- Filename: eccouncil-ceh31250-v10-17-1-1-mobile_hacking.md
- Show Name: CEHv10 (312-50)
- Topic Name: Attacks and Exploits
- Episode Name: Mobile Hacking
- Description: In this episode, Daniel and Zach discuss hacking mobile devices. Here they will look into Mobile as an attack surface and explore vulnerabilities found therein. Then they will turn their attention to using Mobile as an attack platform as well as the realities of managing a BYOD environment.

==

Mobile Hacking

- **With mobile devices becoming the most common way that we access the internet and store sensitive information, I'm guessing that they've become popular targets for attackers and maybe even mobile hacking platforms?**
    - Mobile as a target
        - OWASP Top10 Mobile (https://www.owasp.org/index.php/Mobile_Top_10_2016-Top_10)
        - Mobile attack surfaces
            - The Device
                - OS
                - Apps
                - Browsers
            - The Wireless Network(s)
                - Clear wireless transmissions
                - Basically every network-based attack
            - The Data
                - This is what attackers are after once they compromise the device
        - Common attacks
            - Malware
                - Rooted/Jailbroken devices allow for sideloading
                    - Modifying the device to allow full system access to the user
                        - Rooting tools
                    - Untrusted sources could contain malware in software apps
                        - Phishing/SMiShing for downloads(**IMAGE**)
                - App Stores
                    - Malware has found itself in the trusted app stores from time to time
                - Sandbox bypass
                    - Exploits weakness in sandboxing controls to access info and/or other resources
                - Spyware
                    - Monitor all phone activity
                        - GPS
                        - Text
                        - Email
                        - Web history
                - **Can we reduce the likelihood of malware infections?**

                - Run mobile security protection software
                    - *Google search: mobile device security app*
                        - AVAST
                        - Lookout
                        - Kaspersky
                - Perform vulnerability scans
                    - X-ray vuln scanner
                - Keep device updated
                - Don't download from untrusted sources
- **Now that we've looked at system vulnerabilities, can we turn towards physical attacks?**
    - Physical attacks
        - Devices are MOBILE!
            - Easy to steal/lose
                - Enable location features/software
                    - Find My Phone
                    - Where's My Droid
                    - Find My iPhone
                - Use screen locking functions
                    - Auto lock after x amount of time
                    - PIN
                    - Fingerprint
                    - Facial Recognition
- **So we've looked at mobile devices as targets, but can they also be a viable hacking platform?**
    - Hacking with Mobile
        - Hacking tools
            - Footprinting/Enum
                - Hackode
            - DoS
                - NetCut
                - LOIC
            - Spoofing/MITM
                - DroidSheep
            - Sniffing
- **It seems like a BYOD environment can be difficult to manage?**
    - It can be
        - Employ some kind of MDM (Mobile Device Management) system
            - Enable remote management on devices
                - Remote wipe
        - Onboarding and Disposal
        - End user awareness training
        - Personal and Private data on single, mobile device
        - Enforce the use of security software
        - Enforce the use of PIN and lockout