ACHARYA INSTITUTE OF GRADUATE STUDIES

(NAAC Re-Accredited 'A+' Grade and Affiliated to Dr. Manmohan Singh, Bengaluru City University)

Soladevanahalli, Bengaluru-560107

DEPARTMENT OF MCA

Report Submission: 20/02/2026

Semester: ODD	**Academic Year: 2025-26**	**Venue: ECE Seminar Hall, Acharya Institutes**
Event Date:20/02/2026	**Time: 10.00 am to 1.00 pm**	**Duration: 3 Hr**

TYPE OF EVENT: WORKSHOP

EVENT NAME: Cyber Security Tools: A Practical Hands-on

Target Audience: I & III Sem Students	**Number of Participants:108**

Objectives:

In the digital era, cybersecurity plays a vital role in computer applications and information technology. With increasing reliance on digital platforms and network-based systems, cyber threats have become more frequent and complex. This workshop was organized to bridge the gap between theoretical learning and practical exposure for MCA students.

1. To create awareness of major cybersecurity threats such as malware, phishing, ransomware, data breaches, and network intrusions.
2. To introduce industry-relevant cybersecurity tools used for securing systems, networks, and applications.
3. To provide hands-on exposure to practical cybersecurity tools and real-time security scenarios.
4. To enhance practical skills in vulnerability assessment, network monitoring, ethical hacking, and system security.
5. To promote ethical cybersecurity practices and awareness of cyber laws.
6. To motivate students to pursue careers in cybersecurity and information security.
7. To strengthen industry–academia interaction through expert knowledge sharing.

Program Introduction:

The Department of Master of Computer Applications (MCA) organized a hands-On Workshop titled **"Cybersecurity Tools: A Practical Hands-On Workshop"** for MCA 1st and 3rd Semester

students at the ECE Seminar Block. The program aimed to enhance students practical understanding of cybersecurity concepts and tools in alignment with current industry standards. The session commenced with a welcome address delivered by Ms. Farzeen Basith.

The workshop was conducted by Dr. N. Kavitha, Professor at REVA University, an accomplished academician with extensive expertise in cybersecurity and network security. Her insightful lecture, combined with live demonstrations and hands-on activities, provided valuable real-world exposure to students.

The workshop was successfully coordinated by Dr. Deepti A R and Ms. Farzeen Basith, whose dedicated planning and coordination ensured smooth execution. The session witnessed active participation from both junior and senior MCA students, along with faculty members, making it an engaging and academically enriching experience.

Theme of the Event: "Learning Cybersecurity Through Practical Tools and Hands-On Experience."

The workshop highlighted cybersecurity as a hands-on and evolving discipline, emphasizing practical implementation, real-world tools, and understanding threats from both attacker and defender perspectives, along with ethical responsibilities. It was highly relevant for MCA students, aligning with their curriculum and preparing them for careers in software development, system administration, network security, and ethical hacking.

Resourse Person detail:

Dr. N. Kavitha is an accomplished academician and researcher with over 21 years of teaching and research experience in Computer Science and Applications. She has served as a resource person for several workshops, FDPs, and guest lectures on emerging technologies such as Cyber Security, Data Science, Cloud Computing, Python, AI, and NIRF methodologies. With extensive research contributions, patents, and international exposure, she effectively bridges academic knowledge with practical and industry-relevant

Detailed Report:

Introduction

The rapid growth of information technology and digital infrastructure has significantly increased the complexity and frequency of cyber threats. Organizations across the globe are facing challenges related to data security, privacy breaches, and cybercrime. In this context, cybersecurity has emerged as a crucial field that ensures the confidentiality, integrity, and availability of information systems.

Understanding cybersecurity concepts requires more than textbook knowledge. Practical exposure to tools and real-time scenarios is essential for students to grasp how cyberattacks occur and how they can be prevented or mitigated. With this understanding, the Department of MCA organized a hands-on workshop to provide students with an opportunity to learn directly from an expert in the field.

The workshop aimed to introduce students to commonly used cybersecurity tools, their functionalities, and real-world applications. The session was designed to be interactive, practical, and informative, ensuring maximum student engagement.

