RECON
CYBER SECURITY

DEFEND | DETECT | SECURE

OUR PARTNERS

cisco python EY Red Hat CompTIA Microsoft

OVERVIEW

In this course, students will learn the about IOT based Penetration testing and Home automation techniquies. Topics include Vehicles Security, Pandora's Box, IOT interfaces and Services and more.

PRE-REQUISITES

Students should already be familiar with how to operate the Linux Operating system.

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.

IOT SECURITY COURSE CONTENT

COURSE DURATION: 35 hrs

- Lesson 1 : The IOT Security testing Overview
  - Introduction to IoT Security
  - IoT Security Threat Landscape
  - Key IoT Security Challenges
  - Overview of Security Testing Methods
- Lesson 2 : Case Study: Connected and Self-Driving
  - Introduction to Connected Vehicles
  - Security Risks in Self-Driving Technology
  - Case Study Analysis: Recent Vulnerabilities
  - Best Practices for Securing Autonomous Vehicles
- Lesson 3 : Vehicles Security
  - Security Mechanisms in Modern Vehicles
  - Common Attack Vectors
  - Vehicle Communication Protocols
  - Securing Vehicle Firmware and Software
- Lesson 4 : Case Study: Microgrids
  - Understanding Microgrid Systems
  - Security Threats in Microgrids
  - Case Study Analysis: Real-World Incidents
  - Strategies for Enhancing Microgrid Security
- Lesson 5 : Case Study: Smart City Drone System
  - Overview of Smart City Drones
  - Potential Security Issues in Drone Systems
  - Case Study Analysis: Security Breaches
  - Measures for Securing Drone Operations
- Lesson 6 : IOT Hardware and Software
  - Components of IoT Hardware
  - Security Implications of IoT Firmware
  - Best Practices for Securing IoT Devices
  - IoT Software Development Security
- Lesson 7 : Communication and Messaging Protocol
  - Components of IoT Hardware
  - Security Implications of IoT Firmware
  - Best Practices for Securing IoT Devices
  - IoT Software Development Security
- Lesson 8 : IOT Interfaces and Services
  - Overview of IoT Interfaces
  - Securing IoT Services
  - Common Interface Vulnerabilities
  - Best Practices for Interface Security
- Lesson 9 : Threats, Vulnerabilities and Risks
  - Identifying IoT Threats and Vulnerabilities
  - Risk Assessment Techniques
  - Case Examples of IoT Security Breaches
  - Risk Mitigation Strategies
- Lesson 10 : Case Study: The Mirai Botnet Opens Up
  - Introduction to the Mirai Botnet
  - How the Mirai Botnet Operates
  - Analysis of Mirai Botnet Attacks
  - Lessons Learned and Mitigation Strategies
- Lesson 11 : Pandora's Box
  - Overview of Pandora's Box in IoT Security
  - Case Study of Pandora's Box Exploits
  - Implications for IoT Security
  - Recommendations for Avoiding Similar Issues

- Lesson 12 : Today's Attack Vector
  - Current Trends in IoT Attacks
  - Emerging Threats and Attack Vectors
  - Case Studies of Recent IoT Attacks
  - Proactive Measures for Defense
- Lesson 13 : Current IOT Security Regulations
  - Overview of IoT Security Regulations
  - Key Regulatory Bodies and Standards
  - Compliance Requirements
  - Impact of Regulations on IoT Security Practices
- Lesson 14 : Current IOT Privacy Regulations
  - Overview of IoT Privacy Laws
  - Key Privacy Regulations and Standards
  - Compliance Strategies
  - Balancing Security and Privacy
- Lesson 15 : What is Threat Modeling
  - Introduction to Threat Modeling
  - Types of Threat Models
  - Steps in Threat Modeling
  - Applying Threat Models to IoT Systems
- Lesson 16 : An Introduction to IOT Security Architectures
  - Overview of IoT Security Architectures
  - Key Components of IoT Security Architecture
  - Design Principles for Secure IoT Architectures
  - Case Studies of Security Architecture Implementation
- Lesson 17 : Identifying Asset
  - Asset Identification in IoT Systems
  - Classifying IoT Assets
  - Tools and Techniques for Asset Management
  - Securing Identified Assets
- Lesson 18 : Creating a System Architecture
  - Designing IoT System Architecture
  - Incorporating Security into Architecture Design
  - Tools for Architecture Design
  - Review and Validation of System Architecture
- Lesson 19 : Documenting Threats
  - Techniques for Threat Documentation
  - Tools for Documenting Threats
  - Examples of Threat Documentation
  - Using Documentation for Risk Management
- Lesson 20 : Rating Threats
  - Methods for Threat Rating
  - Criteria for Threat Severity
  - Tools for Threat Assessment
  - Incorporating Threat Ratings into Risk Management
- Lesson 21 : IOT Privacy Concerns
  - Common Privacy Issues in IoT
  - Impact of Privacy Concerns on IoT Security
  - Case Studies of Privacy Breaches
  - Strategies for Addressing Privacy
- Lesson 22 : Privacy By Design (PbD)
  - Principles of Privacy By Design
  - Implementing PbD in IoT Systems
  - Case Studies of PbD Implementation
  - Benefits and Challenges of PbD
- Lesson 23 : Conducting a Privacy Impact Assessments
  - Overview of Privacy Impact Assessments (PIAs)
  - Steps in Conducting a PIA
  - Tools and Techniques for PIAs
  - Using PIAs to Enhance IoT Privacy and Security

