CYBERYAAN
TRAINING & CONSULTANCY

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
- Oprators
- 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
- Mutithreading 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

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

- 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

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

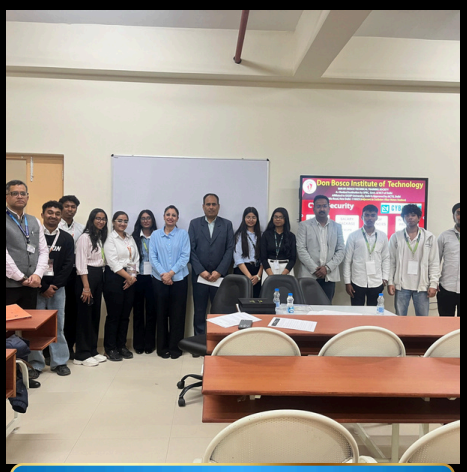
Security Operations Centre (SOC) Specialist is a professional who monitors, detects, and responds to cybersecurity threats to protect an organization's systems and data

13. ISO 27001 LEAD AUDITOR

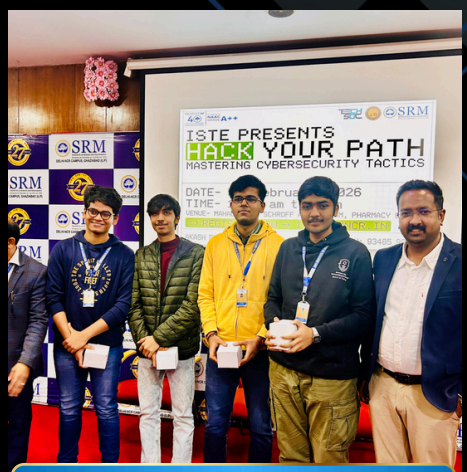
- Fundamental concepts and principles of information security
- ISO/IEC 27001 certification process
- Information Security Management System (ISMS)
- The ISO/IEC 27000 family of standards
- Advantages of ISO/IEC 27001
- Fundamental of information and assets
- Fundamental principles of information security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

GALLERY



Don Bosco Institute of Technology

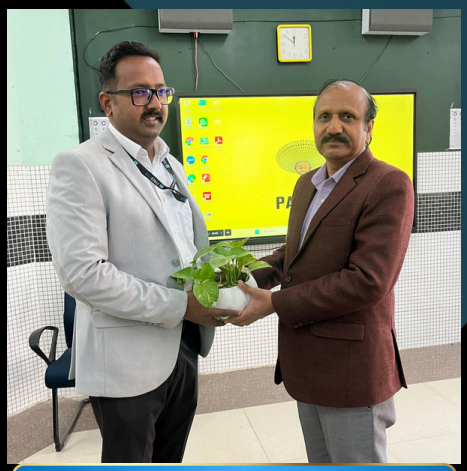


SRM Institute of Science and Technology

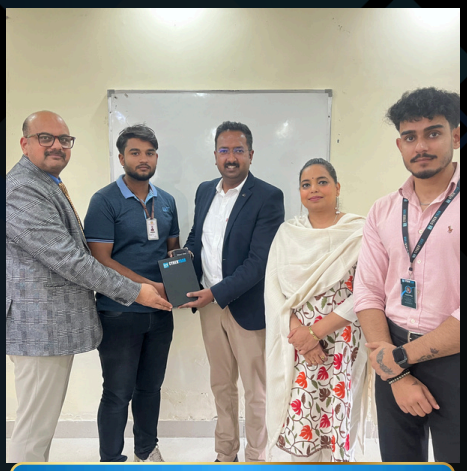
Indraprastha Institute of Information Technology Delhi

Shri Guru Tegh Bahadur Institute of Management & Information Technology (SGTBIMIT)

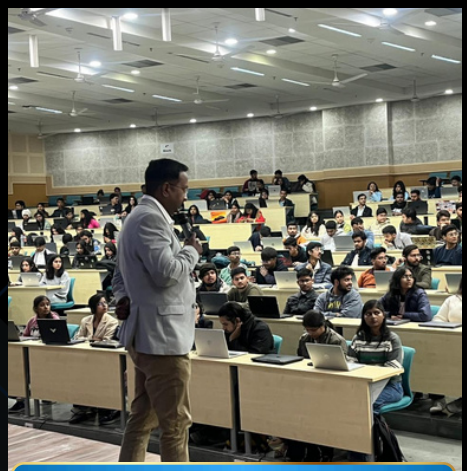
ARI Simulation



CM SHRI SEC-19 DWARKA



IIMT Group Of Colleges Greater Noida



Indraprastha Institute of Information Technology Delhi

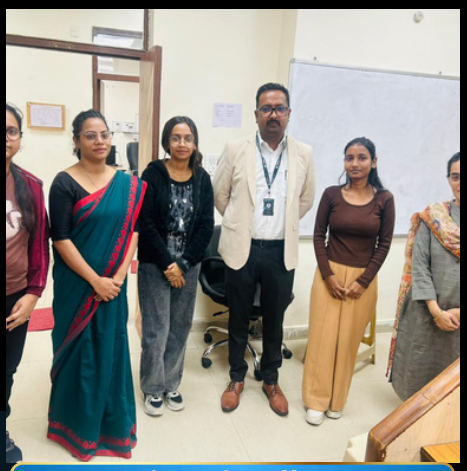
Shri Guru Tegh Bahadur Institute of management & Information technology (SGTBIMIT)

