THROUGHSEC

Beginner Cybersecurity Pathway Syllabus

This learning pathway is designed to introduce beginners to the foundational concepts and tools in cybersecurity. Through a combination of interactive lessons and practical exercises, students will build the technical knowledge required to explore both offensive and defensive security disciplines.

Introduction to Cybersecurity

Overview:
Kick off your journey into the world of cybersecurity with an introduction to its core areas. Learn the differences between offensive and defensive security, and explore career opportunities in the field.

Content:

1. **Offensive Security Introduction**
   - Basics of Offensive Security
   - Understanding Ethical Hacking and Penetration Testing
2. **Defensive Security Introduction**
   - Overview of Defensive Security Principles
   - Tools and Strategies for System Protection
3. **Cybersecurity Careers**
   - Roles in Cybersecurity: Penetration Tester, SOC Analyst, Incident Responder, and more
   - Roadmap to Building a Career in Cybersecurity

Network Fundamentals

Overview:
Understand the backbone of digital communication. This module covers the basics of computer networking, including how data is transmitted, network models, and extending networks.

Content:

1. **Introduction to Networking**
   - What is Networking?
   - Networking Components and Protocols

2. **LAN Basics**
    - Local Area Networks (LANs) Explained
    - Common LAN Devices and Configurations
3. **The OSI Model**
    - Layers of the OSI Model
    - How Data Travels Through the Layers
4. **Packets and Frames**
    - Anatomy of Packets and Frames
    - Understanding Headers, Footers, and Data Segmentation
5. **Extending Your Network**
    - Subnets and VLANs
    - Introduction to WANs and the Internet

How the Web Works

Overview:
Dive into how the internet functions. This module covers web technologies, protocols, and the building blocks of websites.

Content:

1. **DNS in Detail**
    - What is DNS and How it Works?
    - Understanding Domain Names and IP Mapping
2. **HTTP in Detail**
    - How HTTP Enables Communication Between Browsers and Servers
    - HTTP Methods, Status Codes, and Headers
3. **How Websites Work**
    - Structure of a Website: Frontend, Backend, and Databases
    - Interaction Between Users and Websites
    - Key Tools for Web Analysis

Linux Fundamentals

Overview:
Learn the essentials of Linux, a critical operating system in cybersecurity. Develop skills in command-line usage, file management, and system operations.

Content:

1. **Linux Fundamentals Part 1**
   - Introduction to Linux and Distributions
   - Basic Command-Line Operations
2. **Linux Fundamentals Part 2**
   - File and Directory Management
   - Permissions and Ownership
3. **Linux Fundamentals Part 3**
   - Networking Commands and Shell Scripting Basics
   - Managing Processes and Services

Windows Fundamentals

Overview:
Familiarize yourself with Microsoft Windows, a widely used operating system. Understand Active Directory basics, Windows configurations, and user management.

Content:

1. **Windows Fundamentals 1**
   - Introduction to Windows Operating System
   - File Systems and File Management
2. **Windows Fundamentals 2**
   - Users, Groups, and Permissions
   - Basic Windows Networking
3. **Windows Fundamentals 3**
   - Introduction to Active Directory
   - Windows Services and Security Settings

The **Beginner Cybersecurity Pathway** course is ideal for:

1. **Students**: College students or recent graduates pursuing degrees in IT or cybersecurity who want to develop their knowledge base and practical skills in cybersecurity.
2. **Career Changers**: Professionals from non-technical fields who are interested in transitioning into cybersecurity, looking for a structured learning path to build their skills from the ground up.
3. **Entry-Level Security Enthusiasts**: People who have a passion for technology and security but need an introduction to the core principles, including networking, web technologies, and the fundamentals of system administration.