

- Filename: eccouncil-ceh31250-v11-6-4-1-password-extraction-and-cracking.md
  - Show Name: CEHV11 (312-50)
  - Topic Name: System Hacking Phases and Attack Techniques - System Hacking
  - Episode Name: Password Hash Extraction and Cracking
- =====

## Password Extraction and Cracking

### Objectives:

- List common tools utilized to extract password hashes
  - Utilize password hash extraction tools to retrieve password hashes
  - Explain the process of LLMNR/NBT-NS Poisoning
  - Utilize freely available tools to execute LLMNR poisoning attack
  - Define password salting
  - List and explain common password policies used to defend against password attacks
- 

- How do we get the password hashes from target computers?
  - Post-compromise activity (usually)
  - Windows Tools
    - pwdump7
    - fgdump
    - mimikatz
    - responder
  - Linux
    - cat
  - Web/Database attacks
    - Attacker could retrieve hashes from insecure web app
- How do we crack these hashes to reveal the passwords?
  - John the Ripper
    - Dictionary
    - Rules
  - OCL-Hashcat
    - Brute
  - Ophcrack
    - Rainbow Tables
  - Pass-the-Hash
    - Don't even need to crack the hash
    - Some systems will just use the hash
- Any good countermeasures?
  - Good password policies
    - Sufficient length
    - Sufficient character sets
    - No dictionary words
    - Salt

- Any other ways to grab passwords?
  - Key loggers
    - Software-based
    - Hardware-based