CYBERYAAN
TRAINING & CONSULTANCY

Cyber Security 1 Year Diploma v2.0 with A.I.

The 1-Year Diploma in Cyber Security v2.0 provides foundational knowledge and hands-on skills in protecting networks, systems, and data from cyber threats, with an updated curriculum focused on the latest security trends and technologies.

For More Information
☎ +91-7428748576
✉ training@cyberyaan.in

1. Networking Fundamentals

- Introduction to Cybersecurity
- Networking Models & Types
- OSI and TCP/IP Model Overview
- Understanding IP Addressing & Subnetting
- Packet Structure and Protocols (IP, TCP, UDP, ICMP)
- Network Devices: Routers, Switches, and Firewalls
- Network Topologies and Architectures
- NAT, DNS, and DHCP Fundamentals
- Port Forwarding and IP Routing Explained
- Network Security Fundamentals (Firewalls, IDS/IPS, Proxies, VPNs)
- Network Address Translation (NAT) and Security Implications
- Introduction to Wireshark and Packet Capture Analysis
- Introduction to Network Scanning (Nmap, Zenmap)
- Setting Up a Simple Network Attack Simulation Lab
- Detecting Common Network Attacks (DDoS, Spoofing, MITM)
- Preventing Network Attacks (DDoS Mitigation, Firewalls, IDS/IPS)
- Real-World Network Security Best Practices (Securing Routers, Firewalls)

Network Fundamentals refer to the core principles, technologies, and protocols that enable devices to communicate and share resources within a connected system. It encompasses the design, implementation, and management of networks, focusing on how data is transmitted, routed, and secured across wired or wireless connections.

2. Linux for Cybersecurity

- Setting Up Virtual Labs (VirtualBox, VMware, ISO Installation)
- Introduction to Linux (Shell, CLI vs GUI, Distributions)
- Basic Linux Commands (pwd, cd, ls, cp, mv, rm)
- File and Directory Management (mkdir, touch, nano, cat, less)
- User & Group Management (adduser, usermod, groups)
- File Permissions & Ownership (chmod, chown, umask)
- Linux File System Hierarchy & Navigation
- Process Management (ps, top, kill, nice, jobs)
- Package Management (apt, yum, dpkg, snap)
- Networking Basics (IP, DNS, Gateway, netplan)
- Network Commands (ping, netstat, traceroute, ss, ifconfig/ip)
- Essential Security Tools (nmap, netcat, tcpdump, whois)
- Bash Scripting Fundamentals (Variables, Loops, Conditions)
- Automation with Bash (Practical Scripts & Crontab Jobs)
- System Logs & Monitoring (journalctl, syslog, logrotate)
- Hardening Linux Systems (UFW, Fail2ban, SELinux, AppArmor)

Linux is an open-source operating system widely used in cybersecurity due to its flexibility, stability, and robust security features. It serves as the foundation for many security tools, penetration testing frameworks, and secure server environments.

3. Python Programming Language

- 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 is a high-level, interpreted, and general-purpose programming language known for its simplicity, readability, and versatility. Created by Guido van Rossum in 1991, Python emphasizes code readability through its clean, English-like syntax and indentation-based structure.

4. Ethical Hacking

- Introduction to Packet Sniffing (Wireshark, tcpdump)
- Analyzing Live Network Traffic
- ARP Spoofing and MITM Attacks
- DNS Spoofing and Poisoning Techniques
- Information Gathering (Active & Passive)
- Understanding Port Scanning (SYN, ACK, FIN Scans)
- Using Nmap for Advanced Network Reconnaissance
- Packet Crafting and Injection (Scapy, Hping3..)
- Network Tunneling and Evasion Techniques
- Wireless Security Protocols (WEP, WPA, WPA2)
- Wireless Network Cracking
- Evil Twin Attacks and Rogue Access Point Setup
- Network Defense Mechanisms (Segmentation, VLANs, NAC)
- Setting Up IDS/IPS Systems (Snort, Suricata)
- Detecting and Responding to Network Attacks
- Final Lab: Full Network Penetration Testing Simulation

Ethical Hacking refers to the authorized and legal practice of bypassing system security to identify potential vulnerabilities and threats in a network or computer system. Unlike malicious hacking, ethical hacking is performed with the explicit permission of the organization or individual owning the system, with the goal of improving security rather than exploiting it.

5. Active Directory Training

- 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 Training refers to structured learning programs designed to teach IT professionals how to install, configure, manage, and secure Microsoft Active Directory, a critical directory service used in Windows-based networks. AD is essential for user authentication, authorization, and centralized management of network resources (users, computers, groups, policies, etc.).

6. Web Application Hacking

- Introduction to HTTP/HTTPS (Request Methods, Headers)
- 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 (XSS)
- 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 Hacking refers to the process of identifying, exploiting, and mitigating security vulnerabilities in web applications (websites, APIs, or web services) to assess their security posture. Unlike malicious hacking, ethical hackers perform these tests with permission to improve defenses, while cybercriminals exploit flaws for data theft, fraud, or service disruption.

