N.S.S COLLEGE OF ENGINEERING

PALAKKAD, KERALA - 678008

Industrial Visit Report

To

EHACKIFY CYBERSECURITY RESEARCH & TRAINING

Submitted By: Tour Coordinators

SREEJITH M VARMA NSS22CS060

VAISAKH V NSS22CS065

SAM JAMES LNSS22CS073

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING March 2025

N.S.S COLLEGE OF ENGINEERING

PALAKKAD, KERALA - 678008

This is to certify that this is the bona-fide record for the Industrial visit to "Ehackify Cybersecurity Research & Training " on 04/03/25 done by S6CSE (2022 Admission) in partial fulfilment of requirements for the award of degree of bachelor of Technology in COMPUTER SCIENCE AND ENGINEERING under APJ Abdul Kalam Technological University.

Group Tutor
Kiran V K

Head Of Department
Dr. Viji Rajendran V

ACKNOWLEDGEMENT

I would like to express my sincere gratitude and thanks to the Management of NSS College of Engineering, Palakkad, especially to Dr. Rajeev N, Principal, NSS College of Engineering, Palakkad.

I would also like to express my heartfelt thanks to Dr. Viji Rajendran V, Head of the Department of Computer Science and Engineering, Kiran V K our Group Tutor for giving us proper guidance and help for the successful completion of the visit.

In this context, I would also like to express my special thanks to the entire team at Ehackify Cybersecurity Research & Training for arranging such informative and inspiring sessions at their training centre.

Last, but not the least I am extremely grateful to all my friends who made this journey a grand success.

ABSTRACT

The visit to Ehackify Cybersecurity Research & Training, Kochi provided an in-depth understanding of modern cybersecurity threats and countermeasures. The session covered data breaches in email and social media, highlighting phishing attacks, credential leaks, and security best practices. We were introduced to Flipper Zero, a multi-functional penetration testing tool used for RFID cloning, wireless security analysis, and infrared signal manipulation. The risks associated with USB-based attacks were demonstrated through USBKill and BadUSB techniques, emphasizing the need for USB security policies and access restrictions. Additionally, the session on lock picking showcased the importance of physical security in cybersecurity assessments. The visit provided valuable hands-on experience, reinforcing the significance of ethical hacking, penetration testing, and a holistic approach to cybersecurity.

TABLE OF CONTENTS

LIST OF FIGURES

Ehackify Cybersecurity Research & Training

1.1 INTRODUCTION

The visit to Ehackify Cybersecurity Research & Training, Kochi, was conducted on 4th March 2025 as part of an industry visit program. Ehackify is a well-established cybersecurity training and research institute specializing in ethical hacking, penetration testing, and cybersecurity awareness. The institute is known for its hands-on approach to cybersecurity education, providing in-depth training on various cyber threats and security tools. The objective of our visit was to gain practical knowledge of cybersecurity threats, understand modern hacking techniques, and explore the tools used by both security professionals and cyber attackers. The session covered critical aspects of data breaches, penetration testing tools like Flipper Zero, hardware-based attacks such as USBKill, and physical security techniques like lock picking. Through live demonstrations and interactive discussions, we were able to understand the real-world applications of cybersecurity measures and the importance of ethical hacking in safeguarding digital and physical assets

1.2 DATA BREACH IN SOCIAL MEDIA

The session began with an insightful discussion on data breaches in email and social media. Trainers explained how attackers exploit weak passwords, phishing scams, and leaked credentials to gain unauthorized access to user accounts. Real-world examples of major data breaches were analyzed, highlighting the consequences of exposed personal and corporate data. Participants were introduced to various preventive measures, such as enabling two-factor authentication (2FA), using password managers, and regularly monitoring accounts for suspicious activity. Tools like Have I Been Pwned were demonstrated to check for compromised credentials, emphasizing the importance of proactive security practices.

1.3 FLIPPER ZERO

The session featured a demonstration of Flipper Zero, a multi-functional cybersecurity tool widely used for security testing and ethical hacking. Trainers showcased its ability to interact with RFID, NFC, infrared signals, and wireless frequencies, making it a versatile device for penetration testers. Practical demonstrations included cloning RFID access cards, analyzing radio signals, and testing NFC security flaws. Participants were made aware of the ethical implications of such tools and how they can be leveraged for security assessments while ensuring responsible use.

1.4 USBKILL – USB-BASED ATTACKS

A significant portion of the session focused on USBKill, a device designed to test the resilience of hardware against power surge attacks. The trainers explained how malicious USB devices can be used to execute attacks such as power destruction, malware injection (BadUSB), and keylogging. Demonstrations included examples of how compromised USB devices can manipulate system functionality or permanently damage hardware. Attendees were advised on best practices, including restricting USB access, using data blockers for secure charging, and implementing strict USB security policies in corporate environments.

