RECON
CYBER SECURITY

DEFEND | DETECT | SECURE

OUR PARTNERS

cisco python EY Red Hat CompTIA Microsoft

OVERVIEW

In this course, students will learn the about Web Application based Penetration Testing techniques. Topics include Reconnaissance, Scanning, Exploitation, Post Exploitation and more.

PRE-REQUISITES

Students should have prior knowledge with Operation System such as : Windows 7, 8, 10, or 11 etc.

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.

MOBILE APP PEN-TESTING COURSE CONTENT

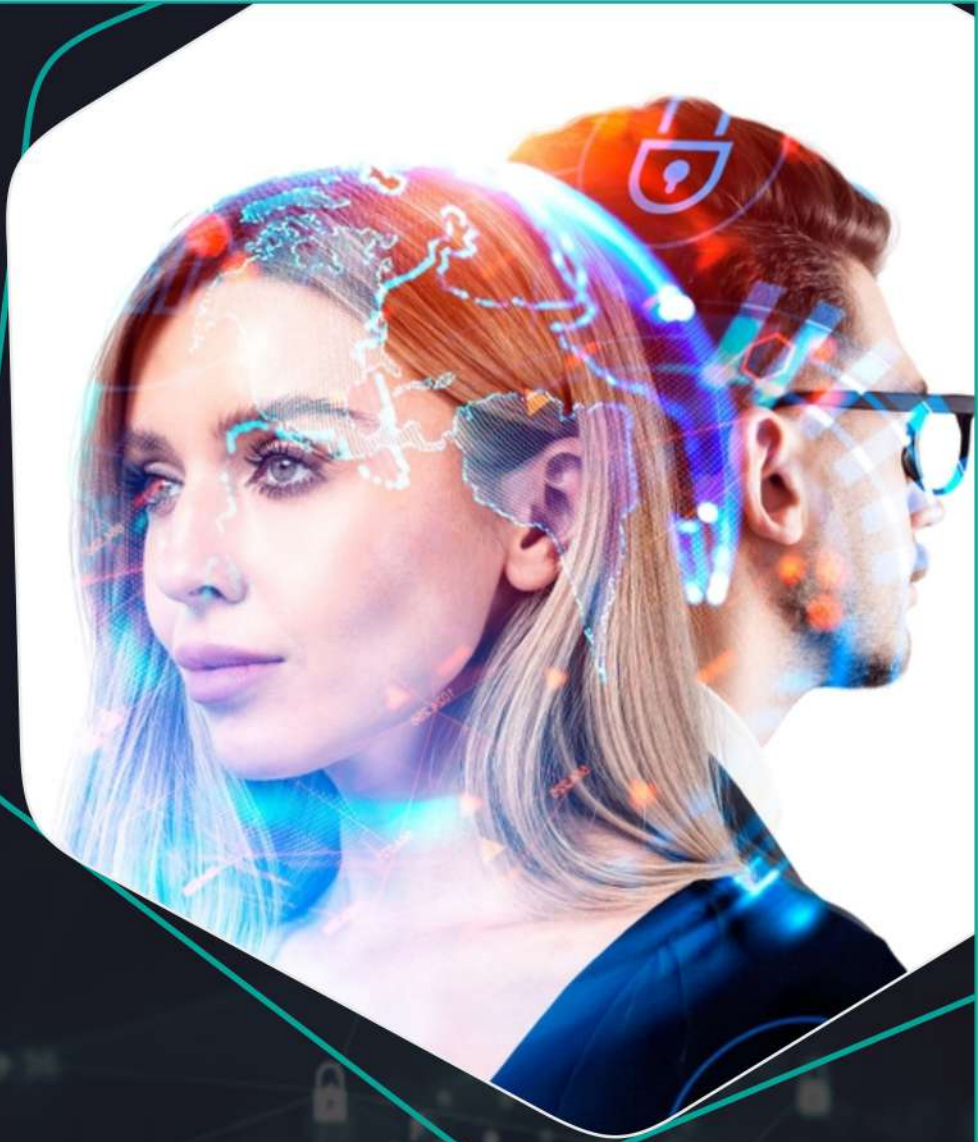
COURSE DURATION: 40 hrs

- Lesson 01 : Android Fundamentals
  - Introduction to Android OS
  - Android Application Components
  - Android Security Model
  - Android Permissions and Manifest File
  - Android Development Environment
- Lesson 02 : Introduction to Mobile-App Testing
  - Overview of Mobile App Testing
  - Types of Mobile App Testing
  - Tools and Frameworks for Mobile Testing
  - Mobile App Testing Lifecycle
- Lesson 03 : Lab Setup
  - Setting Up Android Studio
  - Installing Required SDKs
  - Configuring Emulators and Devices
  - Setting Up Testing Tools
- Lesson 04 : Android Architectur
  - Android System Architecture
  - Android Runtime and Libraries
  - Application Framework
  - Application Components Overview
- Lesson 05 : APK File Structur
  - Understanding APK Components
  - APK Manifest File
  - Resources and Assets
  - DEX Files and their Role
- Lesson 06 : Reversing with APK tool / JADx-GUI
  - APK Tool Usage
  - Decompiling APK Files
  - Understanding Decompiled Code
  - Using JADx-GUI for Code Analysis
- Lesson 07 : Reversing with MobSF
  - Introduction to Mobile Security Framework (MobSF)
  - MobSF Installation and Setup
  - Analyzing APK Files with MobSF
  - Understanding MobSF Reports
- Lesson 08 : Static Analysis
  - Static Analysis Techniques
  - Tools for Static Analysis
  - Identifying Common Vulnerabilities
  - Analyzing Code for Security Issues
- Lesson 09 : Scanning Vulnerabilities with Drozer
  - Introduction to Drozer
  - Installing and Configuring Drozer
  - Scanning for Vulnerabilities
  - Interpreting Drozer Results
- Lesson 10 : Improper Platform Usage
  - Common Platform Usage Issues
  - Identifying Improper Platform Usage
  - Mitigating Risks of Platform Misuse
  - Best Practices for Platform Usage

- Lesson 11 : Log Analysis
  - Understanding Log Files
