🔐 3 Months Cyber Security Program

From Beginner to Web Security Expert

– *Designed for Students & Beginners*

🚀 Course Overview

Start your journey in Cyber Security from scratch and build real-world skills step by step.
This program is designed to take you from **basic concepts to advanced web security**, with practical exposure and industry-relevant tools.

🗓️ Month 1 – Foundations (Cyber Security + Linux)

📌 Week 1 – Cyber Security Basics

- **Introduction to Cyber Security**
  Understand the digital world, threats, and why security is critical today.
- **Types of Hackers & Attacks**
  Learn how different attackers operate and common real-world threats.
- **Core Security Principles (CIA Triad)**
  Build a strong foundation with essential security concepts.

📌 Week 2 – Linux Essentials

- **Introduction to Linux (Kali Linux)**
  Set up the most widely used OS in cyber security.
- **Basic Commands & Navigation**
  Learn how to control and manage systems through terminal.
- **User & Permission Management**
  Understand access control and system security basics.

📌 Week 3 – Linux + Networking Intro

- **Process & Package Management**
  Manage running applications and install security tools.
- **Networking Commands**
  Learn how systems communicate in a network environment.
- **Shell Basics**
  Improve efficiency using command-line operations.

📌 Week 4 – Networking Fundamentals 🌐

- **OSI & TCP/IP Models**
  Understand how data travels across networks.
- **IP Addressing & Subnetting**
  Learn how devices are identified and connected.
- **Ports & Protocols**
  Explore real-world protocols like HTTP, FTP, SSH.

🗓️ Month 2 – Networking + Attacks + Defense

📌 Week 5 – Network Practical Concepts

- **DNS & DHCP Working**
  Understand domain resolution and IP allocation.
- **Packet Flow Analysis**
  Learn how data moves between systems.
- **Wireshark Basics**
  Capture and analyze network traffic.

📌 Week 6 – Network Attacks 🔥

- **ARP Spoofing**
  Learn how attackers intercept network traffic.
- **Man-in-the-Middle (MITM)**
  Understand real-world interception techniques.
- **DoS Attack Basics**
  Explore how servers are overwhelmed and disrupted.

📌 Week 7 – Wireless Security 📡

- **Wi-Fi Security & Encryption**
  Understand WPA2/WPA3 and secure configurations.
- **Deauthentication Attack**
  Learn how attackers disconnect users from networks.
- **Evil Twin Attack**
  Simulate fake Wi-Fi attacks used in real scenarios.

📌 Week 8 – Network Defense 🛡️

- **Firewall Configuration**
  Control and secure network traffic effectively.
- **IDS/IPS (Snort)**
  Detect and prevent cyber attacks in real time.
- **Log Analysis**
  Identify suspicious activities using system logs.

🗓️ Month 3 – Web Security (High Demand Skills) 🌐🔥

📌 Week 9 – Web Fundamentals

- **How Websites Work**
  Understand client-server architecture.
- **HTTP & HTTPS**
  Learn secure vs insecure communication.
- **Cookies & Sessions**
  Explore authentication and session handling.

📌 Week 10 – Web Attacks (Part 1)

- **Cross-Site Scripting (XSS)**
  Learn how attackers inject malicious scripts.
- **SQL Injection (SQLi)**
  Understand database exploitation techniques.
- **Authentication Vulnerabilities**
  Identify weak login systems and bypass flaws.

📌 Week 11 – Web Attacks (Part 2)

- **CSRF Attack**
  Perform unauthorized actions on behalf of users.
- **File Upload Vulnerabilities**
  Exploit insecure file handling systems.
- **IDOR**
  Access unauthorized data due to poor controls.
- **Os command execution**

  Access OS commands to get data from web

📌 Week 12 – Tools + Real-World Project 🚀

- **Burp Suite**
  Intercept, analyze, and modify web requests.
- **Directory Bruteforcing**
  Discover hidden endpoints and admin panels.
- **Final Project + Report Writing**
  Perform full website testing and create a professional report.