Government of Pakistan

National Vocational and Technical Training Commission

Prime Minister Youth Skills Development Program

"Skills for All"

Course Contents / Lesson Plan
Course Title: CEH (Certified Ethical Hacking)
Duration: 3 Months

Revised Edition

Trainer Name	
Author Name	**Sabah-ud-din Afzal (CEO Amal IT Solution)**
Course Title	**CEH (Certified Ethical Hacking)**
Objectives and Expectations	**Employable skills and hands-on practice in CEH (Certified Ethical Hacking)** This is a special course designed to address unemployment in the youth. The course aims to achieve the above objective through hands on practical training delivery by a team of dedicated professionals having rich market/work experience. This course is therefore not just for developing a theoretical understanding/back ground of the trainees. Contrary to that, it is primarily aimed at equipping the trainees to perform commercially in a market space in independent capacity or as a member of a team. The course therefore is designed to impart not only technical skills but also soft skills (i.e. interpersonal/communication skills; personal grooming of the trainees etc.) as well as entrepreneurial skills (i.e. marketing skills; freelancing etc.). The course also seeks to inculcate work ethics to foster better citizenship in general and improve the image of Pakistani work force in particular. **Main Expectations:** In short, the course under reference should be delivered by professional instructors in such a robust hands-on manner that the trainees are comfortably able to employ their skills for earning money (through wage/self-employment) at its conclusion. This course thus clearly goes beyond the domain of the traditional training practices in vogue and underscores an expectation that a market-centric approach will be adopted as the main driving force while delivering it. The instructors should therefore be experienced enough to be able to identify the training needs for the possible market roles available out there. Moreover, they should also know the strengths and weaknesses of each trainee to prepare them for such market roles during/after the training. **i.** Specially designed practical tasks to be performed by the trainees have been included in the Annexure-I to this document. The record of all tasks performed individually or in groups must be preserved by the management of the training Institute clearly labeling name, trade, session, etc. so that these are ready to be physically inspected/verified through monitoring visits from time to time. The weekly distribution of tasks has also been indicated in the weekly lesson plan given in this document. **ii.** To materialize the main expectations, a special module on **Job Search & Entrepreneurial Skills** has been included in the latter part of this course (5th & 6th month) through which, the trainees will be made aware of the Job search techniques in the local as well as international job markets (Gulf countries). Awareness around the visa process and immigration laws of the most favored labor destination countries also

form a part of this module. Moreover, the trainees would also be encouraged to venture into self-employment and exposed to the main requirements in this regard. It is also expected that a sense of civic duties/roles and responsibilities will also be inculcated in the trainees to make them responsible citizens of the country.

iii. A module on **Work Place Ethics** has also been included to highlight the importance of good and positive behavior in the workplace in the line with the best practices elsewhere in the world. An outline of such qualities has been given in the Appendix to this document. Its importance should be conveyed in a format that is attractive and interesting for the trainees such as through PPT slides +short video documentaries. Needless to say that if the training provider puts his heart and soul into these otherwise non-technical components, the image of the Pakistani workforce would undergo a positive transformation in the local as well as international job markets.

To maintain interest and motivation of the trainees throughout the course, modern techniques such as:

- Motivational Lectures
- Success Stories
- Case Studies

These techniques would be employed as an additional training tool wherever possible (these are explained in the subsequent section on Training Methodology).

Lastly, evaluation of the competencies acquired by the trainees will be done objectively at various stages of the training and a proper record of the same will be maintained. Suffice to say that for such evaluations, practical tasks would be designed by the training providers to gauge the problem-solving abilities of the trainees.

(i) Motivational Lectures

The proposed methodology for the training under reference employs motivation as a tool. Hence besides the purely technical content, a trainer is required to include elements of motivation in his/her lecture. To inspire the trainees to utilize the training opportunity to the full and strive towards professional excellence. Motivational lectures may also include general topics such as the importance of moral values and civic role & responsibilities as a Pakistani. A motivational lecture should be delivered with enough zeal to produce a deep impact on the trainees. It may comprise of the following:

- Clear Purpose to convey the message to trainees effectively.
- Personal Story to quote as an example to follow.
- Trainees Fit so that the situation is actionable by trainees and not represent a just idealism.
- Ending Points to persuade the trainees on changing themselves.

A good motivational lecture should help drive creativity, curiosity, and spark the desire needed for trainees to want to learn more.

The impact of a successful motivational strategy is amongst others commonly visible in increased class participation ratios. It increases the trainees' willingness to be engaged on the practical tasks for a longer time without boredom and loss of interest because they can see in their mind's eye where their hard work would take them in short (1-3 years); medium (3 -10 years) and long term (more than 10 years).

As this tool is expected that the training providers would make arrangements for regular well planned motivational lectures as part of a coordinated strategy interspersed throughout the training period as suggested in the weekly lesson plans in this document.
Course-related motivational lectures online link is available in **Annexure-II**.

(ii) Success Stories

Another effective way of motivating the trainees is using Success Stories. Its inclusion in the weekly lesson plan at regular intervals has been recommended till the end of the training.
A success story may be disseminated orally, through a presentation, or using a video/documentary of someone that has risen to fortune, acclaim, or brilliant achievement. A success story shows how a person achieved his goal through hard work, dedication, and devotion. An inspiring success story contains compelling and significant facts articulated clearly and easily comprehendible words. Moreover, it is helpful if it is assumed that the reader/listener knows nothing of what is being revealed. The optimum impact is created when the story is revealed in the form of:-

- Directly in person (At least 2-3 cases must be arranged by the training institute)
- Through an audio/ videotaped message (2-3 high-quality videos must be arranged by the training institute)

It is expected that the training provider would collect relevant high-quality success stories for inclusion in the training as suggested in the weekly lesson plan given in this document.
The suggestive structure and sequence of a sample success story and its various shapes can be seen in **Annexure III**.

