Information Booklet cum Syllabus

Of

Cyber Security & Ethical Hacking Bootcamp

April 2026

National Institute of Electronics and Information Technology

An Autonomous Scientific Society under

Ministry of Electronics and Information Technology, Government of India

NIELIT Gorakhpur

M.M.M.U.T. Campus, Deoria Road

Gorakhpur (U.P.) -273010

CONTENTS

1. About Course

The Certificate in Cyber Security & Ethical Hacking Fundamentals is designed to provide learners with a strong foundation in cybersecurity concepts, ethical hacking methodologies, networking, Linux, OSINT, Wi-Fi security, digital forensics, and cyber laws.

The course emphasizes ethical practices, awareness-based demonstrations, and investigation-oriented learning, enabling participants to understand how cyber attacks occur and how they can be prevented, detected, and investigated.

2. NIELIT

National Institute of Electronics and Information Technology, NIELIT, (Erstwhile DOEACC Society) is an autonomous scientific society of the Ministry of Electronics& Information Technology, Government of India. The Society is registered under the Societies Registration Act, 1860. NIELIT was set up to carry out Human Resource Development and related activities in the area of Information, Electronics & Communications Technology (IECT). NIELIT is engaged both in Formal & Non-Formal Education in the areas of IECT besides development of industry oriented quality education and training programmes in the state-of-the-art areas. NIELIT has endeavored to establish standards to be the country's premier institution for Examination and Certification in the field of IECT. It is also one of the National Examination Body,

which accredits institutes/organizations for conducting courses in IT and Electronics in the non-formal sector.

3. Objective of Course

The objective of this course is to develop cyber security awareness, ethical hacking fundamentals, and investigative skills.

After completing the course, learners will be able to:

- Understand ethical hacking concepts and cyber attack life cycles.
- Apply networking and Linux fundamentals for security analysis.
- Perform footprinting, reconnaissance, and OSINT investigations.
- Understand Wi-Fi hacking concepts and tracking awareness.
- Analyze system hacking and password attack methodologies.
- Perform basic digital forensics and incident response.
- Follow legal and ethical guidelines while practicing cybersecurity.

4. Job Roles of Course

This course is designed to equip learners with the necessary skills for the following job roles:

- Cyber Security Analyst (Entry Level)
- Ethical Hacking Trainee
- SOC Analyst (L1 – Foundation)
- Cyber Crime Investigation Assistant
- IT Security Support Executive

5. Eligibility

10th / 12th Pass or equivalent with basic computer knowledge. (Students from any academic background can apply.)

6. Total duration of the course

90 Hours (Theory: 35 Hrs, Practical/Tutorial: 55 Hrs)

7. Course Details

7.1. Course Outline and Objective of Each Unit

S. No.	Module Name	Duration (Theory) in Hours	Duration (Practical) in Hours	Total Learning Hrs.	Learning Objectives
1	**Foundation of Networking**	**15**	**15**	**30**	• Introduction to Networking • OSI & TCP/IP Models • LAN, MAN, WAN Concepts • Network Topologies (Star, Mesh, Hybrid, Bus, Ring) • IP Addressing (IPv4 & IPv6) • Basic Networking Commands (Ping, Tracert, ipconfig) • Subnetting & Supernetting • DNS, DHCP, HTTP/HTTPS • Routers, Switches & Firewalls • Network Troubleshooting Basics
2	**Cybersecurity Fundamentals**	**12**	**18**	**30**	• Introduction to Cybersecurity • Types of Cyber Threats & Attacks • Malware (Viruses, Worms, Trojans, Ransomware) • Security Policies & Risk Management • Cryptography Basics (Encryption & Decryption) • Authentication & Authorization • Security Tools & Technologies • Cloud Security Basics • Social Engineering Attacks • Awareness of Government Security Apps (UMANG, M-Kavach 2)
3	**Ethical Hacking**	**13**	**17**	**30**	• Introduction to Ethical Hacking & Types • Lab Environment Setup (VMware, Kali Linux) • Footprinting & Reconnaissance • Scanning & Vulnerability Analysis • System Hacking Techniques • Password Cracking Methods • Web Application Attacks (SQL

					Injection, XSS, CSRF) • Wireless Network Hacking • Sniffing & Session Hijacking • Denial of Service (DoS/DDoS) Concepts • Social Engineering & Phishing • Basics of Digital Forensics & Data Recovery • Hands-on Tools: Kali Linux, Metasploit, Nmap

