# SUMMER INTERNSHIP REPORT

*Submitted By*

**ALBY M BIJU**

**AJC24MCA-2013**

*In Partial fulfillment for the Award of the Degree Of*

**MASTER OF COMPUTER APPLICATIONS (MCA TWO YEARS)**

**AMAL JYOTHI COLLEGE OF ENGINEERING**

**AUTONOMOUS, KANJIRAPPALLY**

[Approved by AICTE, Accredited by NAAC.

Koovappally, Kanjirappally, Kottayam, Kerala –686518]

**2024-2026**

**DEPARTMENT OF COMPUTER APPLICATIONS**

**AMAL JYOTHI COLLEGE OF ENGINEERING**

**AUTONOMOUS, KANJIRAPPALLY**

# CERTIFICATE

This is to certify that the Summer Internship Report is the bonafide work of **ALBY M BIJU (AJC24MCA-2013)**, undertaken as part of the Summer Internship at **Wahy Lab Solutions, Kakkanad**. This report is submitted in partial fulfillment of the requirements for the award of the Degree of Master of Computer Applications under Amal Jyothi College of Engineering (Autonomous), Kanjirappally, during the academic year 2024–25.

Dr. Shelly Shiju George
**Class In - Charge**

Rev. Fr. Dr. Rubin Thottupurathu Jose
**Head of the Department**

# ACKNOWLEDGEMENT

I express my sincere gratitude to **Amal Jyothi College of Engineering** for providing the opportunity to undertake this internship as part of the MCA curriculum. I am grateful to **Rev. Fr. Dr. Roy Abraham Pazhayaparampil** (Director, Administration) and **Dr. Lillykutty Jacob** (Principal) for their continued support in facilitating this program.

I extend my heartfelt thanks to **Rev. Fr. Dr. Rubin Thottupurathu Jose** (Head, Department of Computer Applications) for his encouragement and guidance, and to **Dr. Shelly Shiju George** (Assistant Professor & Class Teacher, Regular MCA 2024–2026) for her mentorship and support during the internship.

I also appreciate the cooperation of all the faculty members of the Department of Computer Applications.

A special thanks to **Wahy Lab Solutions, Kakkanad**, for providing a professional and enriching environment that greatly enhanced my technical skills and practical knowledge.

Lastly, I thank my family, friends, and classmates for their constant encouragement and support.

# INTRODUCTION

The digital era has brought with it countless advancements in connectivity and communication, but it has also introduced a vast landscape of threats and vulnerabilities. In such a world, **cybersecurity** has emerged as a critical discipline. My one-month internship at **Wahy Lab Solutions** from April 1st to April 30th, 2025, served as an intensive exposure to this field, equipping me with practical insights and technical skills that complemented my academic learning.

Cybersecurity is not limited to antivirus software and firewalls; it encompasses a wide range of practices aimed at defending digital assets against attacks from malicious actors. At Wahy Lab Solutions, I worked closely with the cybersecurity team on real-world scenarios including **vulnerability assessment, penetration testing (VAPT), risk analysis, and cyber threat simulations**.

The internship gave me access to professional tools like **Kali Linux**, **Nmap**, **DirBuster**, **Metasploit**, and taught me the importance of **ethical hacking** principles, the structure of **cyber defence strategies**, and how critical documentation is for maintaining security compliance.

In this report, I will walk through my internship journey—detailing the course plan, the objectives I set out to achieve, the technical skills I developed, the real-world tools I used, the challenges I faced, and the overall outcomes of this experience.

# COMPANY PROFILE

**NAME: Wahy Lab Solutions, Kakkanad**

**LOCATION: Door No : D7, 7th floor, Heavenly Plaza, Padamugal, Kakkanad, Ernakulam 682021, Kerala, India**

**EMAIL: info@wahylab.com**

**PHONE: +91 9747776355**

**WEBSITE: www.wahylab.com**

**Wahy Lab Solutions** is one of the top website development companies in Ernakulam, strategically located in Kochi, India. From there, they cater their services across the globe. The company collaborates with clients to build stronger, value-added relationships with their customers by helping them increase the profitability of their business.

