

Unlock Your Future: Cyber security Course

Prepare to embark on an exciting journey into the world of cybersecurity! Our Cyber security Course is meticulously designed to provide you with the essential skills and knowledge to safeguard digital systems, networks, and data against sophisticated cyber threats. This document offers a comprehensive overview of the course, its benefits, and the career opportunities it unlocks.



Ecorporate Trainings
Transforming learners into leaders.

CYBER SECURITY PROGRAM

About Ecorporate Trainings:-

Ecorporate Trainings leading e-learning platform providing live instructor-led interactive online training. We cater to professionals and students across the globe in categories like Big Data & Hadoop, Business Analytics, cybersecurity, NoSQL Databases, Java & Mobile Technologies, System Engineering, Project Management and Programming. We have an easy and affordable learning solution that is accessible to millions of learners.

Ecorporate Trainings Masters Program will provide you in-depth knowledge of front-end and back-end technologies including JavaScript, HTML, CSS, NodeJS, Python, cyber security, AngularJS, MongoDB and many more thereby making you an expert full stack web developer. The program provides access to 200+ hours of interactive online learning, 10+ industry-based use cases, skills specific assessments and other resources. There are no prerequisites for enrollment to the Masters Program. It is designed and developed to accommodate diverse professional backgrounds. Our Masters Program recommends the ideal path for becoming a Full Stack Developer, however, it is learner's preference to complete the courses in any order they intend to.



Ecorporate Trainings
Transforming learners into leaders.



Why Cyber security Now?

High Demand

The digital landscape is expanding rapidly, leading to an unprecedented demand for skilled cybersecurity professionals. Companies are desperately seeking experts to protect their valuable assets.

Evolving Threats

Cyber threats are becoming more complex and frequent. Learning cybersecurity means you'll be at the forefront of defending against these constantly evolving dangers.

Impactful Career

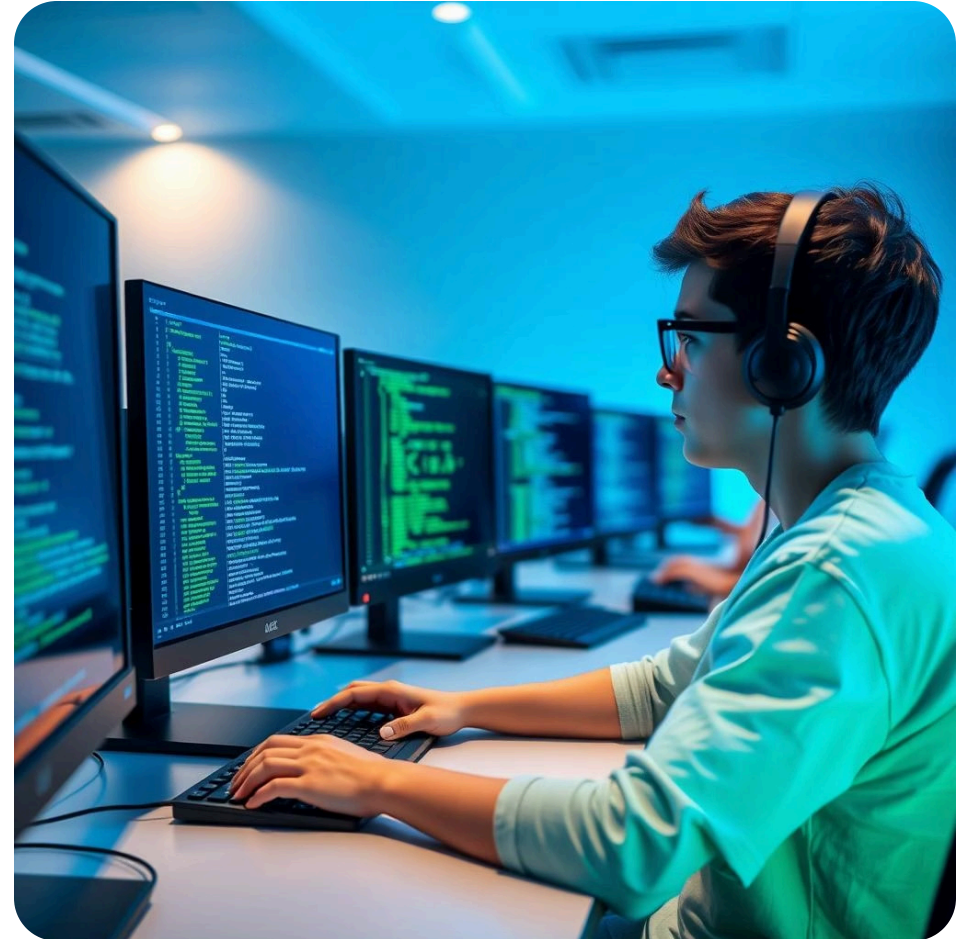
A career in cybersecurity offers the chance to make a real difference, protecting individuals and organisations from devastating attacks. It's a field with purpose and constant innovation.

