ACE HACKER

Write Great Code

acehacker.com

CYBERSECURITY

acehacker.com/learn/cybersecurity

Embark on an immersive journey from digital novice to cyber-hero with our comprehensive cybersecurity course, designed for all skill levels from beginner to advanced.

This engaging program goes beyond traditional training by weaving in the critical power of Machine Learning, teaching you not just to defend against current threats but to proactively predict and neutralize future attacks.

CHOOSE YOUR LEVEL

Select your starting point - **Beginner**, **Intermediate**, or **Advanced**, and embark on your journey to mastering cybersecurity.

BEGINNER

This is your starting point. This level prepares you for certifications that are designed to build a strong, core understanding of cybersecurity principles, terminology, and essential practices.

INTERMEDIATE

You've got the basics down. This level is for professionals who want to dive deeper into specific domains like ethical hacking, cloud security, or auditing.

ADVANCED

This is the pinnacle of cybersecurity expertise. Advanced certifications are for experienced professionals who manage security programs, oversee risk, and develop strategic security architecture.

CYBERSECURITY

acehacker.com/learn/cybersecurity

Beginner level introduces learners to the fundamentals of cybersecurity, digital safety, and basic defense strategies. Students gain awareness of common cyber threats, system vulnerabilities, and foundational protection methods through interactive labs and real-world scenarios.

After completing the beginner level, you'll have the strong conceptual knowledge needed to ace the most recognized entry-level certifications in the industry. These are your first major credentials on the path to becoming a cybersecurity professional.

This level prepares you for the following certifications:

- **CompTIA Security+:** Ideal for IT professionals and anyone seeking a baseline of security knowledge. It's often considered the first certification one should earn.
- **(ISC)2 Certified in Cybersecurity (CC):** A great choice for students, recent graduates, and career changers looking to enter the cybersecurity workforce.
- **GIAC Information Security Fundamentals (GISF):** Suitable for anyone new to information security who needs to understand fundamental concepts and terminology.
- **Cisco Certified CyberOps Associate (CCCA):** Best for aspiring Security Operations Center (SOC) analysts.

SYLLABUS

Introduction to Cybersecurity

- What is cybersecurity?
- Importance of Cybersecurity in the digital age.
- Key roles and career paths.
- The CIA Triad: Confidentiality, Integrity, and Availability.
- Meet the players: Black Hat, White Hat, and Grey Hat hackers.

Security Principles & Best Practices

- Confidentiality, integrity, availability (CIA Triad).
- Authentication, authorization, accounting (AAA).
- Password hygiene, multi-factor authentication.
- Understanding Antivirus and Anti-malware software.
- Basics of Firewalls and their role.
- Safe Browsing Habits: Spotting suspicious links and websites.

Cyber Hygiene & Safe Practices

- Securing devices (laptops, mobiles, IoT).
- Recognizing phishing attempts.
- Data backup and recovery basics.

Introduction to Cryptography

- What is Encryption and why we need it.
- Symmetric vs. Asymmetric Encryption.
- Understanding Hashing and Digital Signatures.

Cyber Threats & Attacks

- Malware: viruses, worms, Trojans, ransomware.
- Ransomware: The digital hostage crisis.
- Phishing & Spear Phishing: The art of the digital con.
- Social Engineering: Hacking the human mind.
- Denial of Service (DoS) basics.

Network Security Basics

- Firewalls and antivirus tools.
- Basics of VPNs and encryption.
- Securing home and office Wi-Fi.
- What are IP Addresses, DNS, and Ports?
- The TCP/IP Model explained simply.

Introduction to ML in Security

- What is Machine Learning (ML) in simple terms?
- How ML helps in identifying spam and phishing emails.
- Understanding the concept of “normal” vs. "anomaly."

CYBERSECURITY

acehacker.com/learn/cybersecurity

Intermediate level focuses on applying cybersecurity principles in practice. Learners gain hands-on skills in ethical hacking, vulnerability management, network defense, and incident handling. Machine learning concepts are introduced for anomaly detection and smarter defenses.

Designed for practitioners who want to move from theory to application, we'll also dive deep into both offensive (Red Team) and defensive (Blue Team) techniques, equipping you with the tools and mindset to actively hunt for vulnerabilities and defend against sophisticated attacks.