Wahy Lab Solutions is renowned for its foundation of quality and customer satisfaction. Their success is entirely the success of their clients.

They supply and support a broad range of IT application solutions and services, including IoT Healthcare, Industrial Automation, ERP-CRM Applications, Mobile App Development, Website and Application Development (Flutter Development), Digital Marketing and SEO Services, and Customized Software Solutions.

They provides cybersecurity internships for freshers. Cybersecurity is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It is also known as information technology security or electronic information security.

A few common categories of cybersecurity include network security, application security, information security, operational security, disaster recovery and business continuity, and end-user education.

The company offers one of the best cybersecurity internships in Kochi, focusing on real-world applications and skill development for beginners.

# COURSE PLAN

The internship was structured to simulate a cybersecurity analyst's responsibilities, offering exposure to both **offensive and defensive security practices**. The plan was broken down week-by-week as follows:

**Week 1: Orientation & Fundamental Concepts**

- Introduction to cybersecurity domains
- Understanding common cyber threats: phishing, ransomware, DDoS
- Overview of security layers: physical, network, endpoint, application, data
- Setting up a lab with **Kali Linux** and essential tools

**Week 2: Vulnerability Scanning & Risk Assessment**

- Learning **Nmap** for network scanning and service enumeration
- Using **Nikto** and **OpenVAS** for vulnerability scanning
- Identifying open ports, outdated software, and weak configurations
- Documenting risk levels using CVSS (Common Vulnerability Scoring System)
- Hands-on creation of vulnerability report

**Week 3: Penetration Testing & Exploitation**

- Conducting **directory brute-force attacks** using **DirBuster**
- SQL Injection simulations on test environments
- Exploring **Metasploit Framework** for payload generation and reverse shells
- Exploiting known CVEs in sandboxed environments
- Writing exploitation steps and post-exploitation documentation

**Week 4: Threat Simulation & Final Documentation**

- Participation in internal **red team vs blue team** drills
- Role-playing cyber threat incident response
- Creating awareness posters and materials
- Final compilation of reports: vulnerability logs, risk assessments, and threat response plans

# OBJECTIVES OF THE INTERNSHIP

The primary goal of the internship was to obtain practical experience in real-world cybersecurity practices. Key objectives included:

1. **Understand Vulnerability Assessment Methodologies**
    - Learn to identify and categorize vulnerabilities using tools like **Nmap**, **Nikto**, and **OpenVAS**
    - Analyze system weaknesses and determine exploitability

2. **Gain Hands-on Penetration Testing Skills**
    - Use Kali Linux utilities for attacking and defending test systems
    - Conduct **manual and automated penetration tests** following OWASP guidelines

3. **Perform Threat Analysis and Risk Documentation**
    - Create professional reports documenting threats, affected systems, and suggested remediations
    - Evaluate business risks using **asset-threat-vulnerability** models

4. **Learn Ethical Hacking Protocols**
    - Respect ethical boundaries while simulating attacks
    - Follow legal guidelines and obtain permissions before any testing

5. **Participate in Team-Based Simulations**
    - Engage in **cyber drills**, learn how security teams respond to real incidents
    - Develop communication skills needed to report findings to stakeholders

Through these objectives, I hoped to gain not just technical fluency, but also a strategic understanding of how cybersecurity fits into broader organizational structures.

# SKILLS ACQUIRED

During the course of my internship at Wahy Lab Solutions, I acquired a blend of **technical, analytical, and professional skills** that prepared me for real-world roles in cybersecurity. These skills were developed through hands-on application in simulated environments and guided mentorship.

### 1. Network Scanning & Mapping

I learned how to perform active and passive reconnaissance using tools like **Nmap** and **Netdiscover**. Nmap enabled me to identify open ports, running services, and even operating system fingerprints. This skill is foundational to both vulnerability assessment and penetration testing, as it helps define the attack surface of a system.

