RECON
CYBER SECURITY

DEFEND | DETECT | SECURE

OUR PARTNERS

cisco python EY Red Hat CompTIA Microsoft

OVERVIEW

In this course, students will learn the about Apple IOS Application based Penetration Testing techniques. Topics include IOS lab setup, XCODE, SSL Pinning attack, Network attack and more.

PRE-REQUISITES

Students should have prior knowledge with Linux Operating System and Penetration Testing.

WHO WE ARE

We promise to offer the best training and certification programs to our students. We provide the programs and resources you need to succeed if you are just beginning your Cyber security career or are an experienced expert wishing to develop your skills. Contact us today to learn more about our training and certification options!

WHY CHOOSE US

Welcome to our Cyber Security Training Institute, where we are committed to giving individuals and organisations who want to protect their digital assets thorough training and certification programmes. Our knowledgeable Trainers will bring you through the complexities of cyber security with their cutting-edge expertise and practical experience. You will learn useful methods and abilities to protect yourself from online dangers, such as ethical hacking, network security, incident response, and other things. Our programmes give you the opportunity to hone your skills and grow your profession through practical lab experiences and individualised coaching.

APPLE IOS APP PEN-TESTING COURSE CONTENT

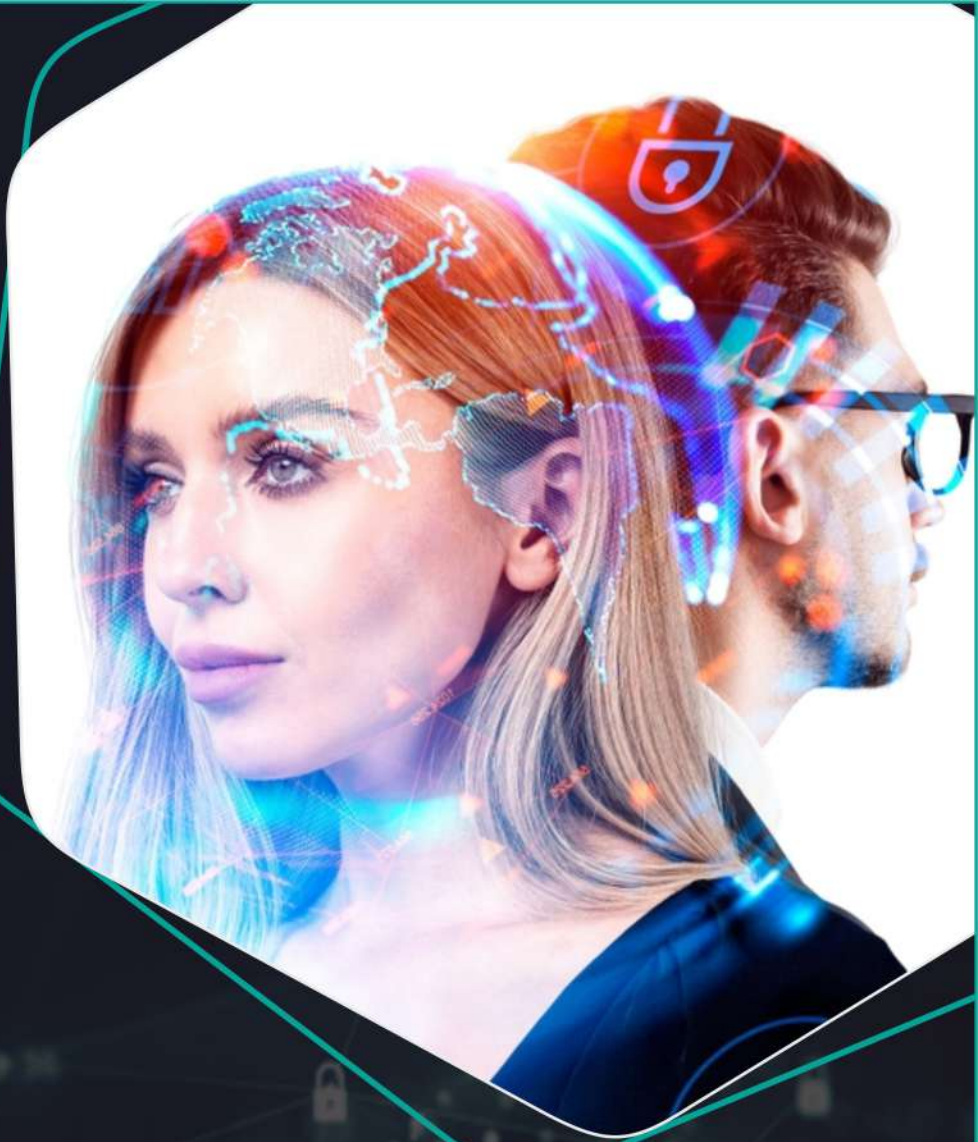
COURSE DURATION: 40 hrs

- Module 12: Introduction to Frida / Frida CLI
  - What is Frida?
  - Using Frida CLI for iOS app testing
  - Setting up Frida for real-time analysis
- Module 01: Introduction
  - Overview of iOS penetration testing
  - Importance of securing iOS applications
  - Objectives of the course
- Module 02: Introduction to IOS Apps
  - iOS application architecture
  - IOS app development environment
  - Basic components of iOS applications
- Module 03: Challenges with IOS lab setup
  - Limitations of iOS environment for testing
  - Common challenges faced in lab setup
  - Security features that complicate penetration testing
- Module 04: Lab setup with jailbreaken IOS device
  - What is jailbreaking?
  - Tools and techniques for jailbreaking iOS devices
  - Setting up a secure lab environment with a jailbroken device
- Module 05: Setting up XCODE
  - Introduction to Xcode for iOS app development
  - Setting up Xcode for penetration testing
  - Basics of using Xcode in iOS testing
- Module 06: Installing Apps in IOS device
  - Methods to install apps on iOS devices
  - Installing third-party applications
  - Security considerations during app installation
- Module 07: Decrypting IOS applications
  - Overview of app encryption in iOS
  - Techniques to decrypt iOS apps
  - Tools for decrypting iOS applications
- Module 08: Introduction to SecureStorev2
  - What is SecureStorev2?
  - How iOS apps utilize SecureStorev2
  - Security implications of using SecureStorev2
- Module 09: Dumpping class information
  - Understanding iOS application class structures
  - Tools to dump class information
  - Analyzing dumped class data
- Module 10: Jailbreak detection bypass
  - Jailbreak detection mechanisms in iOS apps
  - Techniques to bypass jailbreak detection
