A Report on
"One-Week Advanced Cybersecurity and Ethical Hacking Skill Development Program"
Organized by
Department of Computer Science & Technology
in association with
Institution's Innovation Council (IIC) and MHRD's Innovation Cell, Government of India

on 05-01-2026 to 10-01-2026

Report Submitted by: **Mr. Junnubabu Noorbhasha,** Assistant Professor, Department of Computer Science & Technology.
Event Coordinators: **Mr. Junnubabu Noorbhasha,** Assistant Professor, Department of Computer Science & Technology ,
Mr. N. Saikiran, Assistant Professor, Department of Computer Science & Technology.
Resource Person details: Mr. Kuppam Johari, Freelance Cybersecurity Consultant.
Participants: III CST A,B,C & II CST A
Attendance: 78 participants (Internal)
Venue: Seminar Hall - B
Mode of Conduct: Offline
Report Received on 12.1.2026.

Introduction
The Department of Computer Science & Technology, MITS (Deemed to be University) organized a **One-Week Advanced Cybersecurity and Ethical Hacking Skill Development Programme** from **05 January 2026 to 10 January 2026** at **Seminar Hall – B**. The programme aimed to enhance students' practical knowledge and hands-on skills in cybersecurity, ethical hacking, and modern cyber defense mechanisms.

Objectives of the Programme
- To provide practical exposure to cybersecurity and ethical hacking tools
- To familiarize students with real-world cyber threats and defense strategies
- To bridge the gap between academic learning and industry requirements
- To promote ethical responsibility and cyber awareness

Inaugural Session
The inaugural session of the programme commenced on **05 January 2026** with the dignitaries taking their seats on the dais. The session began with a welcome address by **Mr. V. Naveen**, Assistant Professor, Department of Computer Science & Technology, who extended a warm welcome to the Principal, Dean, Head of the Department, faculty members, the resource person, and the participating students.

Following the welcome address, the **programme overview** was presented by **Mr. Junnubabu Noorbhasha**, Assistant Professor and Programme Coordinator, who briefly explained the objectives, structure, and expected outcomes of the one-week programme.

Subsequently, **Dr. K. Dinesh**, Associate Professor & Head, Department of Computer Science & Technology, addressed the gathering and emphasized the growing need for skilled and ethically responsible cybersecurity professionals in the present digital landscape.

The session was further enriched by the address of **Dr. Chandra Prakash Gupta**, Professor & Dean, School of Computing, who highlighted the importance of skill-based and industry-oriented education in preparing students to meet emerging technological challenges.

The inaugural session concluded with the **inaugural address by Dr. P. Ramanathan**, Professor & Principal, MITS (Deemed to be University). In his address, he encouraged students to actively participate in the programme, make effective use of the learning opportunity, and formally declared the programme inaugurated.

Prayer Song

Before the commencement of the ceremonial lamp lighting, a **prayer song was melodiously rendered by the II-Year students**, invoking blessings for the successful conduct of the programme and creating a solemn and auspicious atmosphere for the inauguration.

Ceremonial Lighting of the Lamp

After the prayer song, the dignitaries and the resource person were invited to perform the **ceremonial lighting of the lamp**. The lamp lighting ceremony symbolized the commencement of knowledge dissemination and formally marked the inauguration of the **One-Week Advanced Cybersecurity and Ethical Hacking Skill Development Programme**.

Introduction of the Resource Person

Following the lamp lighting ceremony, the distinguished **Resource Person, Mr. Kuppam Johari**, Freelance Cybersecurity Consultant and Bug Bounty Hunter, was formally introduced to the gathering by **Mr. V. Naveen**, Assistant Professor, Department of Computer Science & Technology. During the introduction, Mr. Naveen highlighted the resource person's professional experience in ethical hacking, vulnerability assessment, penetration testing, and cybersecurity training. He also emphasized Mr. Johari's extensive industry exposure and valuable contributions to cybersecurity education and real-world security practices.

Complete One-Week Programme Plan

Date	Day	Topics Covered
05-01-2026	Day 1	01: Introduction to Ethical HackingModule 02: Footprinting & ReconnaissanceModule 03: Network ScanningModule 04: Enumeration
06-01-2026	Day 2	05: Vulnerability AnalysisModule 06: System Hacking
07-01-2026	Day 3	07: Social EngineeringModule 08: Session Hijacking
08-01-2026	Day 4	09: Hacking Web ServersHacking Web ApplicationsModule 10: SQL Injection (SQLi)Module 11: Cross-Site Scripting (XSS)
09-01-2026	Day 5	12: CryptographyModule 13: Vulnerability Identification & CTF Techniques
10-01-2026	Day 6	Review of Programme Topics, Interaction with Resource Person, Assessment Examination

Cyber Security Tools Installation

As part of the practical training sessions, participants were guided through the installation and basic configuration of essential cybersecurity tools. These tools were extensively used during hands-on laboratory sessions, real-time demonstrations, and practical exercises throughout the programme.

S. No.	Tool Name	Purpose
1	Kali Linux	Penetration testing operating system with pre-installed cybersecurity tools
2	Nmap	Network scanning, port scanning, and service enumeration
3	Burp Suite	Web application security testing and traffic interception
4	OWASP ZAP	Automated web application vulnerability scanning
5	TryHackMe	Online platform for guided hands-on cybersecurity labs and practice

Programme Outcomes

At the end of the **One-Week Advanced Cybersecurity and Ethical Hacking Skill Development Programme**, the participants were able to:

1. Gain a **strong understanding of cybersecurity fundamentals and ethical hacking concepts**, including real-world cyber threat scenarios.
2. Acquire **hands-on experience with essential cybersecurity tools** used for network scanning, web application testing, and vulnerability assessment.
3. Identify and analyze **system and web application vulnerabilities**, such as SQL Injection and Cross-Site Scripting (XSS).
4. Apply **ethical hacking methodologies** through practical laboratory sessions and Capture The Flag (CTF) challenges.
5. Develop **ethical awareness, problem-solving skills, and industry readiness** for careers in cybersecurity.

Results of the Assessment

As part of the **One-Week Advanced Cybersecurity and Ethical Hacking Skill Development Programme**, an **online assessment examination** was conducted on **10 January 2026** to evaluate the participants' understanding of the concepts and practical knowledge gained during the programme. The examination consisted of **50 multiple-choice questions**, covering topics from ethical hacking fundamentals, network and system security, web application vulnerabilities, cryptography, and Capture The Flag (CTF) concepts.

A total of **78 participants** appeared for the examination. The overall performance of the students was highly encouraging, with an **average accuracy of 91%**, indicating a strong grasp of the concepts delivered during the sessions. The results demonstrated that the majority of participants were able to effectively apply theoretical knowledge to problem-solving scenarios related to cybersecurity and ethical hacking. The assessment outcomes reflected the effectiveness of the programme's **hands-on training approach**, practical laboratory sessions, and real-time demonstrations. The strong performance of the participants validated that the programme successfully enhanced students' technical competency, analytical skills, and readiness to address real-world cybersecurity challenges.

Conclusion

The **One-Week Advanced Cybersecurity and Ethical Hacking Skill Development Programme** was successfully conducted by the Department of Computer Science & Technology, MITS (Deemed to be University), with active participation from students and faculty members. The programme effectively achieved its objectives by providing participants with hands-on exposure to ethical hacking techniques, cybersecurity tools, and real-world security scenarios. Through expert guidance, practical laboratory sessions, and interactive discussions, the programme enhanced students' technical competencies, ethical awareness, and industry readiness in the field of cybersecurity. Overall, the programme served as a valuable learning platform and contributed significantly to the professional development of the participants.