YUHASPRO

INSTITUTE OF TECHNOLOGY

Certified Professional Diploma in

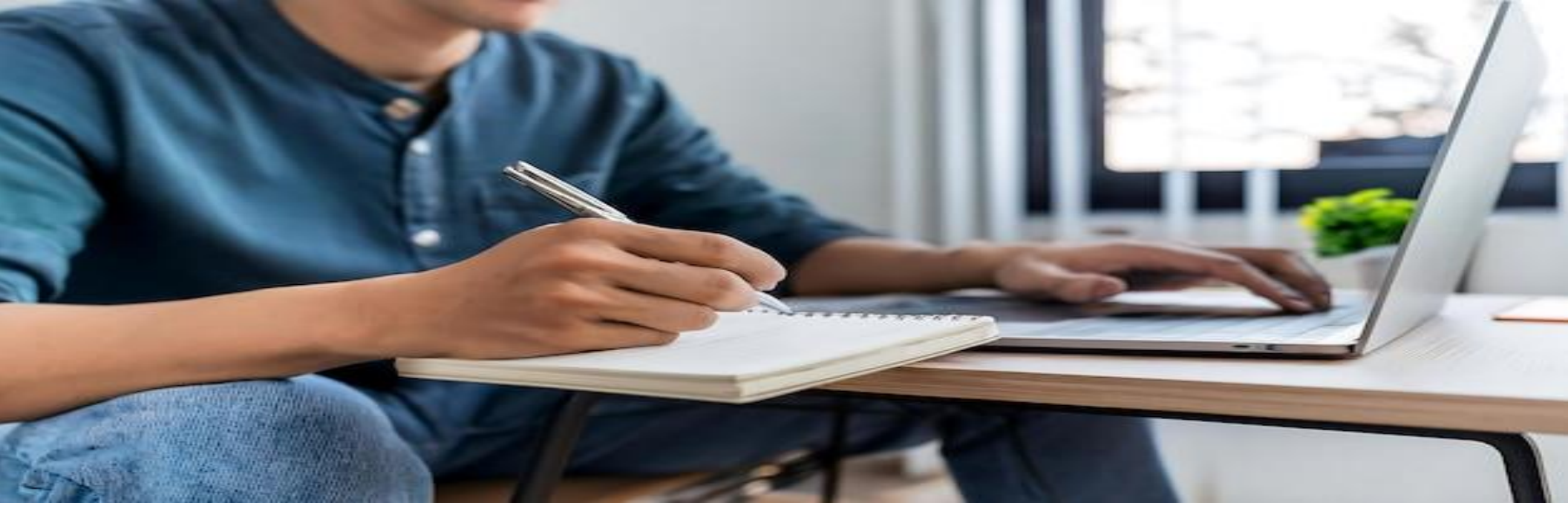
CYBER SECURITY

- Practical Training
- Training From Expert Trainer
- Interview Preparation
- Complete Placement Assistance

https://www.yuhaspro.com/

8108104851 / 52

CERTIFICATIONS OPTIONS AVAILABLE



ABOUT US

YuHasPro is a premier training institute specializing in cutting-edge, job-ready courses in the field of IT, CAD & Accounts. With a focus on practical, hands-on learning, we offer industry-recognized certifications and personalized training programs. Our expert instructors are committed to helping students and professionals enhance their skills and advance their careers. Located in **Thane**, **Mumbai** and **Navi Mumbai**, YuHasPro is dedicated to providing quality education and fostering a culture of continuous learning and innovation. We Prepare You To Be The Talent The Industry Needs!

25%
Theory

75%
Practical

CYBER SECURITY TOPICS

- CCNA
- BASIC TO ADVANCE KALI LINUX
- CEHv12
- NETWORK PENTESTING
- WEB-APPLICATION PENTESTING
- ACTIVE DIRECTORY PENTESTING
- API PENTESTING
- ANDROID PENETRATION TESTING
- CLOUD SECURITY
- CYBER LAW

ABOUT CYBER SECURITY

The **Cyber Security** Course at **YuHasPro** Institute equips students with the essential skills to protect digital infrastructure. This comprehensive program covers key areas such as network security, ethical hacking. Students engage in hands-on training with real-world scenarios, enhancing their ability to anticipate and mitigate cyber threats. The curriculum is designed by industry experts, ensuring up-to-date knowledge in a rapidly evolving field.

