

- Filename: eccouncil-ceh31250-v12-1-15-1-ceh-hacking-methodology-and-goals.md
- Show Name: CEHv12 (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

1. What do we mean by 'Methodology'?

- Systematized approach to reaching a goal
 - System is derived from research and observation

2. What is the CEH Methodology?

- EC-Council's system for successfully hacking a target
- <https://www.eccouncil.org/ethical-hacking/>

3. What are the steps/phases in the CEH Hacking Methodology(CHM)?

- *Planning and Reconnaissance*
 - Footprinting
 -
- *Scanning*
 - Vulnerability discovery phase
 - Techniques
 - Host Discovery Scanning
 - Port/Service Scanning
 - Vulnerability scanning
- *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
- *Maintaining Access*
 - Techniques
 - Malware
 - C2
 - Backdoors
 - *Hiding Files*
 - Data exfil

- stego
- *Clearing/Covering Tracks*
 - Hide/obfuscate evidence
 - Techniques
 - Log clearing