Techonquer

TECHONQUER CERTIFIED MOBILE PENETRATION TESTING

MASTER MOBILE PENETRATION TESTING & APPLICATION SECURITY WITH A COMPREHENSIVE, HANDS-ON PROGRAM DESIGNED FOR REAL-WORLD ANDROID AND IOS SECURITY TESTING

CHAPTER 1 - ANDROID FUNDAMENTALS

1. HISTORY OF ANDROID
2. UNDERSTANDING ANDROID HARDWARE AND SOFTWARE ARCHITECTURE
3. ANDROID OS VERSIONS AND COMPATIBILITY
4. ANDROID SECURITY MODEL
5. ANDROID PERMISSION MODEL FOR APPLICATION SECURITY
6. SANDBOXING AND DEVICE ROOTING
7. UNDERSTANDING SELINUX AND APP SECURITY
8. SECURING ANDROID WITH GOOGLE PLAY PROTECT

CHAPTER 2 - IOS FUNDAMENTALS

1. HISTORY OF IOS
2. UNDERSTANDING IOS HARDWARE AND SOFTWARE ARCHITECTURE
3. IOS OS VERSIONS AND COMPATIBILITY
4. IOS SECURITY MODEL
5. IOS PERMISSION MODEL FOR APPLICATION SECURITY
6. SANDBOXING AND DEVICE JAILBREAKING
7. UNDERSTANDING APPLE'S SECURE ENCLAVE
8. APP STORE SECURITY STANDARDS

CHAPTER 3 - MOBILE APP SECURITY BASICS

1. UNDERSTANDING APK AND IPA PACKAGE STRUCTURES
2. KEY DIRECTORIES AND FILES IN APK / IPA PACKAGES
3. CODE SIGNING AND APPLICATION ENCRYPTION
4. MOBILE APP SECURITY THREAT LANDSCAPE
5. ANDROID AND IOS APP STORES: SECURITY REQUIREMENTS AND POLICIES
6. MOBILE APP HARDENING TECHNIQUES

CHAPTER 4 - MOBILE APPLICATION VULNERABILITIES

1. Weak Server-Side Controls (M1): Understanding and Exploiting
2. Insecure Data Storage (M2): Risks and Mitigations
3. Insufficient Transport Layer Protection (M3): Exploiting and Fixing
4. Unintended Data Leakage (M4): Vulnerabilities in Caches and Logs
5. Poor Authentication & Authorization (M5): Types and Avoidance
6. Broken Cryptography (M6): Symmetric, Asymmetric & Key Management
7. Client-Side Injections (M7): Testing for XSS and SQLi on Mobile
8. Security Decisions via Untrusted Input (M8): Common Risk

CHAPTER 4 - MOBILE APPLICATION VULNERABILITIES

9. Improper Session Handling (M9): Session Management in Mobile Apps
10. Lack of Binary Protection (M10): Reverse Engineering and Patching
11. Additional Vulnerabilities: Intent Spoofing, Tapjacking, and Side-Channel Attacks

CHAPTER 5 - SETTING UP MOBILE PENTESTING ENVIRONMENT

1. Mobile Pentesting Setup for Android and iOS
2. Device Emulators and Simulators for Testing
3. Rooting and Jailbreaking for Research Purposes
4. Using Drozer for Android Security Testing
5. Analyzing AndroidManifest.xml and App Permissions
6. Configuring Burp Suite for Traffic Interception
7. Bypassing Traffic Interception Protections
8. Working with Frida for Dynamic Instrumentation
9. Static and Dynamic Analysis Tools Setup

CHAPTER 6- MOBILE APPLICATION ATTACKS

1. Exploiting Android and iOS Vulnerabilities
2. Penetration Testing Workflow and Methodologies
3. Essential Mobile Security Testing Tools (MobSF, QARK, OWASP ZAP)
4. Techniques for Bypassing Security Controls (SSL Pinning, Root Detection)
5. Dynamic Analysis and Hooking with Xposed and Frida
6. Reverse Engineering Android and iOS Apps
7. Working with Proxies and Analyzing API Calls
8. API Security Testing in Mobile Applications

CHAPTER 7- ADVANCED MOBILE APPLICATION ATTACKS

1. Advanced Exploitation Techniques and Tools
2. Bypassing Multi-Layered Security Controls
3. Advanced Dynamic Instrumentation for Vulnerability Analysis
4. Mobile Device Forensics and Data Recovery Techniques
5. Exploiting Zero-Day Vulnerabilities in Mobile Apps
6. Advanced Reverse Engineering with IDA Pro and Ghidra

CHAPTER 8- MOBILE PENTESTING BEST PRACTICES

1. Comprehensive Mobile Pentesting Methodologies
2. Mobile App Security Testing Frameworks (OWASP MASVS, MSTG)
3. Recommended Tools for Professional Mobile Pentesters
4. Reporting and Documentation Best Practices
5. Effective Vulnerability Disclosure and Communication

CHAPTER 9- MOBILE CTF CHALLENGES AND LABS

1. Basic Android CTF Challenges: Reverse Engineering and Permissions Bypass
2. Advanced Android CTFs: Exploiting Insecure Data Storage and SSL Pinning Bypass
3. Basic iOS CTF Challenges: Jailbreaking and Binary Analysis
4. Mixed Mobile CTFs: Multi-Platform Challenges on API Security
5. Capture the Flag Labs: Real-World Scenarios and Vulnerability Exploitation
6. Guided Walkthroughs for CTF Challenges and Solutions

Techonquer

CONTACT US NOW

STILL CONFUSE ?
HAVE ANY QUERIES

+91 6367098233

INFO@TECHONQUER.ORG

TECHONQUER.ORG