ACTIVITY 01

Workshop on Ethical Hacking & Penetration Testing

This hands-on workshop will provide participants with practical exposure to ethical hacking and penetration testing techniques. The session will cover the fundamentals of ethical hacking, including reconnaissance, scanning, enumeration, exploitation, and post-exploitation. Participants will learn to use popular tools like Nmap, Metasploit, Burp Suite, and Wireshark to identify vulnerabilities in systems and networks. The workshop will emphasize legal and ethical aspects, ensuring that students understand the importance of responsible hacking. Live demonstrations and hands-on labs will allow participants to test their skills in a controlled environment. By the end of the workshop, attendees will be able to conduct security assessments, analyse risks, and propose mitigation strategies to protect systems from cyber threats.

Resource Person : Dr. Terrance Frederick Fernandez, Professor and Asst. HoD (Research), Department of Information Security, Institute of CSE, Saveetha School of Engineering, Saveetha Institute of Technical and Medical Sciences..

Fund Proposed : $ 250

Participants : All the Cyber security students

ACTIVITY 02

Seminar on Cyber Threat Intelligence

This seminar aims to introduce students and faculty to the field of Cyber Threat Intelligence (CTI), which involves collecting, analysing, and interpreting data related to cyber threats. It will cover the various types of cyber threats, including malware, ransomware, phishing, and Advanced Persistent Threats (APTs). Industry experts will discuss real-world cyber incidents, attack methodologies, and preventive measures. The seminar will also explore threat intelligence frameworks such as MITRE ATT&CK, STIX, and TAXII, helping students understand how organizations leverage intelligence to enhance their security posture. Attendees will gain insights into how cybersecurity professionals monitor and respond to cyber threats, making them better equipped for careers in cybersecurity.

Resource Person : Dr. A. Arulmurugan ,Assistant Professor, Department of Computing Technologies, School of computing, SRM University, Kattankulathur Campus, Tamil Nadu, India

Fund Proposed : $150

Participants (100) : All Cyber security students

ACTIVITY 03

SKILL DEVELOPMENT PROGRAM

Skill Development Program on Cybersecurity

This program aims to enhance students' practical skills in cybersecurity domains such as network security, penetration testing, secure coding, and digital forensics. Industry experts and certified trainers will provide hands-on training with real-world cybersecurity tools. The program will also offer mentorship and career guidance to help participants prepare for cybersecurity certifications like CEH, CISSP, and CompTIA Security+. Through workshops, lab sessions, and projects, students will gain practical expertise and industry-ready skills to excel in cybersecurity careers

Resource Person : Dr. P. Harikrishna, Associate Professor, Dept. of CSE (AIML), Malla Reddy College of Engineering and Technology, Hyderabad

Fund Proposed : $250

Participants (100) : IEEE Students & The students who are interested in this domain

ACTIVITY 04

TECHNICAL QUIZ

The **Technical Quiz** competition is a pursuit of technical knowledge and actually tests the students retention and accumulation of knowledge towards application of concepts. It would be greatly helpful in acknowledging their position on their journey to technical excellence.

The **Objective** behind the Quiz competition is to evaluate the knowledge of the participants within academics as well as beyond academics and to make them familiar with the prospects of quizzes and the objectivity of the questions. With practicing quizzes, students can do critical thinking, and get into a habit of innovative learning. These quizzes integrate the game mechanics into the learning process, they help students understand the weaker areas.

Quizzes help students identify what they know and what they don’t know. The students then have a better idea of how well they are grasping the material, hopefully motivating them to study more and helping them allocate their study time effectively by focusing on the information that still needs more practice. A questioning teacher creates incentives for students to learn more. Teachers set up effective and definite goals for learning; giving oral or written examinations is a good incentive for the students to study harder or to do better work.

Participants (150) : IEEE & NON IEEE Members

Fund Proposed : $50

ACTIVITY 05

Paper Presentation on Emerging Cybersecurity Trends

This activity will encourage students and faculty members to research and present papers on current and emerging cybersecurity trends such as AI-driven security, zero-trust architecture, quantum cryptography, and cyber resilience. Participants will submit research papers, which will be reviewed by a panel of experts. Selected papers will be presented in front of an audience, followed by discussions and Q&A sessions. This event will promote knowledge sharing, academic research, and innovation in cybersecurity. The best papers will be awarded certificates, and outstanding research will be encouraged for publication in journals or conferences.

Participants (50) : All cyber security students

Fund Proposed : $100

ACTIVITY 06

POSTER PRESENTATION

The "**POSTER PRESENTATION**" which will be very helpful to students to get an idea about their skill by presenting PPT.