This level prepares you for the following certifications:

- **Certified Ethical Hacker (CEH):** Best for those aspiring to be Penetration Testers and Security Analysts who need to understand an attacker's mindset.
- **CompTIA PenTest+:** A practical certification for Penetration Testers and Vulnerability Analysts that assesses hands-on skills.
- **Certified Cloud Security Professional (CCSP):** A must-have for IT and security professionals who design, manage, and secure data and applications in the cloud.
- **Certified Information Systems Auditor (CISA):** The global standard for professionals in Information Systems Auditing, Control, and Security roles.
- **CompTIA Cybersecurity Analyst (CySA+):** Best for future security analysts focused on threat detection and defense.
- **GIAC Security Essentials (GSEC):** Best for professionals who want strong, practical technical skills in security.

SYLLABUS

Operating System & Application Security

- Securing Windows and Linux systems.
- Patching and updates.
- Application hardening basics.

Ethical Hacking Methodologies

- The Cyber Kill Chain framework.
- Reconnaissance: Gathering intelligence using OSINT tools.
- Scanning & Enumeration: Using tools like Nmap to map networks.
- Exploitation: Gaining access using frameworks like Metasploit.
- Post-Exploitation: Maintaining access and covering tracks.
- Penetration testing lifecycle (reconnaissance → exploitation → reporting).
- Common tools: Nmap, Wireshark, Metasploit.
- Legal and ethical considerations.

Intrusion Detection & Prevention

- IDS vs IPS.
- SIEM tools and log monitoring.
- Anomaly detection using ML basics.

Machine Learning in Cybersecurity (Intro)

- ML for malware detection.
- Spam and phishing email classification.
- Building a Malware Classifier using supervised learning.
- Anomaly Detection in network logs using unsupervised learning.
- Hands-on labs with Python libraries (Scikit-learn, Pandas, TensorFlow).
- Understanding how to train, test, and evaluate ML models for security.

The Blue Team Playbook - Active Defense & Incident Response

- Introduction to Security Information and Event Management (SIEM).
- Reading the signs: Basic log analysis and traffic monitoring.
- Foundations of Digital Forensics and Incident Response (DFIR).
- Creating a basic incident response plan.

Securing the Web - Application Security

- Introduction to the OWASP Top 10 vulnerabilities.
- Hands-on labs for SQL Injection (SQLi) and Cross-Site Scripting (XSS).
- Understanding authentication and session management flaws.
- Secure coding principles.
- Secure network design principles.

Cloud Security Essentials

- Cloud Computing Models: IaaS, PaaS, SaaS.
- Common cloud security threats and misconfigurations.
- Identity and Access Management (IAM) in the cloud (AWS/Azure).
- Container & Kubernetes security basics.

CYBERSECURITY

acehacker.com/learn/cybersecurity

Advanced level is for experienced practitioners ready to transition into leadership and strategic roles. You'll move beyond individual tools and tactics to architecting comprehensive security programs, managing risk at an enterprise level, and leveraging cutting-edge AI to build autonomous, resilient defense systems.

At this level, learners develop expertise in penetration testing, advanced forensics, and leadership roles in security management. This is where you learn to think like a CISO (Chief Information Security Officer).

This level prepares you for the following certifications:

- **Certified Information Systems Security Professional (CISSP):** The gold standard for experienced Security Practitioners, Managers, and Executives like CISOs and Security Directors.
- **Certified Information Security Manager (CISM):** Perfect for professionals who manage an enterprise's information security program, especially those in Information Security Management roles.
- **Offensive Security Certified Professional (OSCP):** A highly respected, hands-on certification for elite Penetration Testers and Ethical Hackers who want to prove their practical hacking skills.

SYLLABUS

Advanced Security Architecture

- Designing secure networks with the Zero Trust model.
- Secure Software Development Lifecycle (SSDLC) and DevSecOps.
- Advanced Endpoint Detection and Response (EDR) strategies.
- Threat Modeling and Security by Design.

Threat Hunting & Intelligence

- Developing and testing hypotheses for threat hunting.
- Leveraging threat intelligence platforms and feeds.
- Malware Reverse Engineering basics.
- Deception technology (Honeypots).

Cloud & IoT Security

- Cloud infrastructure vulnerabilities (AWS, Azure, GCP basics).
- Securing containers and Kubernetes.
- IoT device risks and mitigation.

Governance, Risk, and Compliance (GRC)

- Implementing Security Frameworks (e.g., NIST Cybersecurity Framework, ISO 27001).
- Conducting quantitative and qualitative risk assessments.
- Navigating compliance requirements (e.g., GDPR, HIPAA).
- Communicating risk effectively to executives and the board.