  - Log Collection and Storage
  - Analyzing Log Files for Security Issues
  - Tools for Log Analysis
- Lesson 12 : Insecure Storage
  - Types of Data Storage in Android
  - Identifying Insecure Storage Practices
  - Mitigating Insecure Storage Risks
  - Best Practices for Secure Storage
- Lesson 13 : Insecure Communication
  - Common Communication Issues in Mobile Apps
  - Securing Communication Channels
  - Implementing Secure Protocols
  - Testing for Communication Security
- Lesson 14 : Hard Coding Issues
  - Understanding Hard Coding
  - Identifying Hard Coded Secrets
  - Mitigating Hard Coding Risks
  - Best Practices for Secure Coding
- Lesson 15 : Insecure Authentication
  - Common Authentication Vulnerabilities
  - Testing Authentication Mechanisms
  - Mitigating Authentication Risks
  - Implementing Secure Authentication Practices
- Lesson 16 : Insufficient Cryptography
  - Understanding Cryptographic Basics
  - Identifying Insufficient Cryptography
  - Using Strong Cryptographic Algorithms
  - Testing Cryptographic Implementations
- Lesson 17 : Code Tempering
  - Types of Code Tampering
  - Identifying Tampered Code
  - Protecting Against Code Tampering
  - Testing for Code Integrity
- Lesson 18 : Extraneous Functionality
  - Understanding Extraneous Functionality
  - Identifying Unnecessary Features
  - Mitigating Risks from Extraneous Functionality
  - Best Practices for Feature Management
- Lesson 19 : SSL Pinning Attack
  - Introduction to SSL Pinning
  - Types of SSL Pinning Attacks
  - Mitigating SSL Pinning Vulnerabilities
  - Testing SSL Pinning Implementations
- Lesson 20 : Intercepting The Network Traffic
  - Techniques for Intercepting Network Traffic
  - Using Tools for Traffic Interception
  - Analyzing Intercepted Traffic
  - Mitigating Risks from Traffic Interception
- Lesson 21 : Dynamic Analysis
  - Overview of Dynamic Analysis
  - Tools for Dynamic Analysis
  - Conducting Dynamic Testing
  - Interpreting Dynamic Analysis Results
- Lesson 22 : Report Preparation
  - Creating Effective Security Reports
  - Key Components of a Security Report
  - Documenting Findings and Recommendations
  - Best Practices for Report Presentation

- **10 gb toolkit**
- **Weekend / weekdays classes**
- **Online and offline classes**
- **1 year membership**
- **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