*Real-world use*: Network admins use Nmap regularly to audit and secure their systems; attackers also use it in early stages of an attack chain.

### 2. Vulnerability Identification

Using tools like **Nikto**, **OpenVAS**, and **Nessus**, I gained experience in identifying:

- Outdated server software
- Weak encryption configurations
- Missing security headers
- Publicly known CVEs (Common Vulnerabilities and Exposures)

I also documented findings using CVSS ratings to prioritize threats and recommend mitigation strategies.

### 3. Brute Force and Directory Attacks

Using **DirBuster** and **Hydra**, I simulated brute force attacks to identify weak password policies and unsecured admin directories. I observed how dictionary attacks can be used to gain unauthorized access to web directories and accounts.

*Ethical takeaway*: These simulations reinforced the importance of strong password policies and user access controls.

### 4. Exploitation with Metasploit

One of the highlights of my internship was learning how to use the **Metasploit Framework**. Under supervision, I conducted attacks using:

- Reverse shells
- Exploitation of known vulnerabilities (e.g., EternalBlue, MS17-010)
- Post-exploitation enumeration

This experience emphasized the **ethical responsibility** involved in exploitation and how it should only be done in authorized environments.

### 5. Report Writing and Risk Analysis

I developed the ability to write concise, professional **security reports** including:

- Executive summaries
- Vulnerability lists
- Risk ratings and business impact
- Recommended mitigation steps

*Industry use*: Such reports are often submitted to compliance bodies, stakeholders, and IT teams after a penetration test.

### 6. Team Collaboration and Threat Simulation

I participated in a red team vs blue team drill where we practiced:

- Offensive techniques to simulate threats
- Defensive strategies like firewall tuning and SIEM monitoring
- Communication under pressure during incident response

This enhanced my **teamwork and communication skills**, both essential in any cybersecurity operation.

# CHALLENGES FACED AND SOLUTIONS

Like any hands-on experience in cybersecurity, this internship presented a variety of challenges, both technical and operational. Overcoming these taught me valuable problem-solving skills and reinforced my commitment to continuous learning.

**1. Complex Tool Interfaces**

Initially, using tools like **Metasploit** and **OpenVAS** was overwhelming due to their extensive configurations and command-line interfaces.

*Solution*: I overcame this by following documentation, watching expert-led tutorials, and practicing in virtual labs daily. My familiarity improved through repetitive tasks and trial-error exploration.

**2. False Positives in Scanning**

During vulnerability assessments, I encountered numerous **false positives**—alerts that indicated issues where none existed.

*Solution*: I learned to cross-verify results using multiple tools and manual inspection techniques (e.g., validating input fields to confirm SQL injection vulnerabilities). This refined my analytical thinking and judgment.

**3. Simulated Exploits Not Working**

Some simulated attacks (e.g., payload delivery using reverse shells) failed due to incorrect configurations in the virtual network.

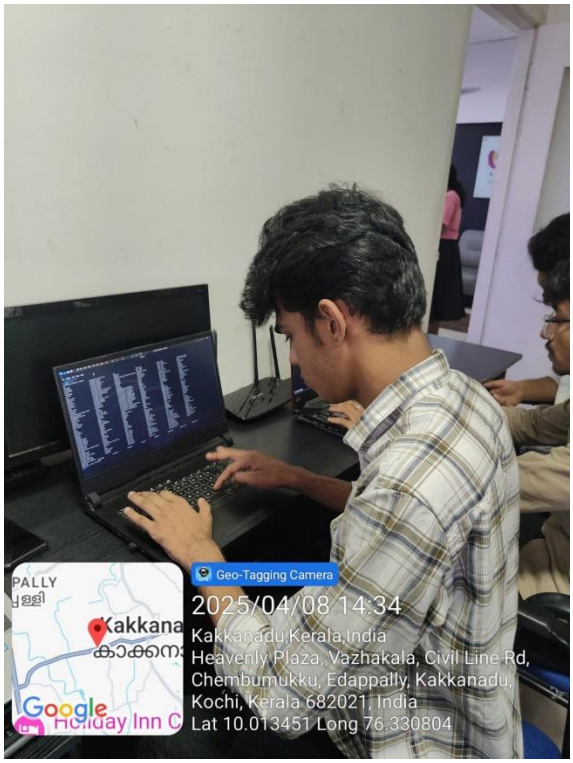
*Solution*: By debugging port forwarding issues, confirming firewall settings, and using tools like **Wireshark** for packet inspection, I learned how environment setup deeply affects penetration testing outcomes.

