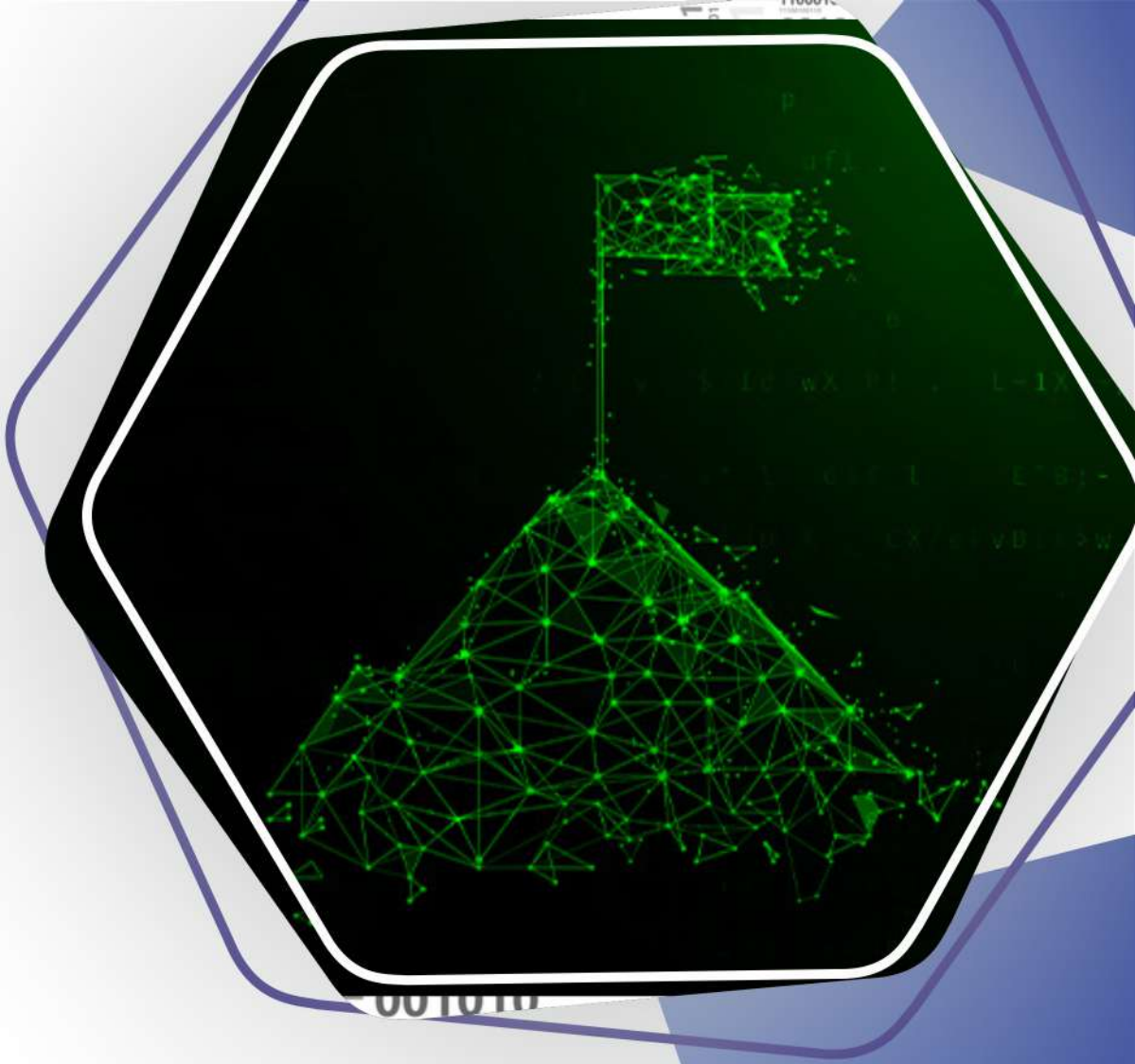
RECON CYBER SECURITY

CTF CHALLENGE

DURATION 2.5 MONTHS



OVERVIEW

In this course, students will learn about Advance Capture the Flag (CTF) Challenges. Like: Vuln-hub Machines, Hack the Box, etc.

Pre-Requisites

Students should already know about Penetration Testing and Web-Application Penetration Testing. Also hands-on practice on Kali Linux. [Note: Student should already knowledge of any Programming Languages]

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

CTF Challenge Course Module

01. Introduction
- Finding Files
- Services in Kali SSH Service
- FTP Services
- HTTP Service
- Mysql Services
- Service Management

02. Basic Linux and Commands

03. Netcat Tutorials
- Getting started with NC
- Connecting to a Server
- Fetching HTTP header
- Chatting
- Creating a Backdoor
- Verbose Mode
- Save Output to Disk

04. Port Scanning
- Reverse TCP Shell Exploitation
- Randomize Port
- File Transfer
- Reverse Netcat Shell Exploitation
- Banner grabbing
- Nmap Firewall Scan

05. Enumeration

06. Passive Info Gathering

07. Reverse Shell

08. Intro to Overflows

09. Windows BO Example

10. Linux BO Example

11. Using Public Exploits

12. File Transfers

13. Linux Privilege Escalation

14. Web Application Attacks

15. Password Cracking

16. Port Fun

17. Metasploit Framework
- Exploits
- Payloads
- Meterpreter
- Additional Payloads
- Binary Payloads
- Porting Exploits
- Post Exploitation

18. Antivirus Avoidance
- Overview
- Shellter
- Veil – Evasion
- Thefatrat

Tools and Benefits of the Diploma course

- 50 Gb Toolkit
- Online and Offline classes
- Certificate after completion
- 1 Year Membership
- Training by experienced trainers
- Checkpoint based 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

www.reconforce.in | www.reconcybersecurity.com