TECHDIVE COMPUTER INSTITUTE

Tosin block, Magbon via Ita-Oluwo, Ogijo, Ogun state

09058263561

🛡️ **16-Week Cybersecurity & Ethical Hacking Curriculum**

📅 **Weekly Breakdown:**

- **4 Days Learning** (Theory & Hands-on)
- **2 Days Practical Projects**
- **Saturday: Hands-on Project & Real-world Simulations**

🗓️ **WEEK 1: Cybersecurity Fundamentals & Ethical Hacking**

Monday: Introduction to Cybersecurity

- Overview of cybersecurity, cyber threats, and career opportunities
- Types of cybersecurity (Network, Information, Application, Operational)
- 🔧 **Practical:** Identify security vulnerabilities in daily life

Tuesday: Cybersecurity Careers & Certifications

- Cybersecurity career paths (Penetration Tester, Security Analyst, etc.)
- Certifications: CEH, CISSP, CompTIA Security+
- 🔧 **Practical:** Research and present a cybersecurity career path

Wednesday: Ethical Hacking & Cybersecurity Frameworks

- What is ethical hacking?
- Phases of ethical hacking (Recon, Scanning, Exploitation, Post-exploitation)
- 🔧 **Practical:** Identify cybersecurity risks in an organization

Thursday: Introduction to Virtual Machines

- What is a Virtual Machine?
- Setting up **VirtualBox & Kali Linux**
- 🔧 **Practical:** Boot and explore Kali Linux

🔥 **Saturday Project: Set up a secure virtual environment**

🗓️ **WEEK 2: Cybersecurity Threats & Cryptography**

Monday: Cyber Threats (Malware, Ransomware, Phishing)

- How hackers use malware and social engineering
- 🔧 **Practical:** Identify phishing emails

Tuesday: Cryptography Basics

- Symmetric vs. Asymmetric encryption
- 🔧 **Practical:** Encrypt & decrypt files using GPG

Wednesday: Data Security & SSL/TLS

- How data is encrypted over networks
- 🔧 **Practical:** Use an SSL certificate checker

Thursday: Password Security

- Password cracking (Brute force, Dictionary attacks)
- 🔧 **Practical:** Test password strength with online tools

🔥 **Saturday Project: Encrypt & decrypt files using VeraCrypt**

🗓️ **WEEK 3: Network Security & Hacking Basics**

Monday: Introduction to Network Security

- Firewalls, IDS/IPS, VPNs
- 🔧 **Practical:** Configure a simple firewall rule

Tuesday: Network Scanning Basics

- How hackers scan networks
- 🔧 **Practical:** Use Nmap to scan a local network

Wednesday: Packet Sniffing & Network Analysis

- Using **Wireshark** to analyze network traffic
- 🔧 **Practical:** Capture and inspect network packets

Thursday: Man-in-the-Middle (MITM) Attacks

- How MITM works
- 🔧 **Practical:** Perform a basic MITM attack (test environment)

🔥 **Saturday Project: Conduct a network scan & identify devices using Nmap**

🗓️ **WEEK 4: Web Application Security**

Monday: Web Security Basics

- Common web vulnerabilities (**SQL Injection, XSS, CSRF**)

Tuesday: SQL Injection

- How SQLi works & how hackers exploit databases
- 🔧 **Practical:** Perform SQL injection on a test web app

Wednesday: Cross-Site Scripting (XSS)

- Types of XSS & prevention methods
- 🔧 **Practical:** Perform a simple XSS attack

Thursday: Setting Up a Vulnerable Web App

- Installing **DVWA & WebGoat**
- 🔧 **Practical:** Test vulnerabilities in a controlled environment

🔥 **Saturday Project: Perform an SQL Injection attack in DVWA**

🗓️ **WEEK 5: Social Engineering & Phishing**

Monday: Social Engineering Tactics

- How hackers manipulate people
- 🔧 **Practical:** Identify real-world social engineering tactics

Tuesday: Phishing Attacks

- Types of phishing attacks
- 🔧 **Practical:** Analyze real phishing emails

Wednesday: Social Engineering Toolkit (SET)

- 🔧 **Practical:** Simulate a phishing attack using SET

Thursday: Preventing Social Engineering Attacks

- How to detect & report phishing attempts

🔥 **Saturday Project: Create a phishing email & analyze phishing techniques**

🗓️ **WEEK 6: Penetration Testing**

- **Monday: Introduction to Penetration Testing (Phases, Methodologies)**
- **Tuesday: Setting up a Penetration Testing Lab (Kali Linux, Metasploitable)**
- **Wednesday: Metasploit Basics (Exploit Framework, Modules)**

- **Thursday: Using Burp Suite for Web Testing (Intercepting Requests, Attacks)**
- **Friday: Hands-on Penetration Testing (Scanning, Exploitation)**
- **Saturday Project: Conduct a penetration test on a vulnerable application**