Cybersecurity is not just a job; it's a critical global need. Join us to become a vital part of the solution in this dynamic and rewarding field.

Course Overview: What to Expect

Our comprehensive Cybersecurity Course is tailored for both beginners and experienced IT professionals aiming to enhance their skills. The curriculum covers foundational concepts to advanced techniques, ensuring a well-rounded learning experience.

- Interactive lectures and practical demonstrations
- Hands-on labs and real-world case studies
- Expert instructors with industry experience
- Access to a dedicated online learning platform



We believe in learning by doing, which is why our course heavily emphasises practical application and hands-on experience.

Key Learning Modules



Introduction to Cyber Security

- What is Cyber Security?
- Importance of Cyber Security
- Cyber Security Domains
- CIA Triad
- Vulnerability, Threat and Risk

Linux Essentials

- History and Features of Linux
- Architecture of Linux OS
- Linux Distributions
- Linux Command Line
- Software Package Management

Linux Administration

- File System
- Users and Groups
- File/Folder Permissions
- Special Permissions
- Disk Management
- Service and Process Management

Networking Fundamentals

- Computer Networks and Types of Networks
- Network Devices
- IP and MAC Address
- IPv4 and IPV6 Packet Structure
- Addressing and Subnetting
- OSI Model and TCP/IP Model
- Network Protocols (TCP, UDP, ICMP, ARP)
- Network Services (DNS, DHCP, SNMP, FTP)
- Packet Analysis using Wireshark

Network Security

- Internet, Intranet, and Extranet
- DMZ
- DNSSEC
- Firewalls
- IDS, IPS and IDPS
- VPN and tunneling
- Network Address Translation (NAT) and PAT
- Honeypots & Deception Technology
- Practical Assignment - I

Vulnerability Management

- Fundamentals of Vulnerability Assessment and Management
- Vulnerability Assessment tool Deployment Strategy
- Scanning Methodologies
- Authenticated vs Non-Authenticated Scanning
- Planning and Performing Infrastructure Security Assessment
- Interpreting and Calculating CVSS Score
- Risk Identification and Categorization
- Reporting
- Patches and Updates

Network Penetration Testing

- Introduction to Penetration Testing
- Types of Penetration Testing
- Pentesting Services
- Penetration Testing Phases
- Pre-Engagement Actions
- OSINT
- Exploitation (Automated)
- Password Cracking

Advanced Network Pentesting

- Manual Exploitation of System Vulnerabilities
- Post-Exploitation
- Privilege Escalation (Linux and Windows)
- Pivoting and Double Pivoting
- Resolution & Retesting
- File Security

Cryptography

- Introduction to Cryptography
- Symmetric Ciphers
- Asymmetric Ciphers
- Pseudo-Random Number Generator
- Building SSL certificates
- Digital Certificates and Digital Signatures
- Disk Encryption
- Hashing
- Encoding
- Steganography

Active Directory Pentesting

- Introduction to Active Directory
- Active Directory Setup
- Active Directory Enumeration
- Kerberos Authentication
- Active Directory Attack Vectors
- Active Directory Post Enumeration
- Active Directory Post Attacks
- AD Defense- Detection

Cyber Security Compliance

- Cyber Security Compliance (GDPR, HIPAA, SOX)
- ISO IEC 27001/ISO 27002
- PCI-DSS
- Penetration Testing Standards (OWASP, WASC, SANS25, PTES, OSSTMM)
- Risk Governance & Risk Management
- Cyber Crime & Classification of Cyber Crimes
- NIST Cybersecurity Framework
- Case Studies
- Practical Assignment - II & Capture The Flag (CTF) - I

Web Fundamentals

- Web application Technologies
- Web Application offence and defence
- Web Reconnaissance
- Web Application Vulnerability Assessment
- CMS Enumeration and Exploitation
- Tools - Nikto, OWASP-Zap, gobuster, wpscan

Web Application Pentesting

- OWASP Top 10 Web Risks
- Web Application Pentesting Checklist
- Authentication & Authorization
- Session Management
- File Security
- Web Application Firewalls
- Tools - BurpSuite, Sqlmap, wafw00f
- Practical Assignment - III & Capture The Flag (CTF) - II

Mobile Application Pentesting

- Android OS Architecture
- IOS Architecture
- Android app structure
- Rooting Concept
- Compromising Android OS with malware
- Android Application Reverse Engineering
- Android App Penetration Testing