Advanced Red Teaming & Adversary Emulation

- Evading modern security controls (AV, EDR, Firewalls).
- Advanced post-exploitation and lateral movement techniques.
- Attacking and defending Active Directory environments.
- Simulating Advanced Persistent Threats (APTs).

AI & ML for Strategic Defense

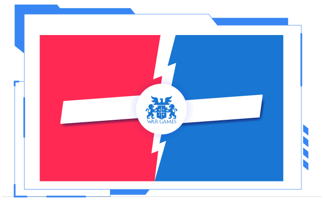
- Using Deep Learning for advanced intrusion detection systems.
- Supervised learning for intrusion classification.
- Unsupervised learning for anomaly detection
- Applying Natural Language Processing (NLP) to analyze threat intelligence reports.
- Deep learning for malware image analysis.
- Introduction to Security Orchestration, Automation, and Response (SOAR).
- Reinforcement learning for automated defense systems.
- Designing and deploying ML-powered security solutions.

CYBERSECURITY

acehacker.com/learn/cybersecurity

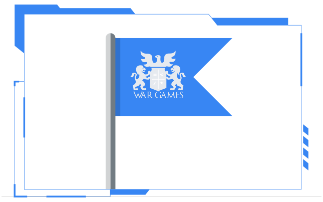
WAR GAMES

You will participate in simulated environments and scenarios that would imitate real-world cyber attacks, defences, and strategies. These games are used to enhance your skills, knowledge, and preparedness in dealing with cyber threats and attacks.



Red Team vs. Blue Team

These simulations involve two teams—the Red Team (attackers) and the Blue Team (defenders). The Red Team's goal is to breach the security of a network or system while the Blue Team works to defend it. These simulations will help you understand attack techniques, defensive strategies, and the importance of proactive security measures.



Capture The Flag (CTF)

CTF competitions involve various challenges where you'll have to find and exploit vulnerabilities in different systems or applications to capture digital flags. Challenges will include cryptography, reverse engineering, web exploitation, binary exploitation, and more. CTF challenges will enhance your skills in penetration testing, forensics, and exploit development.

Fire Sale

You will participate in simulations of a coordinated cyber attack that are directed towards a country's critical infrastructure and financial systems and aims to cripple various essential services and systems causing widespread chaos and disruption. Learn to develop strategies on how to prevent, counter & launch Fire Sale category attacks.

Bug Bounty

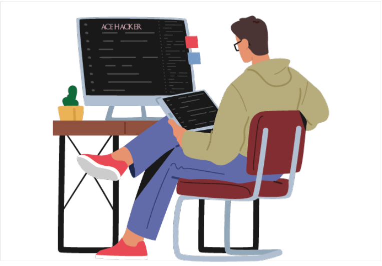
While not direct competitions, bug bounty programs offer a platform for ethical hackers to find vulnerabilities in software or systems. This practice encourages responsible disclosure and rewards for discovering and reporting vulnerabilities, contributing to improving overall cybersecurity. Learn how to set-up & operate Bug Bounty programs for your organization.

CYBERSECURITY

acehacker.com/learn/cybersecurity

SHARPEN YOUR AXE

Use Lab Exercises, Projects, Coding Competitions, and Hackathons as opportunities to practice and apply your programming skills in real-world scenarios.



To augment your proficiency in Cybersecurity, you will be regularly challenged with various assignments like coding challenges, algorithmic puzzles, trick logical, analytical, and mathematical problems - designed to enable you to think creatively and outside the box.
Expect 4 levels of difficulty in these assignments:

- **Beginner**: Exercises that test your understanding of the subject.
- **Intermediate**: Exercises that add new and thought-provoking information to the subject.
- **Advanced**: Exercises that are intended to challenge you.
- **Expert**: Exercises that are extremely difficult by comparison with most others.

The projects are designed to ensure that you not only understand the theoretical concepts of Cybersecurity & Cyber Warfare also gain hands-on experience in applying those concepts to real-world scenarios. You'll be required to collaborate as a team to attempt some projects while working as a Lone Wolf / individual contributor on others.

- **Four Cornerstone projects** that will reinforce in you the strong foundational knowledge of Cybersecurity & Cyber Warfare.
- **Two Keystone projects** will be more challenging, building on the knowledge you have gained through the Cornerstone projects.
- **One Capstone project,** which will be the culmination of your learning experience in this course.

