- Filename: eccouncil-ceh31250-v11-6-1-1-ceh-hacking-methodology-and-goals.md
- Show Name: CEHv11 (312-50)
- Topic Name: System Hacking Phases and Attack Techniques - System Hacking
- Episode Name: CEH Hacking Methodology and Goals
===

CEH Hacking Methodology and Goals

Objectives:

- List and describe the phases of the CEH Hacking Methodology
- List and describe the goals of an attacker at specific phases of CEH Hacking Methodology

---

- What do we mean by 'Methodology'?

    - Systematized approach to reaching a goal

        - System is derived from research and observation

- What is the CEH Methodology?

    - EC-Council's system for successfully hacking a target

- Where does it fit in what we've learned so far?

    - Recon/Footprinting
    - Scanning
    - Enumeration
    - Vuln Assessment
    - **System Hacking**

        - Gaining Access

            - Password Cracking
            - Vulnerability Exploitation

        - Priv Esc
        - Maintaining Access
        - Clearing Logs

- What are our goals in System Hacking?

    - *Gaining access*

        - Bypass security controls, or finding system misconfigurations to access the target system

            - Techniques

                - Password cracking
                - Vuln Exploitation
                - Social Engineering

    - *Priv Esc*

        - Horizontal priv esc
        - Vertical priv esc

            - Techniques

                - Vuln Exploitation
                - Security misconfiguration

- *Execute Apps*
  - aka Maintaining Access
    - Techniques
      - Malware
      - C2
      - Backdoors
- *Hiding Files*
  - Data exfil
    - Techniques
      - stego
- *Covering Tracks*
  - Hide/obfuscate evidence
    - Techniques
      - Log clearing