TECNIA INSTITUTE OF ADVANCED STUDIES
NAAC ACCREDITED GRADE "A" INSTITUTE
Approved by AICTE, Ministry of Education Govt. of India, Affiliated to GGSIP University
Recognized Under Sec. 2(f) of UGC Act 1956
INSTITUTIONAL AREA MADHUBAN CHOWK,ROHINI,DELHI 110085
Tel:91-11-27555121-24, E-Mail : directortias@tecnia.in, Website: www.tiaspg.tecnia.in

EGAC Accredited ISO 21001:2018 51001:2018

TIAS/ACl/2021-22/35

Date:20/1/2022

Course Completion Certificate

This is to certify that the course module for the Certificate Course in Ethical Hacking scheduled from 3/1/22 to 19/1/22 , comprising of 30 Hours, running in 2 batches deliverance has been completed by the resource person Mr. Harsh, with the module contents as under:-

S.No.	Contents Deliverance	Learning Outcomes
1	Introduction to Ethical Hacking (2 hr)	Understand the principles, methodologies, and legal considerations of ethical hacking.
2	Networking Fundamentals (3hr)	Identify and exploit vulnerabilities in computer systems, networks, and applications using ethical hacking techniques.
3	Information Gathering and Footprinting (4hr)	Conduct comprehensive reconnaissance and information gathering to assess the target environment.
4	Scanning and Enumeration (3 Hr)	Perform vulnerability assessments and penetration testing to identify and exploit weaknesses in network infrastructure and web applications.
5	System Hacking (2 hr)	Utilize various hacking tools and techniques, such as scanning, enumeration, and exploitation, to gain unauthorized access.
6	Web Application Security (4 Hr)	Demonstrate proficiency in different types of attacks, including network attacks, web application attacks, wireless attacks, and social engineering attacks.
7	Cryptography (2 Hr)	Understand the principles of cryptography and cryptographic attacks, as well as how to implement secure cryptographic practices.
8	Social Engineering (2 Hr)	Use advanced techniques for bypassing security controls, evading intrusion detection systems, and maintaining persistence on compromised systems.
9	Wireless Security (3 hr)	Understand and analyze malware, including reverse engineering and analyzing malicious

		code.
10	Incident Response and Digital Forensics (5 hr)	Apply techniques for securing computer systems and networks, including configuring firewalls, implementing intrusion detection and prevention systems, and implementing secure coding practices.

All the above contents are delivered to the best of my knowledge and belief and nothing is withheld.

Signature
Name of Faculty: Mr. Harsh
Submitted to HoD- Department of Information Communication and Technology, TIAS