NIAI

NETSOL Institute of AI

Cyber Security (CEH) Training Program

Hands-on Training & Real-World Skills to Prepare for the Future

1. Cyber Security (CEH) Curriculum Breakdown

Course Name:	**Cyber Security (CEH)**
Course Duration:	3 Months (12 Weeks)
No. Of Days per week:	4 Days per week (Course only)
Class Hours	3 hours per class
Total In-Class Credit hours	144

Module	Description	Content Breakdown
1. Introduction to CEH	Learn the fundamentals and key issues in information security, including the basics of ethical hacking, information security controls, relevant laws, and standard procedures.	· Intro Lecture · Course Intro · Success stories · Job Market · Intro to CEH · Roles of Security Expert · What is cyberspace. · What is hacker and its different types. · Different types of attacks. · Hands-on Practice on LAB Setup for testing **Quiz and Tasks** Assignment (Research): - Jobs, Domains.
2. Lab Setup	This module guides students through setting up a secure virtual cybersecurity lab using tools like VirtualBox/VMware, Kali Linux, Windows VMs, and networking	· Setup virtual machines for LAB environment. · Install and configure Kali Linux · Intro Kali Linux. **Quiz and Tasks**

	simulations. It covers isolation, snapshots, safe testing practices, and proper configuration of forensic, networking, and penetration testing environments. Students will prepare their machines for hands-on exercises throughout the course.	**Assignment:** Setting up virtual environment and related tools
3. System Administration	This module builds foundational system administration skills across both Linux and Windows platforms. Students learn command-line usage, user and permission management, service configuration, file system navigation, and basic automation. These skills prepare students for cyber operations, incident response, and forensic investigations later in the course.	· Important Linux Commands · Important Windows Commands **Quiz and Tasks** **Assignment:** - Practice OS commands and tools.
4. Networking Essentials	Students learn the core concepts of computer networking, including protocols, ports, IP addressing, OSI model, and packet flow. The module explains how networks operate in real environments and why attackers target network weaknesses. Practical exercises include basic packet analysis, subnetting, and understanding routing and switching behaviors.	· Get familiar with OSI Layers · Different functions of OSI layers. · Protocols of each layer. · Get familiar with TCP/IP suit. · Different protocols and ports. · Basic Network Configuration **Quiz and Tasks** **Assignment:** - Packet Tracer lab activity.
5. Information Gathering (Foot	Learn how to use the latest techniques and tools for footprinting and reconnaissance, a	· Open Source Intelligence (OSINT) Overview · Passive vs. Active Information Gathering · Information Gathering Methodologies

printing & Reconnaissance)	critical pre-attack phase of ethical hacking	· Ethical Considerations in OSINT
		· Foot printing and Reconnaissance
		· Search Engine Hacking
		· Social Media Intelligence
		· Email and Domain Information Gathering
		· Metadata Analysis
		· WHOIS Data and Domain Ownership
		· DNS Enumeration
		· Enumeration of Network Services
		· Shodan and IoT Device Information
		· Maltego for Data Link Analysis
		· The Harvester for Gathering Emails and Subdomains
		· Spokeo and People Search Tools
		· Data Scraping Techniques
		· Google Dorks and Advanced Search Queries
		· Geolocation and IP Tracing
		· Social Engineering for Information Gathering Algorithms
		· Gathering Information on Mobile Apps
		· Deep Web and Dark Web Information Gathering
		· Tor and Onion Sites Exploration
		· Threat Intelligence Feeds
		· OSINT Frameworks and Tools
		· Visualizing OSINT Data
		· OSINT for Digital Forensics
		· OSINT for Incident Response
		· Legal and Ethical Aspects of OSINT
		Quiz and Tasks

		Assignment (1.5 hr per week)**:** - Hands-on Practice with an Information Gathering - Practical on OSINT Investigations
6. Scanning	Learn different network scanning techniques and countermeasures.	· Network Scanning Fundamentals · Types of Network Scans · Port Scanning Techniques · TCP Connect Scanning · UDP Scanning · Banner Grabbing · Network Enumeration Methods · Scanning Tools and Utilities · Nmap - Network Mapper · Ping Sweeps and Sweep Detection · Network Mapping and Topology Discovery · Vulnerability Scanning · Operating System Detection · Automated Scanning Workflows · Scanning for Web Applications · Threat Intelligence Integration · Wireless Network Scanning · Automating Scans with Scripts · Scanning Best Practices · Scanning Ethics and Legal Considerations · Post-Scanning Analysis · Scanning for Insider Threats **Quiz and Tasks** **Assignment** (1.5 hr per week)**:** Build and train models. - Practical on Comprehensive Network Scan
		· Enumeration Basics · NetBIOS Enumeration

