Academic Year: 2025-2026 **Date:** 04-02-2026

Activity: Five-Day Student Enrichment Program (Workshop) on Cyber Skill Accelerator

Consolidated Report

A Five-Day Student Enrichment Program (Workshop) on "Cyber Skill Accelerator" was organized by the Department of Computer Science and Engineering from 27th January 2026 to 31st January 2026 at CSE Seminar Hall. A total of 140 students from **III Year CSE & IT** actively participated in the sessions, divided into two batches – Batch: 1 (9:15 AM to 12:50 PM) and Batch: 2 (1:30 PM to 4:00 PM). The sessions were conducted by **Mr. Prabhudas Thanneeru**, Founder of Hackers Gurukul & HTech Solutions, Head of IT for Triventa Group who served as the resource person for the workshop.

Day 1 – Introduction to Cybersecurity & Ethical Hacking: The workshop began with an inaugural session at 9:15 AM. **Dr. K. Rameshwaraiah**, Head of the Department of CSE, inaugurated the event and highlighted the importance of Cybersecurity with Ethical Hacking in modern mobile and web applications. After a brief introduction, **Mr. Prabhudas Thanneeru** initiated the first session, covering the workshop began with an overview of cybersecurity fundamentals, types of cyber threats, attack vectors, and the ethical hacking process. Students were introduced to Kali Linux and explored essential cybersecurity terminology. This session laid the foundation for understanding the importance of securing digital assets.

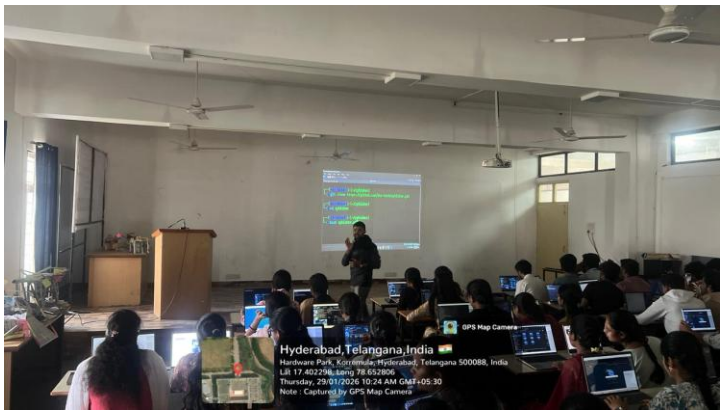
NALLA NARASIMHA REDDY
Education Society's Group of Institutions - Integrated Campus
(UGC AUTONOMOUS INSTITUTION)

EAMCET/ECET/ICET/PGECET Code NNRG

SCHOOL OF ENGINEERING
DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

Day 2 – Mobile Hacking , Windows and Android Attack: This session focused on building an understanding of security threats and attack techniques targeting mobile devices and desktop systems, with special emphasis on Android and Windows platforms. Participants were introduced to common vulnerabilities, major attack vectors, and real-world attack scenarios used by cybercriminals. The session also examined notable security incidents to provide practical context. It concluded with recommended security measures and best practices aimed at strengthening the protection of both systems and mobile devices.

Day 3 – Phishing and Cross-Platform Exploitation: This session focused on understanding how phishing attacks are designed and executed across multiple platforms, including email, SMS, and social media. Participants explored the methods used to craft phishing campaigns, with particular attention to how AI-generated content is leveraged to enhance realism and effectiveness. Real-world phishing incidents were analyzed to identify common attack patterns and their potential impact. The session concluded with an overview of essential prevention strategies, emphasizing user awareness, verification practices, and the implementation of strong authentication mechanisms



Day 4 – Website Creation and Phishing Detection: This session focused on the fundamentals of website creation and an understanding of how fake or malicious websites are designed to imitate legitimate ones. Participants learned to identify key indicators of phishing websites by analyzing elements such as layout, URLs, forms, and content patterns. The session emphasized recognizing deceptive features, comparing genuine and fraudulent websites, and applying best practices to detect and avoid phishing-based web attacks.

Day 5 – Capture The Flag (CTF) & Career Paths: The final day featured a competitive Capture the Flag (CTF) challenge in which a total of 20 teams participated. Students worked on problems spanning cryptography, web security, forensics, and reverse engineering. Out of the 20 teams, 2 teams successfully completed the assigned challenges, demonstrating strong analytical and technical skills. These two teams were awarded a Token of Appreciation in recognition of their outstanding performance. The day concluded with an informative session on cybersecurity career pathways, certifications, and emerging opportunities in industry.

Outcome : Upon successful completion of the Five-Day Student Enrichment Program on "Cyber Skill Accelerator",

- Developed a strong foundation in core cybersecurity concepts and ethical hacking methodologies.
- Gained practical, hands-on experience with industry-standard tools including Kali Linux, Nmap, Burp Suite, Aircrack-ng, Metasploit, Netdiscover, and VirusTotal.
- Learned to identify, analyze and mitigate common cyber threats and vulnerabilities.
- Acquired knowledge of real-world attack techniques such as phishing, social engineering, Open-Source Intelligence (OSINT), and penetration testing practices.

- Strengthened analytical thinking, problem-solving abilities, and teamwork skills through collaborative technical activities.
- Gained awareness of diverse cybersecurity career pathways, industry-recognized certifications, and future learning opportunities in the field.

Additional Outcome : A total of 10 students were declared as Workshop CTF Winners, and the CTF Winners List was announced and appreciated for their excellence

Group Photo of CTF Winners with the Resource Person– Batch 1

Group Photo of CTF Winners with the Resource Person– Batch 2

S. No	Name	Certificate ID
1	JAMPANI BHAVITHA	cert_5c469542cd32250c
2	APPALA ANUSHA	cert_0ffd299b7b415e90
3	ALE ANUSHA	cert_466c4d9c426aeb6d
4	AILENI MAHESHWARI	cert_70aa4d2eb9e864cf
5	KESAVA REDDY POOJA	cert_7867733e6d2c5a4d
6	GADE BABY DEEPIKA	cert_cee82d28433bd85f
7	S RAJINIKANTH	cert_347e83e6d6e7fb09
8	IPPALA AMARNADH REDDY	cert_da994e79fb5a986c
9	K SRINIVAS	cert_7af5f47fa4e9025a
10	GANDIPALLY SHRAVAN KUMAR	cert_af62b7fe3cb1838e

Valedictory Session and Student Reflections: The workshop concluded with a valedictory session in which students shared their experiences and key takeaways. Participants expressed how the sessions enhanced their understanding of cybersecurity concepts, real-world threats, and practical defense techniques. Several students spoke about the value of hands-on activities, interactive discussions, and exposure to current industry practices. They conveyed appreciation for the opportunity to strengthen their technical knowledge and awareness of digital safety. The session ended on a positive note, with students expressing enthusiasm to further explore learning and career opportunities in the field of cybersecurity.

Student feedback from the closing session of the Workshop

Group Photo of Faculty and Students with the Resource Person – CSE A.

Group Photo of Faculty and Students with the Resource Person – CSE B.

Group Photo of Faculty and Students with the Resource Person – CSE C.

Group Photo of Faculty and Students with the Resource Person – IT.

FACULTY COORDINATOR

HEAD-CSE