Wi-Fi Security

- Wi-Fi Security
- Aircrack-ng Essentials
- Attacking Wi-Fi security protocols (WEP, WPA/WPA2)
- Rogue Access Points
- Attacking Captive Portals

Social Engineering

- Phishing Attacks
- Social Engineering Campaigns
- Human based attacks
- Defense against Social Engineering

Cloud Security

- Architectural Concept and Design Requirements
- Deployment Models and Security
- Cloud Platform and Infrastructure Security
- Container Security
- Cloud Data Security
- Legal and Compliance Implications

Scripting Basics for Pentesting

- Basics of Shell Scripting
- Basics of Python Programming
- Automating Pentesting with Python

Binary Exploitation

- Understanding Buffer Overflow
- Exploiting Buffer Overflow Vulnerability
- Writing Exploit Code using Python

Security Operations (QRadar & Splunk)

- BM Qradar - Log Analysis
- IBM Qradar - Network/Flow Analysis
- Offense Management
- SOC Analysis using Splunk
- Data Visualization with Pivots and Databases
- Search Processing Language Basics
- Splunk Knowledge Objects
- Generating Alerts
- Practical Assignment - IV

Threat Analysis and Risk Management

Learn to identify, assess, and mitigate various cyber threats and vulnerabilities, developing strategies to minimise organisational risk.

- **Introduction to Information Security**
 - Definition of threats, vulnerabilities, and risks
 - Security triad: Confidentiality, Integrity, Availability (CIA)
- **Types of Threats**
 - Internal vs. External threats
 - Malware, Phishing, Social Engineering
 - Insider threats
 - Advanced Persistent Threats (APT)
- **Risk Management Fundamentals**
 - Risk Identification
 - Risk Assessment & Analysis (Qualitative & Quantitative)
 - Risk Mitigation strategies
 - Risk Acceptance, Transfer, Avoidance
- **Threat Modeling**
 - STRIDE model (Spoofing, Tampering, Repudiation, etc.)
 - DREAD model (Damage, Reproducibility, Exploitability, etc.)
 - Attack surface identification
- **Vulnerability Assessment**
 - Vulnerability scanning tools
 - CVE, CVSS scoring system
 - Patch management
- **Security Controls & Countermeasures**
 - Administrative, Technical, Physical controls
 - Preventive, Detective, and Corrective controls
- **Incident Response Planning**
 - Threat detection & monitoring
 - Incident response lifecycle
 - Post-incident review & reporting
- **Risk Management Frameworks**
 - NIST RMF
 - ISO/IEC 27005
 - FAIR (Factor Analysis of Information Risk)
- **Business Impact Analysis (BIA)**
 - Identifying critical assets & processes
 - Estimating potential impact of threats
- **Compliance & Legal Considerations**
 - Data protection regulations (GDPR, HIPAA, etc.)
 - Security audit & governance

Ethical Hacking and Penetration Testing

Master the techniques used by ethical hackers to find weaknesses in systems, all within a legal and ethical framework for defensive purposes.

Sure! Here's a concise list of **topics for Ethical Hacking and Penetration Testing**, ideal for course outlines, training programs, or study planning:

Introduction to Ethical Hacking

- What is Ethical Hacking?
- Types of Hackers (White, Black, Grey Hat)
- Legal & Ethical Issues
- Phases of Ethical Hacking

Footprinting & Reconnaissance

- Passive vs. Active Reconnaissance
- WHOIS, DNS Enumeration
- Google Hacking (Dorking)
- Social Engineering Basics

Scanning & Enumeration

- Network Scanning (Nmap, Angry IP Scanner)
- Port Scanning & Service Detection
- Banner Grabbing
- Enumeration of Users, Shares, and Services

Vulnerability Analysis

- Vulnerability Scanning Tools (Nessus, OpenVAS)
- Identifying known vulnerabilities (CVEs)
- Misconfigurations and Patch Gaps

System Hacking

- Password Cracking (John the Ripper, Hydra)
- Privilege Escalation Techniques
- Keyloggers, Backdoors, and Rootkits
- Clearing Logs & Covering Tracks



Web Application Hacking

- OWASP Top 10 (SQL Injection, XSS, CSRF, etc.)
- Tools: Burp Suite, OWASP ZAP
- Input Validation Bypass
- Directory Traversal & File Inclusion Attacks

Wireless Network Hacking

- Wi-Fi Cracking (WEP/WPA/WPA2)
- Packet Sniffing (Wireshark, Aircrack-ng)
- Rogue Access Points

Sniffing & Spoofing

- ARP Poisoning
- DNS Spoofing
- MAC Spoofing
- Packet Capture Techniques

Social Engineering

- Phishing Techniques
- Pretexting & Baiting
- Human Manipulation Attacks

Denial-of-Service (DoS) Attacks

- DoS vs DDoS
- Botnets & Flooding Tools
- Mitigation Techniques

Penetration Testing Process

- Planning & Scoping
- Exploitation & Post-Exploitation
- Reporting & Documentation
- Pen Testing Methodologies (PTES, OSSTMM)

Tools and Platforms

- Kali Linux
- Metasploit Framework
- Netcat, Nikto, SQLmap
- Exploit-DB and GitHub Repos



Real-time Case Studies and Practical Projects

Apply your knowledge to solve complex, real-world cybersecurity challenges through engaging case studies and hands-on projects.