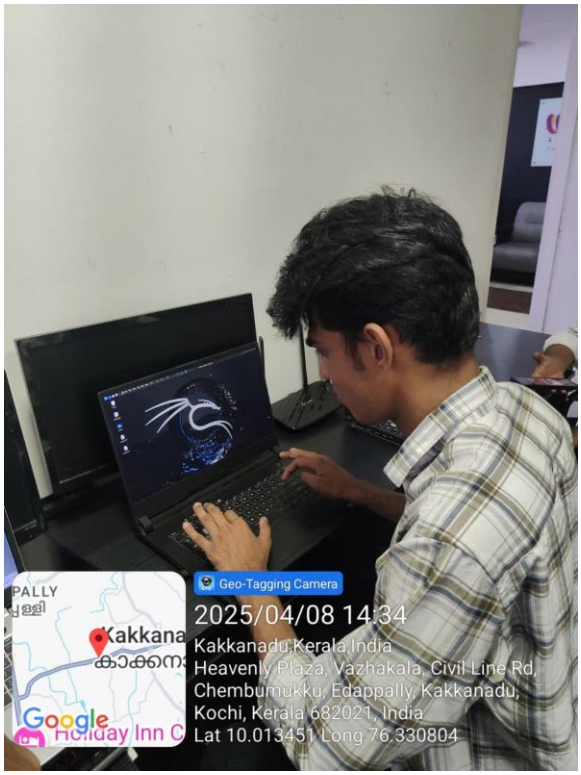
**4. Ethical Dilemmas and Responsibility**

Practicing ethical hacking brings with it a constant awareness of legality and intent. It's easy to overlook boundaries when performing offensive simulations.

*Solution*: My mentors ensured that we always operated within legally permissible environments, and I read about frameworks like **CEH (Certified Ethical Hacker)** code of conduct and **NIST** standards.

# PHOTOS


Geo-Tagging Camera
2025/04/08 14:34
Kakkanadu,Kerala,India
Heavenly Plaza, Vazhakala, Civil Line Rd, Chembumukku, Edappally, Kakkanadu, Kochi, Kerala 682021, India
Lat 10.013451 Long 76.330804


Geo-Tagging Camera
2025/04/08 14:34
Kakkanadu,Kerala,India
Heavenly Plaza, Vazhakala, Civil Line Rd, Chembumukku, Edappally, Kakkanadu, Kochi, Kerala 682021, India
Lat 10.013451 Long 76.330804

# CONCLUSION

This internship at Wahy Lab Solutions was a transformative experience that extended far beyond classroom theory. It immersed me in the **realities of cybersecurity**, where I learned not only how to use powerful tools but also how to think like a security professional.

I developed fluency in using open-source tools like **Kali Linux**, **Nmap**, **DirBuster**, **Hydra**, and **Metasploit**, all while understanding their strategic purpose in identifying, exploiting, and documenting system vulnerabilities. I also gained soft skills—team collaboration, report writing, incident handling—all critical in a professional cyber defense context.

This experience taught me that cybersecurity is not only about technology but also about **people, policies, and proactive thinking**. It's about protecting information with integrity, respecting ethical boundaries, and staying a step ahead of evolving threats.

Going forward, I am more confident in my ability to contribute meaningfully in roles related to penetration testing, SOC analysis, vulnerability management, or cyber risk consulting

This internship laid the foundation of what I hope will be a long and impactful journey in the field of cybersecurity.