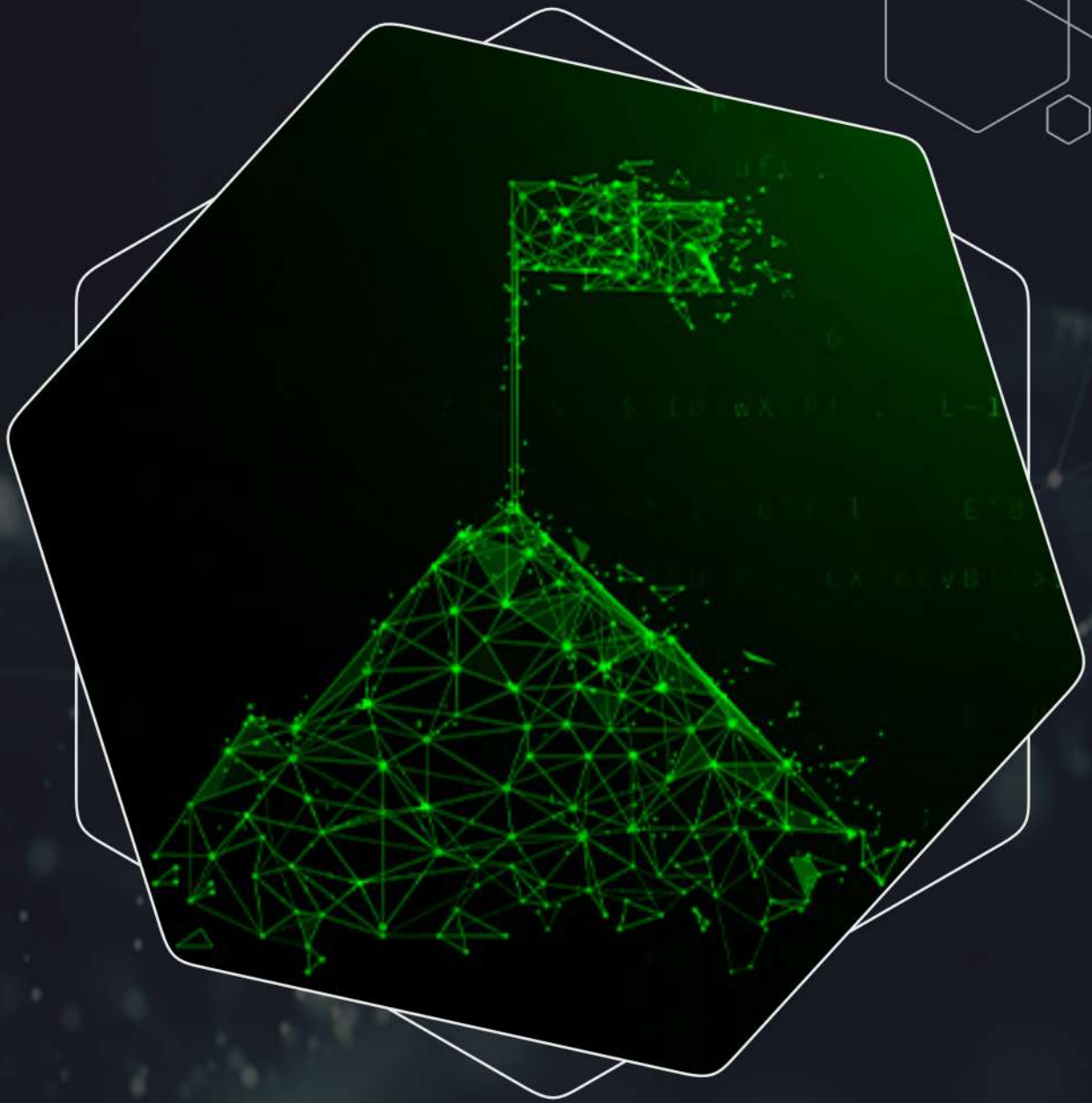
RECON
CYBER SECURITY

DEFEND | DETECT | SECURE



OUR PARTNERS

cisco python EY Red Hat CompTIA Microsoft

OVERVIEW

In this course, students will learn the about Basic to Expert CTF Challenge techniques. Topics include Reconnaissance, Scanning, Exploitation, Post Exploitation and more.

PRE-REQUISITES

Students should already be familiar with how to operate the Linux Operating system and VA/PT Techniques.

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.

