RECON
CYBER SECURITY

DEFEND | DETECT | SECURE

OUR PARTNERS

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

OVERVIEW

In this course, student will learn Basic to Professional Penetration Testing techniques to find out vulnerabilities and how to exploit them Like: Penetration Testing, Mobile Pen-testing, Website Hacking, Mobile Hacking, etc Participant Learn to use Kali Linux

PRE-REQUISITES

Students should already be familiar with any operating system (Like: Windows Or Linux).

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.

SIX MONTHS VA/PT DIPLOMA IN CYBER SECURITY

ADVANCED NETWORKING

LEVEL 1 : COURSE DURATION: 45 hrs

- Module 01: Introduction To Networking
- Module 02: Fundamentals of Networking
- Module 03: OSI Model v/s TCP/IP
- Module 04: TCP v/s UDP
- Module 05: Mac Address
- Module 06: IP Addressing
- Module 07: IP Addressing v4 (IPv4)
- Module 08: IP Addressing v6 (IPv6)
- Module 09: Subnetting
- Module 10: Network Cabling
- Module 11: Router Fundamentals
- Module 12: Lab Configuration on Packet tracer
- Module 13: Router, Switch And PC Communication
- Module 14: Routing Protocols
- Module 15: Default Routin
- Module 16: Static Routing
- Module 17: Static routing With Subnetting
- Module 18: Dynamic Routing
- Module 19: RIP
- Module 20: EIGRP
- Module 21: OSPF
- Module 22: DHCP
- Module 23: NAT - Network Address Translation
- Module 24: VLAN - Virtual Local Aria Network
- Module 25: ACL - Access Control Line
- Module 26: BGP

LINUX ESSENTIALS

LEVEL 2 : COURSE DURATION: 45 hrs

- Module 01: Introduction to Linux Evolution
- Module 02: Linux Distribution
- Module 03: Linux Embedded System
- Module 04: Hardware Requirement
- Module 05: Installing Linux
- Module 06: OS Differences
- Module 07: Open Software Application
- Module 08: What is Open Source
- Module 09: Desktop and server application
- Module 10: Languages and tools
- Module 11: Packages installs and repositories
- Module 12: The Linux Environments
- Module 13: Linux Desktop Environments
- Module 14: Linux Shell and Commands
- Module 15: Managing Softwares Packages
- Module 16: The Command Line
- Module 17: Difference b/w shells
- Module 18: Command Line
- Module 19: Command Usage
- Module 20: Man Pages
- Module 21: Directories And Files
- Module 22: Searching and Extracting Data From File
- Module 23: Package Installation in Different Directory
- Module 24: User Account and Groups
- Module 25: Creating Account From The Shell
- Module 26: Modifying And Deleting Account
- Module 27: Working as Root
- Module 28: Managing File Ownership And Permission

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

ETHICAL HACKING

LEVEL 3 : COURSE DURATION: 50 hrs

- Module 01: Introduction to Ethical Hacking
- Module 02: Reconnaissance
- Module 03: Active Foot-Printing
- Module 04: Passive Foot-Printing
- Module 05: Finger Printing A/P
- Module 06: Scanning Networks
- Module 07: Host Discovery
- Module 08: TCP/UDP Port Scanning
- Module 09: Vulnerability Scanning
- Module 10: Enumeration
- Module 11: System Hacking
- Module 12: Physical Access (Win. / Linux OS)
- Module 13: Malware & Threats
- Module 14: Virus / Worms
- Module 15: Trojan Horse
- Module 16: Ransomware
- Module 17: Polymorphic Virus
- Module 18: Macro Virus
- Module 19: Micro Virus
- Module 20: Rootkit
- Module 21: Social Engineering
- Module 22: Phishing Attacks
- Module 23: Vishing Attacks
- Module 24: Denial of Service
- Module 25: DOS (Deial of Service)
- Module 26: DDOS
- Module 27: Session Hijacking
- Module 28: Wireless Hacking
- Module 29: WEP / WPA / WPA2 Wi-Fi Hacking
- Module 30: Mobile Hacking
- Module 31: Hacking Web-Application
- Module 32: SQL Injection
- Module 33: Automatic tool based
- Module 34: Manual SQL Injection
- Module 34: Hacking Web Server
- Module 36: Sniffing / Sniffers
- Module 37: MITM Attack
- Module 38: DNS Attack
- Module 39: DHCP Attack
- Module 40: MAC Address Attack
- Module 41: IDS, Firewall, Honeypot
- Module 42: Cryptography
- Module 43: Basics of Cloud Computing/ Hacking
- Module 44: IoT Hacking
- Module 45: Basics of Penetration Testing

