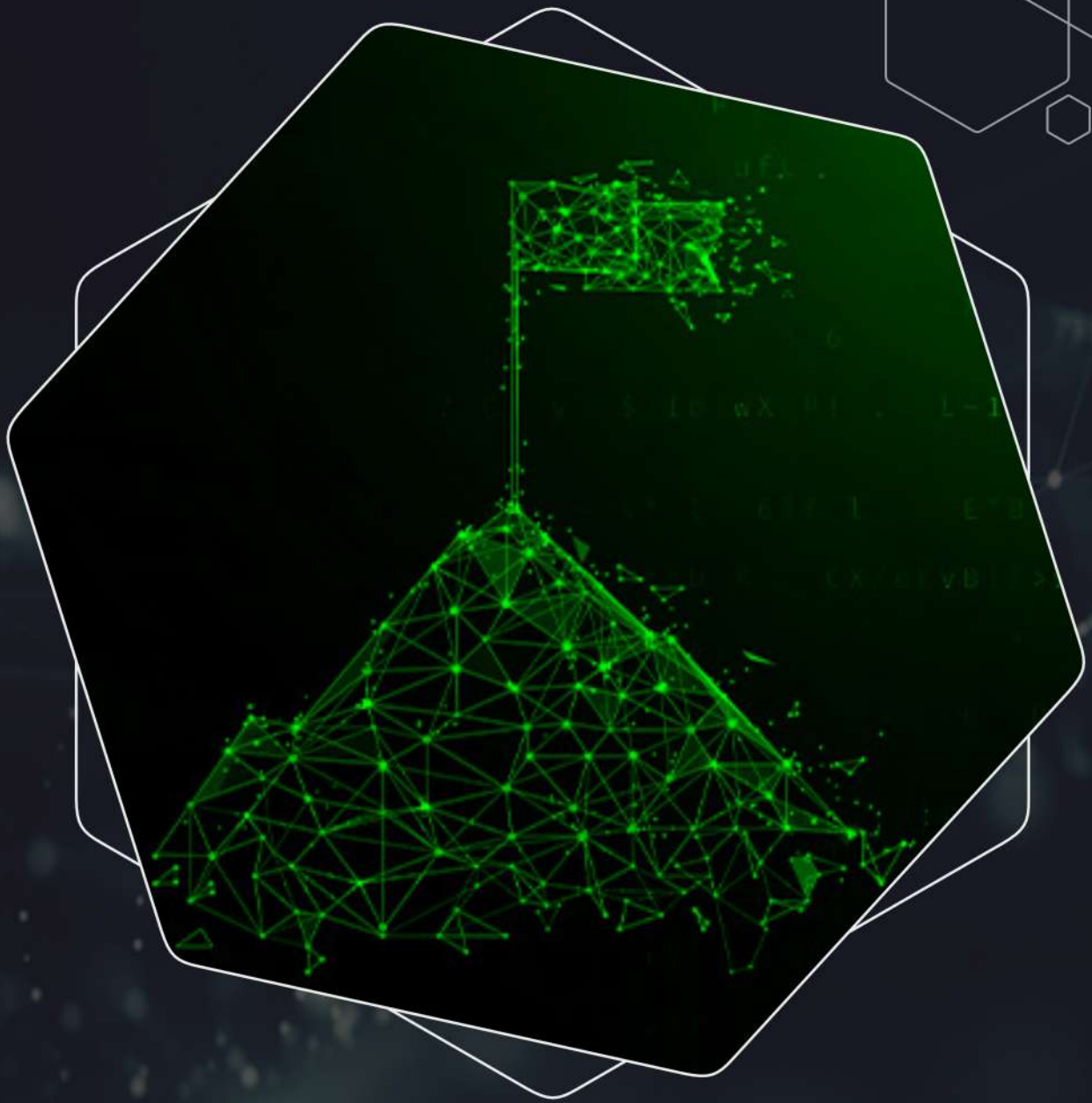
RECON
CYBER SECURITY

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

- Lesson 01 : Introduction
  - Finding Files
  - FTP Services
  - HTTP Service
  - Mysql Services
  - Service Management
- Lesson 02 : Basic Linux and Commands
  - Locate
  - Which
  - Find
  - Sed
  - Awk
  - Cut
  - Sort
  - Grep
  - Head
  - Tail
  - Wget
  - Cat
- Lesson 03 : Netcat Tutorials
  - Overview
  - Google Search
  - Google Hacking
  - GHDB
  - Directory Bruteforce Attack
  - Dirb
  - Dirbuster
  - Dirsearch
  - Metasploit
- Lesson 04 : Port Scanning
  - TCP Delay Scan
  - UDP Scan
  - Reverse TCP Exploitation
  - Randomize Port
  - File Transfer
  - Reverse Netcat Shell Exploitation
  - 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
- Lesson 05 : 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
  - SNMP Enumeration
  - SNMP MiB
  - SNMPWal
- Lesson 06 : Passive Info Gathering
  - Overview
  - Google Search
  - Google Hacking
  - GHDB
  - Directory Bruteforce Attack
  - Dirb
  - Dirbuster
  - Dirsearch
  - Metasploit
- Lesson 07 : Reverse Shell
  - Php reverse shell
  - Python reverse shell
  - Perl reverse shell
  - Bash reverse shell
  - Msfvenom shell
- Lesson 08 : Intro to Overflows
  - Overview
  - Vulnerable Code
  - Stack Overflow
- Lesson 09 : Windows BO Example
  - Overview
  - Fuzzing
  - Crash Replication
  - Controlling EIP
  - Introducing Shellcode
  - Bad Characters
  - Redirecting Execution
  - Introducing Mona
  - Shellcode Payload
- Lesson 10 : Linux BO Example
  - Controlling EIP
  - Locating Space
  - First Stage Shellcode
  - Locating RET
  - Generating Shellcod
- Lesson 11 : Using Public Exploits
  - Overview
  - Finding Exploits
  - Exploit – DB
  - Fixing Exploits 1
  - Fixing Exploits 2
  - Cross – Compiling

