

Basics of Cyber Security



Course Overview

This course offers a practical foundation in cyber security, covering key concepts like cyber threats, hacking methods, security controls, and online tracking. You'll explore real-world attack techniques such as phishing, brute force, MITM, and social engineering, along with essential tools like firewalls, encryption, and antivirus. By the end, you'll understand how cyber attacks happen, how systems are protected, and how individuals are tracked online — making you better equipped to stay safe in the digital world or pursue a career in cyber security.

Course Objective

By the end of this course, learners will be able to:

- Understand the fundamentals of cyber security and its real-world importance
- Learn about various types of cyber attacks including phishing, brute force, and MITM
- Explore the roles and responsibilities of cyber security professionals
- Gain knowledge of core security concepts such as the CIA triad and hacking methodology
- Identify and analyze common vulnerabilities and threat vectors
- Understand penetration testing, security controls, and cyber security policies
- Learn the structure of firewalls, encryption methods, and anti-virus tools
- Explore the Cyber Kill Chain framework and its phases
- Analyze how users are tracked online through cookies, browser fingerprinting, and scripts
- Develop practical skills to safeguard personal and organizational digital assets

Skills you will learn

- Cyber Threat Analysis
- Ethical Hacking Basics
- Penetration Testing
- Vulnerability Assessment
- Social Engineering Detection
- Phishing & Brute Force Prevention
- Network Security Fundamentals
- CIA Triad Understanding
- WHOIS & Ping Command Usage
- MITM (Man-in-the-Middle) Attack Awareness
- Firewall Configuration
- Encryption Techniques
- Antivirus & Malware Protection
- Cyber Security Policy Knowledge
- CVE & CVSS Understanding
- Incident Response Handling
- Risk Management & GRC
- Cyber Kill Chain Framework
- Online Tracking & Browser Fingerprinting
- Password and Identity Management

Program Highlights

Eligibility

10+2

No.
of Sessions

44

Language
English

**Shareable
Certificate**

Curriculum

Introduction to Cyber Security


- Introduction
- Why Cyber Security is Important?
- Role of Cyber Security Engineer
- CIA Triad
- The Hacking Methodology
- The WhoIS Query
- Social Engineering
- Brute Force Attacks
- Phishing
- Bots and Botnets
- DoS and Dots
- Ping Command
- Man in the Middle Attacks (MITM)

Basic Concepts of Vulnerability


- Types of Hackers & Hacktivism
- Understanding Terminologies
- Vulnerability & Pen testing
- Cyber Security Controls
- Cyber Security Policies
- CVE & CVSS



Security Basics

- Attacks & Threats
 - Architecture & Design
 - Implementation
 - Operations & Incident Response
 - Governance, Risk & Compliance
 - Firewalls
 - Encryption
 - Biometrics
 - Anti Virus
 - Password Management
 - What is Cyber Kill Chain?
 - Reconnaissance and Weaponization
 - Delivery and Exploitation
 - Installation, Command & control (C2) & Actions on Objectives
- 

How we are tracked and targeted online

- Types of Tracking
 - IP Address
 - 3rd Party Connections
 - HTTP Referer
 - Cookies and Scripts
 - Super Cookies
 - Browser Fingerprinting and Browser Volunteered Information
 - Browser & Browser Functionality
 - More Tracking
 - Browsing in Incognito Mode
 - Browser and Internet Profiling
- 
- 