- Filename: eccouncil-ceh31250-v10-6-5-1-hidden_files.md
- Show Name: CEHv10 (312-50)
- Topic Name: Attacks and Exploits
- Episode Name: Hidden Files
- Description: In this episode, Daniel and Zach explore hiding files during an engagement. Here they will explain why hiding files is necessary and show the use of Alternate Data Streams and Steganography as tactics for hiding information.

==

Hidden Files

- **Why would we need to hide files?**
    - Stealth
        - We want to keep our activities under the radar
            - Gathered data
            - Execute programs
- **In what ways can we hide files?**
    - Alternate Data Streams (ADS)
        - Allows you to hide text, binaries, video, audio
        - Doesn't affect the size of the file hiding it
        - DEMO
            - Hide malware.exe in text file
                - `type c:\path\to\malware.exe > c:\path\to\file.txt:malware.exe`
            - Make link to hidden exe
                - `mklink good.exe c:\path\to\file.txt:malware.exe`
            - Execute hidden exe
                - `C:\> good.exe`
- **Are these hidden files detectable at all?**
    - `lads c:\`
    - `streams -s c:\` (SysInternals)
    - GUI *Stream Armor*
    - FTK
- **Is this technique similar to Steganography?**
    - Superficially, yes
    - Other types of Stego
        - Image
            - DEMO: Steghide
                - `steghide embed -cf picture.jpg -ef secret.txt`
                - `steghide extract -sf picture.jpg`
            - OpenStego (GUI)
        - Audio
        - Video
        - Whitespace
        - Folders
        - Mobile
        - Email
- **Are there techniques for detecting these files too?**

- Called *"Steganalysis"*
- Tools
    - https://www.wetstonetech.com/products/gargoyle-investigator/
    - Use various ways to detect hidden stego files
        - May only have the stego file
        - May know the all the parts of the stego file
            - Algorithm
            - Cover
            - Stego file
        - May have stego file and cover medium
        - May use known stego Algorithm to generate stego file
            - Use that to discover other stego files
    - Different tells with different media
        - Audio
            - May contain distortions
            - Perform frequency analysis
        - Image
            - May contain odd renderings
            - Statistical analysis to scan image