PYTHON PROGRAMMING

LEVEL 4 : COURSE DURATION: 50 hrs

- Module 01: Introduction To Python
- Module 02: Environment Setup
- Module 03: Basic Syntax
- Module 04: Comments
- Module 05: Variables
- Module 06: Data Types
- Module 07: Operators
- Module 08: Division Making
- Module 09: Loops
- Module 10: Numbers Module 11: Strings
- Module 12: Lists
- Module 13: Tuples
- Module 14: Dictionary
- Module 15: Date & type
- Module 16: Function
- Module 17: Modules
- Module 18: Files I/O
- Module 19: Exceptions

PENETRATION TESTING

LEVEL 5 : COURSE DURATION: 40 hrs

- Module 01: How to plan your PT
- Module 02: Scooping your Penetration Testing
- Module 03: Network & Web-Application
- Module 04: Scanning Vulnerability
- Module 05: Port Scanning
- Module 06: Script scanning
- Module 07: Enumeration
- Module 08: Service & Version Scanning
- Module 09: Web-Application Scanning
- Module 10: Exploitation with Metasploit
- Module 11: Exploit Vulnerability
- Module 12: Bind & Reverse Shell
- Module 13: Payload Creation, etc.
- Module 14: Post-Exploitation
- Module 15: Pivoting Attack
- Module 16: Browser exploitation
- Module 17: BEEF Exploit
- Module 18: In-Depth Password Attacks
- Module 19: John the Ripper

WEB-APPLICATION PENETRATION TESTING

LEVEL 6 : COURSE DURATION: 40 hrs

- Module 01: Introduction to Web-App Pen-Testing
- Module 02: Finding Subdomains
- Module 03: Understanding HTTP
- Module 04: Access Control Flaws
- Module 05: Ajax Security
- Module 06: Authentication Flaws
- Module 07: Buffer overflows
- Module 08: Code Quality
- Module 09: Concurrency Flaws
- Module 10: Cross-Site Scripting
- Module 11: Improper Error Handling
- Module 12: Injection Flaws
- Module 13: Denial of Service
- Module 14: Insecure Communication
- Module 15: Insecure Configuration
- Module 16: Insecure Storage
- Module 17: Malicious File Execution
- Module 18: Parameter Tampering
- Module 19: Session Management Flaws
- Module 20: Challenge Online Platform

MOBILE-APP PENETRATION TESTING

LEVEL 7 : COURSE DURATION: 40 hrs

- Module 01: Introduction to Mobile-App Testing
- Module 02: Lab setup
- Module 03: Android Architecture
- Module 04: APK File Structure
- Module 05: Reversing with APKtool/ Jadx-GUI
- Module 06: Reversing with MobSP
- Module 07: Static Analysis
- Module 08: Scanning Vulnerabilities with Drozer
- Module 09: Improper Platform Usage
- Module 10: Log Analysis
- Module 11: Insecure Storage
- Module 12: Insecure Communication
- Module 13: Hard Coding Issues
- Module 14: Insecure Authentication
- Module 15: Insufficient Cryptography
- Module 16: Code Tempering
- Module 17: Extraneous functionality
- Module 18: SSL pinning
- Module 19: Intercepting The Network Traffic
- Module 20: Dynamic Analysis
- Module 21: Report Preparation

CERTIFICATION PATH AFTER TRAINING

6 MONTHS DIPLOMA IN CYBER SECURITY

EC-Council

CEH (Certified Ethical Hacker) Theory
CEH (Certified Ethical Hacker) Practical
ECSA (EC-Council Security Analyst)

