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.

Basic to Advance Diploma Course **Duration: 1 Year**

Overview

In this course, students will learn **Basic to Expert Level Penetration Testing** techniques to find out vulnerabilities and how to exploit them. Like: Bug Hunting, VAPT, IoT Security, CTF Expert, etc.

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.

- **500 Gb Toolkit**
- **24x7 Online Classes Available**
- **Cyber Security Expert Diploma Certificate**
- **6 Months Internship Letter**
- **Interview Preparation**
- **2 Year Membership**
- **Training by experienced trainers**
- **Live Hunting**
- **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**

LEVEL 6: BUG Hunting Course Content

- Module 1 : Cross Site Scripting (XSS)
- Module 2 : Host Header Attack
- Module 3 : URL Redirection
- Module 4 : Command Injection
- Module 5 : Critical File Found
- Module 6 : File inclusion
- Module 7 : Source code disclosure
- Module 8 : File Upload
- Module 9 : Parameter Tampering
- Module 10 : SPF attack
- Module 11 : SQL Injection
- Module 12 : No Rate Limiting
- Module 13 : Long Password DOS
- Module 14 : Insecure Direct Object Reference
- Module 15 : Joomla Security vulnerabilities
- Module 16 : Account Lockout
- Module 17 : Apache HTTP server byte range DOS
- Module 18 : Apache struts RCE Hunting
- Module 19 : Application Server Vulnerabilities
- Module 20 : Authentication Testing
- Module 21 : Buffer Overflow
- Module 22 : CMS Hunting
- Module 23 : Comprehensive Command Injection

- **Module 24 : Cryptographic Vulnerabilities**
- **Module 25 : CSRF**
- **Module 26 : Drupal Security Vulnerabilities**
- **Module 27 : Account takeover through support service**
- **Module 28 : Exposed Source Control**
- **Module 29 : Extraction Information and GEO location through uploaded images**
- **Module 30 : Heart bleed**
- **Module 31 : HSTS**
- **Module 32 : HTTPOXY Attack**
- **Module 33 : Identity Management Testing**
- **Module 34 : Advanced Indirect Object reference**
- **Module 35 : Multi Factor Authentication (2FA) Security Testing**
- **Module 36 : Password Reset Poisoning**
- **Module 37 : Server Side Injection (SSI)**
- **Module 38 : Session Fixation**
- **Module 39 : Shell Shock RCE Testing**
- **Module 40 : SSRF**
- **Module 41 : Testing for Session Management**
- **Module 42 : Ticket Security Testing**
- **Module 43 : Web cache deception Attack**
- **Module 44 : WebMin unauthentic RCE**
- **Module 45 : Word Press Security testing**
- **Module 46 : Application Logic Vulnerabilities**
- **Module 47 : Broken Authentication**
- **Module 48 : Browser cache weakness**

- Module 49 : Cache Testing
- Module 50 : CAPTCHA Security Testing
- Module 51 : Code Injection
- Module 52 : Cookies Testing
- Module 53 : CORS
- Module 54 : CRLF Injection
- Module 55 : CSS Injection
- Module 56 : Dangerous HTTP Methods
- Module 57 : Testing for default Configuration
- Module 58 : Directory listing testing
- Module 59 : DOM clobbering
- Module 60 : HTTP Parameter Pollution
- Module 61 : Identity Management Testing
- Module 62 : LDAP Injection
- Module 63 : Log injection
- Module 64 : Null Byte Injection
- Module 65 : OAUTH Security Testing
- Module 66 : Open redirection
- Module 67 : Web Application Firewall Testing
- Module 68 : Parameter Modification Testing
- Module 69 : PHP Object Injection
- Module 70 : RACE condition Vulnerability
- Module 71 : Relative Path Overview
- Module 72 : Remote Code Injection
- Module 73 : HTTP Headers Testing

- Module 74 : HTTP Headers Testing
- Module 75 : SSL Security Testing
- Module 76 : SSTI Testing
- Module 77 : Template Injection
- Module 78 : Virtual Host Misconfiguration
- Module 79 : Vulnerable Remember me Testing
- Module 80 : Weak Password Reset
- Module 81 : XML Quadratic Blowup
- Module 82 : XML RPC Pingback
- Module 83 : XXE Injection
- Module 84 : Advanced Training About Burp Suite

LEVEL 7: Malware Analysis Course Content

- Module 1 : Introduction to Malware Analysis
- Module 2 : Basic of Analysis
- Module 3 : Advanced Static Analysis
- Module 4 : Analyzing Windows Programs
- Module 5 : Advanced Dynamic Analysis
- Module 6 : Malware Behavior
- Module 7 : Data Encoding and Malware Countermeasures
- Module 8 : Convert Malware Launching
- Module 9 : Anti-Analysis
- Module 10 : Packing and Unpacking

- **Module 11 : Rootkit Techniques**

LEVEL 8: IoT Security Course Content

- **Module 1 : The IoT Security testing Overview**
- **Module 2 : Case Study: Connected and Self-Driving**
- **Module 3 : Vehicles Security**
- **Module 4 : Case Study: Microgrids**
- **Module 5 : Case Study: Smart City Drone System**
- **Module 6 : IoT Hardware and Software**
- **Module 7 : Communication and Messaging Protocols**
- **Module 8 : IoT Interfaces and Services**
- **Module 9 : Threats, Vulnerabilities and Risks**
- **Module 10 : Case Study: The Mirai Botnet Opens up**
- **Module 11 : Pandora's Box**
- **Module 12 : Today's Attack Vector**
- **Module 13 : Current IoT Security Regulations**
- **Module 14 : Current IoT Privacy Regulations**
- **Module 15 : What is Threat Modeling**
- **Module 16 : An Introduction to IoT Security Architectures**
- **Module 17 : Identifying Assets**
- **Module 18 : Creating a System Architecture**
- **Module 19 : Documenting Threats**
- **Module 20 : Rating Threats**

