

Cybersecurity 101: Hands-On Fundamentals

Course Overview

Cybersecurity 101 is a comprehensive introduction to cybersecurity fundamentals inspired by TryHackMe's learning paths. This hands-on course is designed for beginners who want to build practical skills in cybersecurity through interactive labs, capture-the-flag challenges, and real-world scenarios.

Prerequisites

- Basic computer skills and familiarity with operating systems
- Interest in information technology and security
- No prior cybersecurity experience required

Tools and Technologies

Kali Linux Wireshark Nmap Burp Suite (Community Edition) Metasploit Framework OWASP ZAP John the Ripper Maltego (Community Edition)

Why Choose This Course

- Hands-on, practical approach to learning cybersecurity
- Real-world labs and challenges inspired by TryHackMe
- Small class sizes with personalized instruction
- Focus on both offensive and defensive security techniques
- Teaches methodology and thinking like a security professional
- Builds practical skills that immediately transfer to the workplace
- Includes a complete virtual lab environment

Career Opportunities

- Junior Security Analyst
- SOC Analyst (Tier 1)
- IT Support with Security Focus
- Junior Penetration Tester
- Cybersecurity Technician
- Help Desk with Security Responsibilities
- Junior Vulnerability Analyst

Course Curriculum

Module 1: Introduction to Cybersecurity

- The Cybersecurity Landscape
- Threat Actors and Attack Vectors
- Basic Security Principles
- Introduction to Security Tools
- Lab: Setting Up Your Security Lab

Module 2: Linux Fundamentals for Security

- Linux Basics and Navigation
- File Manipulation and Permissions
- Basic Shell Scripting
- Package Management and Updates
- Lab: Linux Security Hardening

Module 3: Network Security Fundamentals

- Networking Basics for Security
- Network Scanning Techniques
- Analyzing Network Traffic
- Firewalls and Network Defense
- Lab: Network Reconnaissance

Module 4: Web Application Security

- Web Technologies Overview
- OWASP Top 10 Vulnerabilities
- Web Application Reconnaissance
- Basic Web Exploitation
- Lab: Identifying Web Vulnerabilities

Module 5: Cryptography and Password Security

- Cryptography Fundamentals
- Password Attacks and Defense
- Secure Communications
- Authentication Methods
- Lab: Password Cracking Techniques

Module 6: OSINT (Open Source Intelligence)

- OSINT Methodology
- Information Gathering Techniques
- Social Media Intelligence
- OSINT Tools and Automation
- Lab: Creating an OSINT Investigation

Module 7: Windows Security

- Windows Security Architecture
- Windows Authentication
- Windows Privilege Escalation
- Windows Defense Techniques
- Lab: Windows Security Assessment

Module 8: Capture The Flag Challenges

- Introduction to CTF Competitions
- Reconnaissance Challenges
- Web Challenges
- Cryptography Challenges
- Final CTF Competition

Certification

Upon completion, participants will receive a Krisol IT Training certificate of completion. This course also prepares students for entry-level cybersecurity certifications like CompTIA Security+.

Certification Benefits

- Industry-recognized credential
- Enhanced job opportunities and career growth
- Validation of specialized skills and knowledge
- Increased earning potential
- Demonstrates commitment to professional development

Course Features

Hands-on Labs

OSINT Techniques

CTF Challenges

Duration: 6 Weeks

Level: Beginner

Frequently Asked Questions

Is this course suitable for complete beginners?

Yes, the course is specifically designed for beginners with basic computer skills. All concepts are introduced from the ground up, with plenty of hands-on practice to reinforce learning.

Do I need to have programming experience for this course?

No programming experience is required. While some basic scripting concepts are introduced, they are taught from scratch with a focus on practical security applications.

What kind of computer do I need for this course?

You'll need a modern laptop or desktop computer with at least 8GB RAM and 50GB of free disk space to run the virtual machines for the labs. Both Windows and Mac systems are supported.

Will this course help me start a career in cybersecurity?

Absolutely! This course provides the fundamental knowledge and hands-on skills that are essential for entry-level cybersecurity positions. It also serves as a solid foundation for more advanced security courses and certifications.

Are the labs similar to TryHackMe rooms?

Yes, our labs are inspired by TryHackMe's practical, challenge-based approach. They provide guided, hands-on experience with real-world security scenarios in a safe, controlled environment.