🗓️ WEEK 7: Malware Analysis & Attack Techniques

- **Monday: What is a Brute Force Attack? (How it Works, Tools Used)**
- **Tuesday: How DDoS Attacks Work (Botnets, SYN Flood, Amplification)**
- **Wednesday: How Hackers Use Bots (Creating Malicious Bots, Prevention)**
- **Thursday: Basic DDoS Attack Simulation (Testing in a Safe Lab Environment)**
- **Friday: Preventing Brute Force Attacks (Rate Limiting, CAPTCHAs, Password Policies)**
- **Saturday Project: Simulate a simple brute-force attack in a test environment**

🗓️ WEEK 8: Web Security & Kali Linux Advanced Usage

- **Monday: Introduction to Kali Linux vs Parrot Security OS**
- **Tuesday: Configuring Kali Linux for Security Testing (Updating, Installing Tools)**
- **Wednesday: Web Application Security Best Practices (Secure Authentication, Input Validation)**
- **Thursday: Setting Up a Secure Web Server (SSL/TLS, Security Headers)**
- **Friday: Hands-on Web Security Audits (Scanning Websites for Vulnerabilities)**
- **Saturday Project: Set up Parrot Security OS and explore security tools**

🗓️ WEEK 9: Python for Cybersecurity

- **Monday: Why Learn Python for Cybersecurity? (Automating Security Tasks)**
- **Tuesday: Basic Python Programming (Lists, Variables, Loops)**
- **Wednesday: Writing a Simple Port Scanner (Using Python and Scapy/Nmap)**
- **Thursday: Automating Security Tasks with Python (Log Analysis, Brute Force)**
- **Friday: Using Python for Cybersecurity Tools (Creating a Simple Keylogger)**
- **Saturday Project: Write a script to scan open ports on a network**

🗓️ WEEK 10: Application Security & Secure Coding

- **Monday: Secure Coding Practices (Input Validation, Proper Error Handling)**
- **Tuesday: Common Vulnerabilities in Software (Buffer Overflow, Insecure APIs)**
- **Wednesday: Fixing Security Bugs in Python Code**
- **Thursday: Writing Secure Code (Authentication, Encryption)**
- **Friday: Hands-on Security Testing (Analyze and Fix Bugs in Open-Source Apps)**
- **Saturday Project: Fix security issues in a given Python script**

🗓️ **WEEK 11: Digital Forensics & Incident Response**

- **Monday: Introduction to Digital Forensics (Forensic Process, Tools)**
- **Tuesday: Hard Drive & Memory Forensics (Extracting Data from Images)**
- **Wednesday: Windows & Linux Forensics (Registry Analysis, Log Review)**
- **Thursday: Network Forensics (Packet Capture, Traffic Analysis)**
- **Friday: Incident Response Best Practices (SOC, IR Steps)**
- **Saturday Project: Conduct forensic analysis on a test machine**

🗓️ **WEEK 12: Security Challenges & Final Review**

- **Monday: Cybersecurity Challenges (CTF, Real-World Hacking Challenges)**
- **Tuesday: Secure System Design (Defense in Depth, Zero Trust)**
- **Wednesday: Mock Cybersecurity Interview (Common Interview Questions)**
- **Thursday: Ethical Hacking Final Practice (Solving Real Scenarios)**
- **Friday: Final Exam Review (Covering All Topics)**
- **Saturday Project: Work on final cybersecurity project**

🗓️ **WEEK 13: Advanced Cybersecurity Tools & Threat Hunting**

- **Monday: Threat Hunting Basics (Indicators of Compromise, SIEM Tools)**
- **Tuesday: Advanced Threat Detection (YARA, Snort, Suricata)**
- **Wednesday: Setting Up a SIEM System (ELK, Splunk)**
- **Thursday: Identifying and Responding to Threats**
- **Friday: Practical Hands-on Threat Hunting (Analyzing Logs, Detecting Malware)**
- **Saturday Project: Perform a threat-hunting exercise on a simulated network**

🗓️ **WEEK 14: Cloud Security & DevSecOps**

- **Monday: Cloud Security Basics (AWS, Azure, GCP Security)**
- **Tuesday: IAM and Access Control in the Cloud**
- **Wednesday: Securing Cloud Infrastructure (Misconfigurations, Best Practices)**
- **Thursday: Introduction to DevSecOps (CI/CD Security)**
- **Friday: Container Security (Docker, Kubernetes Security)**
- **Saturday Project: Secure a cloud application using IAM and security policies**

🗓️ **WEEK 15: Real-World Cybersecurity Scenarios & Case Studies**

- **Monday: Cyber Attack Case Study (WannaCry, SolarWinds, Colonial Pipeline)**
- **Tuesday: Lessons from Real Cybersecurity Breaches**
- **Wednesday: Security Policy & Compliance (ISO 27001, GDPR, NIST)**

- **Thursday: Creating Security Awareness Programs**
- **Friday: Incident Response Simulation (Handling a Cyber Attack)**
- **Saturday Project: Analyze a real-world cyber attack and present a report**

🗓️ WEEK 16: Final Project & Certification

- **Monday – Friday: Work on final cybersecurity project**
- **Saturday: Presentation and certification**

This structure ensures progressive learning, moving from the basics to advanced concepts while incorporating hands-on projects every week to solidify understanding