In addition, the program focused on familiarizing students with the evolving nature of cyber threats and the importance of proactive security measures. Emphasis was placed on understanding attacker methodologies, system vulnerabilities, and defense mechanisms used by organizations to safeguard digital assets. This exposure helped students develop a security-oriented mindset and a deeper appreciation of cybersecurity as a continuous process rather than a one-time solution.

The workshop also highlighted the relevance of cybersecurity in various domains such as banking, healthcare, e-commerce, cloud computing, and government systems. By discussing real-world incidents and case studies, students were able to relate theoretical concepts to practical situations. This approach enhanced their analytical thinking and enabled them to understand the impact of cybersecurity breaches on businesses and society.

Furthermore, the session encouraged students to explore emerging trends in cybersecurity, including ethical hacking, digital forensics, incident response, and security compliance. The interactive discussions motivated students to actively participate, ask questions, and seek clarity

on advanced concepts. Overall, the workshop served as a valuable learning platform that strengthened students technical competence and prepared them to face real-world cybersecurity challenges with confidence.

Event Overview

The workshop was conducted for MCA 1st Semester and MCA 3rd Semester students and witnessed enthusiastic participation from both batches. The program commenced with a formal welcome, followed by the technical session and hands-on workshop.

Session Highlights

Dr. N. Kavitha began the session by explaining the fundamentals of cybersecurity, including:

- Definition and scope of cybersecurity
- Importance of cybersecurity in modern IT systems
- Common cyber threats and attack vectors
- Role of cybersecurity professionals

She emphasized that cybersecurity is not limited to protecting systems but also involves risk assessment, compliance, monitoring, and incident response.

Technical Session: Cybersecurity Tools

The core of the workshop focused on cybersecurity tools that are widely used in industry and academia. The speaker explained each tool with real-time examples and demonstrated how these tools are applied in practical scenarios.

1. Network Security Tools

Students were introduced to tools used for monitoring and analysing network traffic. Dr. N. Kavitha explained how attackers exploit network vulnerabilities and how security professionals detect suspicious activities using network analysis tools. Key concepts covered included:

- Packet sniffing
- Network traffic analysis
- Detection of malicious packets
- Monitoring unauthorized access attempts

Live demonstrations helped students understand how data flows through a network and how anomalies can be detected.

2. Vulnerability Assessment Tools

The session included a detailed explanation of vulnerability assessment and scanning tools. Students learned how these tools help identify weaknesses in systems, servers, and applications before attackers can exploit them.

Topics covered:

- Importance of vulnerability assessment
- Types of vulnerabilities
- Scanning techniques
- Interpretation of scan results
- Risk prioritization and mitigation

Dr. N. Kavitha stressed the importance of regular vulnerability assessments in maintaining system security.

3. Ethical Hacking Tools

One of the most engaging parts of the workshop was the discussion on ethical hacking tools. The speaker clarified the difference between ethical hackers and malicious attackers, emphasizing the ethical and legal responsibilities involved. Students were introduced to:

- Penetration testing concepts
- Reconnaissance and scanning techniques
- Password security and cracking awareness
- System exploitation basics (conceptual understanding)

Hands-on demonstrations allowed students to see how ethical hackers test systems in controlled environments.

4. Malware Analysis and Protection Tools

The session also covered malware-related topics, including:

- Types of malwares (viruses, worms, trojans, ransomware)
- How malware infects systems
- Basic malware analysis techniques
- Antivirus and anti-malware tools

Real-life examples of recent cyberattacks were discussed to help students understand the seriousness of cyber threats.

5. Cybersecurity Best Practices

In addition to tools, Dr. Kalavathi shared best practices followed by cybersecurity professionals, such as:

- Strong password policies
- Multi-factor authentication
- Regular system updates and patching
- Secure coding practices
- User awareness and training

She highlighted that human error is often the weakest link in cybersecurity and emphasized the importance of awareness and responsibility.

Hands-On Workshop Experience

The hands-on segment of the workshop was highly appreciated by the students. Under the guidance of the resource person, students actively participated in tool demonstrations and practical exercises.

