# RECON CYBER SECURITY

## CYBER SECURITY BEGINNER DIPLOMA COURSE

## DURATION 6 MONTHS

## 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 cybersecurity 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.

# COURSE SYLLABUS

WWW.RECONFORCE.IN

# Level 1 Advanced Networking

01. Introduction To Networking
02. Fundamentals of Networking
03. OSI Model v/s TCP/IP
04. TCP v/s UDP
05. Mac Address
06. IP Addressing
    - IPv 4
    - IPv 6
07. Subnetting
08. Network Cabling
09. Router Fundamentals
10. Lab Configuration on Packet tracer
11. Router, Switch And PC Communication
12. Routing Protocols
    - Default Routing
    - Static Routing
    - Static routing With Subnetting
    - Dynamic Routing
        - RIP
        - EIGRP
        - OSPF
13. DHCP
14. NAT - Network Address Translation
15. VLAN - Virtual Local Aria Network
16. ACL - Access Control Line
17. BGP

# Level 2 Linux Essentials

01. Linux Evolution And Popular Operating System
    - Introduction
    - Linux Distribution
    - Linux Embedded System
    - Hardware Requirement
    - Installing Linux
    - OS Differences
02. Open Software Application
    - What is Open Source
    - Desktop and server application
    - Languages and tools
    - Packages installs and repositories
03. The Linux Environments
    - Linux Desktop Environments
    - Linux Shell and Commands
    - Managing Softwares Packages
04. The Command Line
    - Difference b/w shells
    - Command Line
    - Command Usage
    - Man Pages
05. Directories And Files
06. Searching and Extracting Data From File
07. Package Installation in Different Directory
08. User Account and Groups
    - Creating Account From The Shell
    - Modifying And Deleting Account
    - Working as Root
09. Managing File Ownership And Permission

# Level 3 Ethical Hacking

01. Introduction to Ethical Hacking
02. Reconnaissance
    - Active Foot-Printing
    - Passive Foot-Printing
    - Finger Printing Active/Passive
03. Scanning Networks
    - Host Discovery
    - TCP/UDP Port Scanning
    - Vulnerability Scanning
04. Enumeration
05. System Hacking
    - Physical Access (Windows / Linux OS)
06. Malware & Threats
    - Virus / Worms
    - Trojan Horse
    - Ransomware
    - Polymorphic Virus
    - Macro Virus
    - Micro Virus
    - Rootkit, etc.
07. Social Engineering
    - Phishing Attacks
    - Vishing Attacks, etc.
08. Denial of Service
    - DOS (Deial of Service)
    - DDOS (Distributed Denial of Service)
09. Session Hijacking
10. Wireless Hacking
    - WEP / WPA / WPA2 Wi-Fi Hacking
11. Mobile Hacking
12. Hacking Web-Application (with BurpSuite)
13. SQL Injection
    - Automatic tool based
    - Manual SQL Injection
14. Hacking Web Server
15. Sniffing / Sniffers
    - MITM Attack
    - DNS Attack
    - DHCP Attack
    - MAC Address Attack, etc.
16. IDS, Firewall, Honeypot
17. Cryptography
18. Basics of Cloud Computing / Hacking
19. IoT Hacking
20. Basics of Penetration Testing

# Level 4 Python Programming

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

# Level 5 Network Pen-Testing

01. How to plan your Penetration Testing
02. Scoping your Penetration Testing
03. Network & Web-Application
04. Scanning Vulnerability
    - Port Scanning
    - Script scanning
    - Enumeration
    - Service & Version Scanning
    - Web-Application Scanning
05. Exploitation with Metasploit
    - Exploit Vulnerability
    - Bind & Reverse Shell
    - Payload Creation, etc.
06. Post-Exploitation
07. Pivoting Attack
08. Browser exploitation
    - BEEF Exploit
09. In-Depth Password Attacks
    - John the Ripper
    - Brute Force Attack
    - Dictionary Attack
    - Rainbow Table Attack
    - Other Password Cracking Tools
10. Cracking / Solving CTFs
    - Final Analysis
12. Final Report Generation
    - Manual Reporting
    - Automatic Reporting

# Level 6 Web-App Pen-Testing

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

# Level 7 Mobile-App Pen-Testing

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

# Tools and Benefits of the Diploma course

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

# Contact Us:


**Call or WhatsApp**

+91-8595756252 | +91-8800874869

**Email Id**

Info@reconforce.in

enquiry@reconforce.in

**Branch 1:**

Street No. 08, Plot No.308,
Main Market Sant Nagar
Burari - 110084

**Branch 2:**

D-64, Main Vikas Marg, Laxmi Nagar
Delhi - 110092