BENEFITS OF CYBER SECURITY

- 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
- 150+ Case Studies
- 150+ Projects

CCNA

1. Network Fundamentals

Explain the role and function of network components

- Routers
- L2 and L3 switches
- Next-generation firewalls and IPS
- Access points
- Controllers (Cisco DNA Center and WLC)
- Endpoints
- Servers

Describe characteristics of network topology architectures

- 2 tier
- 3 tier
- Spine-leaf
- WAN
- Small office/home office (SOHO)
- On-premises and cloud

Compare physical interface and cabling types

- Single-mode fiber, multimode fiber, copper
- Connections (Ethernet shared media and point-to-point)
- Concepts of Poe

Identify interface and cable issues (collisions, errors, mismatch duplex, and/or speed)

Compare TCP to UDP

Configure and verify IPv4 addressing and submitting

Describe the need for private IPv4 addressing

Configure and verify IPv6 addressing and prefix

Compare IPv6 address types

- Global unicast
- Unique local
- Link-local
- Any cast
- Multicast
- Modified EUI 64

Verify IP parameters for Client OS (Windows, Mac OS, Linux)

Describe wireless principles

- No overlapping Wi-Fi channels
- SSID
- RF
- Encryption

Explain virtualization fundamentals (virtual machines)

2. Network Access

Configure and verify VLANs (normal range) spanning multiple switches

- Access ports (data and voice)
- Default VLAN
- Connectivity

Configure and verify inters witch connectivity

- 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)

Configure and verify (Layer 2/Layer 3) Ether Channel (LACP)

Describe the need for and basic operations of Rapid PVST+ Spanning Tree Protocol and identify

Basic operations

- Root port, root bridge (primary/secondary), and other port names
- Port states (forwarding/blocking)
- Port Fast benefits

Compare Cisco Wireless Architectures and AP modes

Describe physical infrastructure connections of WLAN components (AP,WLC, access/trunk ports, and LAG)

Describe AP and WLC management access connections (Telnet, SSH, HTTP,HTTPS, console, and TACACS+/RADIUS)

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

Interpret the components of the routing table

- Routing protocol code
- Prefix
- Network mask
- Next hop
- Administrative distance
- Metric
- Gateway of last resort

Determine how a router makes a forwarding decision by default

- Longest match
- Administrative distance
- Routing protocol metric

Configure and verify IPv4 and IPv6 static routing

- Default route
- Network route
- Host route
- Floating static

Configure and verify single area OSPFv2

- Neighbor adjacencies
- Point-to-point
- Broadcast (DR/BDR selection)
- Router ID

Describe the purpose of first hop redundancy protocol

4. IP Services

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

5. Security Fundamentals

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

6. Automation and Programmability

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

And Many More...

Basic to Advanced Kali Linux

- Basic to Advanced Kali Linux
- Open Source v/s Closed Source
- What is Linux and Linux Kernel?
- About Kali Linux and its Specifications
- Install Kali Linux & Virtualization Technology
- Basic Understanding of Linux
- Troubleshoot Issues of Kali Linux Old Versions
- Useful Commands
- Analysis of Is Command
- Analysis of cd Command
- Helping Yourself and Getting Help in Kali Linux
- Configuration Files in Kali Linux
- Passed File Analysis
- Permissions in Linux
- Managing Network in Kali Linux
- Machinery (change mac address for hide yourself)
- Staying Anonymous with Proxy Chains
- Virtual Private Network (VPN) Setup

CEHv12

- Introduction to Ethical Hacking
- Lab Setup
- Kali Linux
- Foot Printing and Reconnaissance
- Scanning Networks
- Enumeration
- Vulnerability Analysis
- System Hacking
- Malware threats
- Sniffing
- Social Engineering
- Denial-of-service
- Session Hijacking
- Evading IDS, Firewalls & Honeypots
- Hacking Web servers
- Hacking web Application
- SQL Injection
- Hacking Wireless Networks
- Hacking Mobile Platforms

- IoT for hacking & OT platforms
- Cloud Computing
- Cryptography
- Steganography

