




Cyber Security Training Program V3.0 with AI


The Cyber Security Training Program V3.0 with AI offers structured learning through **Diploma Courses, Career Oriented Programs**, and specialized **Cyber Security training** designed to build strong fundamentals and advanced technical skills.

It also includes globally recognized certification tracks such as **CompTIA, Cisco, AWS Cloud**, and **ISACA** to provide industry-standard knowledge across multiple security domains.

The program focuses on practical exposure to modern tools, real-world cyber threats, and professional security practices to prepare learners for successful careers in cybersecurity and IT security fields.

For More Information

 +91-7428748576

 training@cyberyaan.com

Cyber Security 1 Year Diploma V3.0 With AI

In 1 Year Diploma in Cyber Security V3.0 Provides Complete Knowledge from Basic to Advance with Latest Cyber Threats and Technologies

For More Information

☎ +91-7428748576

✉ training@cyberyaan.com

1.

Networking

- Introduction to Networking
- Networking Models and Types
- OSI and TCP/IP Model
- Understanding IP Addressing and Subnetting
- Packet Structure and Protocols (IP, TCP, UDP, ISMP)
- Network Devices: Routers, Switches and Firewall
- Network Topologies and Architecture
- NAT, DNS, and DHCP Fundamentals
- Port Forwarding and IP Routing
- Network Security Fundamentals (Firewalls, IDS/IPS, Proxies, VPNs)
- Network Address Translation (NAT) and Security Implications
- Simulation through CISCO Packet Tracer



Networking is the process of connecting devices to share data and communicate efficiently and securely.

2.

Kali - Linux

- Introduction Kali Linux and Lab Set (Virtual Box, VMware, ISO Installation)
- Shell, CLI vs GUI, Distribution
- Basic Linux Commands (pwd, cd, ls, cp, mv, rm)
- Files and Directory Management (mkdir, touch, nano, cat, less)
- User and Group Management (adduser, usermod, groups)
- File Permissions & Ownership (chmod, chown, unmask)
- Linux File System Hierarchy & Navigation
- Process Management (ps, top, kill, nice, jobs)
- Package Management (apt, yum, dpkg, snap)
- Networking commands (ping, netstat, traceroute, ss, ifconfig/ip)
- Essential Security Tools (nmap, netcat, tcpdump, whois)
- Bash Scripting Fundamentals (Variables, Loops, Condition)
- Automation with Bash (Practical Scripts & Crontab Jobs)
- System Logs & Monitoring (Journalctl, syslog, logrotate)



Kali Linux is a specialized Linux distribution used for ethical hacking, penetration testing, and cybersecurity analysis, equipped with powerful security tools.

3.

Python Programming

- Introduction to code and platforms
- Python variables & Data Types
- Operators
- Python number and Strings
- List and tuples
- Dictionary and Type casting
- Arrays and Numpy
- Python Conditional Statements
- Loops Concept and Questions
- Control Statements
- Functions
- All about OOPS Concept
- Multithreading and image processing
- File Handling in python
- Mail Sending Program and Use Case
- Database Connection (My SQL)
- Sockey: Building and Working
- Web Scraping: A trick for Bug Bounty
- Libraries: Hacks for Tools to Hack



Python Programming is a versatile and easy-to-learn language used for automation, data analysis, web development, and cybersecurity applications.

4.

Ethical Hacking

- Introduction to Networking
- Introduction to Linux
- Introduction to Ethical Hacking
- Information Gathering
- Scanning
- Enumeration
- Vulnerability Analysis (VA)
- System Hacking
- Malware | Worms | Trojans
- Sniffing
- Social Engineering Techniques
- DOS | DDOS Attack
- Session Hijacking
- Honeypots, Firewalls, IDS
- Hacking Web Server
- Web Application Hacking
- SQL Injection & Types
- WiFi- Hacking
- Exploit Mobile Platform
- IOT & OT Exploit
- Cloud
- Cryptography




Ethical Hacking is the practice of legally testing systems and networks to identify vulnerabilities and strengthen security against cyber threats.

5.

