially leading to further breaches or data theft.

1. Short Length - Less than eight characters
2. Lack of Complexity - Consists of simple patterns without numbers, symbols or Uppercase letters
3. Predictable Characters - Use of common words and sequences (e.g. 123456. password)

4. Personal Information - Incorporates personal data such as birthdays or family names

TODO 1 was written in "command" language, 2 was written in "..ing" language (also making this not a valid sentence), and 3 was written in passive voice "are used". Pick one and stick with it. My recommendation is referring to "an attacker" in the third person and wording it subject → action, so "Brute Force Attacks - attackers try all possible character combinations to guess simple passwords”

TODO - include some more reputable references with guidance for what makes a password strong - does NIST have any guidance? Compliance frameworks like PCI? Microsoft?