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.

Details for CTF Expert Duration: 2 to 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 **Python Programming Language]**

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.

- CTF Expert toolkit
- 24x7 Online Classes Available
- CET Expert Certificate
- Interview Preparation
- 1 Year Membership
- Training by experienced trainers
- Live Hunting
- Checkpoint based training
- Class recording
- 24x7 Support

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