Network Penetration Testing

- Introduction to Kali Linux
- Command Line Fun
- Bash Scripting
- Passive Footprinting
- Active Footprinting
- Advanced Scanning
- Initial access CTFs

- Introduction to Linux Privilege Escalation
- Introduction to Windows Privilege Escalation
- Root Access CTFs
- Buffer overflow overview
- Antivirus Evasion
- Active Directory Overview
- Report Generation




Network Penetration Testing is the process of simulating cyber attacks on networks to identify vulnerabilities and improve overall security

6.

Privilege Escalation (Windows Based)

- Introduction to window privilege escalation
- Gaining Foothold
- Initial Enumeration
- Exploring Automated tools
- Kernel Exploits
- Password and Port Forwarding
- Windows subsystem for linux
- Impersonation and Potato attacks
- Getsystem

- Runas
- Registry
- Executables Files
- Startup Applications
- DLL Hijacking
- Service Permissions (paths)
- CVE 2019 – 1388
- Challenge




Privilege Escalation (Windows-Based) is the technique of gaining higher-level access on a Windows system by exploiting vulnerabilities or misconfigurations.

7.

Privilege Escalation (Linux Based)

- Introduction to Linux Privilege Escalation
- Lab Overview
- Initial Enumeration
- Exploring Automated Tools
- Kernel Exploits
- Password and File Permissions
- Sudo

- SUID
- Capabilities
- Scheduled Tasks
- NFS Root Squashing
- Docker
- Challenge



Privilege Escalation (Linux-Based) is the process of gaining higher-level access on a Linux system by exploiting vulnerabilities or misconfigurations.

8.

Active Directory

- Introduction to Active Directory
- Active Directory Installation and Configuration
- Users and Groups Management in AD
- Organizational Units and Delegation
- Active Directory Group Policy Overview
- Active Directory Authentication Models
- Advanced Group Policy Management
- Active Directory Federation Services (ADFS)
- Trusts in Active Directory
- Active Directory Security Best Practices
- Monitoring and Auditing Active Directory
- Active Directory Backup and Disaster Recovery
- Advanced Active Directory Security
- Active Directory Penetration Testing
- Active Directory Monitoring and SIEM Integration
- Capstone: Securing and Auditing Active Directory



Active Directory is a directory service by Microsoft used to manage users, computers, and permissions within a network.

9.

WEB APPLICATION PENETRATION TESTING

- Introduction to HTTP/HTTPS (Request Methods)
- Understanding the Web Application Attack Surface
- Introduction to OWASP Top 10 Vulnerabilities
- Lab Setup: Installing and Configuring Burp Suite
- Exploring Burp Suite Basics (Proxy, Repeater)
- Understanding and Exploiting Cross-Site Scripting
- Preventing and Mitigating Cross-Site Scripting (XSS)
- Cross-Site Request Forgery (CSRF) Attacks and Prevention Techniques
- Identifying and Exploiting Input Validation Vulnerabilities
- Introduction to SQL Injection Attacks (Manual Exploitation)
- SQL Injection Attacks (Automated Exploitation)
- Using SQLmap for Automated Database Exploitation
- Techniques for Preventing SQL Injections (Prepared Statements, ORM)
- Understanding and Exploiting File Upload Vulnerabilities
- Preventing Arbitrary File Execution via File Uploads
- Directory Traversal Attacks and Exploitation Techniques
- Mitigating Directory Traversal Attacks
- Session Management Vulnerabilities (Session Hijacking, Fixation)
- Preventing Session Hijacking and Session Fixation
- Authentication and Authorization Flaws (Insecure Password Storage)
- Exploiting Broken Access Control and Mitigation Techniques
- Exploiting Insecure Direct Object References (IDOR)
- Using Burp Suite for Automated Vulnerability Scanning
- Final Case Study: Performing a Full Web Application Penetration Test




Web Application Penetration Testing is the process of identifying and exploiting vulnerabilities in web applications to improve their security.

10.

API Hacking

- Introduction to REST APIs and JSON Structure
- Understanding API Endpoints and Methods
- Enumerating API Endpoints and Parameters
- Identifying Broken Object Level Authorization (BOLA)
- Exploiting Common API Vulnerabilities
- Injection Attacks in APIs (SQLi, Command Injection, XXE)
- API Testing with Postman
- API Analysis using Burp Suite
- Exploiting API Authentication Flaws
- API Security Best Practices (OAuth 2.0, JWT)
- API Hardening and Mitigation Techniques
- Final Lab: Performing a Complete API Penetration Test




API Hacking is the practice of testing APIs for vulnerabilities to identify security flaws and prevent unauthorized access or data breaches.