ADVANCE PENETRATION TESTING

NETWORK SECURITY PENTESTING

- INTRODUCTION OF PENTESTING
- Ports and Service Exploitation
- Detecting Live Systems and Analyzing Results
- Nmap Advance Port Scan
- Metasploit
- Dictionary & Passwords Attacks
- FTP Penetration Testing
- SSH Penetration Testing
- Telnet Penetration Testing
- SMTP Penetration Testing
- DNS & DHCP Penetration Testing
- NetBIOS & SMB Penetration Testing
- MySQL Penetration Testing
- Credential Dumping
- BIND SHELL REVERSE SHELL
- DOS Attack Penetration Testing

- Network Vulnerability Assessment Tool
- All About CTF
- Begnner level CTF LAB
- INTERMEDIATE LEVEL CTF LAB
- HARDLEVEL CTF LAB

Linux Privilege Escalation

- Introduction
- What is Privilege Escalation?
- Enumeration
- Automated Enumeration Tools
- Privilege Escalation: Kernel Exploits
- Privilege Escalation: Sudo
- Privilege Escalation: SUID
- Privilege Escalation: Capabilities
- Privilege Escalation: Cron Jobs
- Privilege Escalation: PATH
- Privilege Escalation: NFS
- Capstone Challenge

Windows PrivEsc

- Registry Escalation - Autorun
- Registry Escalation - AlwaysInstallElevated
- Service Escalation - Registry
- Service Escalation - Executable Files
- Privilege Escalation - Startup Applications
- Service Escalation - DLL Hijacking
- Service Escalation - binPath
- Service Escalation - Unquoted Service Paths
- Potato Escalation - Hot Potato
- Password Mining Escalation - Configuration Files
- Password Mining Escalation - Memory
- Privilege Escalation - Kernel Exploits

And Many more …….

WEB APPLICATION PENTESTING

- Introduction to Web Application Pentesting
- Web Server Configuration
- Web Application Lab Setup
- Burpsuite Installation and proxy setup
- Web Application Penetration Testing
- Tools
- Web Hacking Methodology
- Footprinting
- Server Footprinting
- Port Footprinting
- Service Footprinting
- Banner Grabbing or Footprinting
- WAF Detection
- Hidden Content Footprinting
- Load Balancer Detection
- Web Application Analyze
- OWASP TOP10

- A1 Injection Flaws
- A2 Broken Authentication
- A3 Sensitive Data Exposure
- A4 XML External Entities (XXE)
- A5 Broken Access Control
- A6 Security Misconfiguration
- A7 Cross-Site Scripting (XSS)
- A8 Insecure Deserialization
- A9 Using Components with Known Vulnerabilities
- A10 Insufficient Logging & Monitoring
- Other Web Application Threats
- Solving Web-CTF Machine

LIVE BUG BOUNTY

- HackerOne
- Bugcrowd
- Open Bug Bounty
- Vulnerability Lab

And Many more …….

ACTIVE DIRECTORY PENTESTING

- INTRODUCTION
- Why AD Enumeration
- Credential Injection
- Enumeration through Microsoft Management Console
- Enumeration through Command Prompt
- Enumeration through PowerShell
- Enumeration through Bloodhound
- Conclusion

API PENTESTING

- INREODUCTION TO API
- Hands-On API Testing with Postman
- Set Up API Testing Labs
- Analyze GET Requests

- Query Parameters in API
- Path Parameter in API Analysis Your API Calls
- Analysis POST Calls
- Analysis PUT Calls
- Analysis DELETE Calls
- Automating API Tests in Postman
- Postman Collections Validating APIs with Postman
- Requests Sharing Code Between Tests in Postman
- Mocking with Postman
- Running the collection using Newman
- Build Better APIs with Postman API
- API Debugging
- API Monitoring
- Use Postman API Advanced Practices in Postman
- Data Driven Testing with Postman
- Postman Proxy Importing Existing API
- Validate API Schema with tv4

And Many more …….