GALLERY

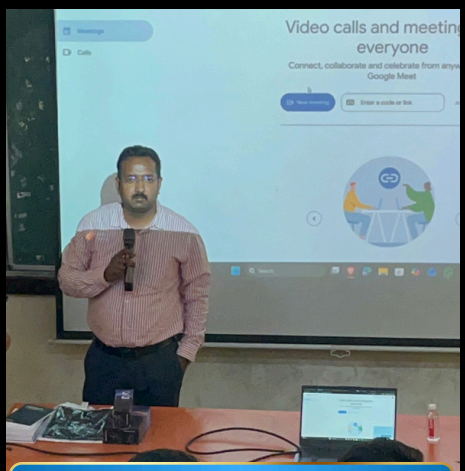
Shri Aurobindo College, of commerce and management

G.C.R.G. Group of Institutions, Lucknow

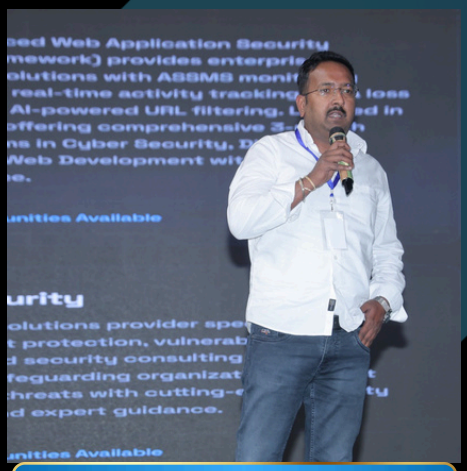
Maitreyi College, University of Delhi



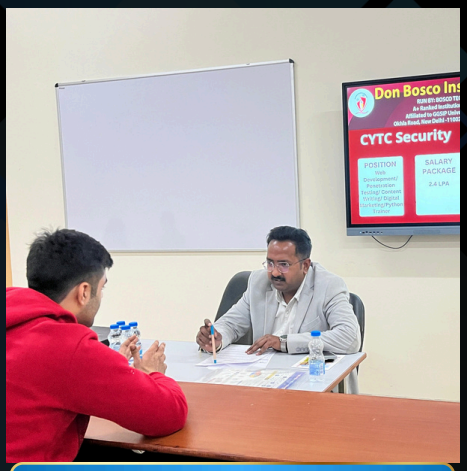
Maitreyi College, University of Delhi



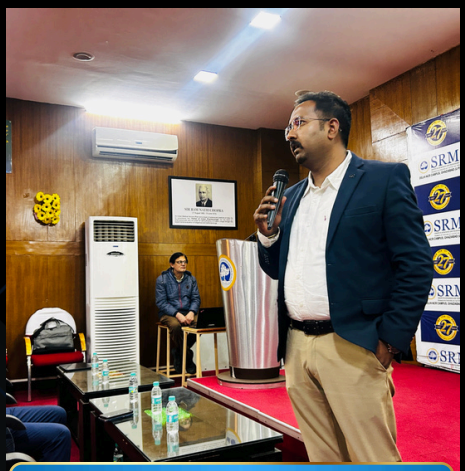
Daulat Ram College, DU



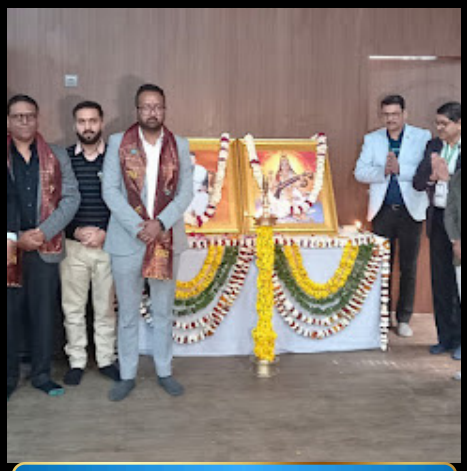
Hack Defence Summit 2026



Don Bosco Institute of Technology



SRM Institute of Science and Technology



Hackathon

PLACEMENTS

Jahanvi Khurana
Placed in Cynox Security LLP
As a Cyber Security Analyst

Yash Garg
Placed in Cynox Security LLP
As a Cyber Security Analyst

Ravinshu Chauhan
Placed in Innspark
As a Soc Analyst

Chandan Jha
Placed in HCL Tech
As a Cyber Security Consultant

Ajay
Placed in Codec Networks
As a Cyber Security Analyst

Ritik
Placed in SBI
As a Cyber Security Analyst

Prince Bhardwaj
Placed in Accenture
As a Cyber Security Analyst

Aditi Goyal
Placed in Capgemini
As a Cisco Tac engineer (network analyst)