11.

Mobile Penetration Testing

- Introduction to Android Application Security
- Setting up Your Android Application Security
- Android Penetration Testing Methodologies Detailed Explanation
- Lab Setup Design
- Traditional Android Penetration Testing Report - Test Cases
- Traditional Android Penetration Testing Approach and Guidelines
- Android Attack Surface – Client Side Vulnerabilities
- Android Attack Surface Server Side Vulnerabilities
- Android Attack Surface Logical Security Threats Module
- OWASP Mobile Top 10
- Set up Android Debug Bridge Utility (adb)
- Vulnerable Android Application Source Code Review
- Structure of an Android Application Package (APK)
- Reversing an Android Application using dex2jar
- Reversing an Android Application using apktool
- Signing an Android Application Manually
- Android Code Obfuscation and Code Protection
- Adding Malicious Code to Android Apps
- Debugging Detection
- Root Detection
- VM Detection
- iOS Application Basic Standards



Mobile Penetration Testing is the process of identifying security vulnerabilities in mobile apps to protect data and prevent unauthorized access.

12.

Security Operations Centre Specialist | SOC with EDR

- Risk Management and Security
- Cyber Threats and Attack Patterns
- Incidents, Events and logging
- Security Incident and Recovery with SIEM
- Advanced Threat Detection and Analysis
- Security Event Response and Resolution
- Introduction to Splunk
- Installing and Configuring Splunk
- Searching and Reporting in Splunk
- Indexing and Data
- Splunk Search Language (SPL)
- Creating Dashboards and Visualization
- Alerts and Notification
- Splunk Administration and Security
- Splunk App Development
- Splunk Enterprise Security
- Endpoint Monitoring / Data Collection
- Detection Engine
- Alerting & Incident Management
- Investigation / Threat Hunting
- Response & Remediation
- Multi-Tenant & API Layer
- The Sensor & Data Collection Layer
- The Forensic & Hunting Module
- Identity & Lateral Movement Tracking module
- Reporting & Dashboard



Security Operations Centre (SOC) Specialist is a professional who monitors, detects, and responds to cybersecurity threats to protect an organization's systems and data

13.

ISO 27001 LEAD AUDITOR

- Fundamental concepts and principles of information security
- ISO/IEC 27001 certification process
- Information Security Management System (ISMS)
- The ISO/IEC 27000 family of standards
- Advantages of ISO/IEC 27001
- Fundamental of information and assets
- Fundamental principles of information security confidentiality, integrity, and availability



ISO 27001 Lead Auditor is a professional who audits and evaluates an organization's information security management system to ensure compliance with ISO 27001 standards.

COMPTIA A+ TRAINING & CERTIFICATION TRAINING

Course Content

- **Module 01: Mobile Devices**
- **Module 02: Networking**
- **Module 03: Hardware**
- **Module 04: Virtualization and Cloud Computing**
- **Module 05: Hardware and Network Troubleshooting**

Appreciation from Defence Sector



About the Training

COMPTIA A+ TRAINING CERTIFICATION

CyberYaan Training Institute in Delhi offers a comprehensive CompTIA A+ training and certification Training designed to build strong foundational IT skills. The Training covers essential topics like computer hardware, software, networking, and basic security, helping learners prepare for the CompTIA A+ certification exam and entry-level IT support roles.



Duration
40 hours



Yes



Language
Hindi & English

SCAN ME



Community



Youtube



Linkdin



Instagram



25/28, Tilak Nagar, Upper Ground Floor, Opposite Raj Mandir Hypermarket, New Delhi - 110018



training@cyberyaan.com



+91-742 874 8576

www.cyberyaan.com

COMPTIA N+ TRAINING & CERTIFICATION TRAINING

Course Content

- **Module 01: Networking Concepts**
- **Module 02: Network Installation and Configuration**
- **Module 03: Network Media and Topologies**
- **Module 04: Network Management Module 05: Network Security**

Appreciation from Defence Sector



About the Training

COMPTIA N+ TRAINING & CERTIFICATION

CyberYaan Training Institute in Delhi offers a comprehensive CompTIA Network+ (N+) training and certification Training designed to develop strong networking skills. The Training covers key concepts such as network infrastructure, protocols, troubleshooting, and security fundamentals, helping learners prepare for the CompTIA Network+ certification exam and build a career in networking and IT support.