(iii) Case Studies

Where a situation allows, case studies can also be presented to the trainees to widen their understanding of the real-life specific problem/situation and to explore the solutions.
In simple terms, the case study method of teaching uses a real-life case example/a typical case to demonstrate a phenomenon in action and explain theoretical as well as practical aspects of the knowledge related to the same. It is an effective way to help the trainees comprehend in depth both the theoretical and practical aspects of the complex phenomenon in depth with ease. Case teaching can also stimulate the trainees to participate in discussions and thereby boost their confidence. It also makes the classroom atmosphere interesting thus maintaining the trainee interest in training till the end of the course.
Depending on suitability to the trade, the weekly lesson plan in this document may suggest case studies be presented to the trainees. The trainer may adopt a PowerPoint presentation or video format for such case studies whichever is deemed suitable but only those cases must be selected that are relevant and of a learning value.
The Trainees should be required and supervised to carefully analyze the cases.
For this purpose, they must be encouraged to inquire and collect specific information/data, actively participate in the discussions, and intended solutions to the problem/situation.
Case studies can be implemented in the following ways: -

	i. A good quality trade-specific documentary (At least 2-3 documentaries must be arranged by the training institute) ii. Health &Safety case studies (2 cases regarding safety and industrial accidents must be arranged by the training institute) iii. Field visits(At least one visit to a trade-specific major industry/ site must be arranged by the training institute)
Entry-level of trainees	For an advanced course of Cyber Security (CEH) proposed entry level is minimum bachelors in relevant subject, so expectations from the trainees are: • Fundamentals of Networking. • Fundamentals of script programming. • Basic Cyber Security Concepts. • Basic Ethical Hacking Tools. • Ethical Hacking Methodology.
Learning Outcomes of the course	By the end of this course, students will be able to: **Understanding of Ethical Hacking Concepts** • Define ethical hacking and its role in cybersecurity. • Differentiate between ethical hacking and malicious hacking. • Comprehend the ethical and legal considerations in penetration testing. **Network Security Fundamentals** • Demonstrate knowledge of network protocols and their vulnerabilities. • Understand network security architecture and defenses. • Identify and mitigate common network-based attacks. **Information Security Technologies:** • Familiarity with various security tools and technologies. • Proficiency in using penetration testing tools such as Nmap, Metasploit, Wireshark, etc. • Understanding of intrusion detection and prevention systems. **Web Application Security** • Identify and exploit common web application vulnerabilities. • Implement secure coding practices. • Perform web application security assessments. **Wireless Network Security** • Analyze and secure wireless networks. • Identify vulnerabilities in wireless protocols. • Implement measures to secure wireless communications. **System Security** • Evaluate and secure operating systems. • Implement host-based security measures. • Understand and mitigate common system-level vulnerabilities. **Bug Bounty Concepts and Practices** • Understand the bug bounty ecosystem. • Comprehend the role of bug bounty hunters and security researchers. • Develop skills for responsible disclosure of security vulnerabilities. **Practical Application of Ethical Hacking** • Execute penetration testing methodologies. • Conduct vulnerability assessments on various targets. • Develop and execute a penetration testing plan.

	Legal and Ethical Considerations • Understand the legal and ethical aspects of ethical hacking. • Comply with laws and regulations related to penetration testing. • Adhere to ethical guidelines and responsible disclosure practices.
Course Execution Plan	The total duration of the course: **3 months (12 Weeks)** Class hours: **4 hours per day** Theory: **20%** Practical: **80%** Weekly hours: **20 hours per week** Total contact hours: **260 hours**
Companies offering jobs in the respective trade	• Trillium • Afinity • NetSole • I2c • Multinet • Nescom • Transworld • Netcom • Systems • Web Work Solution • Purelogics • Nets-international • Ebryx
Job Opportunities	• Security Operations Centre (SOC) Engineer • Network Administrator • IT Support Officer • Manager / Assistant Manager IT • Network support engineer • Security Analysts • Penetration tester
No of Students	25
Learning Place	Classroom / Lab
Instructional Resources	1. Introduction to Cyber Security: https://www.youtube.com/watch?v=z5nc9MDbvkw 2. Cyber Security Crash Course in English: https://www.youtube.com/watch?v=hXSFdwIOfnE 3. Ethical Hacking Crash Course in Urdu: https://www.youtube.com/watch?v=596WPxrBFqo 4. Network Hacking Crash Course in Urdu: https://www.youtube.com/watch?v=2hoeSbrtmLQ

	5. Bug Bounty Crash Course in Urdu: https://www.youtube.com/watch?v=-t95lFMndw4

MODULES

Scheduled Weeks	Module Title	Days	Hours	Learning Units	Home Assignment
Week 1	**Introduction to CEH and LAB Setup**	**Day 1**	**Hour 1**	• Motivational Lecture • Course Intro • Success stories • Job Market • Intro to CEH • Roles of Security Expert • What is cyberspace. • What is hacker and its different types.	
			Hour 2	• What is virus and its different types	
			Hour 3	• Different types of attacks.	
			Hour 4	• Setup virtual machine for LAB environment.	• **Task 1** *Details may be seen at Annexure-I*
		Day 2	**Hour 1**	• Install and configure Kali Linux	
			Hour 2	• Intro Kali Linux. • Important Linux Commands	
			Hour 3	• Get familiar with OSI Layers • Different functions of OSI layers.	
			Hour 4	• Protocols of each layers	
		Day 3	**Hour 1**	• Get familiar with TCP/IP suit.	
			Hour 2	• Different protocols and ports.	

