TECNIA INSTITUTE OF ADVANCED STUDIES
NAAC ACCREDITED GRADE "A" INSTITUTE
Approved by AICTE, 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

Department of Information Communication & Technology

Report
On
Value Added Course: Certificate in Ethical Hacking

ACTIVITY : Value Added Course

TITLE : Certificate in Ethical Hacking

VALUES: Domain Knowledge; Modern Tool Usage;Professional Ethical Edification

LEARNING OUTCOMES: Ability to recall information, facts, definitions, jargons, technical terms, classifications, categories and criteria; Understanding, grasping meaning and information,Acquainted with internet; Demonstrate correct usage of method or procedure; identify vulnerabilities in computer systems, networks, and applications, identify weaknesses that could be exploited by attackers, to exploit vulnerabilities ethically, Use Hacking Tools and Techniques, Understand Exploit Mitigation and Countermeasures, Apply Ethical and Legal Principles; Enhance Security Awareness and Risk Management

Organized by : Department of Information Communication & Technology

Program Theme : Value Added Course of Ethical Hacking

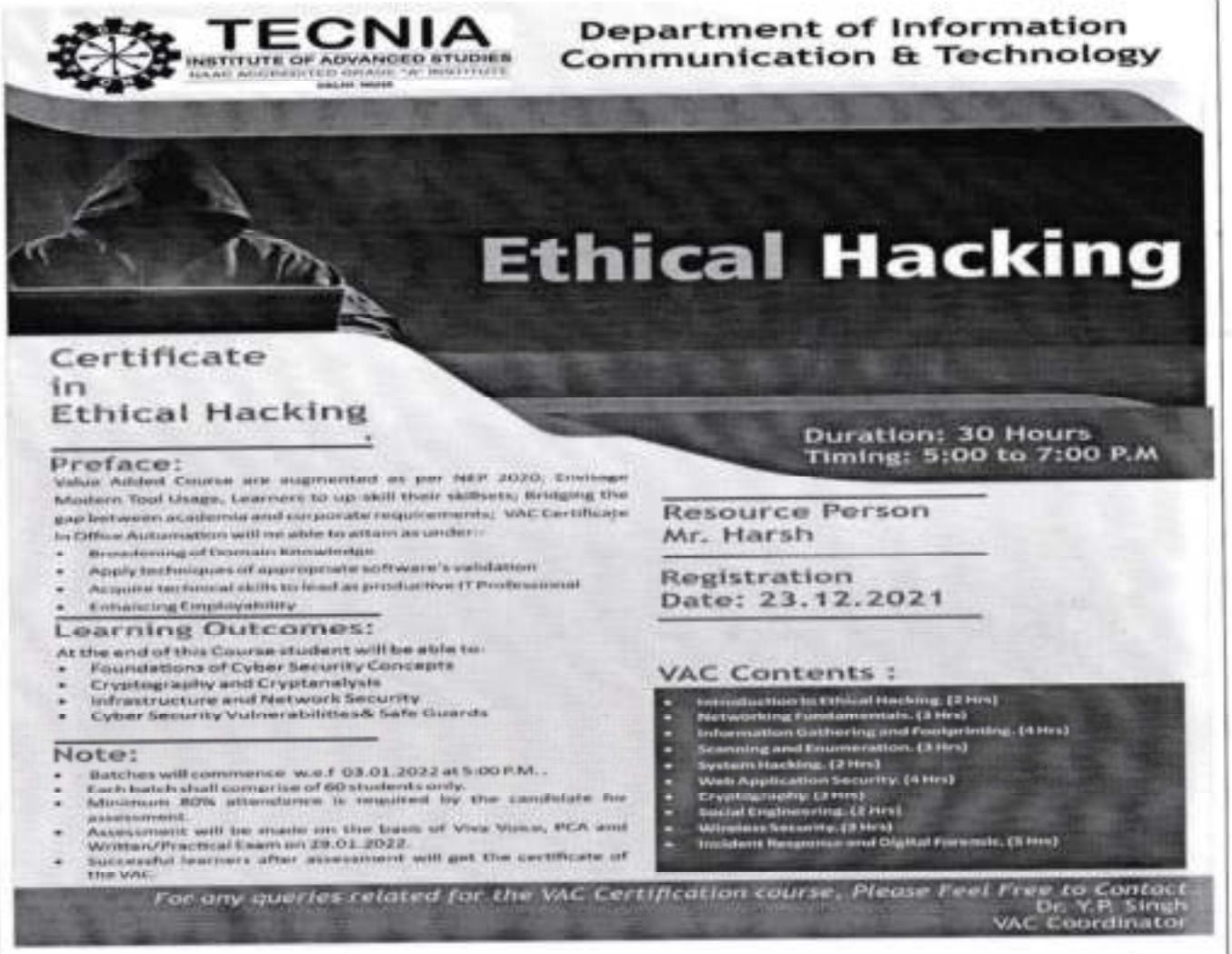
External Expert : Mr. Harsh

HoD
BCA-TIAS

Dr. Deepak Sonker
HOD ICT

Date : 03-01-2022	
Time	: 5:00 pm onwards
Venue	: Online, MS Team

Poster/Flyer/Notice*



Social media link *(promoting in any one Facebook/Instagram/Twitter is mandatory)*	Link of facebook, Instagram
No. of Students* *(only no. to be written, list in excel or word should be maintain at department level as proof for any further requirement)*	112
No. of Faculty* *(only no. to be written , list in excel or word should be maintain at department level as proof for any further requirement)*	01
No. of External Participants (students +	6

HoD Dr. Deepak Sonker
BCA-TIAS HoD BCA

faculty) *[write NA if not applicable]*	
(Geotag) Photograph*	
Photograph of the Event with the Caption	
Report: Description in (min 250 to max 800 words)*	Ethical hacking refers to the authorized practice of probing computer systems, networks, and applications with the intention of identifying vulnerabilities that malicious actors could exploit. Ethical hackers, often employed by organizations or working as independent security professionals, employ their skills and knowledge to simulate real-world cyber attacks in a controlled environment. The objective is to expose weaknesses and provide recommendations to improve security. In an era dominated by digital landscapes and interconnected systems, the need for robust cybersecurity measures has become paramount. Ethical hacking, also known as penetration testing or white-hat hacking, plays a pivotal role in identifying vulnerabilities, strengthening security defenses, and safeguarding digital assets. This article delves into the world of ethical hacking, exploring its purpose, methodologies, and the