Duration
40 hours



Yes



Language
Hindi & English

SCAN ME



Community



Youtube



Linkdin



Instagram



25/28, Tilak Nagar, Upper Ground Floor, Opposite Raj Mandir Hypermarket, New Delhi - 110018



training@cyberyaan.com



+91-742 874 8576

www.cyberyaan.com

COMPTIA SECURITY+ TRAINING & CERTIFICATION TRAINING

Course Content

- **Module 01: Threats, Attacks, and Vulnerabilities**
- **Module 02: Architecture and Design**
- **Module 03: Implementation**
- **Module 04: Operations and Incident Response**
- **Module 05: Governance, Risk, and Compliance**

Appreciation from Defence Sector



About the Training

COMPTIA SECURITY+ TRAINING CERTIFICATION

CyberYaan Training Institute in Delhi offers a comprehensive CompTIA Security+ training and certification Training designed to build a strong foundation in cybersecurity. The Training covers key topics such as network security, threat management, risk mitigation, cryptography, and security protocols, helping learners prepare for the CompTIA Security+ certification exam and pursue careers in cybersecurity and information security roles.



Duration
40 hours



Yes



Language
Hindi & English

SCAN ME



Community



Youtube



Linkdin



Instagram



25/28, Tilak Nagar, Upper Ground Floor, Opposite
Raj Mandir Hypermarket, New Delhi - 110018



training@cyberyaan.com



+91-742 874 8576

www.cyberyaan.com

COMPTIA PENTEST+ TRAINING & CERTIFICATION TRAINING

Course Content

- **Module 01: Planning and Scoping**
- **Module 02: Information Gathering & Vulnerability Identification**
- **Module 03: Attacks and Exploits**
- **Module 04: Penetration Testing Tools**
- **Module 05: Reporting and Communication**

Appreciation from Defence Sector



About the Training

COMPTIA PENTEST+ TRAINING & CERTIFICATION

CyberYaan Training Institute in Delhi offers a comprehensive CompTIA PenTest+ training and certification Training designed to develop practical skills in penetration testing and ethical hacking. The Training covers topics such as vulnerability assessment, network and application testing, exploitation techniques, and reporting, helping learners prepare for the CompTIA PenTest+ certification exam and build a career in cybersecurity and ethical hacking.



Duration
40 hours



Certificate of Completion
Yes



Language
Hindi & English

SCAN ME



Community



Youtube



Linkdin



Instagram



25/28, Tilak Nagar, Upper Ground Floor, Opposite
Raj Mandir Hypermarket, New Delhi - 110018



training@cyberyaan.com



+91-742 874 8576

www.cyberyaan.com

COMPTIA CYSA+ TRAINING & CERTIFICATION TRAINING

Course Content

- **Module 01: Threat Management**
- **Module 02: Vulnerability Management**
- **Module 03: Cyber Incident Response**
- **Module 04: Security Architecture and Tool Sets**

Appreciation from Defence Sector



About the Training

COMPTIA CYSA+ TRAINING & CERTIFICATION

CyberYaan Training Institute in Delhi offers a comprehensive CompTIA CySA+ (Cybersecurity Analyst) training and certification Training designed to build skills in threat detection and response. The Training covers topics such as security monitoring, vulnerability management, incident response, and data analysis, helping learners prepare for the CompTIA CySA+ certification exam and pursue roles in cybersecurity analysis and defense.



Duration
40 hours



Yes



Language
Hindi & English

SCAN ME



Community



Youtube



Linkdin



Instagram



25/28, Tilak Nagar, Upper Ground Floor, Opposite
Raj Mandir Hypermarket, New Delhi - 110018



training@cyberyaan.com



+91-742 874 8576

www.cyberyaan.com

COMPTIA CASP+ TRAINING & CERTIFICATION TRAINING

Course Content

- **Module 01: Security Architecture**
- **Module 02: Security Operations**
- **Module 03: Security Operations**
- **Module 04: Governance, Risk, and Compliance**

Appreciation from Defence Sector



About the Training

COMPTIA CASP+ TRAINING & CERTIFICATION

CyberYaan Training Institute in Delhi offers a comprehensive CompTIA CASP+ (Advanced Security Practitioner) training and certification Training designed for advanced cybersecurity professionals. The Training covers enterprise security, risk management, security architecture, and advanced threat analysis, helping learners prepare for the CompTIA CASP+ certification exam and take on senior-level roles in cybersecurity.