			Hour 3	• Basic Network Configuration	
			Hour 4	Hands-on Practice on LAB Setup for testing	
		Day 4	**Hour 1**	• Open Source Intelligence (OSINT) Overview • Passive vs. Active Information Gathering	
			Hour 2	• Information Gathering Methodologies	
			Hour 3	• Ethical Considerations in OSINT • Footprinting and Reconnaissance	
			Hour 4	• Search Engine Hacking • Social Media Intelligence	
		Day 5	**Hour 1**	• Email and Domain Information Gathering • Metadata Analysis	
			Hour 2	• WHOIS Data and Domain Ownership • DNS Enumeration	
			Hour 3	• Enumeration of Network Services	
			Hour 4	Hands-on Practice with an Information Gathering	
Week 2	**Information Gathering**	**Day 1**	**Hour 1**	• Shodan and IoT Device Information	• **Task 2**
			Hour 2	• Maltego for Data Link Analysis	

			Hour 3	• The Harvester for Gathering Emails and Subdomains	*Details may be seen at Annexure-I*
			Hour 4	• Spokeo and People Search Tools	
		Day 2	**Hour 1**	• Data Scraping Techniques	
			Hour 2	• Google Dorks and Advanced Search Queries	
			Hour 3	• Geolocation and IP Tracing	
			Hour 4	• Social Engineering for Information Gathering Algorithms • Gathering Information on Mobile Apps	
		Day 3	**Hour 1**	Deep Web and Dark Web Information Gathering	
			Hour 2	Tor and Onion Sites Exploration	
			Hour 3	Threat Intelligence Feeds	
			Hour 4	OSINT Frameworks and Tools	
		Day 4	**Hour 1**	Visualizing OSINT Data	
			Hour 2	OSINT for Digital Forensics	
			Hour 3	OSINT for Incident Response	
			Hour 4	Legal and Ethical Aspects of OSINT	
		Day 5	**Hour 1-4**	Practical on OSINT Investigations	

Week 3	**Scanning & Enumeration**	**Day 1**	**Hour 1**	• Network Scanning Fundamentals • Types of Network Scans • Port Scanning Techniques	• **Task 3** *Details may be seen at Annexure-I*
			Hour 2	• TCP Connect Scanning • UDP Scanning • Banner Grabbing	
			Hour 3	• Network Enumeration Methods • Scanning Tools and Utilities • Nmap - Network Mapper	
			Hour 4	• Ping Sweeps and Sweep Detection • Network Mapping and Topology Discovery • Vulnerability Scanning	
		Day 2	**Hour 1**	• Operating System Detection • Automated Scanning Workflows • Scanning for Web Applications	
			Hour 2	• Threat Intelligence Integration • Wireless Network Scanning • Automating Scans with Scripts	
			Hour 3	• Scanning Best Practices • Scanning Ethics and Legal Considerations • Post-Scanning Analysis	
			Hour 4	• Scanning for Insider Threats • Enumeration Basics	

				• NetBIOS Enumeration	
		Day 3	**Hour 1**	• SNMP Enumeration • LDAP Enumeration • SMB Enumeration	
			Hour 2	• DNS Enumeration • SMTP Enumeration • NTP Enumeration	
			Hour 3	• SSH Enumeration • RDP Enumeration • Port Enumeration Techniques	
			Hour 4	• User Enumeration • Share Enumeration • Vulnerability Enumeration	
		Day 4	**Hour 1**	• Enumeration Tools and Scanners • Nmap Scripts for Enumeration • SNMP Enumeration Tools	
			Hour 2	• LDAP Enumeration Tools • SMB Enumeration Tools • DNS Enumeration Tools	
			Hour 3	• SMTP Enumeration Tools • Enumeration for Active Directory • Enumeration for Linux	
			Hour 4	• Enumeration for Windows • Enumeration Best Practices • Enumeration Ethics and Legal Considerations	
		Day 5	**Hour 1-2**	Practical on Comprehensive Network Scan	
			Hour 3-4	Practical on Comprehensive Enumeration	

Week 4	**Vulnerability Analysis**	**Day 1**	**Hour 1**	• Vulnerability Assessment Fundamentals • Types of Vulnerabilities	
			Hour 2	Vulnerability Scanning Techniques	
			Hour 3	Automated Vulnerability Scanners	
			Hour 4	Manual Vulnerability Assessment	
		Day 2	**Hour 1**	• Common Vulnerability Databases • Common Vulnerability Scoring System (CVSS)	
			Hour 2	Vulnerability Management Practices	• **Task 4** *Details may be seen at Annexure-I*
			Hour 3	Vulnerability Analysis Tools	
			Hour 4	Nmap Scripting Engine (NSE) for Vulnerability Scanning	
		Day 3	**Hour 1**	OpenVAS - Open Vulnerability Assessment System	
			Hour 2	Nessus Vulnerability Scanner	
			Hour 3	Qualys Vulnerability Management	
			Hour 4	• Vulnerability Assessment in Web Applications • OWASP Top Ten Vulnerabilities	