7.2. Detailed Course

Module Name	Unit	Contents	Hrs.
Foundation of Networking	**Introduction to Networking**	• Definition of networking • Types of networks (LAN, MAN, WAN) • Network architecture basics • Importance of networking • Real-world networking applications	**30**
	OSI & TCP/IP Models	• OSI model layers • TCP/IP model overview • Comparison of OSI vs TCP/IP • Data encapsulation process • Protocol layering concepts	
	IP Addressing & Subnetting	• IPv4 and IPv6 concepts • Classes of IP addresses • Subnetting and supernetting • Private vs public IP • CIDR notation	
	Network Protocols & Services	• DNS, DHCP working • HTTP vs HTTPS • FTP, SSH basics • Port numbers and services • Packet flow explanation	
	Network Devices & Troubleshooting	• Routers, switches, firewalls • Network topologies • Basic commands (ping, tracert, ipconfig) • Troubleshooting techniques • Network security basics	

Cybersecurity Fundamentals	**Introduction to Cybersecurity**	• Definition of cybersecurity • CIA triad (Confidentiality, Integrity, Availability) • Security principles • Types of security domains • Importance of cybersecurity	**30**
	Cyber Threats & Malware	• Types of cyber attacks • Malware (virus, worm, trojan, ransomware) • Attack lifecycle • Real-world examples • Prevention techniques	
	Cryptography & Authentication	• Encryption and decryption • Symmetric vs asymmetric cryptography • Hashing concepts • Authentication methods • Digital signatures	
	Security Policies & Cloud Security	• Risk management basics • Security policies and standards • Cloud security fundamentals • Data protection techniques • Access control mechanisms	
	Social Engineering & Awareness	• Phishing and spear phishing • Social engineering attacks • Human vulnerabilities • Awareness techniques • Government security apps (UMANG, M-Kavach 2)	
Ethical Hacking	**Introduction to Ethical Hacking**	• Definition of ethical hacking • Types of hackers • Cyber kill chain • Ethical vs unethical hacking • Career opportunities	**30**
	Lab Setup (Kali Linux, VMware)	• Kali Linux overview • Virtualization concepts • Installation and setup • Basic Linux commands • Environment configuration	
	Footprinting & Reconnaissance	• Passive and active reconnaissance • Google dorking • WHOIS and DNS lookup • OSINT techniques • Metadata analysis	
	Scanning & Vulnerability	• Network scanning techniques • Vulnerability scanning tools	

Analysis	• Port scanning • Risk identification • Analysis methods
System Hacking & Password Attacks	• Password cracking techniques • Brute force and dictionary attacks • Privilege escalation • Hashing and salting • System vulnerabilities
Web Application Attacks	• SQL Injection • Cross-Site Scripting (XSS) • Cross-Site Request Forgery (CSRF) • Web vulnerabilities • Secure coding basics
Wireless Hacking & Sniffing	• Wi-Fi security standards • Packet sniffing • Man-in-the-Middle attack (theory) • Session hijacking • Network monitoring
Digital Forensics & Incident Response	• Digital forensics basics • Evidence handling • Log analysis • Incident response lifecycle • Investigation techniques
Final Project & Career Guidance	• Hands-on project • CTF practice • Resume building • Interview preparation • Career roadmap

8. Reference Books/ Study Materials

1. CEH Official Courseware – EC-Council
2. The Web Application Hacker's Handbook – Dafydd Stuttard
3. Linux Basics for Hackers – OccupyTheWeb
4. OSINT Framework (Online)
5. NIELIT Course Notes & E-Resources

9. Practical Assignments

1. Perform DNS and IP lookup for a given domain
2. Extract metadata using ExifTool
3. Analyze Wi-Fi security configurations
4. Demonstrate IP tracking awareness using sample links
5. Perform basic password attack simulation
6. Analyze logs for incident response.

10. Sample Questions

Q1. Ethical hacking is performed to:
a) Damage systems
b) Steal information
c) Improve system security
d) Hack social media

Q2. Which tool is used for metadata extraction?
a) Nmap
b) ExifTool
c) Wireshark
d) Burp Suite

Q3. DNS is used to:
a) Encrypt data
b) Translate domain names to IP addresses
c) Scan ports
d) Crack passwords

Q4. WPA2 is related to:
a) Web security
b) Wi-Fi encryption

c) Malware
d) DNS

Q5. Which act governs cyber laws in India?
a) IPC
b) IT Act 2000
c) RTI Act
d) Companies