Duration
40 hours



Yes



Language
Hindi & English

SCAN ME



Community



Youtube



Linkdin



Instagram



25/28, Tilak Nagar, Upper Ground Floor, Opposite
Raj Mandir Hypermarket, New Delhi - 110018



training@cyberyaan.com



+91-742 874 8576

www.cyberyaan.com

CISCO CCNA 200 -301 TRAINING

Course Content

- Module 01: Introduction to Networking
- Module 02: OSI Model
- Module 03: TCP IP Model
- Module 04: IP Address
- Module 05: Information About Networking Device.
- Module 06: Subnetting/Summarisation
- Module 07: ARP
- Module 08: Packet Flow in Same & Different Network
- Module 09: APIPA
- Module 10: Routing Protocols Configuration
- Module 11: WAN Technologies
- Module 12: Routing Protocols
- Module 13: NAT
- Module 14: ACL
- Module 15: DHCP
- Module 16: Telnet & SSH
- Module 17: Layers 2 Protocols
- Module 18: Balancing Protocol
- Module 19: Port Security
- Module 20: VPN Security

Appreciation from Defence Sector



About the Training

CISCO CCNA 200 -301

CyberYaan Training Institute in Delhi offers a comprehensive Cisco CCNA 200-301 training and certification Training designed to build strong networking fundamentals. The Training covers topics such as network basics, IP connectivity, security fundamentals, automation, and troubleshooting, helping learners prepare for the CCNA 200-301 certification exam and start a career in networking and IT infrastructure.



Duration
40 hours



Yes



Language
Hindi & English

SCAN ME



Community



Youtube



Linkdin



Instagram



25/28, Tilak Nagar, Upper Ground Floor, Opposite
Raj Mandir Hypermarket, New Delhi - 110018



training@cyberyaan.com



+91-742 874 8576

www.cyberyaan.com

CISCO CERTIFIED NETWORK PROFESSIONAL 350-701 TRAINING

Course Content

- **Module 01: Security Concepts**
- **Module 02: Network Security**
- **Module 03: Securing the Cloud**
- **Module 04: Content Security**
- **Module 05: Endpoint Protection and Detection**
- **Module 06: Secure Network Access, Visibility, and Enforcement**

Appreciation from Defence Sector



About the Training

CISCO CERTIFIED NETWORK PROFESSIONAL 350-701

CyberYaan Training Institute in Delhi offers a comprehensive Cisco Certified Network Professional (350-701) training and certification Training designed to build advanced networking and security skills. The Training covers enterprise security, network infrastructure protection, VPN technologies, and threat management, helping learners prepare for the 350-701 certification exam and advance their careers in network security and professional-level IT roles.



Duration
40 hours



Yes



Language
Hindi & English

SCAN ME



Community



Youtube



Linkdin



Instagram



25/28, Tilak Nagar, Upper Ground Floor, Opposite
Raj Mandir Hypermarket, New Delhi - 110018



training@cyberyaan.com



+91-742 874 8576

www.cyberyaan.com



AWS ASSOCIATE TRAINING

Course Content

- **Module 01: Design Secure Architectures**
- **Module 02: Design Resilient Architectures**
- **Module 03: Design High-Performing Architectures**
- **Module 04: Design Cost-Optimized Architectures**

Appreciation from Defence Sector



About the Training

AWS ASSOCIATE

CyberYaan Training Institute in Delhi offers a comprehensive AWS Associate training and certification Training designed to build strong cloud computing skills. The Training covers core AWS services, cloud architecture, deployment, security, and monitoring, helping learners prepare for AWS Associate-level certification exams and pursue careers in cloud computing and IT infrastructure.