Students were encouraged to:

- Observe live tool executions
- Analyse outputs and reports
- Ask questions during demonstrations
- Understand real-world use cases

The interactive nature of the workshop helped students gain confidence and clarity regarding cybersecurity concepts.

Vote of Thanks

The program concluded with a formal Vote of Thanks delivered by Dr. A. R. Deepti, faculty member of the Department of MCA. She expressed sincere gratitude to Dr. N. Kavitha for graciously accepting the invitation and delivering an insightful, informative, and practically oriented session despite her busy schedule. She also conveyed heartfelt thanks to the Management and the Principal for their constant encouragement and support in organizing the workshop.

Appreciation was extended to the Head of the Department for continuous guidance, to the faculty members for their active coordination and participation, and to the student volunteers for their

dedicated efforts in organizing and managing the event. She further thanked all the participants for their enthusiastic involvement and active engagement throughout the session. The vote of thanks acknowledged the collective efforts of everyone involved, which contributed significantly to the successful conduct of the program.

Photos:

Introduction to the workshop on cybersecurity tools

ACHARYA INSTITUTE OF GRADUATE STUDIES

(NAAC Re-Accredited 'A+' Grade and Affiliated to Dr. Manmohan Singh, Bengaluru City University)

Soladevanahalli, Bengaluru-560107

Overview of cybersecurity concepts and emerging threats

Hands-on demonstration of cybersecurity tools

Interactive question and discussion session

Students expressing gratitude to the resource person

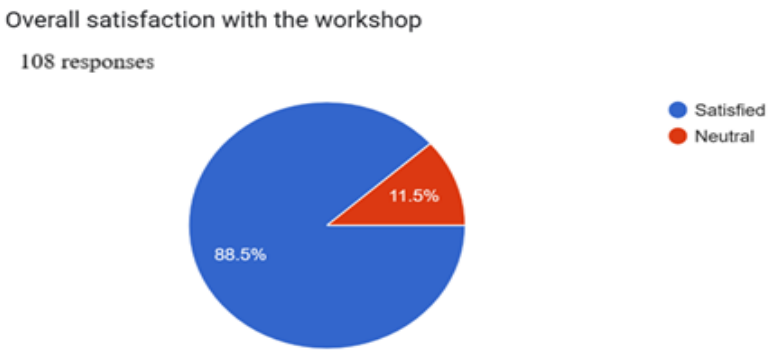
Outcomes:

1. Students gained a clear understanding of fundamental cybersecurity concepts through practical exposure to industry-relevant tools.
2. The workshop enabled students to identify and analyse common cyber threats, system vulnerabilities, and security risks.
3. Participants developed practical skills in network monitoring, vulnerability assessment, and ethical hacking techniques.
4. Hands-on demonstrations improved students' ability to interpret tool outputs and real-time security reports.
5. The session enhanced awareness of ethical cybersecurity practices, cyber laws, and professional responsibilities.
6. Students were motivated to explore career opportunities, certifications, and higher learning in cybersecurity and information security.
7. The workshop effectively bridged the gap between theoretical knowledge and practical application.

Conclusion :

The hands-on workshop on "Cybersecurity Tools: A Practical Hands-On Workshop" was successfully conducted and proved to be a valuable academic initiative for MCA students. The program offered practical insights into real-world cybersecurity challenges and familiarized students with industry-relevant tools and techniques. The interactive sessions, live demonstrations, and expert guidance effectively complemented the academic curriculum and enhanced student's technical competence, ethical awareness, and professional preparedness. The active participation of students and faculty members reflected the relevance and overall impact of the program.

Feedback Analysis:



Consolidated student feedback on Cybersecurity workshop

The audience feedback was overwhelmingly positive, with students and faculty appreciating the practical and hands-on approach adopted during the workshop. Participants expressed that the session improved their understanding of cybersecurity concepts and increased their confidence in applying security tools. The clarity of explanation, real-world case studies, and interactive discussions were particularly well received. Overall, the feedback indicated that the program was informative, engaging, and highly beneficial, and participants expressed interest in similar workshops in the future.