  - Tools for bypassing jailbreak detection
- Module 11: IOS Traffic analysis
  - Introduction to iOS traffic monitoring
  - Tools for capturing network traffic on iOS devices
  - Analyzing traffic for vulnerabilities

- Module 13: Frida Scripts to trace HTTP calls
  - Writing Frida scripts for HTTP tracing
  - Tracking HTTP traffic in iOS apps
  - Analyzing network calls with Frida
- Module 14: Introduction to end-to-end Encryption
  - Basics of end-to-end encryption in iOS apps
  - How encryption protects data transmission
  - Testing for encryption vulnerabilities
- Module 15: Introduction to hopper
  - Overview of Hopper disassembler
  - Using Hopper for iOS reverse engineering
  - Analyzing iOS app binaries with Hopper
- Module 16: Jailbreak detection using hopper
  - Reverse engineering jailbreak detection mechanisms
  - Analyzing iOS apps for jailbreak detection in Hopper
  - Techniques to bypass detection
- Module 17: SSL pinning attack
  - Understanding SSL pinning in iOS apps
  - Methods to bypass SSL pinning
  - Tools to conduct SSL pinning attacks
- Module 18: Pentesting Local Data storage
  - Overview of local data storage in iOS apps
  - Testing for vulnerabilities in stored data
  - Tools for accessing and analyzing local storage
- Module 19: Pentesting Uninteded Data Leakage
  - Types of data leakage in iOS apps
  - Detecting unintended data exposure
  - Mitigating data leakage risks
- Module 20: Pentesting client side injection
  - Common client-side injection attacks in iOS
  - Detecting vulnerabilities in client-side code
  - Exploiting client-side injection
- Module 21: Traffic Analysis
  - Analyzing inbound and outbound traffic in iOS apps
  - Tools for traffic interception and analysis
  - Identifying insecure data transmissions
- Module 22: Run Time Analysis
  - Monitoring iOS applications in real-time
  - Tools and techniques for runtime analysis
  - Identifying vulnerabilities during execution
- Module 23: Network Attacks
  - Common network attacks targeting iOS applications
  - Detecting and exploiting network vulnerabilities
  - Protecting apps against network-based attacks
- Module 24: Reporting
  - Best practices for writing a penetration testing report
  - Documenting vulnerabilities and remediation steps
  - Structuring reports for different audiences (technical vs. non-technical)

- **500 GB Toolkit**
- **Weekend / Weekdays classes**
- **Online and Offline classes**
- **6 Months Internships Latter**
- **2 Year Membership**
- **Diploma Certificate After Completion**
- **Interview Preparation**
- **Live Hacking Training**
- **Class session recordings**
- **Ebooks Tutorials**
- **24x7 Support**

- Every Class Recordings
- Easy Repetations
- Shareable Content
- Hybrid Classes
- Checkpoint Based Training
- 24x7 Support



RECON CYBER SECURITY PVT. LTD

(HEAD OFFICE | LAXMI NAGAR, NEW DELHI)

2nd Floor, Gali no 1, Shakarpur, Laxmi Nagar New Delhi 110092

WhatsApp or Call : +91-8595756252, +91-8800874869

Training@reconforce.in, Info@reconforce.in

RECON CYBER SECURITY PVT. LTD

(BRANCH OFFICE | SANT NAGAR BURARI, NEW DELHI)

Ground Floor, Gali no 8, Main Market, Sant Nagar, Burari, New Delhi 110092

WhatsApp or Call : +91-8595756252, +91-8800874869

Training@reconforce.in, Info@reconforce.in

#RECON CYBER SECURITY