NEXTLEAP

# CYBER SECURITY PROGRAM: 16 WEEKS MODULE PLANNER

POWERED BY: NEXTLEAP EDUCATION

NEXTLEAP

## PROGRAM OVERVIEW

**Program Name:** Cyber Security Program

**Tools Covered:** Kali Linux, Nmap, Wireshark, Metasploit, Hashcat, Nikto, Python

**Duration:** 16 Weeks

**Focus Areas:** Virtualization, Network Security, Web Security, Penetration Testing, Cryptography

**Overall Outcome:**
Learners will be able to identify vulnerabilities, perform security testing, and apply real-world cybersecurity tools to protect systems and networks.



NEXTLEAP

# MODULE 1: FOUNDATIONS & COURSE CONCEPT

***Week 1 –*** *Cybersecurity Fundamentals & Course Concept*

- Cybersecurity basics, CIA Triad
- Types of threats: Malware, Phishing, Social Engineering
- Virtualization concepts
- Install VirtualBox & Kali Linux

**Outcome:** Build strong foundational understanding and set up a working lab environment.

***Week 2 –*** *Linux & Networking Basics*

- Linux commands & file system
- OSI Model & TCP/IP
- IP Addressing & Protocols (HTTP, DNS, FTP)
- Wireshark packet capture

**Outcome:** Understand system navigation and basic networking concepts.



NEXTLEAP

## MODULE 1: FOUNDATIONS & LAB SETUP

***Week 3 –*** *Operating System Security*

- Authentication & Authorization
- Access Control Models
- Windows & Linux Security
- User permissions & firewall basics

**Outcome:** Secure systems and manage access controls effectively.

***Week 4 –*** *Network Scanning*

- Reconnaissance and enumeration
- Nmap scanning
- Netdiscover

**Outcome:** Identify network vulnerabilities and analyze traffic.



NEXTLEAP

## MODULE 2: ETHICAL HACKING

***Week 5-*** *Vulnerability Assessment*

- CVE & CVSS
- Vulnerability scanning concepts
- Nikto scanning

**Outcome:** Identify and assess system vulnerabilities.

***Week 6-*** *Web Security & OWASP*

- OWASP Top 10
- SQL Injection basics

**Outcome:** Understand and exploit common web security flaws.



NEXTLEAP

## MODULE 2:ETHICAL HACKING

***Week 7-*** *Penetration Testing*

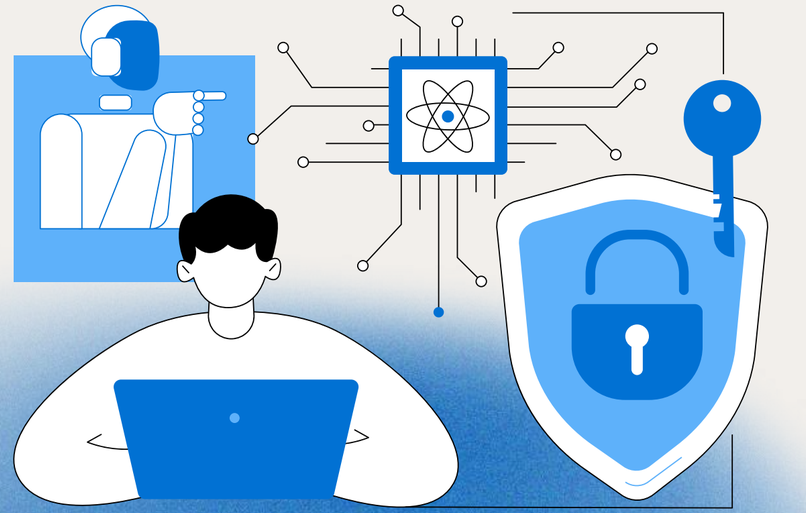
- Pentesting lifecycle
- Metasploit framework

**Outcome:** Perform structured penetration testing.

***Week 8-*** *Cryptography*

- Encryption & hashing
- RSA basics
- Hashcat tool

**Outcome:** Understand data protection techniques.



NEXTLEAP

## MODULE 3: DIGITAL FORENSICS

***Week 9-*** *Introduction to Digital Forensics*

- Types of forensics
- Legal aspects
- Autopsy tool

**Outcome:** Understand forensic investigation basics.

***Week 10-*** *Disk Forensics*

- File systems
- FTK Imager

**Outcome:** Analyze disk-level evidence.



NEXTLEAP

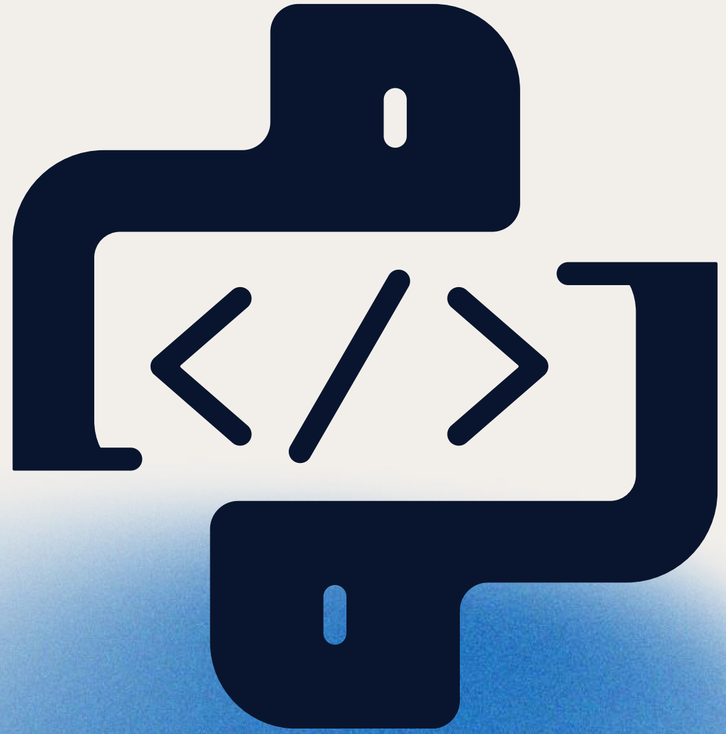
## MODULE 3: DIGITAL FORENSICS

***Week 11-*** *Network Forensics*
- Packet analysis
- PCAP analysis

**Outcome:** Investigate network-based attacks.

***Week 12-*** *Memory Forensics*
- RAM analysis
- Volatility tool

**Outcome:** Analyze memory for hidden threats.



NEXTLEAP

## MODULE 4: ADVANCED SECURITY & CAPSTONE

***Week 13-*** *SIEM & SOC*

- SIEM concepts
- SOC operations
- Splunk basics

**Outcome:** Monitor and analyze security events.

***Week 14-*** *Incident Response*

- Incident response lifecycle
- Attack simulation

**Outcome:** Handle real-world cyber incidents.



NEXTLEAP

## MODULE 4: ADVANCED SECURITY & CAPSTONE

***Week 15-*** *Governance & Risk Management*

- ISO 27001
- NIST framework
- Risk assessment

**Outcome:** Understand compliance and risk handling.

***Week 16-*** *Capstone Project & Final Assessment*

- Penetration testing / Forensics / Network analysis
- Vulnerability scanning & exploitation
- Final report & presentation

**Outcome:** Apply complete cybersecurity skills in real-world scenario.



NEXTLEAP

# Thank you!

**POWERED BY: NEXTLEAP EDUCATION**

For further enquiry: operation@nextleapeducation.com