7. 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 refers to the process of exploiting vulnerabilities in an Application Programming Interface (API) to gain unauthorized access, manipulate data, disrupt services, or extract sensitive information. APIs act as intermediaries between different software systems, and if not properly secured, they can become prime targets for attackers.

8. Digital Forensics

- Introduction to Digital Forensics & Chain of Custody
- Understanding Incident Response Lifecycle
- Memory Acquisition Techniques
- Memory Analysis using Volatility Framework
- Disk Imaging and Evidence Preservation
- File System Forensics (NTFS, FAT32, EXT)
- Using Tools: FTK Imager & Autopsy for Disk Analysis
- Windows Registry Forensics
- Log Analysis and Event Correlation
- Network Forensics (Analyzing PCAP files)
- Investigating Email Headers and Artifacts
- Malware Analysis
- Mobile Forensics
- Reporting & Documentation
- Final Lab: Full Digital Forensics Investigation Simulation

Digital Forensics is the scientific process of identifying, preserving, analyzing, and presenting digital evidence from electronic devices and storage media in a legally admissible manner. It is used in criminal investigations, cybersecurity incidents, civil litigation, and corporate compliance to uncover facts about digital activities.

9. Dark Web Investigation

- Introduction to the Dark Web and Its Ecosystem
- Differences Between Surface Web, Deep Web & Dark Web
- Installing and Configuring Tor Browser Safely
- Navigating Onion Services and Directories
- Accessing and Analyzing Dark Web Marketplaces
- Identifying Illegal Listings and Activities
- Introduction to OSINT in Dark Web Investigations
- Collecting Intel & Monitoring Threat Actors
- Cryptocurrency Basics for Dark Web (Bitcoin, Monero)
- Tracking Crypto Transactions (Wallets, Mixers, Explorers)
- Tools for Dark Web Monitoring & Alerts
- Final Case Lab: Simulated Dark Web Investigation

Dark Web Investigation refers to the process of monitoring, analyzing, and gathering intelligence from hidden online networks (such as Tor, I2P, and Freenet) to uncover illegal activities, track cybercriminals, and support law enforcement or cybersecurity operations.

10. Red Teaming and Blue Teaming

Red Teaming (Offensive Security)

- Introduction to Red Teaming & Adversary Simulation
- Phases of the Attack Lifecycle (Initial Access to Impact)
- Reconnaissance Techniques (Passive & Active)
- Weaponization and Delivery Strategies
- Exploitation Techniques (Web, Network, API)
- Post-Exploitation – Privilege Escalation Methods
- Maintaining Persistence (Backdoors, Schedulers, Services)
- Lateral Movement Techniques and Pivoting
- Social Engineering Attacks (Phishing, Pretexting)
- Bypassing Security Controls (EDR/AV Evasion)
- Physical Security Testing & Red Team Toolkits
- Red Team Report Writing and Documentation

Blue Teaming (Defensive Security)

- Introduction to Blue Teaming & Defense Strategies
- Security Operations Center (SOC) Roles & Tools
- SIEM Platforms (ELK, Splunk, Wazuh Basics)
- Log Collection, Normalization, and Correlation
- Threat Intelligence and IOCs (Indicators of Compromise)
- Malware Analysis Fundamentals (Static & Dynamic)
- IDS/IPS Configuration and Alert Tuning
- Endpoint Detection and Response (EDR) Tools
- Incident Detection and Response Process
- Threat Hunting Techniques and Automation
- Building and Executing Incident Response Playbooks
- Final Lab: Red Team vs. Blue Team Simulation

In this module the student get the idea of RED Teaming and BLUE Teaming as well in RED Teaming the student will Learn about all type of penetration testing tools and approaches.

In BLUE Teaming the student will get the idea of Defend Approach and SOC.

11. Cloud Infrastructure & Security

- Introduction to Cloud Computing Models (IaaS, PaaS, SaaS)
- Understanding the Shared Responsibility Model in Cloud Security
- Identifying Key Cloud Security Risks and Challenges
- Hands-On Lab: Setting Up a Basic Cloud Infrastructure (AWS or Azure)
- Introduction to Major Cloud Providers (AWS, Azure, GCP)
- Cloud Identity and Access Management (IAM) Fundamentals
- Role-Based Access Control (RBAC) and Permissions Management
- Best Practices for Managing Cloud Identities and Permissions
- Multi-Factor Authentication (MFA) in the Cloud
- Securing Cloud Storage and Databases
- Cloud Encryption Techniques and Data Protection Strategies
- Data Backup and Disaster Recovery in the Cloud
- Cloud-Native Security Tools (Security Groups, VPCs, IAM Policies)
- Threat Monitoring and Detection in Cloud Environments
- Incident Response in Cloud-Based Systems
- Hands-On Lab: Configuring Cloud Security Tools and Monitoring

Cloud Infrastructure refers to the hardware and software components (servers, storage, networking, virtualization, and management tools) that enable cloud computing services. These resources are hosted remotely by providers like AWS, Azure, or Google Cloud and delivered over the internet.

