- Filename: eccouncil-ceh31250-v10-6-1-1-password_attacks.md
- Show Name: CEHv10 (312-50)
- Topic Name: Attacks and Exploits
- Episode Name: Password Attacks
- Description: In this episode, Daniel and Zach get into some system hacking by exploring ways to attack password-based authentication. Here they will discuss some password basics as well as exploring both low-tech and high-tech approaches to password attacks. This includes: shoulder surfing, dumpster diving, social engineering, dictionary, brute-force, and rule-based attacks.

==

Password Attacks

- **We're all probably fairly familiar with passwords. What about them do we need to know when it comes to attacking them?**
    - Password use
    - Password attributes
    - Password weaknesses
- **How does one begin to attack a password-based authentication mechanism?**
    - Use your eyes
        - Shoulder surfing
        - Snooping around
            - Desks, Monitors, Keyboards, drawers, trash (desk calendars), etc
        - Try printing cached print jobs
    - Use guile and persuasion
        - Social Engineering to get the user to tell you their password
            - Electronically or audibly
    - Guessing
- **What about a more "high-tech" approach?**
    - Take the idea of guessing and automate it with a program
        - FIRST: We need to understand the types of password attack automations
            - Dictionary
            - Brute-Force
            - Rule-Based
    - Dictionary
        - Show `rockyou.txt`
        - Create a dictionary file with `cewl`
            - Crawls websites for words to make custom password list
                - Rules are user defined
                    - Define size of words to gather
                    - `cewl -o -m 6 www.itpro.tv -w wordlist.txt`
    - Brute-Force
        - Attempting every possible password until you get a hit
            - a, aa, aaa, aaaa, b, bb, bbb, bbbb, etc...
    - Rule-Based
        - Creating a dictionary or brute-force attack with a known set of parameters

- Parameters
    - Password must be longer than X characters
    - Password must NOT be longer than X characters
    - Password must contain at least 1 digit
    - Password must contain at least 1 special character
    - **A word on complexity vs length**
        - Long passwords guard us from Brute-Force attacks
        - Complex password guard from Dictionary attacks
        - A password that is both long and complex guards from BOTH!