AIT
Challenging the convention

CYBER SECURITY COURSE

Career in Cyber Security

Why Build a Career in Cybersecurity?

Demand is So High
For Cybersecurity Pros

There are 3.5 million unfilled cybersecurity jobs globally. There is a shortage of talent and this market has 0% unemployment.

8+ Job Roles
& Career Paths

Opportunity to work in almost every industry and across various roles like Security Admin, Cybersecurity Analyst, Security Consultant, and 5+ more roles.

5.1 Lakh Per Annum
Average Salary

The average salary of a Certified Cyber Security in India is INR 5.10 LPA. In top countries, it is more than $50,920.

Guaranteed Growth
in Job and Career

By acquiring the right skills, you can be on your way to building a fast-growing career in the field of cybersecurity.

Work Remotely
for International Companies

Numerous brands and organizations around the world hire ethical hacking professionals for remote work and offer a lucrative package.

Opportunities in Both
Public & Private Sectors

As a cybersecurity professional, you have the opportunities to work in both public and private sector organizations of all sizes.

Who Can Learn **Cyber Security?**

Learning Cyber Security becomes easier for you with proper guidance & advanced projects by ANSH InfoTech's cybersecurity expert trainers. You can acquire this skill if you are:

College Student

Start shaping your career right from college time by learning in demand cyber security skills.

Graduate

Time for you to upskill, prepare yourself for a bright future, and kickstart a career in cyber security.

College Dropout

Not sure which career is right for you? Not finding any jobs? Learn cyber security with us to instantly land your first job.

Looking to Switch Career

Not satisfied with your current job profile? Switch to cyber security, one of the most demanded and highly-paid skills.

A Brief About
ANSH InfoTech

India's Most Trusted IT Training Institute

Ansh InfoTech is a leading IT training and software development company based in Ludhiana, Punjab, India. Since 2014, Ansh InfoTech has trained over 1.5k students and provided internship opportunities to over 4,500 candidates.

Additionally, Ansh InfoTech is one of the fastest growing tech-enabled company in Ludhiana.

With its expert team of trainers in various technical fields like Ethical Hacking, Web Development, Data Science, Digital Marketing, and many more. Company has helped thousands of students from India and other Asian countries acquire new skills and explore high-paying career opportunities.

Our learners work for top brands, companies and unicorns across India and around the world.

Why Learn **Cyber Security with ANSH InfoTech** Only?

Trusted by **1.5+ Million** Learners

We are the #1 preference of more than 15 lakh learners in India and Asian countries. Our training quality and support system intrigue learners.

Completely **Practical-Oriented**

Cyber Security is a skill that requires immense practice. For that, we offer 100% practical training with regular assignments, assessments, and projects.

Online and **Offline Batches**

Cyber Security is a skill that requires immense practice. For that, we offer 100% practical training with regular assignments, assessments, and projects.

Comprehensive **Curriculum**

The Cyber Security course by ANSH InfoTech includes India's most comprehensive curriculum, covering all breadths and depths in detail & practically.

Job Assistance

On course completion, we assist you with job interviews and resume building. Next, your interviews are arranged with top companies to help you land the job easily.

Expert Trainers

You will learn ethical hacking from expert trainers having 10+ years of experience in the field. We ensure high-quality training always.

Industry-Recognized Certification

The certificate you receive on course completion is valid nationally and internationally. You can easily share it, add it to your resume, and explore great opportunities.

Hands-On Live Projects

You will apply all the practices on real websites (no dummies), do everything on your own, and make use of premium tools.

Cyber Security Course Curriculum

Master all Concepts of CYBER SECURITY!

Module 01

INTRODUCTION TO CYBERSECURITY

- Overview of cybersecurity fundamentals
- Importance of cybersecurity in today's digital landscape
- Common cybersecurity threats and attack vectors
- Introduction to cybersecurity best practices and frameworks

Module 02

NETWORKING FUNDAMENTALS

- Basics of computer networks and network topologies
- TCP/IP protocol suite and OSI model
- IP addressing and subnetting
- Introduction to network devices (routers, switches, firewalls)

Module 03

VIRTUALIZATION

- Introduction to virtualization technologies
- Benefits of virtualization in cybersecurity
- Virtual machine (VM) creation and management
- Networking and security considerations for virtualized environments

Module 04

LINUX FUNDAMENTALS

- Introduction to Linux operating system
- Linux command-line basics and shell scripting
- User and group management in Linux
- Linux file system and permissions

ETHICAL HACKING

Module 01

INTRODUCTION TO ETHICAL HACKING

- Overview of ethical hacking and its importance
- Differentiating ethical hacking from malicious hacking
- Understanding the legal and ethical aspects of ethical hacking
- Introduction to hacking methodologies (reconnaissance, scanning, exploitation, post-exploitation)

