Welcome to

Cybersecurity Essentials Course

Milestone Jan - Jun 2025

COURSE OBJECTIVES

The objective of the **Cybersecurity Essentials Course** is to provide a comprehensive understanding of cybersecurity principles and practices. Students will learn foundational and advanced topics, including computer networking, legal and ethical knowledge, cryptography, ethical hacking, and penetration testing. The course will cover essential tools and technologies such as Windows OS, Kali Linux, Wireshark, and Metasploit. Additionally, students will gain proficiency in securing systems, understanding cyber threats, using penetration testing tools, and exploring emerging technologies like blockchain and generative AI. Through hands-on labs and practical projects, students will develop the skills to identify vulnerabilities, implement robust security measures, and mitigate cyber threats. The course concludes with a final project that integrates all acquired skills, preparing students to handle real-world cybersecurity challenges.

CAREER OBJECTIVES

The career objective of the **Cybersecurity Essentials Course** is to equip students with the essential skills and knowledge required to excel in various cybersecurity roles. Upon completion, students will be prepared for roles such as Cybersecurity Analyst, Penetration Tester, Network Security Engineer, Security Consultant, or IT Risk Analyst. The comprehensive curriculum ensures that students can confidently utilize key tools and technologies, analyse and mitigate cyber threats, and secure systems effectively. This foundation will enable them to pursue career opportunities in various industries, contribute to building secure digital infrastructures, and adapt to the evolving landscape of cybersecurity threats and solutions.

TOOLS REQUIRED

To complete and actively participate in this course, students will require the following tools:

1. A Laptop/Desktop Computer with sufficient specifications.
2. Wi-Fi or Data Connection for accessing course materials and virtual labs.
3. Kali Linux (Installed or Virtual Machine).
4. VirtualBox or VMware for sandboxed environments.
5. Ability to use Google Meet for live sessions and consultations.

RESOURCES/MATERIALS AND ASSESSMENTS

1. Learning Materials: Notes, video tutorials, and online resources provided by instructor.
2. Practical Exercises: Hands-on labs and sandboxed experiments.
3. Assessments: Quizzes, assignments, and knowledge checks to reinforce learning.
4. Projects: Individual and group projects to simulate real-world cybersecurity tasks.
5. Final Assessment: A capstone project to demonstrate mastery of the course content and acquired skills.

WEEKLY COURSE OUTLINE

WEEK 1

Introduction to Cybersecurity Principles

- Overview of cybersecurity essentials and their importance.
- Key concepts: CIA triad (Confidentiality, Integrity, Availability).
- Common cyber threats and attack vectors.
- Overview of legal and ethical considerations in cybersecurity.
- Quiz/Assignment/Assessment.

WEEK 2

Basics of Computer Networking

- Fundamentals of network topologies
- Different type of networks (LAN, WAN, PAN, MAN and Internet).
- Overview of network devices: routers, switches, firewalls.
- Understanding IP addressing and subnetting.
- Basics of protocols: TCP/IP, HTTP/HTTPS, and DNS.
- Network Security
- Quiz/Assignment/Assessment.

WEEK 3

Cyber Threats

- Different types of cyber threats: malware, phishing, DDoS attacks, and many more.
- Threat actors: hackers, outsiders, insiders, and nation-state attackers.
- Basics of risk assessment and threat modelling.
- Quiz/Assignment/Assessment.

WEEK 4

Windows OS for Ethical Hackers

- Overview of Windows Operating System and its architecture.
- Understanding the Windows file system and registry
- Managing services, users, and permissions in Windows.
- Understanding Windows OS features like control panel, disk management, and others
- Introduction Command Prompt and commands for hackers
- Introduction to PowerShell for automation and scripting
- Quiz/Assignment/Assessment.

WEEK 5

Kali Linux OS for Ethical Hackers

- Overview of Kali Linux Operating System, its features and architecture
- Kali Linux OS customization
- Introduction to penetration testing
- Basic Linux commands and file system navigation.
- Installing Kali Linux: Virtual Machine (VM) and VirtualBox or dual boot setup
- Overview of key tools in Kali Linux: Nmap, Metasploit, and Wireshark
- Quiz/Assignment/Assessment.

WEEK 6

Cryptography Essentials

- Introduction to cryptography and its importance in cybersecurity.
- Encryption algorithms: symmetric and asymmetric.
- Hashing techniques and their applications.
- Quiz/Assignment/Assessment.

WEEK 7

Ethical Hacking Principles and Practices

- Introduction to ethical hacking and its scope
- Phases of ethical hacking: reconnaissance, scanning, exploitation, post-exploitation
- Hands-on with Kali Linux tools for reconnaissance
    - Nmap for network scanning and enumeration.
- Quiz/Assignment/Assessment.

WEEK 8

Vulnerability Analysis and Penetration Testing

- Basics of vulnerability scanning
- Hands-on with Metasploit for exploitation
- Reporting vulnerabilities and planning remediation.
- Quiz/Assignment/Assessment.

WEEK 9

Strengthening Endpoint Security

- Overview of endpoint protection
- Securing user devices: antivirus, firewalls, and encryption
- Hardening operating systems: Windows, macOS, Linux
- Quiz/Assignment/Assessment

WEEK 10

Legal and Ethical Frameworks in Cybersecurity

- Overview of global cybersecurity laws and regulations
- Ethical decision-making in cybersecurity scenarios
- Quiz/Assignment/Assessment

WEEK 11

Incident Analysis and Response

- Basics of incident response and forensics
- Steps in incident handling: identification, containment, eradication, recovery
- Analysing security logs and monitoring tools
- Quiz/Assignment/Assessment

WEEK 12

Generative AI and Cybersecurity

- Introduction to generative AI and its implications
- AI in threat detection and prevention
- Risks of AI-driven cyber-attacks and ethical considerations
- Quiz/Assignment/Assessment

WEEK 13

Blockchain in Cybersecurity

- Understand the fundamentals of blockchain technology
- Role of blockchain in enhancing data integrity and securing communications
- Blockchain technology and its core principles (decentralization, immutability, and transparency)
- Understanding blockchain-based solutions for identity management and access control
- Quiz/Assignment/Assessment

WEEK 14

Final Project Preparation

- Recap of tools and techniques learned.
- Collaborative work on a real-world cybersecurity scenario.
- Develop and present a comprehensive security plan.

WEEK 15

FINAL PROJECT

GOOD LUCK!!!