ADVANCED MOBILE PENETRATION TESTING

TABLE OF CONTENT

Duration – 4 Days

Day 1: Introduction to Mobile Security

- Introduction to Mobile Security
- Mobile Problems and Opportunities
- Challenges and Opportunities for Secure Mobile Phone Deployments
- Weaknesses in Mobile Devices
- OWASP Mobile Top 10
- Mobile Architecture & Threats
- Hands-On Lab: Mobile Device Footprinting & Scanning
    - Gathering Information on Mobile Devices (OS, Apps, Network)
    - Identifying Open Ports & Services Running on a Mobile Device(Nmap)
    - Using Reconnaissance Tools to Map Mobile Attack Surface
    - Intercepting TLS Traffic
    - Man-in-the-Middle Troubleshooting

Day 2: iOS & Android Security Fundamentals

- iOS Architecture
- Jailbreaking iOS Devices
- iOS Data Storage and File System Architecture
- iOS Application Interaction
- iOS Malware Threats
- Android Architecture
- Rooting Android Devices
- Root Detection Techniques and Bypass Methods
    - Approaches: Signature Checks, Binary Checks, System Property Checks
    - Methodologies: Static/Runtime Checks, Root Cloaking
- Android Data Storage and File System Architecture

- Android Application Interaction
- Android Malware Threats
- Android Platform Analysis
- Hands-On Lab :
    - MDM – jump cloud
    - Threat Modelling Tool – Microsoft
- Root Detection and Bypass using Magisk
- Exploiting Android ADB with PhoneSploit
    - Understanding Android Debug Bridge (ADB) and Its Security Risks
    - Exploiting ADB Misconfigurations with PhoneSploit
    - Identifying Weaknesses and Securing ADB Against Attacks

Day 3: Static Analysis & Reverse Engineering

- Static Application Analysis
    - Retrieving iOS and Android Apps for Reverse Engineering Analysis
    - Decompiling Android Applications
    - Circumventing iOS App Encryption
    - Header Analysis and Objective-C Disassembly
- Reverse-Engineering Obfuscated Applications
    - Identifying Obfuscation Techniques
    - Decompiling Obfuscated Applications
- Analyzing SSL Pinning and Certificate Pinning
    - Approaches: Manual Code Review, Hooking Methods
    - Techniques: Patching, Runtime Hooking
- Certificate Pinning and SSL Pinning Deep Dive
    - Methodologies: TrustManager Validation, Network Security Config
- Hands-On Lab
    - AndroRAT – Android Remote access
    - Apktool – static analysis
    - MOBSF – Static analysis report

- Frida / Objection Lab – Bypassing SSL Pinning on Android

Day 4: Mobile Penetration Testing

- Mobile Application Security Verification Standard
  - Step-by-Step Recommendations for Application Analysis
  - Taking a Methodical Approach to Application Security Verification
  - Common Pitfalls While Assessing Applications
  - Detailed Recommendations for Jailbreak Detection, Certificate Pinning, and Application Integrity Verification
  - Android and iOS Critical Data Storage: Keychain and Keystore Recommendations
- Application Integrity Verification
  - Approaches: Checksum Validation, Signature Verification
- Hands-On Lab:
  - Drozer – Exploit with Drozer Agent
  - Demo with Sieve Apk
  - Application Integrity Check Bypass on Android – Apktool, objection
- Securing Mobile Devices with Antivirus & Security Tools
  - Overview of Mobile Security Solutions
  - Scanning and Detecting Malware on Mobile Devices
  - Best Practices for Securing Android and iOS Devices

---------- Thank You ----------