Module 02

INFORMATION GATHERING AND VULNERABILITY ASSESSMENT

- Passive and active information gathering techniques
- Open-source intelligence (OSINT) and reconnaissance
- Vulnerability scanning and assessment tools (e.g., Nmap, Nessus)
- Analyzing and interpreting vulnerability scan results

Course Curriculum

Module 03

EXPLOITATION AND PENETRATION TESTING

- Understanding common exploitation techniques
- Exploiting vulnerabilities in web applications and network services
- Post-exploitation activities and privilege escalation
- Introduction to penetration testing methodologies (black-box, gray-box, white-box testing)

Module 05

MAN-IN-THE-MIDDLE (MITM) ATTACKS

- Understanding MITM attacks and their implications
- ARP spoofing and DNS spoofing
- SSL/TLS interception and certificate spoofing
- MITM attack detection and prevention techniques

Module 07

REVERSE ENGINEERING AND MALWARE ANALYSIS

- Introduction to reverse engineering concepts
- Static and dynamic malware analysis techniques
- Decompilation and disassembly of executable files
- Malware behavior analysis and detection techniques

Module 04

WIRELESS HACKING

- Wireless network fundamentals and security protocols (WEP, WPA, WPA2)
- Wireless network reconnaissance and cracking techniques
- Wireless network exploitation and attack scenarios
- Securing wireless networks and mitigating wireless attacks

MODULE 06

DENIAL OF SERVICE (DOS) AND DISTRIBUTED DENIAL OF SERVICE (DDOS) ATTACKS

- Introduction to DoS and DDoS attacks
- DoS attack techniques (e.g., ICMP flood, SYN flood)
- DDoS attack vectors and amplification techniques
- Mitigation and defense against DoS and DDoS attacks

CYBER SECURITY

Module 01

INTRODUCTION TO CYBERSECURITY AND SECURITY FUNDAMENTALS

- Overview of cybersecurity and its importance in modern organizations
- Security goals: confidentiality, integrity, availability (CIA)
- Risk management principles and methodologies
- Security policies, standards, and frameworks (e.g., NIST, ISO 27001)

Course Curriculum

Module 02

NETWORK SECURITY

- Network architecture and design principles with a security focus
- Network security devices and technologies (firewalls, IDS/IPS)
- Network segmentation and isolation techniques
- Network monitoring and incident response

Module 03

SECURE APPLICATION DEVELOPMENT

- Secure coding principles and best practices
- Common web application vulnerabilities (e.g., SQL injection, XSS)
- Secure software development life cycle (SDLC)
- Application security testing techniques (e.g., static analysis, dynamic scanning)

Module 04

DATA PROTECTION AND ENCRYPTION

- Data classification and handling procedures
- Encryption algorithms and protocols (e.g., AES, SSL/TLS)
- Secure key management and distribution
- Data loss prevention (DLP) and data leakage prevention techniques

MODULE 05

INCIDENT RESPONSE AND SECURITY MONITORING

- Incident response process and procedures
- Security information and event management (SIEM) tools
- Log analysis and correlation
- Threat hunting and detection techniques

Module 06

CLOUD SECURITY

- Security considerations for cloud services (IaaS, PaaS, SaaS)
- Cloud security controls and best practices
- Identity and access management (IAM) in the cloud
- Cloud-specific threats and mitigations

Module 07

SECURITY IMPLEMENTATIONS AND BEST PRACTICES

- Security configurations and hardening techniques for various systems (e.g., operating systems, databases)
- Secure network protocols and secure remote access methods
- Implementing secure coding practices in software development
- Security awareness training and promoting a security culture in organizations

Course Curriculum

PENETRATION TESTING

Module 01

INTRODUCTION TO PENETRATION TESTING

- Overview of penetration testing and its importance in cybersecurity
- Penetration testing methodologies (reconnaissance, scanning, exploitation, post-exploitation)
- Legal and ethical considerations in penetration testing
- Introduction to penetration testing tools (e.g., Burp Suite, Metasploit)

Module 02

WEB APPLICATION SECURITY FUNDAMENTALS

- Understanding web application architecture and protocols (HTTP, HTTPS)
- Common web application vulnerabilities (e.g., SQL injection, XSS, CSRF)
- Web application security testing methodologies (black-box, gray-box, white-box testing)
- Web application security tools and scanners (e.g., OWASP ZAP, Nikto)

Module 03

WEB APPLICATION PENETRATION TESTING

- Mapping and analyzing web application attack surfaces
- Exploiting web application vulnerabilities (e.g., SQL injection, XSS, command)
- Session management and authentication testing
- Reporting and documentation of web application vulnerabilities

