



XAVIER INSTITUTE OF ENGINEERING

(An Autonomous Institute under Mumbai University)

Approved by AICTE and recognized by DTE, Government of Maharashtra
Accredited with an "A+" grade by NAAC; EXTC, IT and Computer Engineering are NBA-accredited.
Mahim (W), Mumbai - 400 016. Mobile no:- 2446 0359 / +91 7249371505 / +91 9920407274
Email: principal@xavier.ac.in ; office@xavier.ac.in Website: www.xavier.ac.in



THE ALLYN FUND

Cyber Fortress: Mastering Linux And Windows Security

DATE:- Monday, 8th December 2025 to Saturday, 13th December 2025.

TIME:- 9:00 AM to 4:00 PM.

VENUE:- Blockchain Lab, 1st Floor, X-Tech Building, Xavier Institute of Engineering, Mumbai.



Objective(s): This program offers practical training in ethical hacking and cyber defense, covering Linux and Windows security basics, real-world attack detection, and core skills like network scanning, password attacks, logging, and mitigation. Through live simulations, it sharpens analytical thinking and problem-solving abilities.

Beneficiaries: Allyn Girls students (SE, TE, BE)

No.of Participants: 28

Venue:Blockchain Lab, 1st Floor, X-Tech Building, Xavier Institute of Engineering, Mumbai.

Speaker Details:

The Cyber Fortress: Mastering Linux and Windows Security was conducted by an experienced industry professional from Hacktify Cyber Security. The session provided in-depth technical guidance and hands-on exposure to real-world cyber security challenges. The speaker brought strong industry expertise in vulnerability assessment, penetration testing, and cyber defense, ensuring a highly engaging and skill-oriented learning experience for all participants.

Sr. No.	Name of the Speaker	Organization	Designation	Area of Expertise	Role in the Program
1	Mr. Uddesh Vaidya	Hacktify Cyber Security, Mumbai	Cyber Security Consultant	Vulnerability Assessment & Penetration Testing (VAPT), Web & Mobile Application Security, Network Security, Ethical Hacking	Delivered all technical sessions, conducted hands-on practical labs, demonstrated real-world attack scenarios, guided defensive techniques, and conducted the final examination

Key Points / Day-wise Details:

Day 1 – 08/12/2025 (Linux Security Fundamentals):

- Participants were introduced to Linux operating system fundamentals including essential commands, file handling, directory management, UGO permissions, and octal permission systems.
- Hands-on activities included directory creation, file copying, permission setting, and basic security configurations.
- Core security concepts such as the CIA Triad, symmetric and asymmetric encryption, and hashing were demonstrated using real tools and live examples.

Day 2 – 09/12/2025 (Password Cracking & Network Scanning):

- Sessions focused on password cracking techniques using Hydra.
- FTP and SSH-based attacks were

demonstrated to explain credential exploitation. • Network scanning using Nmap was taught to identify open ports and enumerate services. • Firewall configuration using UFW was also demonstrated.

Day 3 – 10/12/2025 (Intrusion Prevention Systems):

• Participants explored system logging mechanisms and the importance of intrusion prevention systems. • Fail2Ban was configured to detect and block brute-force attacks. • A live attack-and-defense demonstration showcased how proactive security controls help mitigate threats.

Day 4 – 11/12/2025 (Windows Security & Web Attacks):

• Windows security fundamentals were covered, including firewall configuration and essential PowerShell commands. • Participants learned how to report vulnerabilities using official government platforms. • Web security concepts such as SQL Injection were demonstrated using vulnerable test environments. • Burp Suite was used to intercept and modify HTTP requests for better understanding of web attacks.

Day 5 – 12/12/2025 (Event Logs & SMB Attacks):

• Participants learned about important Windows Event IDs and Event Viewer analysis. • SMB enumeration and password spraying techniques were demonstrated using CrackMapExec. • Mitigation strategies such as disabling SMBv1, enforcing strong password policies, and enabling security logging were discussed.

Day 6 – 13/12/2025 (Advanced Hacking Challenge & Examination):

• The final day featured a multi-stage hacking challenge where participants were given an IP address and wordlist. • Tasks included identifying open ports using Nmap, bypassing non-default SSH configurations, gaining access to multiple user accounts, decrypting encrypted files, and accessing a Windows system via RDP to locate hidden flags. • An offline examination and quiz were conducted by Mr. Uddesh Vaidya to assess participants' technical understanding.

Conclusion:

The Cyber Fortress program was a highly impactful and technically enriching initiative that provided students with valuable real-world exposure to cyber attacks and defensive security mechanisms. While the program was conducted for all XIE students, it held special significance for Allyn Girls, as it encouraged them to actively participate in advanced cyber security learning, build confidence in technical domains, and explore career opportunities in the cyber security field.

The collaborative efforts of Hacktify Cyber Security, XIE Cyber Security Cell, and XIE IET On-Campus Chapter ensured the smooth execution and overall success of the program. The event successfully fostered a culture of inclusivity, skill development, and motivation among Allyn Girls, empowering them to aspire for excellence while learning alongside their peers.

Glimpse of the Event:



Fig 1: Day 1



Fig 2: Day 2



Fig 3: Day 3

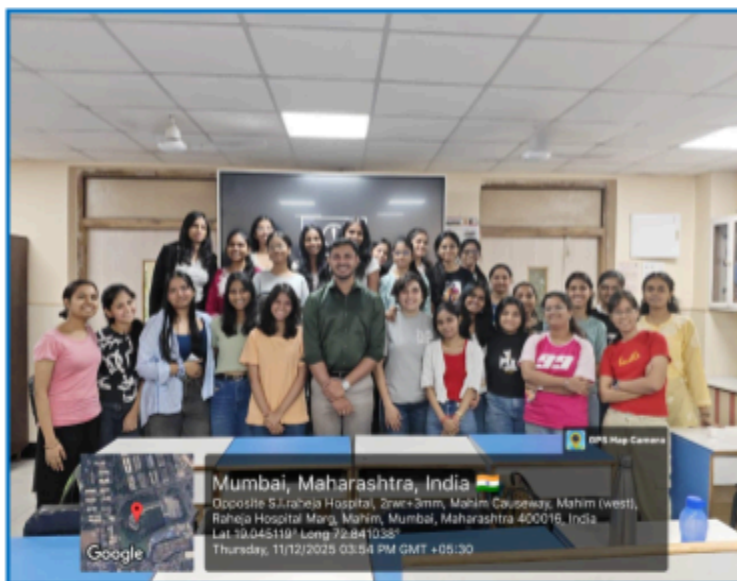


Fig 4: Day 4



Fig 5: Day 5



Fig 6: Day 6

Smita

Prof. Smita Pawar
Allyn Girls Convenor

