RECON
CYBER SECURITY

DEFEND | DETECT | SECURE

OUR PARTNERS

cisco python EY Red Hat CompTIA Microsoft

OVERVIEW

In this course, student will learn Basic to Expert Penetration Testing techniques to find out vulnerabilities and how to exploit them, Like: Bug Hunting, VA/PT, Cloud Pen-Testing, Ctf Expert, etc.

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.

ONE YEAR INDUSTRIAL PROFESSIONAL CYBER SECURITY DIPLOMA

ADVANCED NETWORKING

LEVEL 1 : COURSE DURATION: 50 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

- **500 GB Toolkit**
- **Weekend / Weekdays classes**
- **Online and Offline classes**
- **6 Months Internships Latter**
- **2 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
- 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

CYBER FORENSICS

LEVEL 5 : COURSE DURATION: 40 hrs

- Module 01: Introduction to Digital Forensics
- Module 02: Inevitability During Computer Forensics
  - •Investigation, Maintaining Integrity, Chain of Custody,Write Blocker
- Module 03: Data Acquisition - Copying and Imaging with FTK Imager
- Module 04: OS Forensics
  - •RAM Dump, Ram Dump Analysis
- Module 05: Checking the Integrity of Files using the concept of Hash Value
- Module 06: Browser Forensics
- Module 07: Multimedia Forensics
- Module 08: Anti-Forensics Techniques
- Module 10: Investigation methodology and digital devices
- Module 11: Storage Media
  - •Logical structure, GUID and partition table, File system
- Module 12: Network Forensics
  - •Network protocols and investigating routers
- Module 13: Network Forensics Cont.
- Module 14: Malware
  - •Analyzing malware
- Module 15: Memory Forensics
  - •Memory forensics and analyzing volatile memory
- Module 16: Digital forensics tools
  - •Creating and analyzing disk images
  - •Recovering deleted data and craving files from unallocated space
- Module 17: Cryptanalysis
  - •Encryptions and decryption tools, Forensics data analysis tools
- Module 18: Process of Investigation
  - •Roles and responsibilities
  - •Identifying and containing security breaches
  - •Digital evidence collection and preservation
  - •Incident investigation and reporting
- Module 19: Lab Sessions
  - •Caine Installation
  - •USB packer sniffer
  - •Encryptions practical
  - •Event viewer-windows forensics
  - •Memory forensics
  - •Mail forensics basics
- Module 21: Windows forensics
- Module 22: Dark web forensics
- Module 23: Cloud forensics
- Module 24: Email forensics
- Module 25: Mobile forensics

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

PENETRATION TESTING

LEVEL 6 : 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-APP PENETRATION TESTING

LEVEL 7 : 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 8 : 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

APPLE IOS APP PEN-TESTING

LEVEL 9 : COURSE DURATION: 40 hrs

- Module 01: Introduction
- Module 02: Introduction to IOS Apps
- Module 03: Challenges with IOS lab setup
- Module 04: Lab setup with jailbreaken IOS device
- Module 05: Setting up XCODE
- Module 06: Installing Apps in IOS device
- Module 07: Decrypting IOS applications
- Module 08: Introduction to SecureStorev2
- Module 09: Dumpping class information
- Module 10: Jailbreak detection bypass
- Module 11: IOS Traffic analysis
- Module 12: Introduction to Frida / Frida CLI
- Module 13: Frida Scripts to trace HTTP calls
- Module 14: Introduction to end-to-end Encryption
- Module 15: Introduction to hopper
- Module 16: Jailbreak detection using hopper
- Module 17: SSL pinning attack
- Module 18: Pentesting Local Data storage
- Module 19: Pentesting Uninteded Data Leakage
- Module 20: Pentesting client side injection
- Module 21: Traffic Analysis
- Module 22: Run Time Analysis
- Module 23: Network Attacks
- Module 24: Reporting

BUG HUNTING

LEVEL 10 : COURSE DURATION: 70 hrs

- Module 01: Introduction
- Module 02: Information Gathering
- Module 03: BurpSuite Introduction
- Module 04: Cross Site Scripting (XSS)
- Module 05: Host Header Injection
- Module 06: URL Redirection
- Module 07: Parameter Tempering
- Module 08: HTML Injection
- Module 09: SQL Injection
- Module 10: File Inclution
- Module 11: Missing SRF Record
- Module 12: No rate Limiting
- Module 13: Source Code Discloser
- Module 14: Long Password Attack
- Module 15: IDOR
- Module 16: Server Site Request Forgery (SSRF)
- Module 17: Cross Site Request Forgery (CSRF)
- Module 18: Hostile Subdomain Takeover
- Module 19: S3 Bucket Takeover
- Module 20: Command Injection (RCE)
- Module 21: File Uploading
- Module 22: XML External Entity Injection
- Module 23: Buffer Overflow
- Module 24: Wordpress Vulnerability
- Module 25: Joomla Vulnerability
- Module 26: Drupal Vulnerability
- Module 27: CMS Vulnerability Hunting
- Module 28: HSTS (HTTP Strict transport security)
- Module 29: Session Fixation
- Module 30: Account Lookout
- Module 31: Password Reset Poisoning
- Module 32: Identity Management test Testing
- Module 33: Authentication Testing
- Module 34: Cryptographic Vulnerability
- Module 35: Session Management Testing
- Module 36: Exposed Source Code Control System
- Module 37: Apache Structs RCE Hunting
- Module 38: Web Cache Deceptions
- Module 39: Server Side Includes Injection
- Module 40: Ticket Tricks Bug Bounty
- Module 41: Multi-Factor Authentication
- Module 42: HTTPoxy Attact
- Module 43: Webmin Unauthentication RCE
- Module 44: HeartBleed
- Module 45: Appweb Authentication bypass

