RECON
CYBER SECURITY

DEFEND | DETECT | SECURE

OUR PARTNERS

cisco · python · EY · Red Hat · CompTIA · Microsoft

OVERVIEW

In this course, students will learn the difference between ethical hacking and unethical hacking and gain a lot of knowledge about cybersecurity. Topics include information gathering, scanning, Wi-Fi hacking, mobile hacking, social media hacking, and more.

PRE-REQUISITES

Students should already be familiar with how to operate the Windows 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.

WINTER INTERNSHIP TRAINING

ETHICAL HACKING COURSE CONTENT

COURSE DURATION: 50 hrs

- Lesson 01: Introduction to Ethical Hacking
  - Understanding Ethical Hacking
  - Ethical Hacking vs Malicious Hacking
  - Legal Aspects of Ethical Hacking
- Lesson 02 : Kali Linux Hands on Training
  - Introduction to Kali Linux
  - Installing and Configuring Kali Linux
  - Essential Kali Linux Tools for Ethical Hacking
- Lesson 03 : Reconnnaissance
  - Active Footprinting Techniques
  - Passive Footprinting Techniques
  - Fingerprinting: Active and Passive Methods
- Lesson 04 : Scanning Networks
  - Host Discovery and Enumeration
  - TCP/UDP Port Scanning Methods
  - Vulnerability Scanning Tools and Techniques
- Lesson 05 : Enumeration
  - Network Enumeration Techniques
  - Gathering Usernames, Shares, and Services
  - Enumeration Tools Overview
- Lesson 06 System Hacking
  - Gaining Physical Access to Systems (Windows/Linux)
  - Password Cracking Techniques
  - Privilege Escalation on Windows and Linux Systems
- Lesson 07 : Malware & Threats
  - Types of Malware: Virus, Worms, and Trojan Horses
  - Understanding Ransomware and Its Impact
  - Polymorphic and Macro Viruses
  - Rootkits and Stealth Malware
- Lesson 08 : Social Engineering
  - Phishing Attacks: Detection and Prevention
  - Vishing Attacks: Techniques and Defense
  - Social Engineering Tools and Scenarios
- Lesson 09 : Denial of Service
  - Understanding DoS and Its Mechanisms
  - Distributed Denial of Service (DDoS) Attacks
  - Defense Mechanisms Against DoS/DDoS
- Lesson 10 : Session Hijacking
  - Understanding Session Hijacking
  - Techniques to Prevent Session Hijacking
  - Tools for Hijacking Detection

