RECON
CYBER SECURITY

Call Now:
+91-8595756252
+91-8800874869

SEC_RITY IS NOT COMPLETE WITHOUT U!

The security light made me feel safe, though I know that was an illusion. If there is light, you can just see what's coming for you a little more clearly.

Beginner Diploma Course — Duration: 6 Months

Overview

In this course, students 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. participants learn to use Kali Linux.

Pre-Requisites

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

Who We Are?

Recon Force is a Training and Consulting company and adheres to training standards. We are bringing it to improve its security training and services through technology-enabled IT content. Prepares for an important role as a Penetration Testing expert, instrument analyst, service analyst, network security program manager, and other related roles.

Why Choose Recon Cyber Security?

Recon Force is the best accredited Ethical Hacking training classes in Delhi that offers the best Ethical Hacking training in Delhi on practical exams that help aspirants gain professional skills. The institute offers practical and career-based Ethical Hacking training in Delhi to help students find their dream job at various MNCs. Students are given the opportunity to gain practical experience of participating in real Ethical Hacking projects and 100% placement assistance. The Recon Ethical Hacking Course in Delhi is run under the highly experienced industry professionals. It is recognized among the leading Ethical Hacking Center in Delhi, as it operates on a mix of practical learning and learning theory. This type of comprehensive behavioral training with good exposure facilitates the complete transition of the student into a professional.

- **200 Gb Toolkit**
- **24x7 Online Classes Available**
- **Beginner Cyber Security Diploma Certificate**
- **3 Months Internship Letter**
- **Interview Preparation**
- **1 Year Membership**
- **Training by experienced trainers**
- **Live hacking**
- **Checkpoint based training**
- **Class recording**
- **24x7 Support**

LEVEL 1: Advance Networking

- Module 1 : Introduction to Networking
- Module 2 : Networking Fundamentals
- Module 3 : OSI Model
- Module 4 : TCP/IP Model
- Module 5 : Concept of Layers
- Module 6 : Lab Configuration
- Module 7 : Network Devices Fundamentals
- Module 8 : Internet Protocols
- Module 9 : Difference between IPv4 & IPv6
- Module 10 : Subnetting
- Module 11 : Router Fundamentals
- Module 12 : Routing Protocols
- Module 13 : WAN Protocols
- Module 14 : PPP/ NAT & NAT PAT
- Module 15 : SSH
- Module 16 : DHCP
- Module 17 : BGP

LEVEL 2: Ethical Hacking

- Module 1 : Introduction to Ethical Hacking
- Module 2 : Kali Linux hands on Training
- Module 3 : Reconnaissance

- Active Foot-Printing
- Passive Foo-Printing
- Finger Printing Active/Passive

- **Module 4** : Scanning Networks
  - Host Discovery
  - TCP/UDP Port Scanning
  - Vulnerability Scanning
- **Module 5** : Enumeration
- **Module 6** : System Hacking
  - Physical Access (Windows / Linux OS)
- **Module 7** : Malware & Threats
  - Virus / Worms
  - Trojan Horse
  - Ransomware
  - Polymorphic
  - Macro Virus
  - Micro Virus
  - Rootkit etc.
- **Module 8** : Social Engineering
  - Phishing Attacks
  - Vishing Attack, etc.
- **Module 9** : Denial of Service
  - DOS (Denial of Service
  - DDOS (Distributed Denial of Service)
- **Module 10** : Session Hijacking

- **Module 11 : Wireless Hacking**
  - **WEP / WPA / WPA2 Wi-Fi Hacking**
- **Module 12 : Mobile Hacking**
- **Module 13 : Hacking Web-Application (with BurpSuite)**
- **Module 14 : SQL Injection**
  - **Automatic tool based**
  - **Manual SQL Injection**
- **Module 15 : Hacking Web Server**
- **Module 16 : Sniffing / Sniffers**
  - **MITM Attack**
  - **DNS Attack**
  - **DHCP Attack**
  - **MAC Address Attack, etc.**
- **Module 17 : IDS, Firewall, Honeypot**
- **Module 18 : Cryptography**
- **Module 19 : Basics of Cloud Computing**
- **Module 20 : Basics of IOT hacking**
- **Module 21 : Basics of Penetration Testing**

LEVEL 3: Penetration Testing

- **Module 1 : How to plan your Penetration Testing**
- **Module 2 : Scoping your Penetration Testing**
- **Module 3 : Network & Web-Application**

- **Module 4 : Scanning Vulnerability**
  - Port Scanning
  - Script Scanning
  - Enumeration
  - Service & Version Scanning
  - Web-Application Scanning
- **Module 5 : Exploitation with Metasploit**
  - Exploit Vulnerability
  - Bind & Reverse Shell
  - Payload creation, etc.
- **Module 6 : Post-Exploitation**
- **Module 7 : Pivoting Attack**
- **Module 8 : Browser Exploitation**
  - BEEF exploit
- **Module 9 : Denial of Service**
  - DOS (Denial of Service
  - DDOS (Distributed Denial of Service)
- **Module 10 : In-Depth Password Attacks**
  - John the Ripper
  - Brute Force Attack
  - Dictionary Attack
  - Rainbow Table Attack
  - Other Password Cracking Tools
- **Module 11 : Cracking / Solving CTF's**

- Module 12 : Final Analysis
- Module 13 : Final Report Generation
  - Manual Reporting
  - Automatic Reporting

LEVEL 4: Web-Application Penetration Testing

- Module 1 : Introduction to Web-Application Penetration Testing
- Module 2 : Finding Subdomains
- Module 3 : Understanding HTTP
- Module 4 : Access Control Flaws
- Module 5 : Ajax Security
- Module 6 : Authentication Flaws
- Module 7 : Buffer over flaws
- Module 8 : Code Quality
- Module 9 : 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

LEVEL 5: Mobile-Application Penetration Testing

- Module 1 : Android Fundamentals
- Module 2 : Improper Platform usage
- Module 3 : Insecure Data Storage
- Module 4 : Insecure Communication
- Module 5 : Insecure Authentication
- Module 6 : Insecure Authorization
- Module 7 : Client Code quality
- Module 8 : Trojan & Backdoor
- Module 9 : Code Tampering
- Module 10 : Reverse Engineering
- Module 11 : Live Application Testing
- Module 12 : Testing with BurpSuite
- Module 13 : Testing Application on Genymotion

Contact Details:

- ✓ Phone : +91-8595756252
  +91-8800874869
- ✓ Emai : Training@reconforce.in
  Enquiry@reconforce.in
- ✓ Website : www.reconforce.in
  www.reconcybersecurity.com
- ✓ Address : D-64, Ground floor, Gali no-3 Laxmi Nagar
  Near Metro Exit Gate no-5
  Delhi- 110092