- Filename: eccouncil-ceh31250-v10-6-2-3-privilege_escalation_pt3.md
- Show Name: CEHv10 (312-50)
- Topic Name: Attacks and Exploits
- Episode Name: Privilege Escalation Pt.3
- Description: In this episode, Daniel and Zach guide you through the process of Privilege Escalation. Here they take you through common techniques and tactics for gaining higher privileges such as: Operating System vulnerability exploitation, the use of Webshells, and other various maneuvers.
  ==========

Privilege Escalation Pt.3

- OS vulnerability exploitation
  - DirtyCOW
    - Effective against Linux Kernel version below 3.9
    - Race condition exploit
    - Vulnhub: Zico2
      - `uname -a`
      - `searchsploit Dirty COW`
      - Good hit! **40839.c**
      - Copy that to Zico machine
      - Read instructions and compile accordingly
      - Execute and wait
      - Login with newly created user
    - EternalBlue
      - Metasploit Module `search eternalblue`
      - set RHOST, LHOST, LPORT, TARGET
- Webshells
  - Upload x.php to bWAPP using command injection attack
- Others
  - Access Tokens
    - Golden Ticket
    - Kerberoasting
  - Unquoted Service Paths
    - DIAGRAM