		Day 4	**Hour 1**	Vulnerability Analysis for Mobile Applications	
			Hour 2	Vulnerability Analysis for Network Devices	
			Hour 3	• Reporting and Remediation of Vulnerabilities • Exploitation Frameworks and Vulnerabilities	
			Hour 4	• Vulnerability Analysis Best Practices • Legal and Ethical Aspects of Vulnerability Analysis	
		Day 5	**Hour 1**	Vulnerability Analysis Case Studies	
			Hour 2-4	Practical on Comprehensive Vulnerability Analysis	
Week 5	**System Hacking & Malware Analysis**	**Day 1**	**Hour 1**	• System Hacking Fundamentals • Password Cracking Techniques • Password Cracking Tools	
			Hour 2	• Privilege Escalation Methods • Exploiting Weak Passwords • Brute Force and Dictionary Attacks	• **Task 5** *Details may be seen at Annexure-I*
			Hour 3	• Cracking Windows Passwords • Cracking Linux Passwords • Privilege Escalation on Windows	
			Hour 4	• Privilege Escalation on Linux • Rootkits and Trojans • Hiding Files and Processes	

				• Covering Tracks and Removing Evidence	
		Day 2	**Hour 1**	• Malware and Backdoors • Social Engineering for System Hacking • Phishing Attacks	
			Hour 2	• Spear Phishing and Whaling • Email Spoofing and Impersonation • Bypassing Antivirus Software	
			Hour 3	• Keyloggers and Spyware • Remote Administration Tools (RATs) • Advanced Persistent Threats (APTs)	
			Hour 4	• Fileless Malware • Post-Exploitation Techniques • Exploitation Frameworks • Legal and Ethical Aspects of System Hacking	
		Day 3	**Hour 1**	• Introduction to Malware Analysis • Malware Analysis Fundamentals • Types of Malware and Malicious Code	
			Hour 2	• Malware Analysis Environments and Sandboxes • Static Analysis Techniques • Dynamic Analysis Techniques	
			Hour 3	• Behavioral Analysis of Malware • Memory Analysis and Forensics • Disassembling and Debugging Malicious	

				Code	
			Hour 4	• Code Injection and Hooking Techniques • Deobfuscation and Decryption • YARA Rules for Malware Detection • Identifying and Classifying Malware Families	
		Day 4	**Hour 1**	• Packets Analysis for Malware Detection • Building Custom Malware Analysis Tools • Network Traffic Analysis	
			Hour 2	• Malware Artifacts and Indicators of Compromise (IoC) • Threat Intelligence and Malware Data Sources • Building a Malware Sandbox	
			Hour 3	• Building a YARA Rule Library • Building a Memory Forensics Toolkit • Building Custom Analysis Scripts	
			Hour 4	• Practical Malware Analysis Techniques • Legal and Ethical Aspects of Malware Analysis	
		Day 5	**Hour 1**	System Hacking Case Studies	
			Hour 2	Malware Analysis Case Studies	
			Hour 3	Practical on Comprehensive System Hacking	

			Hour 4	Practical on Analyzing Real-World Malware Samples	
Week 6	**Network Sniffing & Wifi Hacking**	**Day 1**	**Hour 1**	• Introduction to Network Packet Sniffing • Legal and Ethical Aspects of Sniffing • Wireshark and Packet Capture Basics	• **Task 6** *Details may be seen at Annexure-I*
			Hour 2	• Analyzing Captured Packets • Packet Filtering and Display Options	
			Hour 3	• Advanced Protocol Analysis • Packet Decryption Techniques • Capturing and Analyzing SSL/TLS Traffic	
			Hour 4	• Sniffing on Wireless Networks • Sniffing on Switched Networks	
		Day 2	**Hour 1**	• ARP Spoofing and MITM Attacks • DNS Spoofing and Cache Poisoning	
			Hour 2	• VoIP Traffic Sniffing • Sniffing for Malware Traffic	
			Hour 3	• Network Sniffing for Intrusion Detection • Building Custom Sniffing Tools	
			Hour 4	• Sniffing Case Studies and Real-World Scenarios • Sniffing for Security and Troubleshooting • Sniffing Best Practices and Avoiding Detection	
		Day 3	**Hour 1**	• Introduction to Wireless Networks and Security • Legal and Ethical Aspects of Wireless Hacking	

				• Wireless Network Fundamentals (Wi-Fi, WEP, WPA, WPA2)	
			Hour 2	• Wireless Encryption Protocols (WEP, WPA, WPA2, WPA3) • Understanding Wi-Fi Security Vulnerabilities • Scanning for Wireless Networks (SSID, BSSID)	
			Hour 3	• Wireless Access Points (APs) and SSID Enumeration • Rogue AP Detection and Mitigation • Cracking WEP Encryption • Cracking WPA/WPA2 Encryption (Dictionary Attacks, WPS)	
			Hour 4	• 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	
		Day 4	**Hour 1**	• Hacking Public Wi-Fi Hotspots • Wireless Network Auditing Tools (e.g., Kismet, Fern-Wifi-Cracker) • Wireless Sniffing and Packet Injection	
			Hour 2	• Deauthentication and Jamming Attacks • Evading MAC Address Filtering • Wi-Fi Pineapple and Rogue Device Attacks	
			Hour 3	• Wireless Network Intrusion Detection Systems (NIDS)	