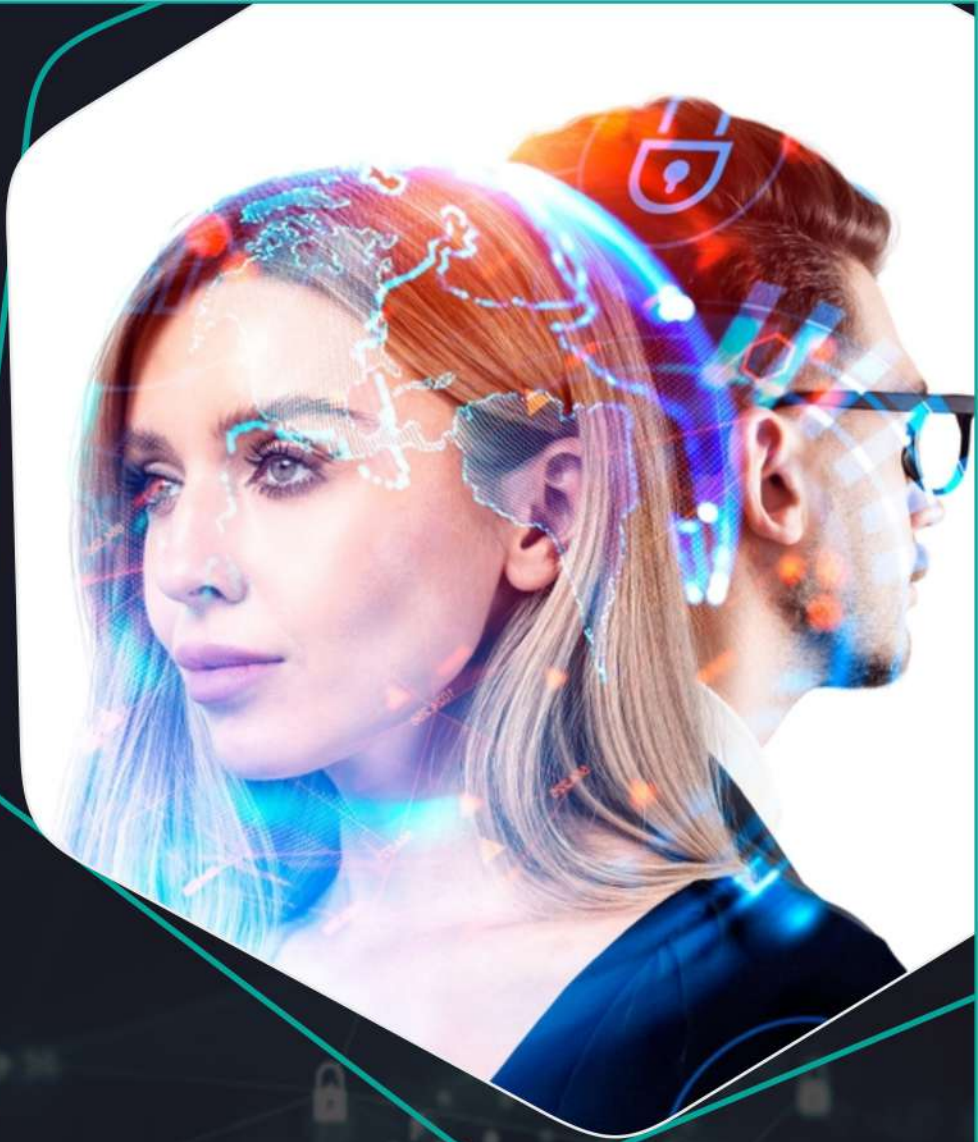
- Lesson 11 : Wireless Hacking
  - WEP/WPA/WPA2 Security Flaws
  - Wi-Fi Hacking Techniques and Tools
  - Wireless Network Defense Strategies
- Lesson 12 Mobile Hacking
  - Mobile OS Vulnerabilities (Android/iOS)
  - Exploiting Mobile Devices
  - Mobile Security Best Practices
- Lesson 13 : Hacking Web-Application (with BurpSuite)
  - Introduction to Web Application Vulnerabilities
  - Using BurpSuite for Vulnerability Scanning
  - Hands-On Web Application Exploitation
- Lesson 14 : SQL Injection
  - Automatic SQL Injection Tools
  - Manual SQL Injection Techniques
  - Preventing SQL Injection Attacks
- Lesson 15 : Hacking Web Server
  - Web Server Exploitation Techniques
  - Common Web Server Vulnerabilities
  - Securing Web Servers
- Lesson 16 : Sniffing / Sniffers
  - Man-in-the-Middle (MITM) Attacks
  - DNS, DHCP, and MAC Address Spoofing
  - Network Sniffing Tools and Countermeasures
- Lesson 17 : IDS, Firewall, Honeypot
  - Intrusion Detection Systems (IDS) and Their Role
  - Configuring Firewalls for Security
  - Deploying Honeypots to Trap Attackers
- Lesson 18 : Cryptography
  - Basics of Cryptography and Encryption
  - Public Key vs Private Key Encryption
  - Implementing Cryptographic Techniques
- Lesson 19 : Basics of Cloud Computing / Hacking
  - Introduction to Cloud Computing
  - Cloud Infrastructure Vulnerabilities
  - Cloud Security Best Practices
- Lesson 20 : IoT Hacking
  - Internet of Things (IoT) Vulnerabilities
  - Exploiting IoT Devices
  - Securing IoT Devices
- Lesson 21 : Basics of Penetration Testing
  - Introduction to Penetration Testing Methodologies
  - Stages of Penetration Testing
  - Penetration Testing Tools and Reporting

BOOTCAMP TRAINING HOURS

- **3 HOURS**
- **4 HOURS**
- **6 HOURS**

- **40 gb toolkit**
- **Weekend / weekdays classes**
- **Online and offline classes**
- **1 month internship letter**
- **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