12. Capstone Project & Final Exam (4 Weeks)

1. Hands-on Project: Full Penetration Testing

- Perform a full penetration test on a virtual environment
- Identify vulnerabilities, exploit them, and conduct post-exploitation tasks
- Report writing and documentation of findings

2. Post-Exploitation Tasks

- Analysis of compromised systems
- Gathering evidence and conducting forensics on the compromised system

3. Final Exam Preparation

- Review all theoretical and practical aspects of the course
- Hands-on practice sessions to solidify knowledge before the final exam

4. Final Exam

- A comprehensive exam covering both theory and practical skills learned throughout the course

Services

Web Application Testing

API & Web Service

Source Code Review

IOT Device Security

Vulnerability Management

Security Operations

Fraud Investigation

ISO 27001 Compliance

Security Infrastructure

Mobile app Security Testing

Threat Management

Firewall Security Review

Cloud Serurity Assesment

Network Penetration

Managed IT Security

Database Assesment

SCADA & ICS System

Ai Machine Learning

Clients and Partners

OFFENSIVE security

EC-Council

भारतीय वायु सेना
नभः स्पृशं दीप्तम्

CISCO

CompTIA

GURUGRAM UNIVERSITY
गुरुग्राम विश्वविद्यालय
विद्या जीवनाय न तु जीविकाय

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

SRI AUROBINDO COLLEGE
तमसो मा ज्योतिर्गमय
UNIVERSITY OF DELHI
Sri Aurobindo College

eSec Forte®

4ACHiEVERS

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

PELORUS
Enabling Technology in the Right Direction

GNIOT
Group of Institutions
Since 2001
GNIOT
GROUP OF INSTITUTIONS
Approved by AICTE & PCI, New Delhi and Affiliated to AKTU-Lucknow, GGSIPU-New Delhi & BTE-Lucknow

IITM
Nurturing Excellence

Maharaja Agrasen
Institute of Technology

NSG
सर्वत्र सर्वोत्तम सुरक्षा

aws

GIET UNIVERSITY
GUNUPUR, ODISHA
EXCELLENCE · OUR ESSENCE
2018

OSFA
IT Solutions Pvt. Ltd.

KLTIF
KL Technology
Incubators Foundation

Gallery

GLA University - Mathura

GNA University - Punjab

SGTBIMIT - Delhi

CT Group Institute - Jalandhar

Shree Atam Vallabh Jain College- Ludhiana

eryaan had the honor of sharing knowledge and learning alongsid
esteemed Principal, Prof. (Dr.) Vishal Kumar, SACCM"
Sri Aurobindo College - Ludhiana

GNIOT - Greater Noida

GIET University - Odisha

Guru Jambheshwar University - Hisar

GAIL (India Limited) - Noida

Microsoft Azure - Gurugram

NSG - Manesar

Placements

Pranav

CYNOX SECURITY

Placed in Cynox Security
as a Security Analyst Trainee

Harsh Verma

HALOOCOM

Placed in Haloocom
as a Technical Support
Implementation Engineer

Indiverpal

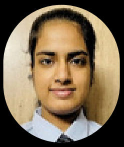
CeTF

Placed in CETF
as a Digital Forensic
Examiner Trainee

Isha

CYWARDEN

Placed in cywarden inc
as a Security Analyst



Himadri

CeTF

Placed in CETF
as a Digital Forensic
Examiner - Trainee

Arshpreet Kaur

CYNOX SECURITY

Placed in CYNOX Security
as a Cybersecurity Analyst

Harsh Vardhan Verma

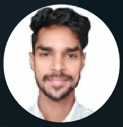
CISAI

Placed in CISAI
SOC Analyst

Dinesh Kumar

Infosys

Placed in Infosys
as a Cyber Security Analyst



Suraj Ashok Rathor

CYNOX SECURITY

Placed in CYNOX Security
as a Security Analyst - Trainee

Pratik

Placed in Indian Army
as a Security Analyst

Ritik Chaudhary

SBI

Placed in SBI
as a Security Analyst

Hansika Rawat

CYNOX SECURITY

Placed in CYNOX Security
as a Cybersecurity Analyst

CONTACT US

☎ +91 7428748576

✉ training@cyberyaan.in

🌐 www.cyberyaan.com

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

📍 Entry Gate No-1 , 2nd Floor, Gaurav Plaza,
opp. Metro Pillar No-50, near Guru
Dronacharya Metro Station, Sikanderpur,
DLF Phase 1, Gurugram, Haryana 122002

📍 First Floor, Gurudwara Service Lane,
1/56A, Vikas Marg, next to Joey's Hostel
and Topper's Institute, Lalita Park,
Laxmi Nagar, Delhi, 110092

📍 Sector-7, Pocket E-1/9, 3rd Floor, Opp.
M2K Cinema Hall, Rohini, Delhi - 110085

FRANCHISE

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.in