				• Cracking WPA3 Encryption (if applicable) • Security Best Practices for Wireless Networks	
			Hour 4	• Protecting Your Own Wireless Network • Legal Implications of Unauthorized Wireless Hacking • Real-World Wireless Hacking Scenarios	
		Day 5	**Hour 1-2**	Practical on Real-World Sniffing and Analysis	
			Hour 3-4	Practical on Penetration Testing of a Wireless Network	
Week 7	**Social Engineering & Session Hijacking**	**Day 1**	**Hour 1**	• Introduction to Social Engineering • Legal and Ethical Aspects of Social Engineering • Information Gathering for Social Engineering	
			Hour 2	• Pretexting and Impersonation • Phishing and Spear Phishing Attacks	
			Hour 3	• Baiting and Tailgating Attacks • Influence and Persuasion Techniques	• **Task 7** *Details may be seen at Annexure-I*
			Hour 4	• Manipulating Human Behavior • Building Trust and Rapport • Elicitation and Information Extraction	
		Day 2	**Hour 1**	• Psychological Profiling • Social Engineering in the Digital Age • Social Engineering for Physical Access	
			Hour 2	• Social Engineering for Unauthorized Information Access	

				• Building Custom Social Engineering Attacks	
			Hour 3	• Practical Social Engineering Exercises within Kali Linux • Countermeasures and Defense Strategies	
			Hour 4	• Social Engineering Case Studies and Scenarios • Ethical and Responsible Social Engineering	
		Day 3	**Hour 1**	• Introduction to Session Hijacking • Legal and Ethical Aspects of Session Hijacking	
			Hour 2	• Session Management in Web Applications • Session Hijacking Techniques (e.g., Session Fixation)	
			Hour 3	• Cross-Site Scripting (XSS) Attacks • Cross-Site Request Forgery (CSRF) Attacks	
			Hour 4	• Man-in-the-Middle (MitM) Attacks • Session Fixation Attacks	
		Day 4	**Hour 1**	• Session Sidejacking and Sniffing • Session Replay Attacks	
			Hour 2	• Building Custom Session Hijacking Tools • Detecting and Mitigating Session Hijacking	
			Hour 3	• Building Secure Session Management in Web Apps • Real-World Session Hijacking Scenarios	

			Hour 4	• Practical Session Hijacking Exercises and Demonstrations • Countermeasures and Defense Strategies	
		Day 5	**Hour 1-2**	Practical on Executing a Social Engineering Attack within Kali Linux	
			Hour 3-4	Practical on Executing a Session Hijacking Attack	
Week 8	**DOS/DDOS & SQL Injection Attack**	**Day 1**	**Hour 1**	• Introduction to Denial of Service Attacks • Legal and Ethical Aspects of DoS Attacks • Types of DoS Attacks (e.g., Flood, Amplification, Logic Bombs)	
			Hour 2	• Distributed Denial of Service (DDoS) Attacks • Botnets and Botnet Herders	
			Hour 3	• Reflective and Amplification Attacks • Protocol-Based Attacks (e.g., SYN Flood)	
			Hour 4	• Application Layer Attacks (e.g., HTTP Flood) • Denial of Service Attack Tools	• **Task 8** *Details may be seen at Annexure-I*
		Day 2	**Hour 1**	• DoS Attack Techniques and Strategies • Detection and Mitigation of DoS Attacks	
			Hour 2	• Stress Testing and Load Balancing • Building Custom DoS Attack Tools	
			Hour 3	• Legal and Ethical Aspects of DoS Testing • Real-World DoS Attack Scenarios	
			Hour 4	• Protecting Against DoS Attacks • Countermeasures and Defense Strategies	

		Day 3	**Hour 1**	• Introduction to SQL Injection • Legal and Ethical Aspects of SQL Injection Testing • SQL Injection Fundamentals • Union-Based SQL Injection	
			Hour 2	• Blind SQL Injection • Time-Based Blind SQL Injection • Out-of-Band SQL Injection • Second-Order SQL Injection	
			Hour 3	• Error-Based SQL Injection • Stored SQL Injection • Blind Second-Order SQL Injection • Boolean-Based Blind SQL Injection	
			Hour 4	• SQL Injection through Different Attack Vectors • Automated SQL Injection Tools • Detecting and Analyzing SQL Injection Attacks	
		Day 4	**Hour 1**	• Preventing SQL Injection in Web Applications • Error-Based Information Gathering • Union-Based Data Extraction	
			Hour 2	• Time-Based Blind SQL Injection Techniques • Out-of-Band Data Exfiltration • SQL Injection through Form Fields • SQL Injection through URL Parameters	
			Hour 3	• Advanced SQL Injection Techniques • Exploiting SQL Injection for Privilege Escalation	

				• Bypassing Web Application Firewalls (WAFs)	
			Hour 4	• Evading Detection with Obfuscation • Legal and Ethical Implications of Exploiting SQL Injection • Real-World SQL Injection Scenarios • Practical SQL Injection Exercises	
		Day 5	**Hour 1-2**	Practical on Executing a DoS/DDoS Attack	
			Hour 3-4	Practical on Exploiting and Preventing SQL Injection	
Week 9	**Hacking Web Servers & Web Applications**	**Day 1**	**Hour 1**	• Introduction to Web Server Hacking • Legal and Ethical Aspects of Web Server Hacking • Web Server Fundamentals (e.g., Apache, Nginx)	
			Hour 2	• Information Gathering and Reconnaissance • Vulnerability Scanning and Enumeration	
			Hour 3	• Web Server Misconfigurations • Directory Traversal Attacks	• **Task 9** *Details may be seen at Annexure-I*
			Hour 4	• File Inclusion Vulnerabilities • SQL Injection in Web Servers • Remote Code Execution (RCE)	
		Day 2	**Hour 1**	• Exploiting Known Vulnerabilities • Web Shells and Backdoors • Denial of Service Attacks on Web Servers	