CompTIA

CompTIA A+
CompTIA N+
CompTIA Security+
CompTIA Pentest+

RECON CYBER SECURITY

DEFEND | DETECT | SECURE

Recon Cyber Security is a leading provider of comprehensive cybersecurity training, renowned for its commitment to excellence and cutting-edge curriculum.

www.reconforce.in

Every Class Recordings

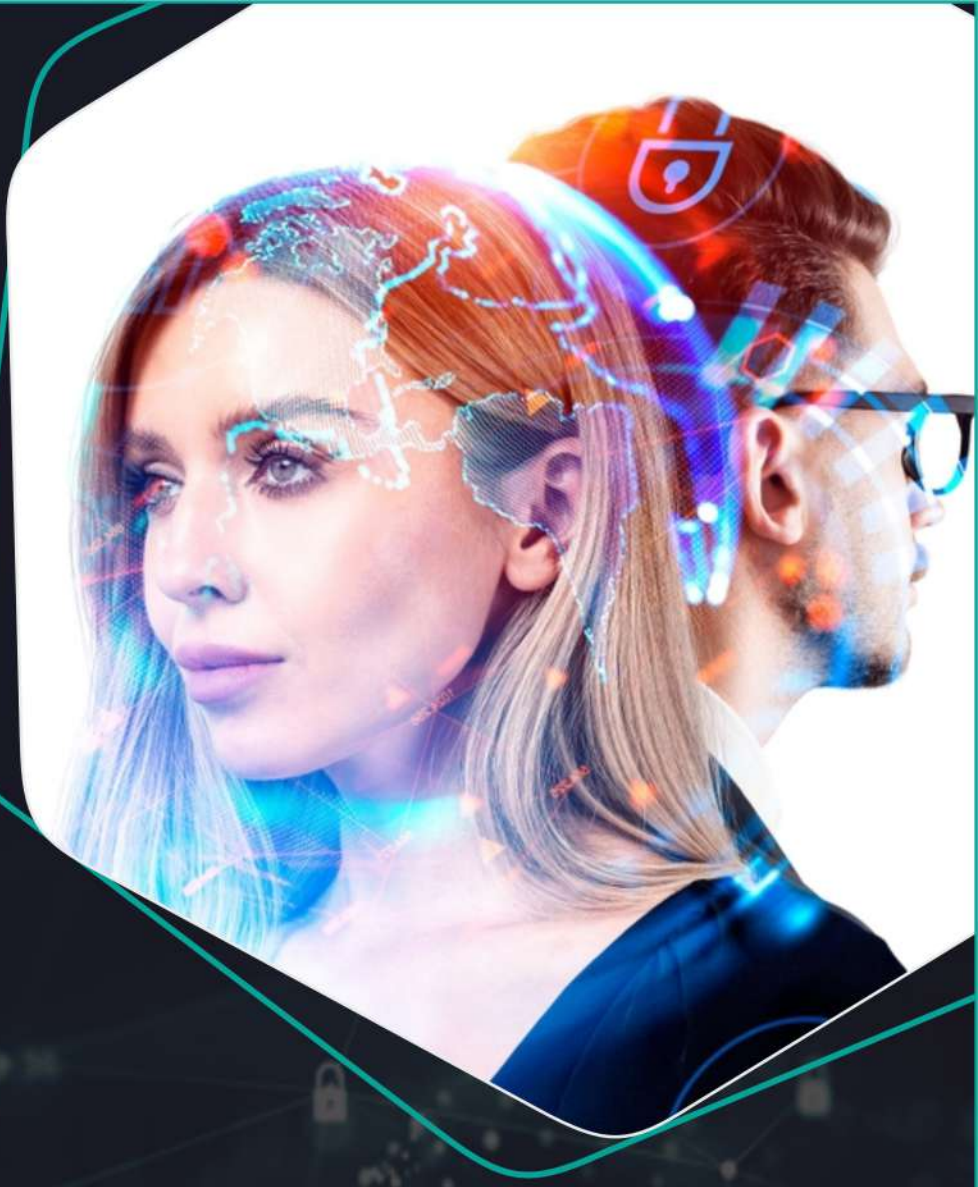
Easy Repetations

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