- Module 46: Ngnix
- Module 47: MySQL Authentication Bypass
- Module 48: DMS Zone Transfer
- Module 49: LOG Injection
- Module 50: Black (Jinja-2) SSTI to RCE
- Module 51: Handloop Vulnerability
- Module 52: CSRF Same Site Bypass
- Module 53: Joot Token Attack
- Module 54: Email Bounce Resource
- Module 55: IVR Call Request Crash
- Module 56: Weak Password Reset
- Module 57: Business Logic Vulnerability
- Module 58: RPC Ping Ball Attack
- Module 59: WAF / MOD Security Bypass
- Module 60: Broken Authentication
- Module 61: Open Redirection
- Module 62: Null Byte Injection
- Module 63: CORS Vulnerability

IOT SECURITY

LEVEL 11 : COURSE DURATION: 35 hrs

- Module 01: The IOT Security Testing Overview
- Module 02: Case Study: Connected
- Module 03: Vehicles Security
- Module 04: Case Study: Microgrids
- Module 05: Case Study: Smart City Drone System
- Module 06: IOT Hardware and Software
- Module 07: Communication and MP
- Module 08: IOT Interfaces and Services
- Module 09: Threats, Vulnerabilities, and Risks
- Module 10: Case Study: The Mirai Botnet O. 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 SA
- 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 Ass.

CLOUD AWS ASSOCIATE AND SECURITY

LEVEL 12 : COURSE DURATION: 50 hrs

- **Section 01 - Cloud Computing with AWS Getting Started**
  - •Introduction to Cloud and AWS Advantages
  - •Getting Started Learn Cloud Computing with AWS
- **Section 2 - AWS Getting Ready**
  - •Creating Your First IAM User
- **Section 3 - AWS Regions and Zones**
  - •Exploring Regions and Availability Zones in AWS
  - •Understanding the Need for Regions and Zones
- **Section 4 - AWS Getting Started with Ec2**
  - •Creating Virtual Machines with Amazon Ec2
  - •Setting up a Web Server in an Amazon EC2 Instance
  - •EC2 Virtual Servers in AWS
- **Section 5 -AWS Exploring Compute Services**
  - •Playing with Lambda Functions
  - •Playing with Amazon ECS
  - •Playing with AWS Elastic Beanstalk
  - •Exploring IaaS vs PaaS Cloud Computing with AWS
  - •Exploring Container Orchestration in AWS
  - •Setting up ECS Cluster with AWS Fargate
  - •Creating Your First Lambda Function
  - •Setting up Web Application with AWS Elastic Beanstalk
  - •Understanding the Need for Docker and Containers
  - •AWS Elastic Beanstalk
- **Section 7 - AWS Exploring Structured and Semi Structured Data**
  - •Creating Tables and Playing with Amazon RDS
  - •Creating a NoSQL Database in AWS with Amazon DynamoDB
  - •Amazon DynamoDB NoSQL Document and Key Value Da
  - •Amazon RDS OLTP Relational Database in AWS
  - •Exploring Semi Structured Data Key Value Graph and Column Family
  - •Creating a Relational Database in AWS with Amazon RDS
- **Section 8 - AWS Exploring Unstructured Data Course**
  - •Object Storage with Amazon S3
  - •Static Website with Amazon S3
  - •Block Storage in AWS Elastic Block Store
  - •Hybrid Storage in AWS Storage Gateway
  - •Object Storage in AWS S3 and S3 Glacier
  - •Getting Started with Unstructured Data
  - •File Storage in AWS EFS
  - •AWS Scenarios related to Data Stores
  - •Block Storage in AWS EBS and Instance Store
- **Section 9 - AWS Exploring Security**
  - •Playing with IAM Demo Encrypting S3 Objects with KMS
  - •Data Encryption in AWS KMS and CloudHSM
  - •IAM Authentication and Authorization in AWS
  - •IAM Best Practices Exploring Security Scenarios in AWS
- **Section 10 - AWS Exploring Private Networks**
  - •Creating Private Networks with VPC and Subnets
  - •VPCs and Subnets
  - •Connecting AWS with On premises DirectConnect and VPN
  - •NAT Devices Enable Outbound Internet Access for Private SU
  - •AWS Quick Review of Networking Services
- **Section 11 - AWS Digital Transformation and Managing Costs**
  - •Cloud Computing in AWS Managing Costs
  - •AWS Services for Managing Costs
  - •Understanding Digital Transformations and the role of Cloud