			Hour 2	• Password Cracking for Server Access • Privilege Escalation Techniques	
			Hour 3	• Web Server Hardening and Security • Building Secure Web Applications	
			Hour 4	• Real-World Web Server Hacking Scenarios • Practical Web Server Hacking Exercises and Demonstrations • Countermeasures and Defense Strategies	
		Day 3	**Hour 1**	• Introduction to Web Application Hacking • Legal and Ethical Aspects of Web Application Hacking • Web Application Fundamentals (e.g., HTML, HTTP, Cookies)	
			Hour 2	• Information Gathering and Reconnaissance • Web Application Scanning and Enumeration	
			Hour 3	• Identifying Common Web Application Vulnerabilities • Cross-Site Scripting (XSS) • SQL Injection in Web Applications	
			Hour 4	• Cross-Site Request Forgery (CSRF) • Insecure Deserialization	
		Day 4	**Hour 1**	• Security Misconfigurations • Session Management Vulnerabilities • Web Application Fuzzing and Testing	
			Hour 2	• Attacking Authentication and Authorization	

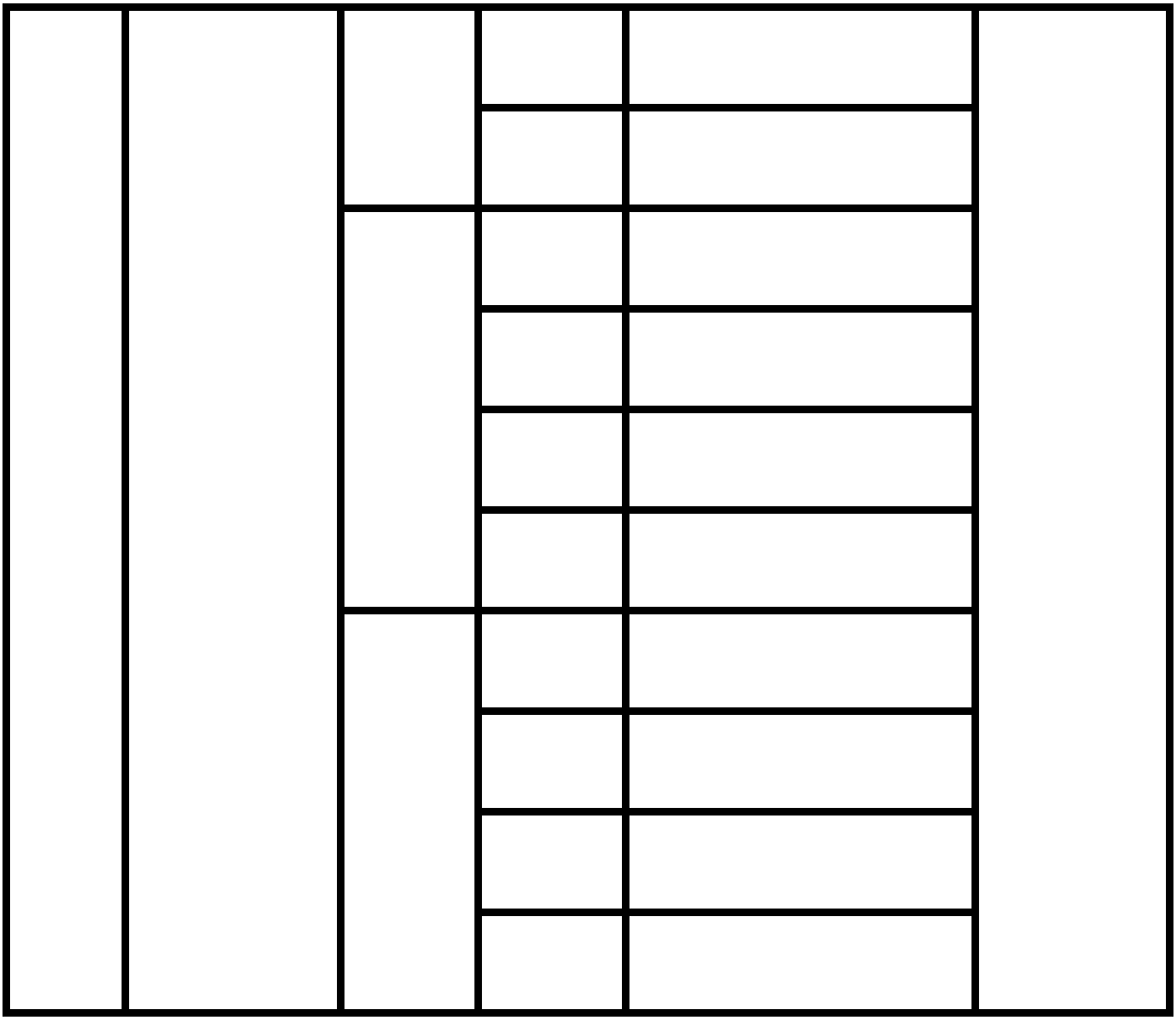
				• File Upload and File Inclusion Vulnerabilities	
			Hour 3	• Web Application Firewalls (WAFs) • Secure Coding and Development Best Practices	
			Hour 4	• Real-World Web Application Hacking Scenarios • Practical Web Application Hacking Exercises and Demonstrations • Countermeasures and Defense Strategies	
		Day 5	**Hour 1-2**	Practical on Hacking a Web Server	
			Hour 3-4	Practical on Hacking a Web Application	
Week 10	**Hacking Mobile Platforms**	**Day 1**	**Hour 1**	• Introduction to Mobile Platform Security • Legal and Ethical Aspects of Mobile Hacking	• **Task 10** *Details may be seen at Annexure-I*
			Hour 2	• Mobile Platform Fundamentals (iOS, Android) • Mobile Application Security Models	
			Hour 3	• Identifying Mobile Security Vulnerabilities • Setting Up a Mobile Hacking Environment	
			Hour 4	• Device and Emulator Testing Jailbreaking (iOS) and Rooting (Android)	
		Day 2	**Hour 1**	Analyzing Mobile Apps for Vulnerabilities	
			Hour 2	• Data Storage and Encryption on Mobile Devices	

