- Filename: eccouncil-ceh31250-v12-6-7-1-privilege-escalataion.md
- Show Name: CEHv12 (312-50)
- Topic Name: System Hacking Phases and Attack Techniques - System Hacking
- Episode Name: Privilege Escalation
  ==

Privilege Escalation

Objectives:

- Explain the concept and practice of Privilege Escalation
- Define the 2 types of Privilege Escalation
- List and describe common Privilege Escalation techniques and tools
- Describe common techniques used to prevent Privilege Escalation attacks

---

- What is privilege Escalation?
  - Horizontal Priv Esc
  - Vertical Priv Esc
- How is Priv Esc accomplished?
  - OS/Software vulnerabilities
    - exploit-db
  - OS/Software Misconfigurations
    - Weak permissions
    - DLL Hijacking
      - Robber
    - Dylib Hijacking
      - Mac OS version of DLL hijacking
  - Unattended Installations
    - unattend.xml
      - `C:\Windows\Panther\`
      - `C:\Windows\Panther\Unattend\`
      - `C:\Windows\System32\`
      - `C:\Windows\System32\sysprep\`
  - Unquoted Service Paths
  - Scheduled Tasks/Cron Jobs/plist
  - SUID/GUID
  - Sudo
- PrivEsc Tools
  - PEAS-ng
  - BeRoot
  - Powersploit
  - Windows Exploit Suggester
  - LinuxPrivChecker
- What can we do to protect against Priv Esc attacks?
  - Updates/patches
  - Careful configuration
  - SAST/DAST
  - Multi-factor Auth
  - Principal of Least Privilege
  - System hardening guides