7. Enumeration	Learn various enumeration techniques, including Border Gateway Protocol (BGP) and Network File Sharing (NFS) exploits and associated countermeasures.	· SNMP Enumeration
		· LDAP Enumeration
		· SMB Enumeration
		· DNS Enumeration
		· SMTP Enumeration
		· NTP Enumeration
		· SSH Enumeration
		· RDP Enumeration
		· Port Enumeration Techniques
		· User Enumeration
		· Share Enumeration
		· Vulnerability Enumeration
		· Enumeration Tools and Scanners
		· Nmap Scripts for Enumeration
		· SNMP Enumeration Tools
		· LDAP Enumeration Tools
		· SMB Enumeration Tools
		· DNS Enumeration Tools
		· SMTP Enumeration Tools
		· Enumeration for Active Directory
		· Enumeration for Linux
		· Enumeration for Windows
		· Enumeration Best Practices
		· Enumeration Ethics and Legal Considerations
		Quiz and Tasks
		Assignment: - Practical on Comprehensive Enumeration
	Learn how to identify security loopholes in a target organization's network, communication	· Vulnerability Assessment Fundamentals
		· Types of Vulnerabilities
		· Vulnerability Scanning Techniques

8. Vulnerability Analysis	infrastructure, and end systems. Different types of vulnerability assessment and vulnerability assessment tools are also included.	· Automated Vulnerability Scanners
		· Manual Vulnerability Assessment
		· Common Vulnerability Databases
		· Common Vulnerability Scoring System (CVSS)
		· Vulnerability Management Practices
		· Vulnerability Analysis Tools
		· Nmap Scripting Engine (NSE) for Vulnerability Scanning
		· OpenVAS - Open Vulnerability Assessment System
		· Nessus Vulnerability Scanner
		· Qualys Vulnerability Management
		· Vulnerability Assessment in Web Applications
		· OWASP Top Ten Vulnerabilities
		· Vulnerability Analysis for Mobile Applications
		· Vulnerability Analysis for Network Devices
		· Reporting and Remediation of Vulnerabilities
		· Exploitation Frameworks and Vulnerabilities
		· Vulnerability Analysis Best Practices
		· Legal and Ethical
		· Aspects of Vulnerability Analysis
		Quiz and Tasks
		Assignment: Hands-On: - Vulnerability Analysis Case Studies - Practical on Comprehensive Vulnerability Analysis
9. System Hacking	Learn about the various system hacking methodologies used to discover system and network vulnerabilities, including	· System Hacking Fundamentals
		· Password Cracking Techniques
		· Password Cracking Tools
		· Privilege Escalation Methods
		· Exploiting Weak Passwords

	steganography, steganalysis attacks, and how to cover tracks.	· Brute Force and Dictionary Attacks
		· Cracking Windows Passwords
		· Cracking Linux Passwords
		· Privilege Escalation on Windows
		· Privilege Escalation on Linux
		· Hiding Files and Processes
		· Bypassing Antivirus Software
		· Keyloggers and Spyware
		· Post-Exploitation Techniques
		· Exploitation Frameworks
		· Covering Tracks and Removing Evidence
		· Legal and Ethical Aspects of System Hacking
		Quiz and Tasks
		Assignment: - System Hacking Case Studies - Practical on Comprehensive System Hacking
10. Malware Analysis	Learn about different types of malware (Trojan, viruses, worms, etc.), APT and fileless malware, malware analysis procedures, and malware countermeasures.	· Malware and Backdoors
		· Rootkits and Trojans
		· Remote Administration Tools (RATs)
		· Advanced Persistent Threats (APTs)
		· Fileless Malware
		· Introduction to Malware Analysis
		· Malware Analysis Fundamentals
		· Types of Malware and Malicious Code
		· Malware Analysis Environments and Sandboxes
		· Static Analysis Techniques
		· Dynamic Analysis Techniques
		· Behavioral Analysis of Malware
		· Memory Analysis and Forensics
		· Disassembling and Debugging Malicious Code
		· Code Injection and Hooking Techniques