				• Insecure Data Transmission (e.g., SSL Pinning Bypass)	
			Hour 3	• Mobile API Testing and Manipulation • Reverse Engineering Mobile Apps	
			Hour 4	• Exploiting Authentication and Authorization Flaws • In-App Purchases and License Verification Bypass	
		Day 3	**Hour 1**	Tampering with Mobile App Logic	
			Hour 2	• Mobile Malware and Spyware • Real-World Mobile Exploits and Vulnerabilities	
			Hour 3	Detecting and Preventing Mobile Exploits	
			Hour 4	• Mobile Application Security Best Practices • Ethical Use of Mobile Hacking Skills	
		Day 4	**Hour 1**	• Mobile Hacking Challenges and CTFs • iOS Jailbreaks and Bypassing Security Features	
			Hour 2	• Android Rooting and Custom ROMs • Mobile App Debugging and Patching	
			Hour 3	• Application Security Testing on Real Devices • Malware Analysis on Mobile Platforms	
			Hour 4	• Mobile Device Forensics	
		Day 5	**Hour 1-4**	Practical on Hacking a	

				Mobile App or Device	
Week 11	**Cryptography & Bug Bounty**	**Day 1**	**Hour 1**	• Introduction to Cryptography • Legal and Ethical Aspects of Cryptography • Basic Concepts of Cryptography (Encryption, Decryption)	• **Task 11** *Details may be seen at Annexure-I*
			Hour 2	• Classical Cryptography (Caesar, Vigenère, etc.) • Modern Cryptography Techniques (AES, RSA, ECC, etc.)	
			Hour 3	• Cryptographic Hash Functions (MD5, SHA, etc.) • Public Key Infrastructure (PKI) • Cryptographic Protocols (SSL/TLS, SSH, etc.)	
			Hour 4	• Cryptanalysis and Attacks on Cryptosystems • Quantum Cryptography and Post-Quantum Cryptography • Secure Key Management and Exchange	
		Day 2	**Hour 1**	• Cryptographic Libraries and APIs • Implementing Cryptographic Algorithms	
			Hour 2	• Digital Signatures and Authentication • Secure Communication with Cryptography • Cryptography in Blockchain Technology	
			Hour 3	• Cryptography in Network Security • Cryptography in Mobile Security	

				• Cryptography in Web Application Security	
			Hour 4	• Real-World Cryptographic Attacks and Defenses • Practical Cryptographic Exercises	
		Day 3	**Hour 1**	• Introduction to Bug Bounty Programs • Legal and Ethical Aspects of Bug Bounty Hunting • Bug Bounty Platforms and Marketplaces	
			Hour 2	• Setting Up a Bug Bounty Hunter Profile • Finding and Researching Bug Bounty Programs • Types of Security Vulnerabilities (OWASP Top Ten)	
			Hour 3	• Reconnaissance and Footprinting for Bug Bounties	
			Hour 4	• Web Application Testing for Security Vulnerabilities • Mobile Application Testing for Security Vulnerabilities	
		Day 4	**Hour 1**	Network and Infrastructure Testing for Security Vulnerabilities	
			Hour 2	• Identifying Security Vulnerabilities • Proof of Concept (PoC) and Exploitation	
			Hour 3	• Bug Triage and Severity Assessment • Creating Detailed Bug Bounty Reports	

			Hour 4	• Communication with Bug Bounty Programs • Bug Bounty Rewards and Payments • Bug Bounty Platform Tools and Resources	
		Day 5	**Hour 1-2**	Practical on Cryptography	
			Hour 3-4	Practical on Bug Bounty Hunting	
Week 12	**Final Exam and Assessment**				• **Task 12** *Details may be seen at Annexure-I* **Final Project**



Tasks for Certificate in AI (Robotics)

