Allyn Girls

allyngirls@xavier.ac.in

Sponsored by Allan & Lynda

REPORT ON : Cyber Security By Bootcamp

DURATION OF EVENT: 19th December 2025 - 3rd January 2026

VENUE: Xavier Institute Of Engineering

TIME: 9:00 AM - 11:00 PM

BENEFICIARIES: TE & BE Students

NO.OF PARTICIPANTS: 13

Allyn Girls

allyngirls@xavier.ac.in

THE ALLYN FUND

Sponsored by Allan & Lynda

Attendance list of Allyn Girls students

Sr. No.	Name	Year	Branch
1	Soni Chaudhary	TE	CSE
2	Piyusha Nandivadekar	BE	Comps
3	Cecilia Dinesh	BE	Comps
4	Bhanavi Pandey	BE	CSE
5	Anoushka Ingle	BE	CSE
6	Harshitha Nakka	TE	IT
7	Vaishnavi Karanje	TE	IT
8	Bhoomika Vaishya	TE	IT
9	Kanchan Kumari	TE	IT
10	Pranjal Balsraf	TE	Comps
11	Sejal Upadhyay	TE	Comps
12	Surabhi Karamarkar	TE	EXTC
13	Priyanka Reddy	BE	CSE

Allyn Girls

allyngirls@xavier.ac.in

Sponsored by Allan & Lynda

Sr.No	Title	Page No
1	Introduction	1
2	Module Details	2-3
3	Day-wise Details	3-4
4	Conclusion	4
5	Glimpse Of Event	5

Allyn Girls

allyngirls@xavier.ac.in

Sponsored by Allan & Lynda

Introduction

The Cyber Security Bootcamp was conducted from 17th December 2024 to 3rd January 2025, between 9:00 AM and 11:00 AM, at Xavier Institute of Engineering, Mumbai. The program was organized by the Training and Placement Office (TPO) for TE and BE students, along with participants from other departments. Students from the Allyn Girls Committee actively participated in the bootcamp.

The bootcamp focused on providing fundamental knowledge of Cyber Security through theoretical sessions and hands-on practicals. Students were introduced to real-world cyber threats, vulnerabilities, cryptography concepts, and ethical hacking practices, including practical exposure using the Hack The Box platform.

Objective(s)

- To introduce students to the fundamentals of Cyber Security
- To create awareness about cyber threats and vulnerabilities
- To provide hands-on experience through practical sessions
- To familiarize students with ethical hacking tools and techniques
- To enhance knowledge of cryptography and secure system practices
- To encourage interest in Cyber Security as a career option

Module Details

Module 1: Cybersecurity Fundamentals Tools

- What is a Vulnerability (Windows/Linux)
- Types of Vulnerabilities
  - OS Vulnerabilities (Windows/Server/Linux)
  - Network Vulnerabilities

Module 2: Vulnerability Categories

- Configuration Vulnerabilities
- OS Services (SSH, Telnet)
- Social Engineering Vulnerabilities (Setoolkit)
- Physical Vulnerabilities related to infrastructure

Module 3: Cyber Threat Landscape

- Types of Cyber Threats
- Malware and Malware Analysis using VirusTotal
- Network Attacks
- Web Attacks
- Insider Threats

Module 4: Cryptography Fundamentals

- Introduction to Cryptography
- Need for Cryptography
- Plaintext and Ciphertext

Module 5: Cryptography Goals & Concepts

- Confidentiality
- Integrity
- Authentication
- Non-repudiation

Module 6: Cryptography Implementation

- Cryptographic Algorithms
- Cryptography using Servers and Certificates

Module 7: Platform-Based Cryptography

- Windows Cryptography (EFS, NTFS Permissions, PKI, Certificate Authority)
- Cisco Packet Tracer (Secret Passwords)
- Linux (Kali Linux)

Day-wise Details

Day 1 (19th December)

Introduction to Cyber Security fundamentals was provided. Students learned about vulnerabilities, their types, and basic security concepts in Windows and Linux environments.

Day 2 (20th December)

The session focused on OS and Network Vulnerabilities. Students were introduced to real-world security flaws and how attackers exploit system weaknesses.

Day 3 (22nd December)

Topics related to Configuration Vulnerabilities, SSH and Telnet services, and Social Engineering attacks using Setoolkit were explained.

Day 4 (23rd December)

Students learned about Physical Security Vulnerabilities and Cyber Threat Landscape, including different types of malware and network attacks.

Day 5 (24th December)

Hands-on sessions on Malware Analysis using VirusTotal and Any.Run were conducted. Students gained practical exposure to analyzing malicious files.

Day 6 (29th December)

Students were introduced to the Hack The Box platform. The session covered account setup, interface navigation, and understanding the basics of ethical hacking labs. Students explored beginner-level machines to understand real-world attack scenarios.

Day 7 (30th December)
Hands-on practicals were conducted on network scanning and enumeration techniques using Hack The Box labs. Students practiced identifying open ports, services, and system information to understand initial stages of penetration testing.

Day 8 (31st December)
The focus of the session was on vulnerability assessment and exploitation techniques. Students analyzed vulnerabilities in target machines and learned how attackers exploit misconfigurations and weak security controls.

Day 9 (2nd January)
Advanced Hack The Box practicals were conducted, focusing on privilege escalation and system access techniques. Students learned the importance of securing user privileges and system permissions.

Day 10 (3rd January)
The final session included hands-on challenge-based practicals on Hack The Box. Students applied all the concepts learned during the bootcamp, including reconnaissance, exploitation, and security best practices. The session concluded with a recap and discussion on ethical hacking guidelines.

Outcomes of the program:

By the end of the program, students will be able to:

1. **Understand core concepts of Cyber Security**, including common threats, vulnerabilities, and attack vectors.
2. **Identify and analyze cyber threats** such as phishing, malware, and social engineering attacks.
3. **Apply basic Cyber Security practices to protect systems**, data, and digital identities.
4. **Demonstrate hands-on skills using ethical hacking tools** in a controlled and responsible environment.

5. **Explain fundamental cryptography concepts** and their role in securing communication and systems.
6. **Implement secure system practices** to reduce risks and improve overall cyber hygiene.
7. **Recognize ethical and legal considerations** in Cyber Security and ethical hacking.
8. **Develop interest and awareness of career opportunities** in the field of Cyber Security.

Conclusion

The Cyber Security program by LA Bootcamp was successfully conducted and provided valuable theoretical and practical knowledge to the students. Hands-on sessions, including Hack The Box practicals, enhanced understanding of real-world cyber security challenges. The program effectively promoted ethical practices and increased student interest in the field of Cyber Security.

Allyn Girls

allyngirls@xavier.ac.in

Sponsored by Allan & Lynda

Glimpse Of Event

Fig 1. First moments of the session

Fig 2. Collaborative learning among students

Fig 3. Hands-on practical session

Allyn Girls

allyngirls@xavier.ac.in

Sponsored by Allan & Lynda

Glimpse Of Certificate Distribution:

Prof. Smita Pawar
Allyn Girls Convener