		· Deobfuscation and Decryption
		· YARA Rules for Malware Detection
		· Identifying and Classifying Malware Families
		· Packets Analysis for Malware Detection
		· Building Custom Malware Analysis Tools
		· Network Traffic Analysis
		· Malware Artifacts and Indicators of Compromise (IoC)
		· Threat Intelligence and Malware Data Sources
		· Building a Malware Sandbox
		· Building a YARA Rule Library
		· Building a Memory Forensics Toolkit
		· Building Custom Analysis Scripts
		· Practical Malware Analysis Techniques
		· Legal and Ethical Aspects of Malware Analysis
		Quiz and Tasks
		Assignment: - Malware Analysis Case Studies - Practical on Analyzing Real-World Malware Samples
11. Network Sniffing	Learn about packet sniffing techniques and their uses for discovering network vulnerabilities, plus countermeasures to defend against sniffing attacks.	· Introduction to Network Packet Sniffing
		· Legal and Ethical Aspects of Sniffing
		· Wireshark and Packet Capture Basics
		· Analyzing Captured Packets
		· Packet Filtering and Display Options
		· Advanced Protocol Analysis
		· Packet Decryption Techniques
		· Capturing and Analyzing SSL/TLS Traffic
		· Sniffing on Wireless Networks
		· Sniffing on Switched Networks
		· ARP Spoofing and MITM Attacks
		· DNS Spoofing and Cache Poisoning

		· VoIP Traffic Sniffing
		· Sniffing for Malware Traffic
		· Network Sniffing for Intrusion Detection
		· Building Custom Sniffing Tools
		· Sniffing Case Studies and Real-World Scenarios
		· Sniffing for Security and Troubleshooting
		· Sniffing Best Practices and Avoiding Detection
		Quiz and Tasks
		Assignment: - Practical on Analyzing Network Packet Samples with Wireshark
12. Wi-Fi Hacking	Learn about different types of encryption, threats, hacking methodologies, hacking tools, security tools, and countermeasures for wireless networks.	· Introduction to Wireless Networks and Security
		· Legal and Ethical Aspects of Wireless Hacking
		· Wireless Network Fundamentals (Wi-Fi, WEP, WPA, WPA2)
		· Wireless Encryption Protocols (WEP, WPA, WPA2, WPA3)
		· Understanding Wi-Fi Security Vulnerabilities
		· Scanning for Wireless Networks (SSID, BSSID)
		· Wireless Access Points (APs) and SSID Enumeration
		· Rogue AP Detection and Mitigation
		· Cracking WEP Encryption
		· Cracking WPA/WPA2 Encryption (Dictionary Attacks, WPS)
		· Evil Twin Attacks and Fake Aps
		· Capturing and Analyzing Wireless Traffic
		· Wi-Fi Password Cracking Tools (e.g., Aircrack-ng)
		· Wardriving and GPS Mapping of Wi-Fi Networks
		· Hacking Public Wi-Fi Hotspots

		· Wireless Network Auditing Tools (e.g., Kismet, Fern-Wifi- Cracker)
		· Wireless Sniffing and Packet Injection
		· Deauthentication and Jamming Attacks
		· Evading MAC Address Filtering
		· Wi-Fi Pineapple and Rogue Device Attacks
		· Wireless Network Intrusion Detection Systems (NIDS)
		· Cracking WPA3 Encryption (if applicable)
		· Security Best Practices for Wireless Networks
		· Protecting Your Own Wireless Network
		· Legal Implications of Unauthorized Wireless Hacking
		· Real-World Wireless Hacking Scenarios
		Quiz and Tasks
		Assignment: - Practical on Real-World Sniffing and Analysis - Practical on Penetration Testing of a Wireless Network
13. Social Engineering	Learn social engineering concepts and techniques, including how to identify theft attempts, audit human-level vulnerabilities, and suggest social engineering countermeasures.	· Introduction to Social Engineering
		· Legal and Ethical Aspects of Social Engineering
		· Information Gathering for Social Engineering
		· Pretexting and Impersonation
		· Phishing and Spear Phishing Attacks
		· Baiting and Tailgating Attacks
		· Influence and Persuasion Techniques
		· Manipulating Human Behavior
		· Building Trust and Rapport
		· Elicitation and Information Extraction
		· Psychological Profiling
		· Social Engineering in the Digital Age
		· Social Engineering for Physical Access

