# ✅ Fixlab Cybersecurity Training Curriculum (4 Weeks)

**📅 Duration: 4 Weeks | 🛠️ Focus: Hands-on Practical + Industry Tools | 🧠 Target: Beginners to Intermediate**

---

## 🔐 Week 1: Cybersecurity Foundation & Compliance

### Class 1: Introduction to Cybersecurity & Frameworks

**Topics:**

- Introduction to Cybersecurity
- My Path to Cybersecurity
- Responsibilities of an entry-level cybersecurity Analyst
- Types of Threats (Malware, Phishing, Ransomware, DDoS)
- Key Terms: Firewall, IDS, SIEM, VPN, Authentication, Encryption
- Core skills for Cybersecurity professional
- Importance of Cybersecurity

**Lab Work:**

- Setup of Virtual Machines (Kali Linux, Ubuntu, Windows)
- Initial lab environment configuration

---

## Class 2: Cybersecurity  Frameworks

**Topics:**

- Introduction to Security Frameworks and Controls
- **The CIA Triad** (Confidentiality, Integrity, Availability)
- Secure Design
- Controls, Frameworks and Compliance
- **Cybersecurity Frameworks:**
    - NIST CSF
    - OWASP Top 10
    - CIS Controls v8
- Introduction to **Security Compliance**:
    - PCI-DSS
    - HIPAA
    - GDPR
    - NDPR (Nigeria)
    - ISO 27001
- Ethics and Compliance in Cybersecurity

**Lab Work:**

- Demonstrate CIA Triad: file permissions (Confidentiality), hash verification (Integrity), service stop/start (Availability).
- Configure rsyslog/log rotation and show how it meets compliance controls.
- Perform a mini NIST CSF self-assessment; test 2 OWASP Top 10 issues on DVWA/Juice Shop; verify 3 CIS Controls on a VM.
- Encrypt/decrypt a file with GPG; capture HTTP vs HTTPS traffic in Wireshark.
- Role-play ethical vs unethical testing scenarios; create a 3-point compliance checklist.

---

## 🔐 Week 2: Linux for  Cybersecurity

### Class 3: Linux for Cybersecurity I

**Topics:**

- Linux Distros for Security: Kali vs Parrot vs Ubuntu
- Linux File System Hierarchy
- Terminal Commands: `ls`, `cd`, `pwd`, `mkdir`, `nano`, `cat`, `cp`, `mv`, etc.

**Lab Work:**

- Practice terminal navigation
- Inspect and create directories/files
- Explore `/etc`, `/var/log`, `/home`

---

### 📘 Class 4: Linux for Cybersecurity II

**Topics:**

- Linux File Permissions: `chmod`, `chown`, `chgrp`
- User & Group Management: `useradd`, `usermod`, `groupadd`
- Sudoers file and privilege escalation risks

**Lab Work:**

- Create users/groups and manage permissions
- Restrict access to sensitive files
- Explore `/etc/passwd`, `/etc/shadow`, and `/etc/sudoers`

---

# 🌐 Week 3: Networking Basics & Monitoring

🎯 **Objective:** Understand network fundamentals, packet structure, and traffic monitoring.

## 📘 Class 5: Networking Fundamentals

**Topics:**

- What is a Network (LAN, WAN, PAN, WLAN)
- Network Devices (Switches, Routers, Firewalls)
- IP Addressing, Subnetting Basics
- TCP/IP, UDP, ICMP Protocols

**Lab Work:**

- Use `ip`, `ifconfig`, `netstat`, `ping`, `traceroute`
- Identify system's IP, MAC, gateway, and DNS

---

## Class 6: Network Monitoring with Wireshark

**Topics:**

- What is Packet Sniffing and Analysis
- Wireshark Filters and Capture Interfaces
- Identifying Protocols and Traffic Behavior

**Lab Work:**

- Capture HTTP, DNS, ICMP packets
- Filter using: `tcp.port == 80`, `http.request`, `icmp`
- Analyze sessions using `tcp.stream eq <ID>`

---

# 🛡️ Week 4: Intrusion Detection & SIEM

🎯 **Objective:** Learn to detect threats using IDS and SIEM tools and simulate real-world attacks.

## Class 71: Intrusion Detection with Snort

**Topics:**

- What is an IDS (Snort vs Suricata)
- Signature-based vs Anomaly-based Detection
- Snort Architecture & Rule Structure

**Lab Work:**

- Install Snort and create custom rules
- Analyze and log Snort alerts in real time

---

## Class 8: Security Event Monitoring with Splunk

**Topics:**

- What is SIEM and use cases
- Installing and using **Splunk Free Edition**
- Log collection: `/var/log/auth.log`, `/var/log/syslog`

**Lab Work:**

- Ingest Linux logs into Splunk
- Search for failed login attempts, privilege escalation
- Create dashboards and alerts

---

# 🧪 Week 5: Digital Forensics & Incident Response

🎯 **Objective:** Analyze memory/disk artifacts and build professional incident response playbooks.

## Class 91: Memory Forensics with Volatility

**Topics:**

- Importance of RAM forensics
- Memory dump acquisition with LiME/AVML
- Volatility plugins: `pslist`, `netscan`, `cmdline`, `dlllist`

**Lab Work:**

- Dump memory from infected VM
- Extract evidence of keyloggers or hidden processes
- Document attack path from memory

---

## Class 10: Disk Forensics with Autopsy

**Topics:**

- Disk structures: GPT, MBR, FAT32, NTFS
- Deleted file recovery and timeline analysis
- FTK Imager, Autopsy, The Sleuth Kit overview

**Lab Work:**

- Analyze `.dd` or `.E01` image file with Autopsy
- Recover deleted chats, pictures, browser history
- Generate chain-of-custody forensic report

---