Duration
40 hours



Yes



Language
Hindi & English

SCAN ME



Community



Youtube



Linkdin



Instagram



25/28, Tilak Nagar, Upper Ground Floor, Opposite
Raj Mandir Hypermarket, New Delhi - 110018



training@cyberyaan.com



+91-742 874 8576

www.cyberyaan.com

AWS CLOUD SECURITY TRAINING

Course Content

- Module 01: Design Resilient Architectures
- Module 02: Design High-Performing Architectures
- Module 03: Design Secure Applications and Architectures
- Module 04: Design Cost-Optimized Architectures
- Module 05: Given an AWS Abuse Notice, Evaluate a Suspected Compromised Instance or Exposed Access Key
- Module 06: Verify that the Incident Response plan includes relevant AWS services
- Module 07: Evaluate the Configuration of Automated Alerting and Execute Possible Remediation of Security Related Incidents and Emerging Issues
- Module 08: Design and implement security monitoring and alerting
- Module 09: Troubleshoot security monitoring and alerting
- Module 10: Design and Implement a Logging Solution
- Module 11: Design Edge Security on AWS
- Module 12: Troubleshoot Logging Solutions
- Module 13: Design and implement a secure network infrastructure
- Module 14: Troubleshoot a secure network infrastructure
- Module 15: Design and implement host-based security
- Module 16: Design and Implement a Scalable Authorization and Authentication System to Access AWS Resources
- Module 17: Troubleshoot an Authorization and Authentication System to Access AWS Resources
- Module 18: Design and implement key management and use
- Module 19: Troubleshoot key management
- Module 20: Design and implement a data encryption solution for data at rest and data in transit

Appreciation from Defence Sector



About the Training

AWS CLOUD SECURITY

CyberYaan Training Institute in Delhi offers a comprehensive AWS Cloud Security training and certification Training designed to build expertise in securing cloud environments. The Training covers topics such as identity and access management (IAM), data protection, network security, compliance, and risk management, helping learners develop skills required for cloud security roles and advanced AWS certifications.



Duration
40 hours



Yes



Language
Hindi & English

SCAN ME



Community



Youtube



Linkdin



Instagram



25/28, Tilak Nagar, Upper Ground Floor, Opposite Raj Mandir Hypermarket, New Delhi - 110018



training@cyberyaan.com



+91-742 874 8576

CERTIFIED INFORMATION SYSTEMS AUDITOR TRAINING

Course Content

- **Module 01: The Process of Auditing Information Systems**
- **Module 02: Governance and Management of IT**
- **Module 03: Information Systems Acquisition, Development and Implementation**
- **Module 04: Information Systems Operations, Maintenance and Support**
- **Module 05: Protection of Information Assets**

Appreciation from Defence Sector



About the Training

CERTIFIED INFORMATION SYSTEMS AUDITOR

CyberYaan Training Institute in Delhi offers a comprehensive Certified Information Systems Auditor (CISA) training and certification Training designed to build expertise in IT auditing and governance. The Training covers key areas such as information systems auditing, risk management, control frameworks, and compliance, helping learners prepare for the CISA certification and pursue careers in IT audit, risk, and assurance roles.



Duration
40 hours



Yes



Language
Hindi & English

SCAN ME



Community



Youtube



Linkdin



Instagram



25/28, Tilak Nagar, Upper Ground Floor, Opposite Raj Mandir Hypermarket, New Delhi - 110018



training@cyberyaan.com



+91-742 874 8576

www.cyberyaan.com

CERTIFIED INFORMATION SECURITY MANAGER TRAINING

Course Content

- **Module 01: Information Security Governance**
- **Module 02: Information Security Risk Management**
- **Module 03: Information Security Program**
- **Module 04: Incident Management**

Appreciation from Defence Sector



About the Training

CERTIFIED INFORMATION SECURITY MANAGER

CyberYaan Training Institute in Delhi offers a comprehensive Certified Information Security Manager (CISM) training and certification Training designed for professionals aiming to build expertise in information security management. The Training covers key areas such as risk management, governance, incident management, and security program development, helping learners prepare for the CISM certification and advance into managerial roles in cybersecurity.