		· Social Engineering for Unauthorized Information Access
		· Social Engineering for System Hacking
		· Phishing Attacks
		· Spear Phishing and Whaling
		· Email Spoofing and Impersonation
		· Building Custom Social Engineering Attacks
		· Countermeasures and Defense Strategies
		· Ethical and Responsible Social Engineering
		Quiz and Tasks
		Assignment: - Social Engineering Case Studies and Scenarios - Practical Social Engineering Exercises within Kali Linux
14. Session Hijacking	Learn the various session-hijacking techniques used to discover network-level session management, authentication, authorization, and cryptographic weaknesses and associated countermeasures.	· Introduction to Session Hijacking
		· Legal and Ethical Aspects of Session Hijacking
		· Session Management in Web Applications
		· Session Hijacking Techniques (e.g., Session Fixation)
		· Cross-Site Scripting (XSS) Attacks
		· Cross-Site Request Forgery (CSRF) Attacks
		· Man-in-the-Middle (MitM) Attacks
		· Session Fixation Attacks
		· Session Sidejacking and Sniffing
		· Session Replay Attacks
		· Building Custom Session Hijacking Tools
		· Detecting and Mitigating Session Hijacking
		· Building Secure Session Management in Web Apps
		· Countermeasures and Defense Strategies
		· Practical on Executing a Session Hijacking Attack
		Quiz and Tasks

		Assignment: - Real-World Session Hijacking Scenarios - Practical Session Hijacking Exercises and Demonstrations - Practical on Executing a Session Hijacking Attack
15. Denial of Service	Learn about different Denial of Service (DoS) and Distributed DoS (DDoS) attack techniques, plus the tools used to audit a target and devise DoS and DDoS countermeasures and protections.	· Introduction to Denial of Service Attacks
		· Legal and Ethical Aspects of DoS Attacks
		· Types of DoS Attacks (e.g., Flood, Amplification, Logic Bombs)
		· Distributed Denial of Service (DDoS) Attacks
		· Botnets and Botnet Herders
		· Reflective and Amplification Attacks
		· Protocol-Based Attacks (e.g., SYN Flood)
		· Application Layer Attacks (e.g., HTTP Flood)
		· Denial of Service Attack Tools
		· DoS Attack Techniques and Strategies | Detection and Mitigation of DoS Attacks
		· Stress Testing and Load Balancing | Building Custom DoS Attack Tools
		· Legal and Ethical Aspects of DoS Testing | Protecting Against DoS Attacks
		· Countermeasures and Defense Strategies
		Quiz and Tasks
		Assignment: - Real-World DoS Attack Scenarios - Practical on Executing a DoS/DDoS Attack
		· Introduction to SQL Injection
		· Legal and Ethical Aspects of SQL Injection Testing
		· SQL Injection Fundamentals
		· Union-Based SQL Injection
		· Blind SQL Injection

16. SQL Injection	Learn about SQL injection attack techniques, evasion techniques, and SQL injection countermeasures.	· Time-Based Blind SQL Injection
		· Out-of-Band SQL Injection
		· Second-Order SQL Injection
		· Error-Based SQL Injection
		· Stored SQL Injection
		· Blind Second-Order SQL Injection
		· Boolean-Based Blind SQL Injection
		· SQL Injection through Different Attack Vectors
		· Automated SQL Injection Tools
		· Detecting and Analyzing SQL Injection Attacks
		· Preventing SQL Injection in Web Applications
		· Error-Based Information Gathering
		· Union-Based Data Extraction
		· Time-Based Blind SQL Injection Techniques
		· Out-of-Band Data Exfiltration
		· SQL Injection through Form Fields
		· SQL Injection through URL Parameters
		· Advanced SQL Injection Techniques
		· Exploiting SQL Injection for Privilege Escalation
		· Bypassing Web Application Firewalls (WAFs)
		· Evading Detection with Obfuscation
		· Legal and Ethical Implications of Exploiting SQL Injection
		Quiz and Tasks
		Assignment: - Real-World SQL Injection Scenarios - Practical SQL Injection Exercises - Practical on Exploiting and Preventing SQL Injection
	Learn about web server attacks, including a comprehensive attack methodology used to audit	· Introduction to Web Server Hacking
		· Legal and Ethical Aspects of Web Server Hacking
		· Web Server Fundamentals (e.g., Apache, Nginx)

