- Filename: eccouncil-ceh31250-v10-6-2-1-privilege_escalation.md
- Show Name: CEHv10 (312-50)
- Topic Name: Attacks and Exploits
- Episode Name: Privilege Escalation
- 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: DLL Hijacking and exploiting file/folder permission misconfigurations.

==========

Privilege Escalation

- What is priv esc?
    - Can be one of two things
        - Obtaining permissions/rights of other users of similar privs
            - Horizontal
        - Obtaining permissions/rights of other users with higher privs
            - Vertical
- How is this done?
    - DLL Hijacking
        - Absolute paths not used when calling .dll
        - Windows looks for dlls in a specific order
            - **AppDir > Current Dir > System Dir > 16-bit Sys Dir > Windows Dir > PATH Dirs**
        - Create malicious dll
            - Put maldll in search dir that is BEFORE actual dir
        - Diagrams
            - Dylib hijacking is similar technique
    - File/Folder permission misconfiguration
        - DEMO: Evil Putty
            1. Search for folders with weak permissions
            - Manual search
            - `icacls "Folder name"` (**add quotes**)
                - (I) = Inherited
                - (OI) = Object Inherit
                - (CI) = Container Inherit
                - (RX) = Read and Execute
                - (AD) = Append data/Add subdir
                - (WD) = Write data/Add file
                - (F) = Full Control
            2. Create evil copy of file
            - backdoor_exe.txt
            3. Copy evil.exe to target
            4. Replace good.exe with evil.exe
            5. Start multi handler in Metasploit
            - Set options (PAYLOAD, LHOST, LPORT)
            6. Wait for action