Course Introduction

This 3-days intensive course is designed for beginners, providing a comprehensive introduction to the fundamental concepts of mobile security and penetration testing techniques. Attendees will gain essential theoretical knowledge and hands-on skills essential for performing penetration testing on mobile applications. This training equips participants with the ability to recognize, exploit, and remediate security vulnerabilities in mobile applications and devices.

Course Objectives

- To understand the fundamental principles of mobile application security with a focus on the OWASP Top 10 vulnerabilities.
- To learn how to use various penetration testing tools and techniques essential for assessing mobile application security.
- To gain the knowledge of mobile application vulnerabilities such as insecure data storage, insecure authentication, root/jailbreak exploits, and other related security threats.
- To acquire practical skills by conducting hands-on penetration testing on mobile applications, identifying security flaws, and exploiting vulnerabilities, including those found in the OWASP Top 10.

Learning Level

- Fundamental

Course Duration

- 3 Days

Target Group

- Junior penetration tester
- IT auditor
- Developer
- IT operation
- General attendees (ผู้สนใจทั่วไป)

Course Outline

© Copyright 2001-2026: ACIS Professional Center Co., Ltd. All rights reserved. All contents of this form constitute the property of ACIS Professional Center Co., Ltd. and may not be copied, reproduced or distributed without prior written permission

Day 1

- Introduction to Mobile Application Penetration Testing
- Goals of Mobile App Penetration Testing
- Mobile operating systems (iOS, Android)
- OWASP Mobile Top 10
  - Improper Credential Usage
  - Inadequate Supply Chain Security
  - Insecure Authentication/Authorization
  - Insufficient Input/Output Validation
  - Insecure Communication
  - Inadequate Privacy Controls
  - Insufficient Binary Protections
  - Security Misconfiguration
  - Insecure Data Storage
  - Insufficient Cryptography
- Setting Up the PenTest Environment

Day 2

- Android Architecture
- Android Virtual machines
- Android Security Model
- Setting up a testing environment
- Android build process
- Reversing APKs
- Bypassing Android app security
- Payload encryption (MiTM)
- Other security controls verification
- Input validation on client/server side

Day 3

- iOS Architecture
- Setting up a testing environment
- iOS build process
- Reversing IPAs

For More Information & Registration, Please Contact Training Division
Tel:(66) 2253-4736, Fax:(66) 2253-4737, Hotline:(66) 86-325-7129, E-mail: registration@acisonline.net

© Copyright 2001-2026: ACIS Professional Center Co., Ltd. All rights reserved. All contents of this form constitute the property of ACIS Professional Center Co., Ltd. and may not be copied, reproduced or distributed without prior written permission

- Bypassing iOS app security
- Payload encryption (MiTM)
- Other security controls verification
- Frida Tutorial
- LAB - Hands-On Mobile Application Pentest

Official Training Partner

For More Information & Registration, Please Contact Training Division
Tel:(66) 2253-4736, Fax:(66) 2253-4737, Hotline:(66) 86-325-7129, E-mail: registration@acisonline.net

© Copyright 2001-2026: ACIS Professional Center Co., Ltd. All rights reserved. All contents of this form constitute the property of ACIS Professional Center Co., Ltd. and may not be copied, reproduced or distributed without prior written permission