



NetTech India

Get Certified



**Post Graduate
Certification
Cybersecurity
Specialization in
PENTESTING**

OUR BRANCHES

Thane

9870803004
9870803005

Andheri

7304639164
7304639165

Nerul

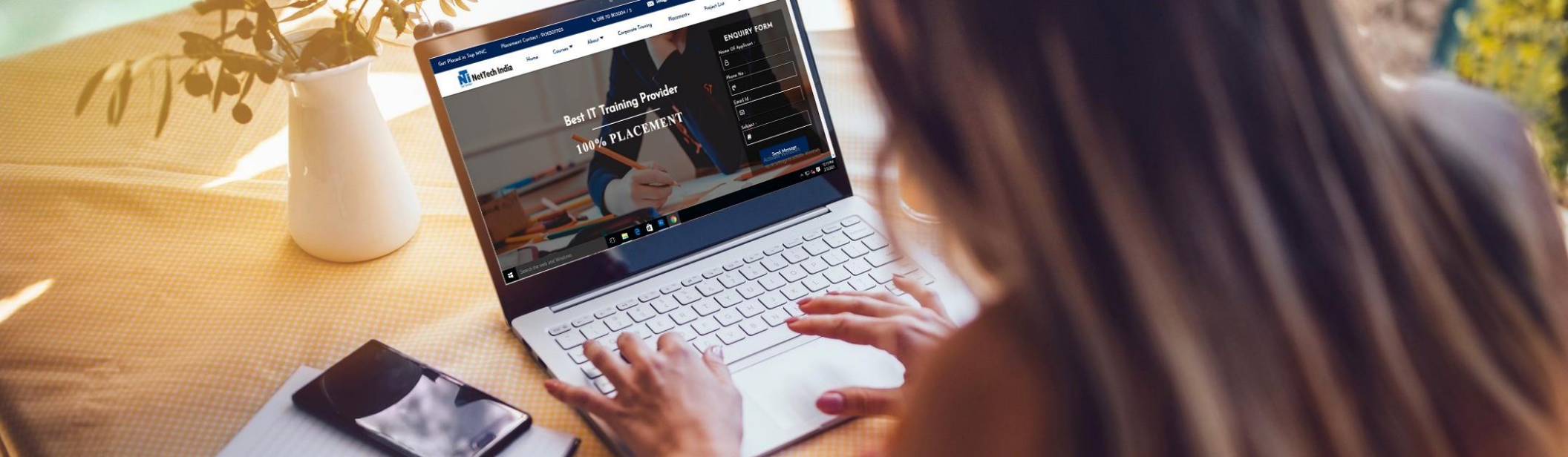
9372435654
9372438197

Dadar

9324826104
9321487176

Pune

8591861770



ABOUT US

NetTech India Training Institute offers a high-quality learning experience in the field of IT training to train students on brand new technologies and train them to deliver the desired results with commercially relevant and re-organized technical skills.

The probability of achieving your dream job will keep on increasing day by day once you complete a course in **NetTech India**. We also focus on improving soft skills in terms of communication, leadership, teamwork, external appearance, and attitude which helps everyone to be professional in all the aspects of their career.



25%
Theory



75%
Practicals

Cybersecurity Specialization in Pentesting

- **CCNA**
- **CEH V12**
- **VAPT / LPT**
- **CLOUD SECURITY TESTING**
- **EXPLOIT WRITING**
- **API/ENDPOINT TESTING**

BENEFITS

- Career Growth - Higher Pay & Position
- Encourages professional Development
- Enriches self-image and Reputation
- Enhances professional Credibility.
- Abundant Job Opportunities
- Used In Many Industries
- Global Recognition
- Secure and Flexible
- 50+ Case Studies
- 50+ Projects



CCNA CONTENT

1 Network Fundamentals

1. Explain the role and function of network components
 - a. Routers
 - b. L2 and L3 switches
 - c. Next-generation firewalls and IPS
 - d. Access points
 - e. Controllers (Cisco DNA Center and WLC)
 - f. Endpoints
 - g. Servers
2. Describe characteristics of network topology architectures
 - a. 2 tier
 - b. 3 tier
 - c. Spine-leaf
 - d. WAN
 - e. Small office/home office (SOHO)
 - f. On-premises and cloud