Divyanshu Shekhar
Placed in Transbank
As a Information Security Officer

Ravi
Placed in hays
As a Soc Analyst

PLACEMENTS

Aksh Yadav
Placed in Skillmine
As a Soc Analyst

Gyan Ranjan
Placed in Cynox Security LLP
As a Cyber Security Analyst

Dinesh kumar
Placed in Infosys
As a Cyber Security Analyst

Debjit Mohapatra
Placed in GL Bajaj
As a Cyber Security Trainer

Pranav
Placed in Cynox Security LLP
As a Security Analyst
Trainee

Suraj Ashok Rathor
Placed in Cynox Security LLP
As a Security Analyst-
Trainee

Mohit Yadav
Placed in National
informatics Center, Meity
As a SOC Analyst

G.Rohit
Placed in KPMG
As a SOC Analyst

kirti
Placed in Cynox Security LLP
As a Cyber Security Analyst

Arpit Hawa
Placed in Capgemini
As a Cisco Tac engineer
(network analyst)

PLACEMENTS

Isha
Placed in Cywarden Inc.
As a Security Analyst

Harsh Vardhan Verma
Placed in CISAI
As a Soc Analyst

Tushal Kumar
Placed in Cyberion Labs
As a Security Analyst

Hansika Rawat
Placed in Cynox Security LLP
As a Cyber Security Analyst

Harsh Verma
Placed in Hoolocom
As a Technical Support
Implementation Engineer

Pratik
Placed in Indian Army
As a Cyber Security Analyst

Gaurav Pathak
Placed in Ministry of Defence
As a Information
Technology Security
Engineer

CLIENTS AND PARTNERS

PELORUS
Enabling Technology in the Right Direction

CompTIA

eSec Forte

4ACHIEVERS
WE BUILD PROFESSIONALS

GURUGRAM UNIVERSITY
विद्या जीवनाय न तु जीविकाय

KLTIF

GNIOT
GROUP OF INSTITUTIONS
Approved by AICTE, New Delhi and Affiliated to AKTU-Lucknow

SAVJC
SHREE ATAM VALLABH JAIN COLLEGE
LUDHIANA, PUNJAB
AFFILIATED TO PANJAB UNIVERSITY, CHANDIGARH
Managed by Shri Atam Nand Jain School Committee

इन्दिरा गाँधी विश्वविद्यालय
INDIRA GANDHI UNIVERSITY
MEERPUR, REWARI
मीरपुर, रेवाड़ी
सा विद्या या विमुक्तये

MAHARAJA AGRASEN INSTITUTE OF TECHNOLOGY
MAIT

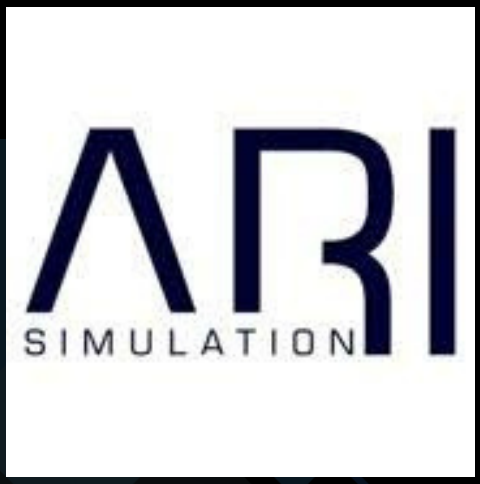
IITM
Nurturing Excellence

NSG
सर्वत्र सर्वोत्तम सुरक्षा

GIET UNIVERSITY
GUNUPUR, ODISHA
EXCELLENCE - OUR ESSENCE

aws

CLIENTS AND PARTNERS



FRANCHISE

Build the Future of Cybersecurity Education
Cybersecurity is no longer optional—it's a necessity. With rising cyber threats and increasing demand for skilled professionals, CyberYaan Training & Consultancy is on a mission to empower the next generation with industry-ready skills.

Now, you can be a part of this fast-growing revolution.

1. Join our franchise network and grow your business with our proven success.

2. Explore franchise opportunities—connect with us to embark on a thriving partnership.

Email: info@cyberyaan.com

CONTACT US

+91 7428748576

training@cyberyaan.com

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

SCAN ME

Youtube

Linkdin

Instagram

www.cyberyaan.com