Task No.	Task	Description	Week
1.	**Introduction to CEH and LAB Setup**	• Hands-on Practice on LAB Setup for testing • Hands-on Practice on an Information Gathering	**Week 1**
2.	**Information Gathering**	• Investigate a suspicious domain or website associated with a potential security incident. Analyze the domain registration details, check for potential malicious activities, and provide actionable intelligence for an incident response team.	**Week 2**
3.	**Scanning & Enumeration**	• Conduct a comprehensive network scan on a given network to identify all active hosts and services. Perform vulnerability scanning on the identified hosts to assess potential security weaknesses. • Perform active enumeration on a Windows-based network to identify Active Directory (AD) users, groups, and systems. Explore potential vulnerabilities for privilege escalation and demonstrate the ability to exploit them.	**Week 3**
4.	**Vulnerability Analysis**	• Conduct a comprehensive vulnerability assessment across an organization's network infrastructure. Identify vulnerabilities in network devices, servers, and applications. Perform a risk analysis to prioritize and mitigate the identified vulnerabilities.	**Week 4**
5.	**System Hacking & Malware Analysis**	• A system administrator accidentally locked themselves out of a critical server by misconfiguring firewall rules. You need to regain access to the server without causing downtime or data loss. • A user's system has been infected with malware, potentially granting unauthorized access. Your task is to investigate the system, identify the attack vectors, and remediate the damage.	**Week 5**
6.	**Network Sniffing & Wifi Hacking**	• A small business is experiencing network connectivity problems, causing disruptions to their operations. Your task is to use sniffing techniques to diagnose the root cause of the issues and propose solutions. • You are tasked with conducting a wireless security assessment for a client's premises. Your goal is to identify any unauthorized or hidden wireless networks that could pose security risks.	**Week 6**

7.	**Social Engineering & Session Hijacking**	• A company's CEO is traveling abroad, and a malicious actor wants to access their confidential emails. They craft a phishing email that appears to be from the IT department, requesting the CEO's password for an urgent security update. • Identify and exploit a session-related vulnerability in a web application. Hijack a user's session and perform actions on their behalf.	**Week 7**
8.	**DOS/DDOS & SQL Injection Attack**	• Use ethical hacking tools like Kali Linux and Metasploit to simulate DoS/DDoS attacks against a test server or network in a controlled environment. • Identify a vulnerable login form on a web application. Use SQL injection techniques to bypass authentication and log in as a different user. Demonstrate how prepared statements can prevent this attack.	**Week 8**
9.	**Hacking Web Servers & Web Applications**	• You are given a web application with a known vulnerability in a shopping cart module. Your goal is to exploit the vulnerability to gain access to the web server and retrieve sensitive user data	**Week 9**
10.	**Hacking Mobile Platforms**	• Bypass authentication mechanisms in a mobile game to gain unauthorized access to premium features or manipulate game scores.	**Week10**
11.	**Cryptography & Bug Bounty**	• Implement password hashing using a secure algorithm like bcrypt or Argon2. Assess the strength of different hashing methods and explore password cracking techniques.	**Week11**
12.	**Final Exam and Assessment**		**Week12**

Annexure-II:

Motivational Lectures
AI (Robotics)

The Rise of Cyber Security: https://www.youtube.com/watch?v=BIsW9jp9NJM

This video provides an overview of the impact that Cyber Security is having on various industries and highlights some of the breakthroughs that have been made in recent years.

How Cyber Security Skill Will Change the World: https://www.youtube.com/watch?v=U3LMnJSNsLY

This video provides an overview of In a hyperconnected world, cybersecurity skills are the new superpower, safeguarding critical infrastructure, fueling innovation, and protecting our digital lives..

Annexure-IV:

Workplace/Institute Ethics Guide

Work ethic is a standard of conduct and values for job performance. The modern definition of what constitutes good work ethics often varies. Different businesses have different expectations. Work ethic is a belief that hard work and diligence have a moral benefit and an inherent ability, virtue, or value to strengthen character and individual abilities. It is a set of values-centered on the importance of work and manifested by determination or desire to work hard.

The following ten work ethics are defined as essential for student success:

1. **Attendance:**
   Be at work every day possible, plan your absences don't abuse leave time. Be punctual every day.
2. **Character:**
   Honesty is the single most important factor having a direct bearing on the final success of an individual, corporation, or product. Complete assigned tasks correctly and promptly. Look to improve your skills.
3. **Team Work:**
   The ability to get along with others including those you don't necessarily like. The ability to carry your weight and help others who are struggling. Recognize when to speak up with an idea and when to compromise by blend ideas together.
4. **Appearance:**
   Dress for success set your best foot forward, personal hygiene, good manner, remember that the first impression of who you are can last a lifetime
5. **Attitude:**
   Listen to suggestions and be positive, accept responsibility. If you make a mistake, admit it. Values workplace safety rules and precautions for personal and co-worker safety. Avoids unnecessary risks. Willing to learn new processes, systems, and procedures in light of changing responsibilities.
6. **Productivity:**
   Do the work correctly, quality and timelines are prized. Get along with fellows, cooperation is the key to productivity. Help out whenever asked, do extra without being asked. Take pride in your work, do things the best you know-how. Eagerly focuses energy on accomplishing tasks, also referred to as demonstrating ownership. Takes pride in work.
7. **Organizational Skills:**

Make an effort to improve, learn ways to better yourself. Time management; utilize time and resources to get the most out of both. Take an appropriate approach to social interactions at work. Maintains focus on work responsibilities.

8. **Communication:**

   Written communication, being able to correctly write reports and memos. Verbal communications, being able to communicate one on one or to a group.

9. **Cooperation:**

   Follow institute rules and regulations, learn and follow expectations. Get along with fellows, cooperation is the key to productivity. Able to welcome and adapt to changing work situations and the application of new or different skills.

10. **Respect:**

    Work hard, work to the best of your ability. Carry out orders, do what's asked the first time. Show respect, accept, and acknowledge an individual's talents and knowledge. Respects diversity in the workplace, including showing due respect for different perspectives, opinions, and suggestions.