RECON CYBER SECURITY

MASTER DIPLOMA IN CYBER SECURITY

DURATION 1 YEAR

WWW.RECONFORCE.IN

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 API 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 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

Level 1 Advanced Networking

01. Introduction To Networking
02. Fundamentals of Networking
03. OSI Model v/s TCP/IP
04. TCP v/s UDP
05. Mac Address
06. IP Addressing
    - IPv 4
    - IPv 6
07. Subnetting
08. Network Cabling
09. Router Fundamentals
10. Lab Configuration on Packet tracer
11. Router, Switch And PC Communication
12. Routing Protocols
    - Default Routing
    - Static Routing
    - Static routing With Subnetting
    - Dynamic Routing
        - RIP
        - EIGRP
        - OSPF
13. DHCP
14. NAT - Network Address Translation
15. VLAN - Virtual Local Aria Network
16. ACL - Access Control Line
17. BGP

Level 2 Linux Essentials

01. Linux Evolution And Popular Operating System
    - Introduction
    - Linux Distribution
    - Linux Embedded System
    - Hardware Requirement
    - Installing Linux
    - OS Differences
02. Open Software Application
    - What is Open Source
    - Desktop and server application
    - Languages and tools
    - Packages installs and repositories
03. The Linux Environments
    - Linux Desktop Environments
    - Linux Shell and Commands
    - Managing Softwares Packages
04. The Command Line
    - Difference b/w shells
    - Command Line
    - Command Usage
    - Man Pages
05. Directories And Files
06. Searching and Extracting Data From File
07. Package Installation in Different Directory
08. User Account and Groups
    - Creating Account From The Shell
    - Modifying And Deleting Account
    - Working as Root
09. Managing File Ownership And Permission

Level 3 Ethical Hacking

01. Introduction to Ethical Hacking
02. Reconnaissance
    - Active Foot-Printing
    - Passive Foot-Printing
    - Finger Printing Active/Passive
03. Scanning Networks
    - Host Discovery
    - TCP/UDP Port Scanning
    - Vulnerability Scanning
04. Enumeration
05. System Hacking
    - Physical Access (Windows / Linux OS)
06. Malware & Threats
    - Virus / Worms
    - Trojan Horse
    - Ransomware
    - Polymorphic Virus
    - Macro Virus
    - Micro Virus
    - Rootkit, etc.
07. Social Engineering
    - Phishing Attacks
    - Vishing Attacks, etc.
08. Denial of Service
    - DOS (Deial of Service)
    - DDOS (Distributed Denial of Service)
09. Session Hijacking
10. Wireless Hacking
    - WEP / WPA / WPA2 Wi-Fi Hacking
11. Mobile Hacking
12. Hacking Web-Application (with BurpSuite)
13. SQL Injection
    - Automatic tool based
    - Manual SQL Injection
14. Hacking Web Server
15. Sniffing / Sniffers
    - MITM Attack
    - DNS Attack
    - DHCP Attack
    - MAC Address Attack, etc.
16. IDS, Firewall, Honeypot
17. Cryptography
18. Basics of Cloud Computing / Hacking
19. IoT Hacking
20. Basics of Penetration Testing

Level 4 Python Programming

01. Introduction To Python
02. Environment Setup
03. Basic Syntax
04. Comments
05. Variables
06. Data Types
07. Operators
08. Division Making
09. Loops
10. Numbers
11. Strings
12. Lists
13. Tuples
14. Dictionary
15. Date & type
16. Function
17. Modules
18. Files I/O
19. Exceptions

Level 5 Network Pen-Testing

01. How to plan your Penetration Testing
02. Scoping your Penetration Testing
03. Network & Web-Application
04. Scanning Vulnerability
    - Port Scanning
    - Script scanning
    - Enumeration
    - Service & Version Scanning
    - Web-Application Scanning
05. Exploitation with Metasploit
    - Exploit Vulnerability
    - Bind & Reverse Shell
    - Payload Creation, etc.
06. Post-Exploitation
07. Pivoting Attack
08. Browser exploitation
    - BEEF Exploit
09. In-Depth Password Attacks
    - John the Ripper
    - Brute Force Attack
    - Dictionary Attack
    - Rainbow Table Attack
    - Other Password Cracking Tools
10. Cracking / Solving CTFs
11. Final Analysis
12. Final Report Generation
    - Manual Reporting
    - Automatic Reporting

