- Filename: eccouncil-ceh31250-v12-6-5-1-password-cracking-enhancement-techniques.md
- Show Name: CEHv12 (312-50)
- Topic Name: System Hacking Phases and Attack Techniques - System Hacking
- Episode Name: Password Cracking Enhancement Techniques
  ==

Password Cracking Enhancement Techniques

Objectives:

- Enhance password cracking attack efforts by utilizing techniques such as Combinator, PRINCE, Toggle-Case, and Markov-Chain Attacks

---

- Combinator

    - Combine 2 or more dictionaries together

- PRINCE

    - PRobability INfinite Chained Elements

        - Like a Combinator approach except

            - Only uses 1 dictionary

    - Create a useful dictionary based on known criteria

        - Example: passwords must be 6 chars long

            - Use only 6+ char words in dictionary
            - Create 6+ char words using combinations of smaller words

                - 2 char words + 4 char words = 6 char words

- Toggle-case

    - Try every case possibility

        - aaa, aaA, aAA, AAA, AAa, Aaa

- Markov Chain

    - A statistical analysis of the passwords cracked through normal means

        - A file is generated with the most common elements

            - 'C' is the most common letter and is most commonly followed by 'a'

        - It then uses those stats to perform a dictionary/brute-force hybrid attack