- **20 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

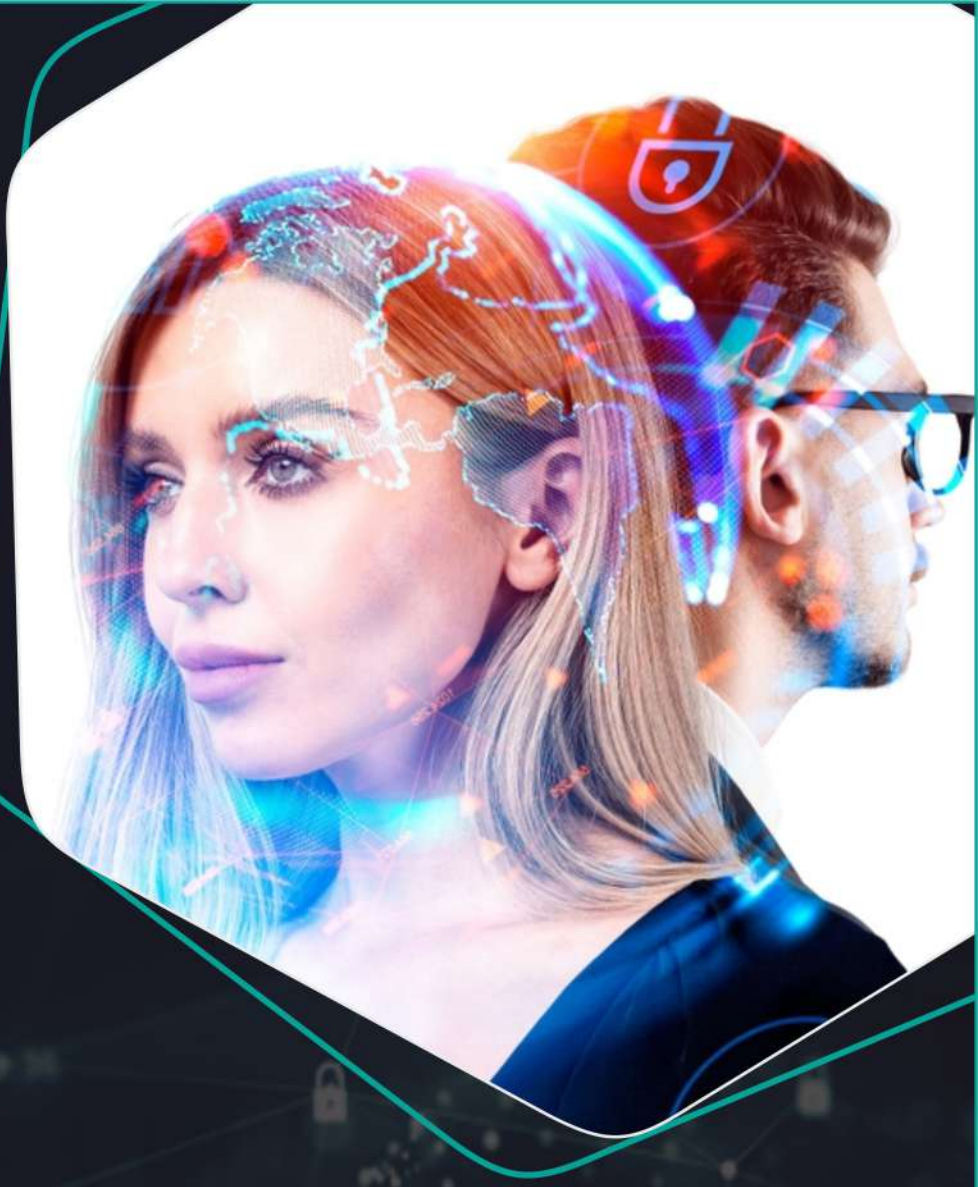
Easy Repetations

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