

- Filename: eccouncil-ceh31250-v12-17-3-1-ios-security.md
- Show Name: CEHv12 (312-50)
- Topic Name: Mobile Platform, IoT, and OT Hacking - Hacking Mobile Platforms
- Episode Name: iOS Security

=====

iOS Security

Objectives:

- Apple iOS
 - Released in 2007
 - Runs on Apple exclusively
 - App Store
 - Has many security features built-in
 - Secure Boot
 - Face ID | Passcode | Touch ID
 - Code signing for 3rd-party apps
 - Sandboxing
- Jailbreaking
 - Gives users root access to OS
 - Pros
 - Removes sandbox restrictions
 - Install 3rd-party unsigned apps
 - Cons
 - Warranty voided
 - Malware Infection
 - Brick the device
 - Jailbreaking Techniques
 - Tethered
 - Devices boots normally
 - May get stuck in a partially booted state
 - Device must be tethered to computer and re-jailbroken
 - Use the 'boot tethered' feature of jailbreaking tool
 - Semi-Tethered
 - Device boots normally
 - If jailbroken functionality is required, device must be tethered to a computer and jailbreaking tool must be used
 - Untethered
 - Device will be in 'jailbroken' state even after reboots
 - Doesn't require the help of a computer
 - The kernel is now patched
 - Semi-Untethered
 - Similar to Semi-Tethered
 - Device boots normally
 - Device can be patched without a computer
 - Patch is applied by an app on the device
 - Jailbreaking Tools
 - Hexxa Plus

- iOS Hacking and Hacking Tools
 - Info Gathering Tool
 - Network Analyzer Pro
 - Trustjacking
 - Attacker can remotely read messages, emails, and sensitive info, etc
 - Apple mobile devices can sync with iTunes over Wifi
 - 'Trust this device'
 - Attacker gets victim to plug mobile into computer
 - Click 'yes' to trust this device prompt
 - Attacker can now access victim data through iTunes 'Wifi Sync'
 - iOS Malware
 - https://www.theiphonewiki.com/wiki/Malware_for_iOS
 - <https://www.washingtonpost.com/investigations/interactive/2021/nso-spyware-pegasus-cellphones/>
 - iOS Hacking Tools
 - Pegasus
 - Elcomsoft Phone Breaker
 - <https://www.elcomsoft.com/eppb.html>
 - Spyic
 - <https://spyic.com/>
- iOS Security Defenses
 - Don't Jailbreak
 - Use screen lock
 - Don't install untrusted 3rd-party apps
 - Don't side-load apps
 - Updates/Patches
 - Don't open links/attachments
 - Use VPN
 - Don't use random Wifi
 - Enable Location services / Find by Device
 - Find my iPhone
 - Use a password manager
 - Disable services like wifi/bluetooth/location when not in use
 - Use a mobile security suite
 - Trend Micro Mobile Security
 - Norton Security for iOS
 - McAfee Mobile Security
 - Should have anti-spyware