MODULE 04

ANDROID APPLICATION SECURITY FUNDAMENTALS

- Introduction to Android application architecture and security model
- Understanding Android application components (activities, services, etc)
- Common Android application vulnerabilities (e.g., insecure storage, input validation)
- Android application security testing methodologies(static & dynamic analysis)

Module 05

ANDROID APPLICATION PENETRATION TESTING

- Setting up an Android testing environment
- Analyzing Android application permissions and intent filters
- Exploiting Android application vulnerabilities (e.g., insecure storage, etc)
- Reverse engineering and analyzing Android application binaries

Module 06

ADVANCED PENETRATION TESTING TECHNIQUES

- Network-based attacks (e.g., ARP spoofing, DNS poisoning)
- Wireless network penetration testing
- Exploiting server-side vulnerabilities (e.g., misconfigurations, privilege escalation)
- Active directory attacks and lateral movement techniques

Course Curriculum

Module 07

POST-EXPLOITATION AND REPORTING

- Post-exploitation techniques and maintaining access
- Privilege escalation and pivoting
- Information gathering and data exfiltration
- Reporting and documentation of penetration testing findings

Module 02

WEB APPLICATION SECURITY FUNDAMENTALS

- Web application architecture and protocols (HTTP, HTTPS)
- Common web application vulnerabilities (e.g., SQL injection, XSS, CSRF)
- Web security testing methodologies (manual testing, automated scanners)
- Tools and techniques for identifying security vulnerabilities in web applications

Module 04

ADVANCED BUG BOUNTY TECHNIQUES

- Privilege escalation and lateral movement
- Business logic vulnerabilities and their impact
- API security testing and vulnerabilities
- Mobile application security testing for bug bounty

BUG BOUNTY

Module 01

INTRODUCTION TO BUG BOUNTY PROGRAMS

- Understanding bug bounty programs and their significance
- Different types of bug bounty programs and platforms
- Rules of engagement and scope considerations
- Responsible disclosure and legal considerations

MODULE 03

BUG HUNTING TECHNIQUES

- Reconnaissance and information gathering
- Mapping and analyzing attack surfaces
- Fuzzing and input validation techniques
- Bypassing client-side and server-side security controls

Job/Placement Assistance

Once you complete the Cyber Security Course, you will get advanced placement assistance to help you prepare for the job. We will evaluate your skills, prepare you for the interview, and arrange interviews with top companies.

- **Interview Preparation and Live Practice**
- **Appealing Resume Building**
- **Conducting Interviews at Various Companies**
- **Internship Opportunities**
- **Getting High-Paying Freelance Projects**

Students We've Trained Work at Renowned Companies, Startups, and Brands

Our Students Speak for Us!

Navdeep Khurmi

"I did not have knowledge of hacking & penetration testing before enrolling in this course. However, everything was taught from scratch. Initially, I thought I can't do this. But the way of teaching and content is really simple and great!"

Surmeet Singh

I recently completed a penetration testing training course in Ansh InfoTech, and I am thoroughly impressed. The instructors were highly skilled. The hands-on labs and real-world scenarios allowed me to gain valuable experience.

Divjot Singh

"This is simply the best ethical hacking course. Rishav sir did a great job and put his heart into teaching all concepts of the course. Whenever I had doubts, he was eager to answer and helped me learn easily. Highly recommended."

Disha Kukreja

"The trainer here makes the content easy to learn and answers all the questions during the classes. I learned a lot of important concepts which looked so complex to me when I started. I recommend this course to anyone who wants to learn ethical hacking."

Vijay Rajput

"The trainer here makes the content easy to learn and answers all the questions during the classes. I learned a lot of important concepts which looked so complex to me when I started. I recommend this course to anyone who wants to learn any course in Ansh InfoTech."

Ramandeep Singh

"I would like to thank the trainer and Ansh InfoTech for the enhanced training provided during the entire course. The trainer has brilliant knowledge. The course content covers beginner to pro. Also, sir is a good motivator and friendly person."

Events & Workshops
at ANSH InfoTech

We Are Difference Makers!

Awarding Star Performers

WORKSHOPS











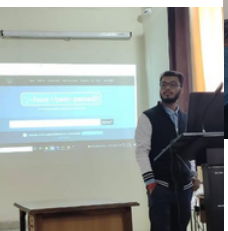

Take Your Career's Most Important Step Today

Towards Building a Thriving Career in **Cyber Security**!

- **Course Duration:** 6 Months

Call Now for more info : +91 94171-68347/ +91 84278-99400

Contacts Us:

www.anshinfotech.org
/Ansh InfoTech
/Ansh Infotech
/anshinfotech