ANDROID PENETRATION TESTING

Module 1

- Introduction of Genymotion 2 Creating devices on Emulator
- Setting up the burp proxy
- Installation of Root Certificate
- Introduction of Burp Proxy
- Traffic Analysis with Burp
- Introduction of adb

Module 2

- Android Architecture
- Android Security Model
- Android Application Development Cycle
- Major Components of Android
- Android Application Components
- Android Startup Process

Module 3

- Android Application Building
- Decompile With Jadx

- Decompile with Apkeasy Tool
- Weak Server Side Controls
- Insecure Data Storage
- Hardcoding Issues
- Detection of Insecure Logging
- Database Insecure Storage
- Reading Temporary Files 10 SQL Injection in Android 11 Web View Vulnerability
- Access-Related Issues
- Authorization Bypass
- Understanding and Exploitation of Content Providers
- Input Validation leading to DOS Attack
- Root Detection BYypass
- SSL Pinning Bypass
- Inspection of Certificate and Signing SchemaReport Preparation
- IOS Penetration Basics

And Many More...

CLOUD SECURITY

Introduction to Cloud Security

- Platform and Infrastructure Security in the Cloud
- Application Security in the Cloud
- Data Security in the Cloud
- Operation Security in the Cloud
- Penetration Testing in the Cloud
- Incident Detection and Response in the Cloud
- Forensics Investigation in the Cloud
- Business Continuity and Disaster Recovery in the Cloud
- Governance, Risk Management, and Compliance in the Cloud
- Standards, Policies, and Legal Issues in the Cloud

Top Tools Covered in the Certified Cloud Security Engineer (C|CSE)

- AWS IAM
- AWS KMS
- AWS VPC
- Web Application Firewall
- Cloud Front
- Amazon RDS
- Amazon Backup
- Amazon Inspector
- AWS Cloud Trial
- CloudWatch
- Cloud Data Fusion
- Amazon Macie
- AWS Security Hub
- AWS Trusted Advisor

- Microsoft Defender for Cloud
- Azure Active Directory
- Azure Monitor
- Network Watcher
- Azure Storage Analytics
- Azure Policy
- ScoutSuite
- Azure Blueprints
- Cloud Security Suite
- PowerZure

- App Engine Firewall
- Cloud Identity
- Cloud Monitoring
- Security Command Center
- Web Application and API protection
- Google Cloud Armor
- Cloud Security Scanner
- GCP-IAM-Privilege-Escalation
- Secrets Manager
- Chronicle Detect
- Cloud Key Management

CYBER LAW

Fundamentals of Cyber Law

- Jurisprudence of Cyber Law
- Overview of Computer and Web Technology
- Electronic Governance - the Indian perspective
- Overview of General Laws and Procedures in India

E-commerce- Legal issues

- Digital Signatures and the Indian Law
- Electronic Contracts
- The UNCITRAL Model law on Electronic Commerce

Intellectual Property Issues and Cyberspace - The Indian Perspective

- Overview of Intellectual Property related Legislation in India
- Copyright law & Cyberspace
- Trademark law & Cyberspace
- Law relating to Semiconductor Layout & Design

