- Filename: eccouncil-ceh31250-v10-9-1-2-social_engineering_pt2.md
- Show Name: CEHv10 (312-50)
- Topic Name: Attacks and Exploits
- Episode Name: Social Engineering Pt.2
- Description: In this episode, Daniel and Zach discuss the practice of performing Social Engineering techniques during a pentest engagement. Here you will learn the concepts and tactics that Social Engineers use to elicit information from their targets. These include phishing, Spear phishing, whaling, SMiShing, Vishing, and more.

==========

Social Engineering Pt.2

- Phishing
    - Phishing
        - Using guile and deception through electronic communications to obtain sensitive info
            - Email
            - Text Messages
            - Fake Websites
                - *DEMO: SETOOLKIT fake facebook login*
            - Phone/VoIP
    - Spear phishing
        - Target specific groups/users
            - Targeted for various reasons
    - Whaling
        - Targeting of high-level officials
            - C-level officers
        - Attack tone and language is more official/executive
            - Customer feedback
            - Business authority
            - Legal document
                - Subpoena
            - Executive issue
    - SMS phishing
        - SMiShing
    - Voice phishing
        - Vishing
    - Pharming
        - Traffic redirected to clone site
            - DNS poisoning
            - Altering the `hosts` file
    - Spimming
        - Spamming IM