Competitions and Hackathons are a great way to reinforce your learning and to challenge you to apply your skills to real-world scenarios. By participating in these events, you will gain practical experience and develop your problem-solving skills. You will be participating in a variety of events, including but not limited to:

- **Sprint Coding Competitions**
- **Marathon Hackathons**
- **Catch-the-Flag (CTF) challenges**
- **War Games**

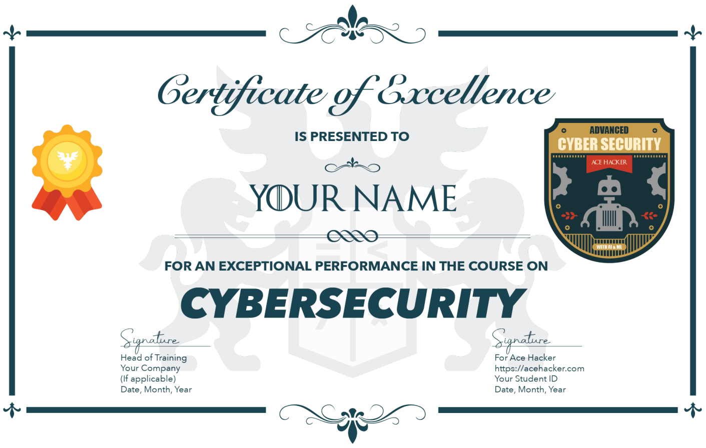
In some competitions, you will collaborate as a team, which will aid you in developing your teamwork skills. In other competitions, you will participate as a Lone Wolf, which will challenge you to think independently and to rely on your own skills and knowledge.

CYBERSECURITY

acehacker.com/learn/cybersecurity

CERTIFICATE IN CYBERSECURITY

Based on your performance you either get a **Certificate of Excellence** or **Certificate of Completion** after successful completion of the course.



Certificate of Excellence

IS PRESENTED TO

YOUR NAME

FOR AN EXCEPTIONAL PERFORMANCE IN THE COURSE ON

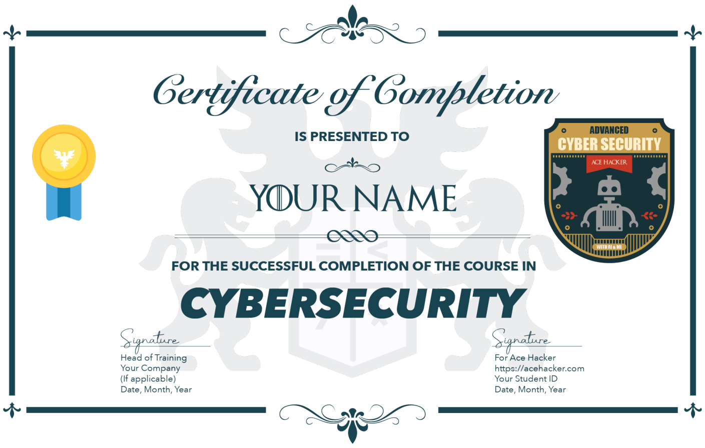
CYBERSECURITY

ADVANCED CYBER SECURITY
ACE HACKER
WITH AI & ML

Signature
Head of Training
Your Company
(If applicable)
Date, Month, Year

Signature
For Ace Hacker
https://acehacker.com
Your Student ID
Date, Month, Year

CERTIFICATE OF EXCELLENCE



Certificate of Completion

IS PRESENTED TO

YOUR NAME

FOR THE SUCCESSFUL COMPLETION OF THE COURSE IN

CYBERSECURITY

ADVANCED CYBER SECURITY
ACE HACKER
WITH AI & ML

Signature
Head of Training
Your Company
(If applicable)
Date, Month, Year

Signature
For Ace Hacker
https://acehacker.com
Your Student ID
Date, Month, Year

CERTIFICATE OF COMPLETION

ACE THAT CYBERSECURITY INTERVIEW

As a part of this course, you'll learn to crack Cybersecurity interviews. You'll be thoroughly trained using:

- **Mock Interviews**: We'll simulate the pressure and format of a real coding interview, allowing you to practice and improve you technical, communication, and presentation skills under similar conditions.
- Through **Whiteboarding**, you'll learn to visually represent your thought process on a physical or a digital whiteboard.
- You'll learn how to handle **Impossible Questions & Kobayashi Maru situations** which are essential in a coding interview to show adaptability, creativity, and resilience under pressure.

CYBERSECURITY

acehacker.com/learn/cybersecurity

Need more information?

Contact us.

- URL: https://acehacker.com/learn/cybersecurity
- connect@acehacker.com
- (+91) 988.011.2117