CTF CHALLENGE COURSE CONTENT

COURSE DURATION: 80 hrs

- Module 01: Introduction
- Module 02: Finding Files
- Module 03: Services in Kali SSH Service
- Module 04: FTP Services
- Module 05: HTTP Service
- Module 06: Mysql Services
- Module 07: Service Management
- Module 08: Basic Linux and Commands
- Module 09: Netcat Tutorials
- Module 10: Getting started with NC
- Module 11: Connecting to a Server
- Module 12: Fetching HTTP header
- Module 13: Chatting
- Module 14: Creating a Backdoor
- Module 15: Verbose Mode
- Module 16: Save Output to Disk
- Module 17: Port Scanning
- Module 18: Reverse TCP Shell Exploitation
- Module 19: Randomize Port
- Module 20: File Transfer
- Module 21: Reverse Netcat Shell Exploitation
- Module 22: Banner grabbing
- Module 23: Nmap Firewall Scan
- Module 24: Enumeration
- Module 25: Passive Info Gathering
- Module 26: Reverse Shell
- Module 27: Intro to Overflows
- Module 28: Windows BO Example
- Module 29: Linux BO Example
- Module 30: Using Public Exploits
- Module 31: File Transfers
- Module 32: Linux Privilege Escalation
- Module 33: Windows privilege escalation
- Module 34: Active directory exploitation
- Module 35: Web Application Attacks
- Module 36: Password Cracking
- Module 37: Port Fun
- Module 38: Metasploit Framework
- Module 39: Antivirus Avoidance
- Module 40: Overview
- Module 40: Shellter
- Module 42: Veil – Evasion
- Module 43: Thefatratework
- Module 44: Exploits
- Module 45: Payloads
- Module 46: Meterpreter
- Module 47: Additional Payloads
- Module 48: Binary Payloads
- Module 49: Porting Exploits
- Module 50: Post Exploitation

- **50 gb toolkit**
- **Weekend / weekdays classes**
- **Online and offline classes**
- **1 year membership**
- **Certificate after completion**
- **Interview preparation**
- **Live hacking training**
- **Class session recordings**
- **Ebooks tutorials**
- **24x7 support**

Every Class Recordings

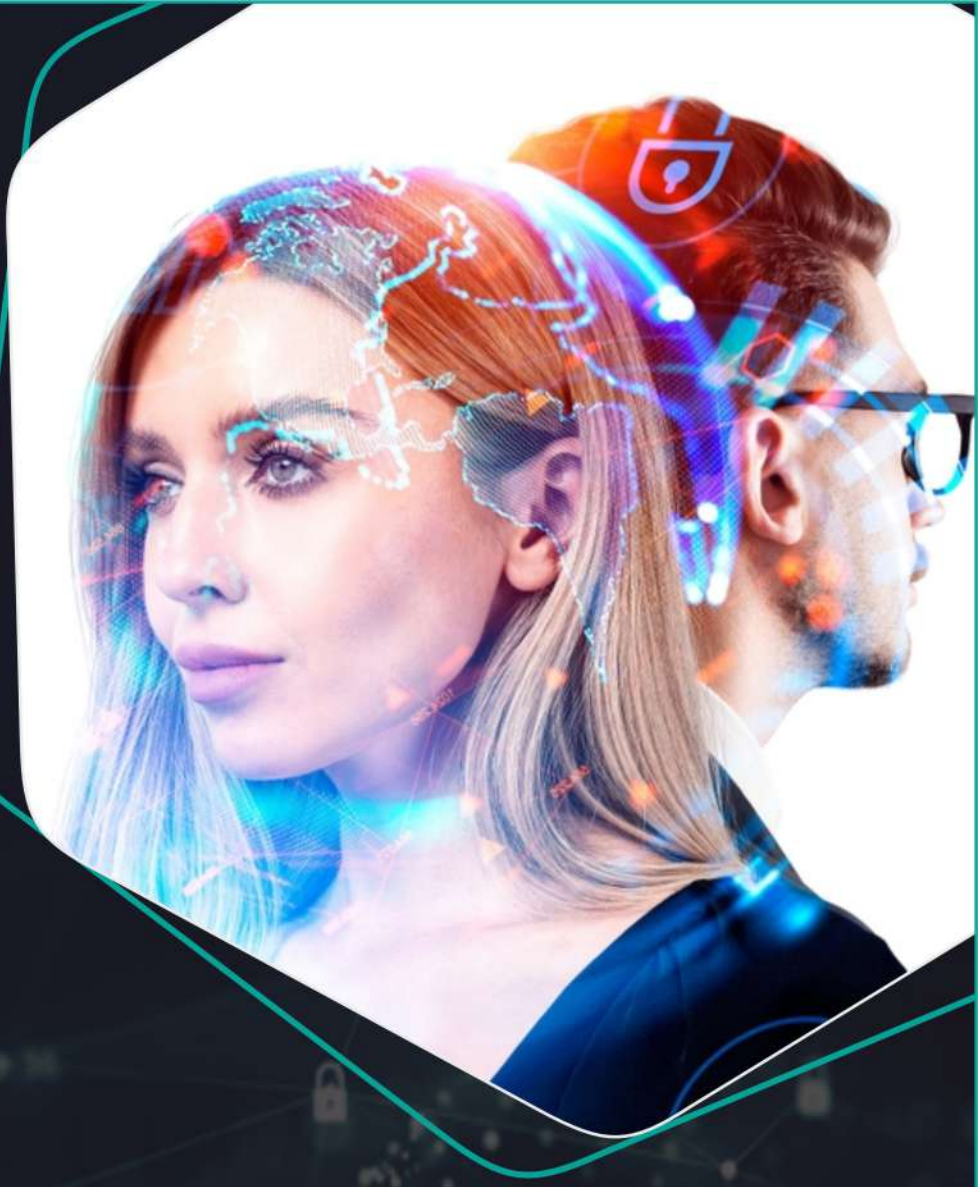
Easy Repetations

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