3. Compare physical interface and cabling types
 - a. Single-mode fiber, multimode fiber, copper
 - b. Connections (Ethernet shared media and point-to-point)
 - c. Concepts of PoE
4. Identify interface and cable issues (collisions, errors, mismatch duplex, and/or speed)
5. Compare TCP to UDP
6. Configure and verify IPv4 addressing and subnetting
7. Describe the need for private IPv4 addressing
8. Configure and verify IPv6 addressing and prefix
9. Compare IPv6 address types
 - a. Global unicast
 - b. Unique local
 - c. Link-local
 - d. Anycast
 - e. Multicast
 - f. Modified EUI 64
10. Verify IP parameters for Client OS (Windows, Mac OS, Linux)

11. Describe wireless principles
 - a. Nonoverlapping Wi-Fi channels
 - b. SSID
 - c. RF
 - d. Encryption
12. Explain virtualization fundamentals (virtual machines)
- 1.12 Explain virtualization fundamentals (virtual machines)

2 Network Access

1. Configure and verify VLANs (normal range) spanning multiple switches
 - a. Access ports (data and voice)
 - b. Default VLAN
 - c. Connectivity
2. Configure and verify interswitch connectivity
 - a. Trunk ports
 - 2.2.b 802.1Q
 - 2.2.c Native VLAN
- 2.3 Configure and verify Layer 2 discovery protocols
(Cisco Discovery Protocol and LLDP)

4. Configure and verify (Layer 2/Layer 3) EtherChannel (LACP)
5. Describe the need for and basic operations of Rapid PVST+ Spanning Tree Protocol and identify
basic operations
 - a. Root port, root bridge (primary/secondary), and other port names
 - b. Port states (forwarding/blocking)
 - c. PortFast benefits
6. Compare Cisco Wireless Architectures and AP modes
7. Describe physical infrastructure connections of WLAN components (AP,WLC, access/trunk ports, and LAG)
8. Describe AP and WLC management access connections (Telnet, SSH, HTTP,HTTPS, console, and TACACS+/RADIUS)
9. Configure the components of a wireless LAN access for client connectivity using GUI only such as WLAN creation, security settings, QoS profiles, and advanced WLAN settings

3 IP Connectivity

1. Interpret the components of the routing table
 - a. Routing protocol code
 - b. Prefix
 - c. Network mask
 - d. Next hop
 - e. Administrative distance
 - f. Metric
 - g. Gateway of last resort
2. Determine how a router makes a forwarding decision by default
 - a. Longest match
 - b. Administrative distance
 - c. Routing protocol metric
3. Configure and verify IPv4 and IPv6 static routing
 - a. Default route
 - b. Network route
 - c. Host route
 - d. Floating static

4. Configure and verify single area OSPFv2
 - a. Neighbor adjacencies
 - b. Point-to-point
 - c. Broadcast (DR/BDR selection)
 - d. Router ID
5. Describe the purpose of first hop redundancy protocol

3 IP Services

1. Configure and verify inside source NAT using static and pools
2. Configure and verify NTP operating in a client and server mode
3. Explain the role of DHCP and DNS within the network
4. Explain the function of SNMP in network operations
5. Describe the use of syslog features including facilities and levels
6. Configure and verify DHCP client and relay
7. Explain the forwarding per-hop behavior (PHB) for QoS such as classification, marking, queuing, congestion, policing, shaping
8. Configure network devices for remote access using SSH
9. Describe the capabilities and function of TFTP/FTP in the network

5 Security Fundamentals

1. Define key security concepts (threats, vulnerabilities, exploits, and mitigation techniques)
2. Describe security program elements (user awareness, training, and physical access control)
3. Configure device access control using local passwords
4. Describe security password policies elements, such as management, complexity, and password alternatives (multifactor authentication, certificates, and biometrics)
5. Describe remote access and site-to-site VPNs
6. Configure and verify access control lists
7. Configure Layer 2 security features (DHCP snooping, dynamic ARP inspection, and port security)
8. Differentiate authentication, authorization, and accounting concepts
9. Describe wireless security protocols (WPA, WPA2, and WPA3)
10. Configure WLAN using WPA2 PSK using the GUI