Level 6 Web-App Pen-Testing

01. Introduction to Web-App Pen-Testing
02. Finding Subdomains
03. Understanding HTTP
04. Access Control Flaws
05. Ajax Security
06. Authentication Flaws
07. Buffer overflows
08. Code Quality
09. Concurrency Flaws
10. Cross-Site Scripting
11. Improper Error Handling
12. Injection Flaws
13. Denial of Service
14. Insecure Communication
15. Insecure Configuration
16. Insecure Storage
17. Malicious File Execution
18. Parameter Tampering
19. Session Management Flaws
20. Challenge Online Platform

Level 7 Mobile-App Pen-Testing

01. Introduction to Mobile-App Testing
02. Lab setup
03. Android Architecture
04. APK File Structure
05. Reversing with APKtool/ Jadx-GUI
06. Reversing with MobSP
07. Static Analysis
08. Scanning Vulnerabilities with Drozer
09. Improper Platform Usage
10. Log Analysis
11. Insecure Storage
12. Insecure Communication
13. Hard Coding Issues
14. Insecure Authentication
15. Insufficient Cryptography
16. Code Tempering
17. Extraneous functionality
18. SSL pinning
19. Intercepting The Network Traffic
20. Dynamic Analysis
21. Report Preparation

Level 8 Apple IOS Application Pen-Testing

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

Level 9 Bug Hunting

01. Introduction
02. Information Gathering
03. BurpSuite Introduction
04. Cross Site Scripting (XSS)
05. Host Header Injection
06. URL Redirection
07. Parameter Tempering
08. HTML Injection
09. SQL Injection
10. File Inclusion
11. Missing SPF Record
12. No rate Limiting
13. Source Code Discloser
14. Long Password Dos Attack
15. IDOR
16. Server Site Request Forgery (SSRF)
17. Cross Site Request Forgery (CSRF)
18. Hostile Subdomain Takeover
19. S3 Bucket Takeover
20. Command Injection (RCE)
21. File Uploading
22. XML External Entity Injection
23. Buffer Overflow
24. Wordpress Vulnerability
25. Joomla Vulnerability
26. Drupal Vulnerability
27. CMS Vulnerability Hunting
28. HSTS (HTTP Strict transport security)
29. Session Fixation
30. Account Lookout
31. Password Reset Poisoning
32. Identity Management test Testing
33. Authentication Testing
34. Cryptographic Vulnerability
35. Session Management Testing
36. Exposed Source Code Control System
37. Apache Structs RCE Hunting
38. Web Cache Deceptions
39. Server Side Includes Injection
40. Ticket Tricks Bug Bounty
41. Multi-Factor Authentication
42. HTTPoxy Attact
43. Webmin Unauthentication RCE
44. HeartBleed
45. Appweb Authentication bypass
46. Ngnix
47. MySQL Authentication Bypass
48. DMS Zone Transfer
49. Log Injection
50. Black (Jinja-2) SSTI to RCE
51. Handloop Vulnerability
52. CSRF Same Site Bypass
53. Jwt Token Attack
54. Email Bounce Resource
55. IVR Call Request Crash
56. Weak Password Reset
57. Business Logic Vulnerability
58. RPC Ping Back Attack
59. WAF / MOD Security Bypass
60. Broken Authentication
61. Open Redirection
62. Null Byte Injection
63. CORS Vulnerability

Level 10 API-Testing

01. introduction to API
02. Postman Lab setup
03. Preparation for API Pen-Testing
04. Lab Setup
05. OWASP API TOP 10
06. SQL injection
07. Command Injection
08. Offensive XXE Exploitation
09. Server Side Request Forgery
10. Cross site scripting
11. Transport layer security issues
12. Mass Assignment attack
13. Broken Object Level Authorization Issues
14. File Path Traversal
15. User Enumeration
16. Information Disclosure
17. JSON web token
18. Unauthorized password change
19. Excessive data exposure
20. Lack of Resource & Rate Limiting
21. Regular Expression DOS attack
22. BFLA Issues
23. Billion laugh attack
24. Hidden API Functionality Exposure
25. RCE Via Deserilization in API

Level 11 Malware Analysis

01. Introduction to Malware Analysis
02. Basic Of Analysis
03. Advanced Static Analysis
04. Analysing Windows Programs
05. Advanced Dynamic Analysis
06. Malware Behaviour
07. Data Encoding and Malware Countermeasures
08. Covert Malware Launching
09. Antianalysis
10. Packing and Unpacking
11. Rootkit Techniques

Level 12 CTF Challenge

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

- 500 GB Toolkit
- Online and Offline classes
- Diploma Certificate After Completion
- 6 Months Internships Latter
- 2 Years Membership
- Interview Preparation
- Live Hacking 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