- Filename: eccouncil-ceh31250-v12-17-2-1-android-security.md
- Show Name: CEHv12 (312-50)
- Topic Name: Mobile Platform, IoT, and OT Hacking - Hacking Mobile Platforms
- Episode Name: Android Security
  ==

Android Security

Objectives:

- Android OS
    - Developed by Google
    - Linux based
    - Open-source
    - Most used OS for smartphones and tablets (since 2011 and 2013 respectively)
    - App development and device administration
        - https://developer.android.com/
        - https://developer.android.com/guide/topics/admin/device-admin
- Rooting
    - Gaining full 'root' level control of device
    - Pros
        - You can bypass device controls
            - Allowing 'privileged' functionality
                - install apps on SD card
                - Tethering
                - Delete bloatware
    - Cons
        - Voided warranty
        - Malware infection
        - Brick the device
    - Rooting Tools
        - Place your device into 'USB debugging' mode then use tool of choice
            - KingoRoot
            - KingRoot
            - Towelroot
            - One Click Root
- Android Hacking Tools
    - Yup!
        - DoS attacks
            - NetCut
            - LOIC
        - Vuln Scans
            - drozer
        - zANTI
            - https://www.zimperium.com/zanti-mobile-penetration-testing
        - Web Session Hijacking
            - DroidSheep
                - https://droidsheep.info
        - Android Debug Bridge (ADB)

        - Android communications
            - Install and debug apps
            - Shell access
    - cSploit
        - https://github.com/cSploit/android

- Android Security Defenses
    - Don't Root
    - Use screen lock
    - Don't install apps from 3rd-party app stores
    - Don't side-load apps
    - Install AV/Anti-Malware
        - Kaspersky
        - Avast
        - Sophos
    - Updates/Patches
    - Don't open links/attachments
    - Use VPN
    - Enable Location services / Find by Device
        - Find my Phone
        - Where's my Droid