The "**POSTER PRESENTATION**" provides the presentation of posters that is likely to take place in a physical event. There will be 1-2 dedicated poster sessions in which poster authors can meet and discuss their work with conference participants. An additional web presence of posters will supplement the traditional physical installation of poster boards. More concrete details will follow soon, with the goal of creating an engaging atmosphere consistent with past in-person poster sessions.

In this session original work that has not been presented previously at any workshop, symposium, or conference, and not published previously in any archived conference proceeding, magazine, or journal and the students can gain the information by attending the session, by presenting you may be able to develop your communication .

At the end of the day the student can gain the knowledge to prepare the poster and PPT ,and students can be able to improve their skill of presentation and their communication.

Participants (100) : IEEE & Non IEEE Students

Fund Proposed : $50

ACTIVITY 07

Five-Day Hands-On Workshop on Digital Forensics & Incident Response

This workshop will provide hands-on training in digital forensics and incident response (DFIR). Participants will learn about forensic investigation techniques, evidence collection, and legal considerations in cybercrime cases. The session will include practical exercises using forensic tools like Autopsy, FTK Imager, and Volatility for memory analysis. The workshop will also cover incident response strategies, including identifying, containing, eradicating, and recovering from security incidents. Real-world case studies will be discussed to help participants understand how cybersecurity professionals handle data breaches and cyberattacks.

Workshop Agenda

Day 1: Introduction to Digital Forensics

Overview of Digital Forensics & Incident Response (DFIR)

Legal and Ethical Considerations in Cybercrime Investigations

Types of Cybercrimes and Digital Evidence

Day 2: Forensic Data Acquisition & Analysis

Evidence Collection & Chain of Custody

Imaging & Hashing Techniques

Hands-on with FTK Imager & Autopsy

Day 3: Memory & Network Forensics

Analysing Volatile Memory using Volatility

Network Traffic Analysis & Log Analysis

Case Study: Real-World Memory Forensics Investigation

Day 4: Incident Response & Threat Hunting

Stages of Incident Response (Identification, Containment, Eradication, Recovery)

Hands-on with SIEM Tools for Threat Detection

Practical Exercises in Threat Hunting

Day 5: Case Studies & Final Assessment

Analysing Real-World Cyber Incidents

Live Incident Response Simulation

Certification of Completion & Closing Remarks

Workshop Outcomes By the end of this workshop, participants will:

Understand the fundamentals of digital forensics and incident response.

Gain hands-on experience with forensic tools like Autopsy, FTK Imager, and Volatility.

Learn to acquire, preserve, and analyse digital evidence while following legal procedures.

Develop skills in memory and network forensics for cyber incident investigation.

Apply incident response methodologies to mitigate cyber threats effectively.

Enhance their ability to detect, analyse, and respond to cyber incidents in real-world scenarios.

Resource Person : Dr. A. Ilavendhan Senior Assistant Professor VIT University, Chennai

Dr.G.Balamurugan Assistant Professor, SRM Institute of Science and Technology (SRM University) Kattankulathur Campus, Tamil Nadu, India

Participants (140) : IEEE Members

Fund Proposed : $ 450

ACTIVITY 08

Seminar on Blockchain & Cybersecurity

This seminar will explore how blockchain technology enhances cybersecurity by providing decentralized, immutable, and secure solutions. Topics covered will include blockchain fundamentals, smart contracts, decentralized identity management, and blockchain's role in securing financial transactions and supply chains. Experts from academia and industry will share insights on how blockchain prevents fraud, enhances data integrity, and secures digital assets. The session will also discuss challenges such as 51% attacks, smart contract vulnerabilities, and scalability issues in blockchain security.

Participants : All the students of cyber security

Fund Proposed : $50

ACTIVITY 09

Cybersecurity Awareness Campaign

This campaign will focus on educating students and faculty about online safety, password hygiene, social engineering attacks, and phishing scams. Activities will include poster-making contests, interactive quizzes, and role-playing scenarios to help attendees recognize and respond to cyber threats. The campaign will also highlight best practices for securing personal and institutional data, along with real-life case studies of cyberattacks.

Participants : All the students of cyber security

Fund Proposed : $50

ACTIVITY 10

Guest Lecture on Career Opportunities in Cybersecurity

This session will invite cybersecurity professionals to discuss career paths in ethical hacking, digital forensics, security analysis, and cyber law. The lecture will provide guidance on certifications such as CEH, CISSP, and OSCP, along with insights into industry trends and job opportunities.

Participants : All the students of cyber security

ACTIVITY 11

AI & Cybersecurity Symposium

This symposium will explore the role of artificial intelligence in cybersecurity, including AI-driven threat detection, analysis, and automated security solutions. Experts will discuss machine learning applications in cyber defence, adversarial AI, and ethical considerations.

Participants : All the students of cyber security