6 Automation and Programmability

1. Explain how automation impacts network management
2. Compare traditional networks with controller-based networking
3. Describe controller-based and software defined architectures (overlay, underlay, and fabric)
 - a. Separation of control plane and data plane
 - b. North-bound and south-bound APIs
4. Compare traditional campus device management with Cisco DNA Center enabled device management
5. Describe characteristics of REST-based APIs (CRUD, HTTP verbs, and data encoding)
6. Recognize the capabilities of configuration management mechanisms Puppet, Chef, and Ansible
7. Interpret JSON encoded data

And Many More...

CEHv12 **CONTENT**

- Introduction
- Basic Networking
- Lab Setup
- Kali Linux
- Footprinting & Reconnaissance
- Scanning Networks
- Enumeration
- System Hacking
- Vulnerability Analysis
- Malware threats
- Sniffing
- Social Engineering
- Denial-of-service
- Session Hijacking
- Hacking Web servers
- Hacking web Application
- SQL Injection
- Hacking Wireless Networks

- Hacking Mobile Platforms
- Identity Theft
- Cryptography
- Cloud Computing
- Evading IDS,IPS, firewalls & honey pot
- Os Hardening & Auditing
- Metasploit
- IoT for hacking & OT platforms
- Password Cracking
- Creating Backdoors
- Report Writing

PENTESTING **CONTENT**

Introduction

- VA
- PT
- Scope
- NDA
- Boundaries
- Web Architecture
- Web apps
- Services
- Response codes

Scanning & Enumeration

- Nmap
- nslookup
- dig
- host
- gobuster
- wfuzz
- dirb
- dirsearch

Exploitation Concepts

- zero day
- whitelisting
- blacklisting
- input sanitization
- honey pot
- Firewall evasion
- filter bypass
- Vulnerability Chaining

Burpsuite

- Intro
- Configuration
- Interception
- Target
- scope
- intruder
- repeater
- decoder
- extender
- spider
- data filtration

WebApp Common Vulns

- XXS
- CSRF
- LFI
- RFI
- CRLF Injection
- HPP
- IDOR
- Session Manipulation
- Clickjacking
- CORS
- Directory Traversal
- Cookie Manipulation
- URL Manipulation
- XXE
- internal DOS
- Reverse Shell uploading
- SDT
- Insecure Redirects and Unvalidated Forwards

Network VAPT

- Wireless Testing
- Eternal Romance
- Sensitive data exposure
- Misconfigured Services
- SSH tunneling
- Network Traffic Analysis
- Service Brute Forcing
- Pass the hash

Owasp Top 10

- Broken Access Control
- Cryptographic failure
- Injection Failure
- Insecure Design
- Security Misconfiguration
- Vulnerable & outdated Components
- Identification & Authentication Failure
- Software & data Integrity failure
- Security logging & monitoring failure
- server-side request forgery

Privilege Escalation

- Writable Binaries
- ExploitDB
- Misconfigured Cron
- kernel abuse
- shell sock
- TTY Shell
- mimikatz
- Docker exploitation
- SUID exploitation
- LeanPease
- WinPease

Automated Scanning

- Acunetix
- Nikto
- ZAP
- IronWasp

CTF's

- Newbies
- Script Kiddies
- Hacker
- Pro Hacker
- Elite Hacker
- Guru
- Omniscient

Bug Hunting

- Hunting Mindset
- Acquisitions
- Hackerone
- Bugcrowd

CLOUD SECURITY TESTING

1 Cloud Computing Introduction

- a. Characteristics of cloud computing
- b. Types of Cloud Computing Services
- c. Cloud Deployment models
- d. Cloud Computing benefits

2 Cloud Computing Threats

- a. Isolation issues
- b. VM level attacks
- c. Abusing cloud services
- d. Data loss/breach
- e. Insecure interfaces
- f. Insecure APIs
- g. Malicious insider

3 Cloud Computing Attacks

- a. Side channel attacks
- b. Service Hijacking
- c. DNS attacks
- d. Sql injection attacks
- e. Wrapping attacks
- f. Network sniffing
- g. Session ridding
- h. DOS / DDOS attacks

4 Securing Cloud computing

- a. Cloud security control layers
- b. Responsibilites in Cloud Security
- c. OWASP top 10 Cloud Security

5 Cloud Security Tools

- a. Core CloudInspect
- b. CloudPassage Halo

And Many More...