CERTIFICATION PATH AFTER TRAINING

1 YEAR PROFESSIONAL CYBER SECURITY DIPLOMA

EC-Council

CEH (Certified Ethical Hacker) Theory
CHFI (Ec-Council forensic Investigator)
CEH (Certified Ethical Hacker) Practical
ECSA (EC-Council Security Analyst)
C-PENT (Certified Pentester)
LPT (Licence Pentester)

CompTIA

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

AWS Cloud Certification

AWS cloud associate solution
AWS cloud security certification

RECON CYBER SECURITY
+91-8595756252
www.reconforce.in

Every Class Recordings

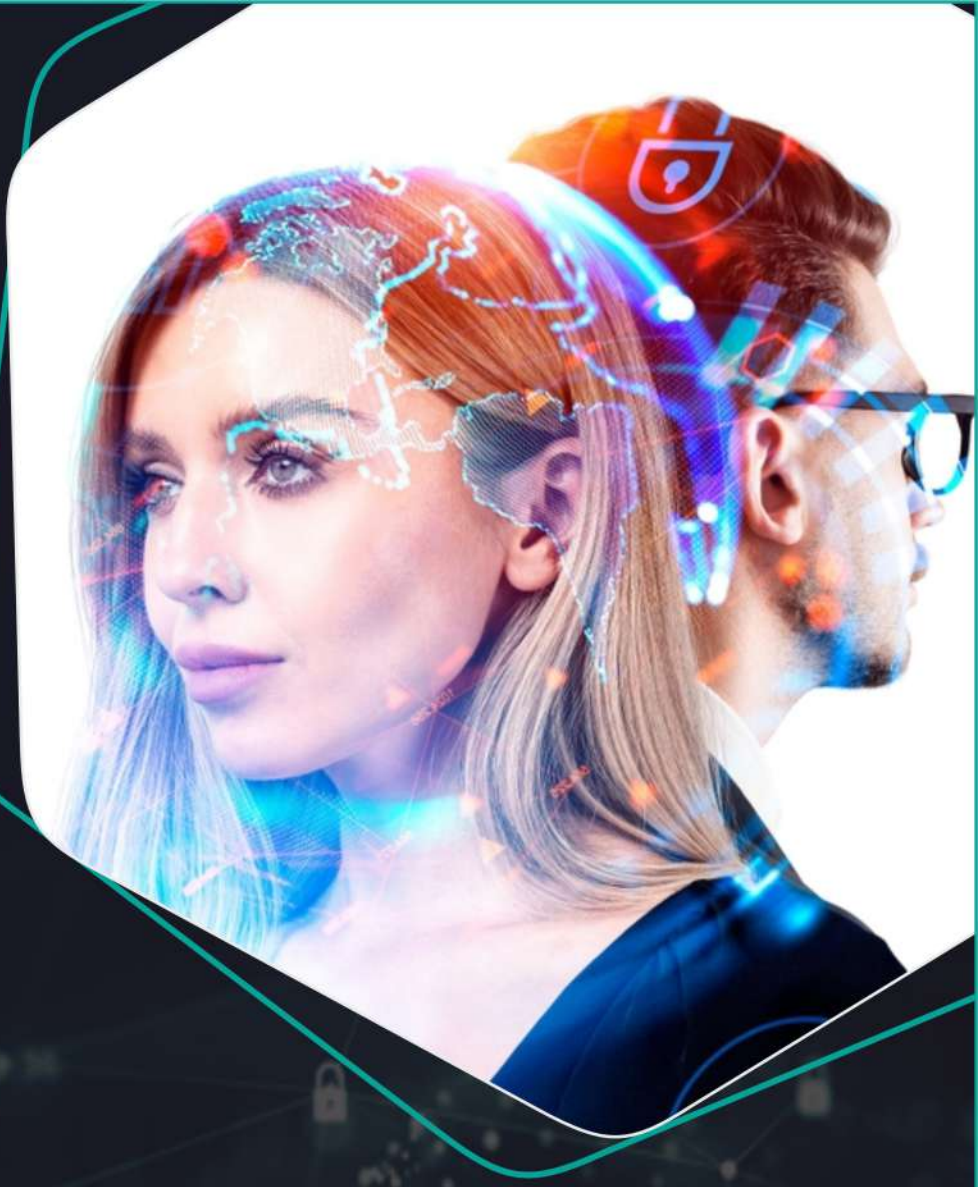
Easy Repetations

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