17. Hacking Web Servers & Web Applications	vulnerabilities in web server infrastructures and countermeasures. Learn about web application attacks, including a comprehensive hacking methodology for auditing vulnerabilities in web applications and countermeasures.	· Information Gathering and Reconnaissance
		· Vulnerability Scanning and Enumeration
		· Web Server Misconfigurations
		· Directory Traversal Attacks
		· File Inclusion Vulnerabilities
		· SQL Injection in Web Servers
		· Remote Code Execution (RCE)
		· Exploiting Known Vulnerabilities
		· Web Shells and Backdoors
		· Denial of Service Attacks on Web Servers
		· Password Cracking for Server Access
		· Privilege Escalation Techniques
		· Web Server Hardening and Security
		· Building Secure Web Applications
		· Countermeasures and Defense Strategies
		· Introduction to Web Application Hacking
		· Legal and Ethical Aspects of Web Application Hacking
		· Web Application Fundamentals (e.g., HTML, HTTP, Cookies)
		· Information Gathering and Reconnaissance
		· Web Application Scanning and Enumeration
		· Identifying Common Web Application Vulnerabilities
		· Cross-Site Scripting (XSS)
		· SQL Injection in Web Applications
		· Cross-Site Request Forgery (CSRF)
		· Insecure Deserialization
		· Security Misconfigurations
		· Session Management Vulnerabilities
		· Web Application Fuzzing and Testing

		· Attacking Authentication and Authorization
		· File Upload and File Inclusion Vulnerabilities
		· Web Application Firewalls (WAFs)
		· Secure Coding and Development Best Practices
		· Countermeasures and Defense Strategies
		Quiz and Tasks
		Assignment: - Real-World Web Server Hacking Scenarios - Practical Web Server Hacking Exercises and Demonstrations - Real-World Web Application Hacking Scenarios - Practical Web Application Hacking Exercises and Demonstrations - Practical on Hacking a Web Server - Practical on Hacking a Web Application
18. Mobile Platforms	Learn mobile platform attack vectors, Android and iOS hacking, mobile device management, mobile security guidelines, and security tools.	· Introduction to Mobile Platform Security
		· Legal and Ethical Aspects of Mobile Hacking
		· Mobile Platform Fundamentals (iOS, Android)
		· Mobile Application Security Models
		· Identifying Mobile Security Vulnerabilities
		· Setting Up a Mobile Hacking Environment
		· Device and Emulator Testing Jailbreaking (iOS) and Rooting (Android)
		· Analyzing Mobile Apps for Vulnerabilities
		· Data Storage and Encryption on Mobile Devices
		· Insecure Data Transmission (e.g., SSL Pinning Bypass)
		· Mobile API Testing and Manipulation
		· Reverse Engineering Mobile Apps
		· Exploiting Authentication and Authorization Flaws

		· In-App Purchases and License Verification Bypass
		· Tampering with Mobile App Logic
		· Mobile Malware and Spyware
		· Real-World Mobile Exploits and Vulnerabilities
		· Detecting and Preventing Mobile Exploits
		· Mobile Application Security Best Practices
		· Ethical Use of Mobile Hacking Skills
		· Mobile Hacking Challenges and CTFs
		· iOS Jailbreaks and Bypassing Security Features
		· Android Rooting and Custom ROMs
		· Mobile App Debugging and Patching
		· Application Security Testing on Real Devices
		· Malware Analysis on Mobile Platforms
		· Mobile Device Forensics
		Quiz and Tasks
		Assignment: - Practical on Hacking a Mobile App or Device
19. Evading IDS, Firewalls, and Honeypots (Optional)	Learn about firewalls, intrusion detection systems (IDS), and honeypot evasion techniques; the tools used to audit a network perimeter for weaknesses; and countermeasures.	Learn about firewalls, intrusion detection systems (IDS), and honeypot evasion techniques; the tools used to audit a network perimeter for weaknesses; and countermeasures.
		Quiz and Tasks
		Assignment: - Research Activity
20. IoT Hacking (Optional)	Learn different types of Internet of Things (IoT) and operational technology (OT) attacks, hacking methodologies, hacking tools, and countermeasures.	Learn different types of Internet of Things (IoT) and operational technology (OT) attacks, hacking methodologies, hacking tools, and countermeasures.
		Quiz and Tasks
		Assignment: - Research Activity