EXPLOIT WRITING

- Introduction
- Intro to programming
- Assembly
- Dot Net
- OOPS
- Python
- Batch Scripting
- Shell Scripting
- Debugging
- Memory allocation
- Memory management
- Cache memory
- flash memory
- Buffers
- Job Ques
- Buffer overflow
- stack based buffer overflow
- Heap based buffer overflow
- shellcoding
- Alphanumeric shellconding

- DLL
- Binary payload
- DLL Hijacking
- DER
- ASLR
- win32egg hunting
- metasploit
- exploiting SEH
- Reverse engineering .exe files

API/ENDPOINT TESTING

- Introduction
- Lab setup
- Postman
- burpsuite
- API Overview
- Building & hacking an API
- REST API testing
- Automation Set
- Validate the Rest API Responses
- Deep Dive on REST API Automation
- Automation Utilities
- Automate
- API Hacking with postman
- API Top 10
- Deep Dive on OAuth Authentication Set Up
- Maven- Build Management
- Jenkins- Continuous Integration Tool
- Testing Reporting Plugin into Jenkins jobs
- Logging Framework
- Integrate
- API security
- Reporting

WHY NETTECH INDIA ?

- We have huge amount of skilled students ready to work in industry
- We have 6500 sq. ft office area
- We value our clients
- When you choose us, you'll feel the benefit of 10 years' experience of working.
- We take the work seriously, but not ourselves. We're not prickly, precious or pretentious.
- For us, it's all about what adds value for you and your business. Above all, we want our words to work for you.
- We provide full consultations
- We have track record of success
- We are always available
- We track our results
- We meet deadlines

CAREER OPPORTUNITIES

- Forensics
- Security Auditor
- Cyber Security Analyst
- Computer Forensics Investigator
- It Security Consultant

And Many More...



OUR RECRUITERS



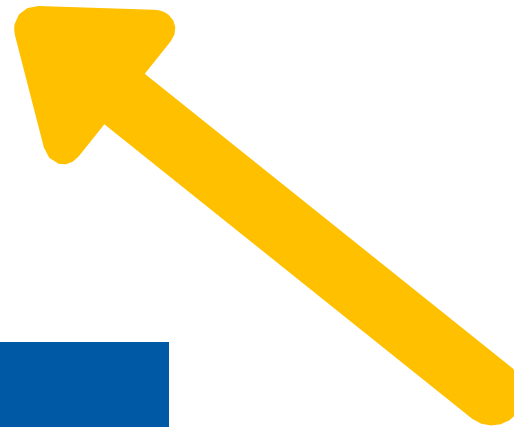
and Many More....

PROCESS FOR SUCCESS

GET PLACED

GET TRAINED

ENROLL



FACILITIES OFFERED

- Practical Training on Live Projects
- Complete Placement Assistance
- Interview Preparation
- Global Certification
- Fully functional labs
- Online / Offline Training
- Study Materials
- Expert Level Industry Recognized Training





Get Certified

NetTech India



THANE

203, Ratnamani Building, Dada Patil Wadi, Opp ICICI ATM, Near Platform No.1, Thane West - 400601



098708 03004 / 5



info@nettechindia.com



ANDHERI

187/A , 1st Floor, Sukhmani Building, S V Road, Opp Nadko Shopping Centre, Above Top 10 Mobile Shop, Andheri West - 400058



7304639164

7304639165



info@nettechindia.com



NERUL

302, A Wing, Om Shivam Center, Sector 20, Akash Tutorial, Opposite Nerul Station West – 400706



9372435654

9372438197



info@nettechindia.com



DADAR

365/A, Rukmini Niketan, 1st Floor, Ranade Road, Next to Post Office, Dadar West, Mumbai 400028



9324826104

9321487176



info@nettechindia.com



PUNE



8591861770



info@nettechindia.com