🔐 5 Months Cyber Security Program including forensics

From Beginner to Cyber Security & Digital Forensics Professional (5 months)

(Industry-Oriented Training Program)

🚀 Program Overview

A complete roadmap to build your career in Cyber Security — starting from fundamentals and advancing into **Digital Forensics & Investigation** with real-world skills.

📅 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.

🕵️ **Month 4 – Digital Forensics (Core Investigation Skills)**

📌 **Week 13 – Introduction to Digital Forensics**

- **What is Digital Forensics?**
  Understand cyber investigations and real-world crime scenarios.
- **Types of Forensics**
  Disk, Network, Memory, and System forensics overview.
- **Forensic Process & Chain of Custody**
  Learn how evidence is collected, preserved, and documented legally.
- **6 Ace's of Forensics**

  Assessment → Acquisition → Analysis → Articulation → Arrival → Action

---

📌 **Week 14 – Disk & File System Forensics**

- **Disk Imaging & Acquisition**
  Create forensic copies without altering original evidence.
- **File Systems (NTFS, FAT)**
  Understand how data is structured and stored.
- **Deleted Data Recovery**
  Recover deleted files and hidden data from systems.

📌 **Week 15 – Memory & System Forensics**

- **Memory Analysis Basics**
  Extract live system data and running processes.
- **System Logs Analysis**
  Investigate system activities through logs.
- **User Activity Tracking**
  Identify user actions performed on the system.

📌 **Week 16 – Browser & Registry Forensics** 🌐

- **Browser Forensics**
  Analyze history, cookies, downloads, and user activity.
- **Windows Registry Forensics**
  Extract system configuration and user behavior evidence.
- **Forensic Tools Practice (Autopsy)**
  Perform real investigation tasks using tools.

🔍 Month 5 – Advanced Forensics + Incident Response

📌 Week 17 – Network Forensics

- **Packet Analysis for Investigation**
  Trace attacker activity using captured network data.
- **Log Correlation**
  Combine logs from different sources to find attack patterns.
- **Intrusion Analysis**
  Understand how systems get compromised.

📌 Week 18 – Password & SAM Forensics 🔐

- **Password Forensics Basics**
  Understand how passwords are stored and analyzed.
- **SAM (Security Account Manager) Analysis**
  Extract and analyze Windows user credentials.
- **Credential Investigation**
  Identify compromised accounts and access patterns.

📌 Week 19 – Incident Response 🚨

- **Incident Response Lifecycle**
  Preparation ⟶ Detection ⟶ Containment ⟶ Recovery
- **Handling Real Security Incidents**
  Step-by-step investigation and response process.
- **Evidence Handling & Documentation**
  Maintain proper forensic reporting standards.

📌 Week 20 – Final Case Study + Project 🎯

- **Complete Cyber Investigation**
  Perform end-to-end forensic analysis of a case.

- **Professional Report Writing**
  Create detailed and structured investigation reports.
- **Career Preparation**
  Interview guidance for Cyber Security & Forensics roles.

🎯 Final Outcome (5 Months Complete)

✔ Strong Cyber Security + Networking + Web Skills
✔ Hands-on Digital Forensics Expertise
✔ Real Investigation & Case Handling Experience
✔ Ready for roles like:

- Cyber Security Analyst
- Web Penetration Tester
- Digital Forensics Investigator
- SOC Analyst