21. Cloud Computing (Optional)	Learn different cloud computing concepts, such as container technologies and serverless computing, various cloud computing threats, attacks, hacking methodologies, and cloud security techniques and tools.	Learn different cloud computing concepts, such as container technologies and serverless computing, various cloud computing threats, attacks, hacking methodologies, and cloud security techniques and tools.
		Quiz and Tasks
		Assignment: - Research Activity
22. Cryptography	Learn about encryption algorithms, cryptography tools, Public Key Infrastructure (PKI), email encryption, disk encryption, cryptography attacks, and cryptanalysis tools.	· Introduction to Cryptography
		· Legal and Ethical Aspects of Cryptography
		· Basic Concepts of Cryptography (Encryption, Decryption)
		· Classical Cryptography (Caesar, Vigenère, etc.)
		· Modern Cryptography Techniques (AES, RSA, ECC, etc.)
		· Cryptographic Hash Functions (MD5, SHA, etc.)
		· Public Key Infrastructure (PKI)
		· Cryptographic Protocols (SSL/TLS, SSH, etc.)
		· Cryptanalysis and Attacks on Cryptosystems
		· Quantum Cryptography and Post-Quantum Cryptography
		· Secure Key Management and Exchange
		· Cryptographic Libraries and APIs
		· Implementing Cryptographic Algorithms
		· Digital Signatures and Authentication
		· Secure Communication with Cryptography
		· Cryptography in Blockchain Technology
		· Cryptography in Network Security
		· Cryptography in Mobile Security
		· Cryptography in Web Application Security
		Quiz and Tasks

		Assignment: - Real-World Cryptographic Attacks and Defenses - Practical Cryptographic Exercises - Practicals on Cryptography (Encryption, Hashing)
23. Bug Bounty		· Introduction to Bug Bounty Programs
		· Legal and Ethical Aspects of Bug Bounty Hunting
		· Bug Bounty Platforms and Marketplaces
		· Setting Up a Bug Bounty Hunter Profile
		· Finding and Researching Bug Bounty Programs
		· Types of Security Vulnerabilities (OWASP Top Ten)
		· Reconnaissance and Footprinting for Bug Bounties
		· Web Application Testing for Security Vulnerabilities
		· Mobile Application Testing for Security Vulnerabilities
		· Network and Infrastructure Testing for Security Vulnerabilities
		· Identifying Security Vulnerabilities
		· Proof of Concept (PoC) and Exploitation
		· Bug Triage and Severity Assessment
		· Creating Detailed Bug Bounty Reports
		· Communication with Bug Bounty Programs
		· Bug Bounty Rewards and Payments
		· Bug Bounty Platform Tools and Resources
		Quiz and Tasks
		Assignment: - Practical on Bug Bounty Hunting
24. Exam Prep & Project	This module reinforces all concepts learned across the course through structured review sessions.	· Certification Exam Preparation
		· Project & Assessment
		Quiz and Tasks

	Students undergo practice exams, scenario walkthroughs, and knowledge assessments. It focuses on exam strategy, troubleshooting weak areas, and developing confidence for certification success.	**Assignment:** - Project Runs in parallel focusing on Penetration Testing simulation with a PenTest Report. - Present and evaluate the project outcome.

Notes:

Activities & Tasks	All Tasks are as per NAVTTC Course Annexure-I, however Quiz, assignments and Capstone Project are additional
Motivational Lecture	We have a separate Soft Skill program which will be conducted every week on Soft Skill day. An Outlined draft of our Soft Skills program is attached Separately

Item	NIAI	Remarks
Course Duration	3 Months (12 Weeks)	All NAVTTC topics covered + Corporate development Soft Skills Program
Total Class Days	5 Days	4 days/week (Course) + 1day for soft skills.
In-Class Hours	3 hours/day	Content coverage sustained
Total In-Class Hours	144 hours (Excluding notional hours)	In-Class subject: 144 hours In-Class Soft Skills: 24 hours Project work: Approx. 100 hours (guided independent and team-based projects)

2. Soft Skills & Leadership Modules

"Delivered by NIAI's (NETSOL Institute of Artificial Intelligence) Organizational Development experts, these modules enhance corporate readiness and professional competencies:"

- Building Future Ready Tech Leaders
- Communication Improvement Program
- Teamwork & Collaboration
- Emotional Intelligence & Empathy

This stream adds 2 hours/week across 12 weeks (24- credit hours), reinforcing Professionalism and Business Skills competencies vital for workplace integration.