- **Module 21 : IoT Privacy Concerns**
- **Module 22 : Privacy By Design (PbD)**
- **Module 23 : Conducting a Privacy Impact Assessments**

LEVEL 9: CTF Challenge Course Content

- **Module 1 : Introduction**
  - **Finding Files**
  - **Services in Kali SSH Service**
  - **FTP Services**
  - **HTTP Service**
  - **MySQL Service**
  - **Service Management**

- **Module 2 : Basic Linux And Commands**
  - **Locate**
  - **Which**
  - **Find**
  - **Sed**
  - **AWK**
  - **Cut**
  - **Sort**
  - **Grep**

- Head
- Tail
- WGet
- Cat

- **Module 3 : Netcat Tutorials**
  - Getting Start with NC
  - Connection to a Server
  - Fetching HTTP Header
  - Chatting
  - Creating a Backdoor
  - Verbose Mode
  - Save Output to Disk

- **Module 4 : Port Scanning**
  - TCP Delay Scan
  - UDP Scan
  - Randomize Port
  - File Transfer Protocol
  - Banner Grabbing
  - Port Scanning With Nmap & Wireshark
  - TCP Connect Scan with Wireshark
  - Network Sweeping with Wireshark

- SYN Scan with Wireshark
- UDP Scan with Wireshark
- FIN Scan with Wireshark
- Null Scan with Wireshark
- OS Discovery with wireshark
- NSE Scripts with Wireshark
- Nmap Firewall Scan

➢ **Module 5 : Enumeration**

- Overview
- DNS Enumeration
- Forward DNS Lookup
- Reverse DNS Lookup
- Zone Transfers
- NetBIOS & SMB Enumeration
- Null Sessions
- Enum4Linux
- SMB NSE Scripts
- MSQL Enumeration
- MSSQL Enumeration
- SMTP Enumeration
- VRFY Script
- Python Port Scan

- SNMP Enumeration
- SNMP MiB
- SNMP Walk

- **Module 6 : Passive Info Gatering**
  - Overview
  - Google Search
  - Google Hacking Database
  - Directory Bruteforce Attack
  - Metasploit

- **Module 7 : Reverse Shell**
  - PHP reverse shell
  - Python reverse shell
  - Perl reverse shell
  - Bash reverse shell
  - MSFvenom shell

- **Module 8 : Intro to Overflows**
  - Overview
  - Vulnerable Code
  - Stack Overflow

- **Module 9 : Windows Buffer Over Flows Examples**
  - Overview
  - Fuzzing
  - Crash Replication
  - Controlling EIP
  - Introducing shellcode
  - Bad Characters
  - Redirecting Execution
  - Introduction Mona
  - Shellcode Payload
- **Module 10 : Linux Buffer Over Flow Examples**
  - Overview
  - Controlling EIP
  - Locating Space
  - First Stage Shellcode
  - Locating RET
  - Generating Shellcode
- **Module 11 : Using Public Exploits**
  - Overview
  - Finding Exploits
  - Exploit-DB
  - Fixing Exploits 1

- Fixing Exploits 2
- Cross – Compiling

- **Module 12 : File Transfer**
  - FTP
  - Python HTTP Server
  - PHP HTTP Server
  - HFS Tool
  - Netcat
  - Curl
  - SMB Server
  - Powershell File Transfer
  - Bitsadmin
  - Wget
  - TFTP
  - PYTHON

- **Module 13 : Privilege Escalation**
  - SUID Binaries
  - Abusing Sudo's Right
  - Kernel Exploit
  - Path Variables
  - Multiple ways to edit /etc/passwd file
  - Windows Privilege Escalation
  - Weak File Permissions

- Always Install Elevated
- Bypass UAC
- Kernel Exploits

- **Module 14 : Web-Application Attacks**
  - Overview
  - Local file Inclusion
  - SQL Injection
  - Authentication Bypass
  - Error Based Enumeration
  - Blind SQL Injection

- **Module 15 : Password Cracking**
  - Overview
  - Crunch
  - Passing the Hash
  - Password Profiling
  - Online Attacks
  - Medusa
  - N-Crack
  - Hydra
  - Password Hashes
  - Cracking Hashes
  - LM / NTLM

- **Module 16 : Port Fun**
  - Overview
  - Port Forwarding
  - SSH Tunnels
  - Dynamic Proxies
  - Proxy Chains

- **Module 17 : Metasploit Framework**
  - Overview
  - AUX Modules
  - SNMP Modules
  - SMB Modules
  - WEBDAV Modules
  - Database services
  - Exploits
  - Payloads
  - Meterpreter
  - Meterpreter in Action
  - Additional Payloads
  - Binary Payloads
  - Multihandler
  - Porting Exploits
  - Post Expoitation

- **Module 18 : Antivirus Avoidance**

- Overview
- Shellter
- Veil –Evasion
- The FAT-RAT

- **Module 19 : Misconfigured Lab Setup**
  - Joomla Lab Setup & Pen-Testing
  - Drupal Lab Setup & Pen-Testing

- **Module 20 : CTF Challenges**
  - Vuln-Hub Machines
  - Hack the Box machines

- **Module 21 : Report Preparation**

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