Real-time Case Studies and Practical Projects

Apply your knowledge to solve complex, real-world cybersecurity challenges through engaging case studies and hands-on projects.

Tools and Technologies You'll Master

Our course provides hands-on experience with industry-standard tools and platforms, ensuring you're job-ready upon completion.



Wireshark

Deep dive into network traffic analysis.



Kali Linux

The leading penetration testing distribution.



Metasploit

Exploit and vulnerability assessment framework.



Security Suites

Explore various commercial security tools.

Proficiency in these tools is crucial for any aspiring cybersecurity professional.



Ecorporate Trainings
Transforming learners into leaders.

Your Career Launchpad

Beyond technical skills, our course offers comprehensive career support to help you successfully transition into a cybersecurity role.



Resume Building

Craft a compelling resume that highlights your new skills.



Interview Preparation

Gain confidence for technical and behavioural interviews.



Career Path Guidance

Explore diverse roles and chart your professional journey.

Whether you aspire to be a Cybersecurity Analyst, Ethical Hacker, or Security Engineer, this course will equip you for success.

Cyber security Career Paths

A cybersecurity qualification opens doors to a wide array of exciting and high-paying positions. Here are some of the most sought-after roles:

Cybersecurity Analyst: Monitors security systems, analyses threats, and responds to incidents.

Ethical Hacker / Penetration Tester: Tests systems for vulnerabilities to strengthen defences.

Security Engineer: Designs, builds, and implements secure network and system architectures.

Incident Responder: Manages and mitigates cyber attacks as they occur.

Forensic Investigator: Gathers and analyses digital evidence for legal purposes.

Security Consultant: Advises organisations on their cybersecurity strategies and implementations.

The demand for these roles continues to grow exponentially across all industries.

CERTIFICATION AND CAREER ADVANTAGE

Upon successful completion of the **CYBER SECURITY** Course, you will be awarded an industry-recognised certification from Ecorporate Trainings. This certification is a testament to your acquired expertise and serves as a valuable credential to significantly boost your CV and enhance your career prospects in the competitive tech landscape.

Our certification validates your skills across the crucial areas of cloud computing, signalling to potential employers that you possess the practical knowledge required for immediate impact. It sets you apart, demonstrating your commitment to professional development and your readiness to tackle complex cloud challenges.

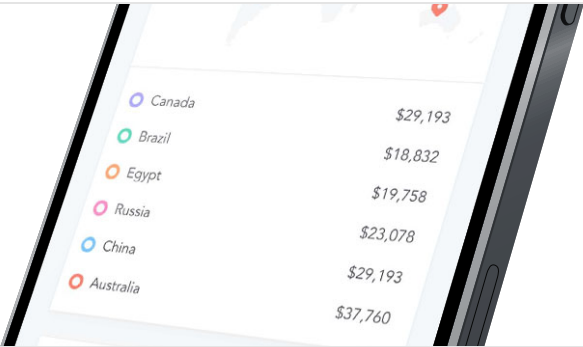



Ready to join..!

The future of digital security depends on skilled professionals, and your journey to becoming one starts here! We are excited to welcome you to our Cyber security Course.

Stay tuned for more details and enrollment updates. Be the first to know when registration opens by following our announcements!

To know more...



 Ecorporate Training

[Home | Ecorporate Training](#)

Our mission is to provide learners with the best corporate learning experience. Comprehensive resources & tutorials, a vibrant community, 24/7 assistance mak...



+91 9663241204.



mail Id: ecorporatetrainings@gmail.com



Ecorporate Trainings
Transforming Leannens into Leaders.

 Twitter

[ecorporate trainings](#)

Transforming Learners into Leaders 🇫🇷 Your on...



Ecorporate Trainings
Transforming Leannens into Leaders.

 [www.facebook.c...](#)

[Ecorporatetrainings...](#)

Ecorporatetrainings Softwaresolutions is on...




Ecorporate Trainings
Transforming Leannens into Leaders.

 Instagram

[Instagram \(@ecorpo...](#)

Instagram photos and videos

orporate Tr
ansforming leannens

 Bluesky Social

[ecorporatetraining...](#)