Cyber crime and Digital Evidence - the Indian Perspective

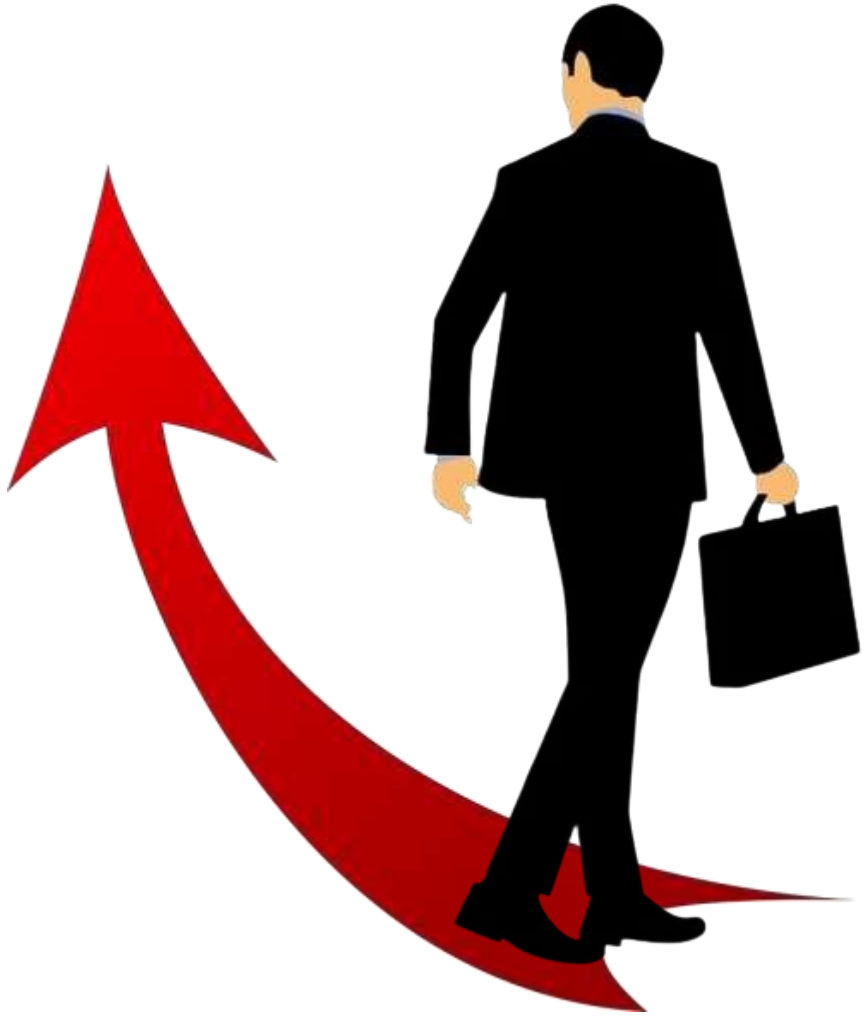
- Penalties & Offences under the Information Technology Act, 2000
- Offences under the Indian Penal Code, 1860
- Issues relating to investigation and adjudication of cyber crimes in India
- Digital evidence

And Many More...

CAREER OPPORTUNITIES

- Incident Response Analyst
- Cybersecurity Consultant
- Information Security Analyst
- Ethical Hacker
- Penetration Tester
- Security Engineer
- Cybersecurity Manager
- Security Architect
- Chief Information Security Officer

And Many More...

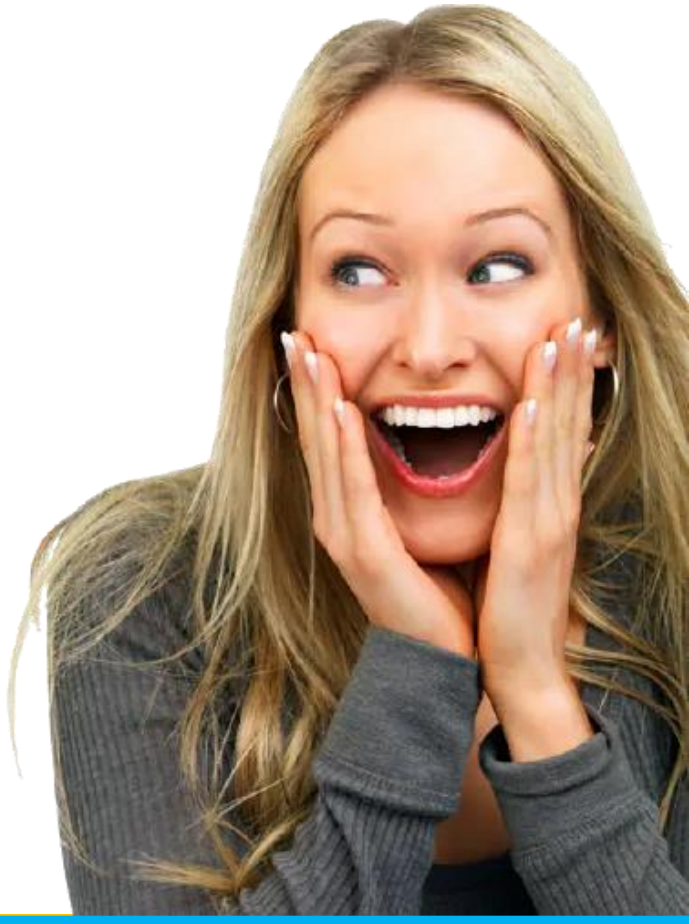


OUR RECRUITERS

And Many More....

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



Note: YuHasPro's job placement assistance is contingent upon students attending and actively participating in the prescribed placement training sessions.


thank you