SYLLABI

For

Value Added Course

Certificate in Ethical Hacking

(w.e.f. 03/01/2022)

Offered by

Department of Information Communication and Technology

TECNIA INSTITUTE OF ADVANCED STUDIES
NAAC ACCREDITED GRADE "A" INSTITUTE
Approved by AICTC, Ministry of HRD, 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

Course Module

For

Value Added Program

Evaluation Pattern: On the basis of practical exam followed by viva

Course Structure

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.
11	Introduction to Ethical Hacking (2 hr)	Develop skills in digital forensics to investigate security incidents, collect evidence, and analyze digital artifacts.

Reference:

1. The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws" by Dafydd Stuttard and Marcus Pinto
2. Metasploit: The Penetration Tester's Guide" by David Kennedy, Jim O'Gorman, Devon Kearns, and Mati Aharoni
3. CEH Certified Ethical Hacker All-in-One Exam Guide" by Matt Walker
4. Gray Hat Hacking: The Ethical Hacker's Handbook" by Allen Harper, Daniel Regalado, Ryan Linn, Stephen Sims, Branko Spasojevic, Linda Martinez, and Michael Baucom
5. Penetration Testing: A Hands-On Introduction to Hacking" by Georgia Weidman