HoD
BCA-TIAS
Dr. Deepak Sonkar

positive impact it has on cybersecurity.

Ethical hackers adopt various methodologies and techniques to uncover vulnerabilities and assess the overall security posture of target systems. Here are some common approaches used in ethical hacking:

1. Reconnaissance: Ethical hackers gather information about the target system, including its infrastructure, network architecture, and potential entry points. This reconnaissance phase helps identify potential vulnerabilities and aids in designing effective attack vectors.

2. Vulnerability Assessment: Ethical hackers utilize specialized tools and manual analysis to identify vulnerabilities within a target system. These assessments involve scanning for known vulnerabilities, analyzing system configurations, and evaluating patch levels. The findings are then used to prioritize and address vulnerabilities before they can be exploited by malicious actors.

3. Exploitation: Once vulnerabilities are identified, ethical hackers attempt to exploit them to gain unauthorized access or elevate privileges. The goal is not to cause harm but to demonstrate the potential impact of the vulnerabilities. By successfully exploiting weaknesses, ethical hackers provide valuable insights into potential attack vectors and weaknesses in the system's defenses.

4. Social Engineering: Ethical hackers also employ social engineering techniques to assess the human element of security. By exploiting human psychology and manipulating individuals through phishing, pretexting, or impersonation, ethical hackers test an organization's resilience against social engineering attacks. This helps identify gaps in employee awareness and training programs.

Ethical hacking has become an indispensable component of modern cybersecurity strategies. By leveraging the skills and knowledge of ethical hackers, organizations can identify vulnerabilities, strengthen security defenses, and protect their digital assets. Ethical hacking empowers organizations to stay one step ahead of cyber

Dr. Ashok Sonkar
HOD BCA-ITAS
HOD ICT

	threats, fosters a proactive security posture, and promotes trust and confidence in an increasingly interconnected digital world.
Resource Person Profile	Mr. Harsh is working in MNC as a Software Developer, he has 6 years of experience in Industry, his expertise in Ethical hacking, cyber security etc
Attendance Sheet*	*Attached at the end of Report*
Feedback	*Sample feedback Attached at the end of Report*
Report Submitted by Convener *(write faculty coordinator name)*	Mr. Harsh
For Office Use	
Signature of Event Coordinator Harsh	**Signature of School/Department Head** *(With Seal)*
List of Beneficiary	HoD BCA-TIAS Dr. Daulat Sinker HoD ICT

Fields marked with '' are mandatory*