- Lesson 13 : Linux Privilege Escalation
  - Suid Binaries
  - Absuing Sudo ‘ s Right
  - Kernel Exploit
  - Path Variables
  - Multiple Ways to edit / etc /
  - passwd fill
  - Windows Privilege Escalation
  - Weak File Permissions
  - Always Install Elevated
  - Bypass UAC
  - Kernel Exploits
  - Lesson 14 : Web Application Attacks
  - Authentication Bypass
  - Error Based Enum
  - Blind SQL Injection
  - Attack Proxies
  - SQLMap
- Lesson 15 : Password Cracking
  - Overview
  - Crunch
  - Passing the Hash
  - Password Profiling
  - Online Attacks
  - Medusa
  - Ncrack
  - Hydra
  - Password Hashes
  - Cracking Hashes
  - LM / NTLM
- Lesson 16 : Port Fun
  - Overview
  - Port Forwarding
  - SSH Tunnels
  - Dynamic Proxies
  - Proxy Chains
- Lesson 17 : Metasploit Framework
  - Overview
  - AUX Lessons
  - SNMP Lessons
  - SMB Lessons
  - WEBDAV Lessons
  - Database Services
  - Exploits
  - Payloads
  - Meterpreter
  - Meterpreter in Action
  - Additional Payloads
  - Binary Payloads
  - Multihandler
  - Post Exploitation
- Lesson 18 : Antivirus Avoidance
  - Overview
  - Shellter
  - Veil – Evasion
  - thefatrat

“

- **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

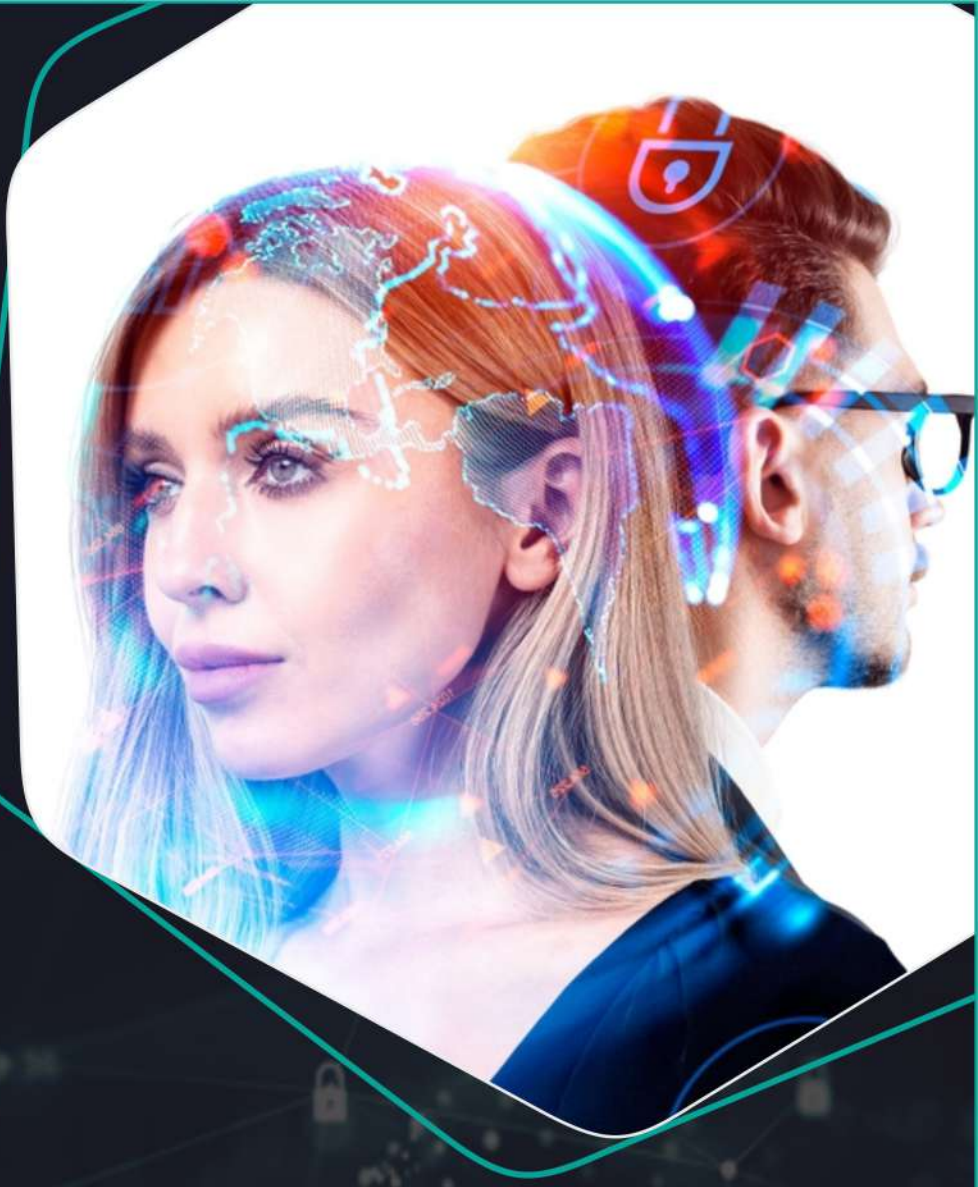
Easy Repetations

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