Duration
40 hours



Yes



Language
Hindi & English

SCAN ME



Community



Youtube



Linkdin



Instagram



25/28, Tilak Nagar, Upper Ground Floor, Opposite Raj Mandir Hypermarket, New Delhi - 110018



training@cyberyaan.com



+91-742 874 8576

www.cyberyaan.com

CERTIFIED IN RISK & INFORMATION SYSTEMS CONTROL TRAINING

Course Content

- **Module 01: Risk Identification (ID)**
- **Module 02: Risk Assessment (RA)**
- **Module 03: Risk Response and Mitigation (RM)**
- **Module 04: Risk and Control Monitoring and Reporting (M&R)**

Appreciation from Defence Sector



About the Training

CERTIFIED IN RISK & INFORMATION SYSTEMS CONTROL

CyberYaan Training Institute in Delhi offers a comprehensive Certified in Risk and Information Systems Control (CRISC) training and certification Training designed to develop expertise in risk management and information systems control. The Training covers key areas such as risk identification, assessment, mitigation, and control implementation, helping learners prepare for the CRISC certification and build careers in risk management and IT governance.



Duration
40 hours



Yes



Language
Hindi & English

SCAN ME



Community



Youtube



Linkdin



Instagram



25/28, Tilak Nagar, Upper Ground Floor, Opposite Raj Mandir Hypermarket, New Delhi - 110018



training@cyberyaan.com



+91-742 874 8576

www.cyberyaan.com

APPLICATION SECURITY PENTESTING

Course Content

- **Module 01: Network Essentials**
- **Module 02: Kali Linux**
- **Module 03: Python Programming**
- **Module 04: Ethical Hacking**
- **Module 05: Web Application Security**
- **Module 06: Mobile Application Security**

Appreciation from Defence Sector



About the Training

APPLICATION SECURITY PENTESTING

CyberYaan Training Institute in Delhi offers a comprehensive Application Security Pentesting course designed to build practical skills in identifying and fixing web application vulnerabilities. The training covers OWASP Top 10, web attacks, vulnerability assessment, and penetration testing techniques to prepare learners for real-world cybersecurity roles.



Duration
40 hours



Yes



Language
Hindi & English

SCAN ME



Community



Youtube



Linkdin



Instagram



25/28, Tilak Nagar, Upper Ground Floor, Opposite
Raj Mandir Hypermarket, New Delhi - 110018



training@cyberyaan.com



+91-742 874 8576

www.cyberyaan.com

Cyber Forensics Analysis Program (CFAP)

Course Content

- **Module 01: Network Essentials**
- **Module 02: Kali Linux**
- **Module 03: Python Programming**
- **Module 04: Ethical Hacking**
- **Module 05: Digital Forensics**
- **Module 06: Threat Hunting**
- **Module 07: Incident Handler and Reporting**

Appreciation from Defence Sector



About the Training

Cyber Forensics Analysis Program(CFAP)

CyberYaan Training Institute in Delhi offers a comprehensive Cyber Forensics Analysis program designed to build practical skills in investigating cyber incidents and analyzing digital evidence. The program covers Network Essentials, Kali Linux, Python Programming, Ethical Hacking, Digital Forensics, Threat Hunting, and Incident Handling & Reporting to prepare learners for real-world cybersecurity and forensic investigation roles.



Duration
40 hours



Yes



Language
Hindi & English

SCAN ME



Community



Youtube



Linkdin



Instagram



25/28, Tilak Nagar, Upper Ground Floor, Opposite
Raj Mandir Hypermarket, New Delhi - 110018



training@cyberyaan.com



+91-742 874 8576

www.cyberyaan.com

Network Vulnerability Testing

Course Content

- **Module 01: Network Essentials**
- **Module 02: Kali Linux**
- **Module 03: Python Programming**
- **Module 04: Ethical Hacking**
- **Module 05: Network Penetration Testing**
- **Module 06: Privilege Escalation - Linux**
- **Module 07: Privilege Escalation - Windows**
- **Module 08: Active Directory**

Appreciation from Defence Sector



About the Training

Network Vulnerability Testing

CyberYaan Training Institute in Delhi offers a comprehensive Network Vulnerability Testing course designed to build practical skills in identifying and assessing security weaknesses in network infrastructures. The training covers network scanning, vulnerability assessment tools, threat analysis, risk mitigation techniques, and reporting methods to prepare learners for real-world roles in network security and cybersecurity operations.



Duration
40 hours



Certificate of Completion
Yes



Language
Hindi & English

SCAN ME



Community



Youtube



Linkdin



Instagram



25/28, Tilak Nagar, Upper Ground Floor, Opposite Raj Mandir Hypermarket, New Delhi - 110018



training@cyberyaan.com



+91-742 874 8576

www.cyberyaan.com