1.5 LOCK PICKING – PHYSICAL SECURITY AWARENESS

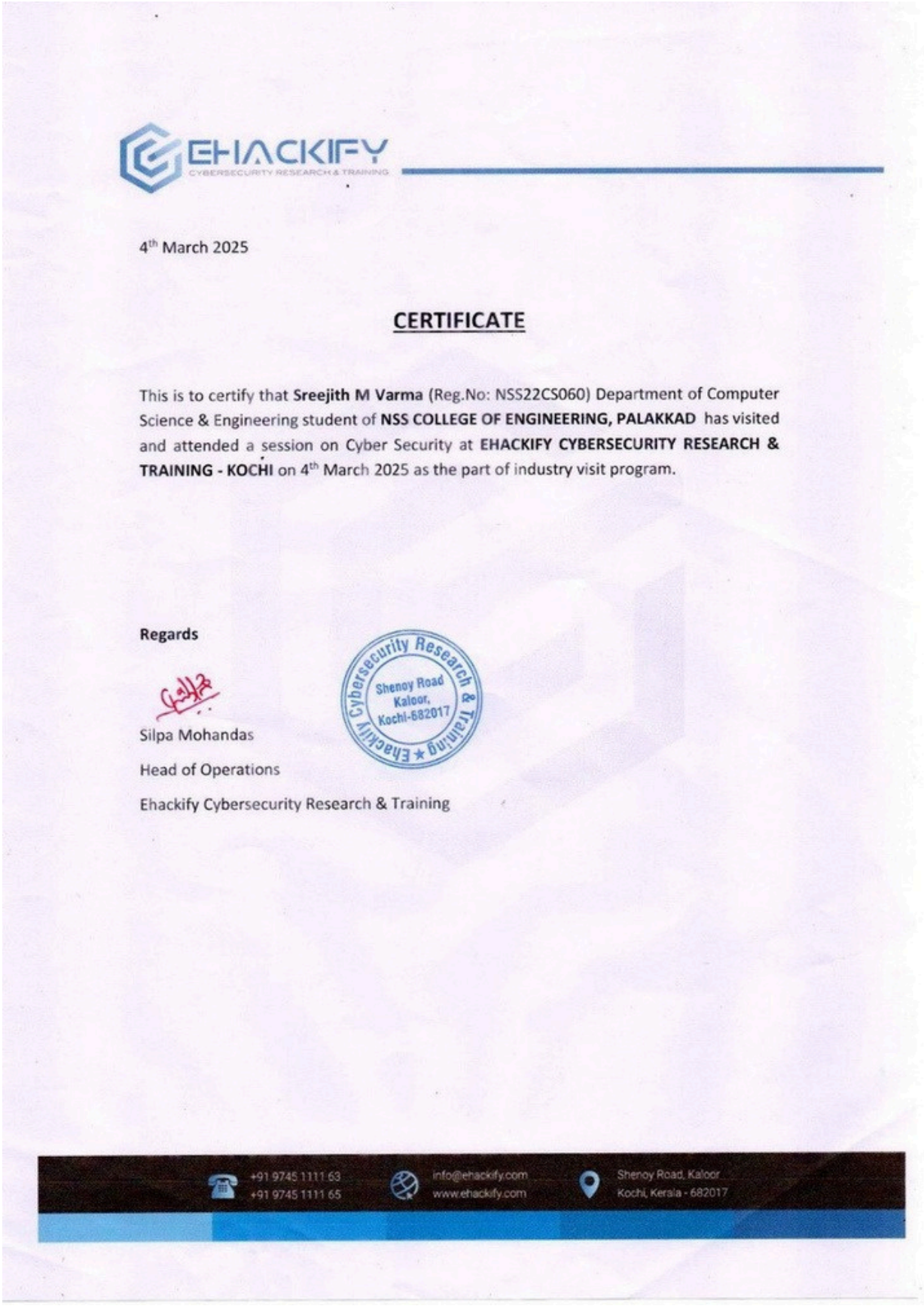
The session also covered lock picking as an essential aspect of physical security awareness. Participants were introduced to different types of lock mechanisms and how they can be vulnerable to unauthorized access. Hands-on demonstrations included lock-picking techniques using standard tools, highlighting the importance of securing critical areas such as server rooms, data centers, and restricted facilities. The discussion emphasized how penetration testers and red team professionals use lock picking to evaluate physical security measures while ensuring ethical and legal compliance.

1.6 DETAILED VISIT

Upon arriving at Ehackify Cybersecurity Research & Training, Kochi, we were welcomed by the training team, who introduced us to the institute's work in cybersecurity research, ethical hacking, and penetration testing. They emphasized the growing risks in both digital and physical security and the importance of proactive defense strategies. The session began with a discussion on data breaches in email and social media, explaining how cybercriminals exploit phishing attacks, credential leaks, and social engineering to compromise sensitive information. We were shown tools like Have I Been Pwned and learned best practices for password security, multi-factor authentication, and breach monitoring to prevent unauthorized access. Next, we explored Flipper Zero, a powerful cybersecurity tool used for penetration testing and security research. Trainers demonstrated its ability to clone RFID/NFC cards, manipulate infrared signals, and analyze wireless protocols. The session highlighted how ethical hackers use such tools to identify security vulnerabilities while adhering to legal guidelines. We then moved on to USBKill and USB-based attacks, where we learned how malicious USB devices can deliver payloads, log keystrokes, or physically damage hardware through power surge attacks. A BadUSB attack demonstration showed how plugging in a compromised device can manipulate system functionality. The trainers emphasized USB security measures, including access control policies, disabling unauthorized USB ports, and using data blockers to prevent such threats. The final part of the session focused on lock picking as an essential aspect of physical security awareness. We were introduced to different lock mechanisms, including pin tumbler locks, wafer locks, and combination locks. Through live demonstrations, we saw how penetration testers use lock-picking tools to assess physical security. The discussion stressed the importance of securing server rooms, data centers, and other restricted areas to prevent unauthorized access.

The visit to Ehackify Cybersecurity Research & Training provided an interactive and engaging learning experience, combining theoretical insights with real-world cybersecurity applications. Through live demonstrations and hands-on exposure, we gained a deeper understanding of cybersecurity threats, ethical hacking techniques, and preventive measures. The session reinforced the importance of cybersecurity in today's digital world and provided valuable knowledge for securing both digital infrastructures and physical assets

Fig 1.1. Ehackify Cybersecurity Research & Training Industrial Visit


EHACKIFY
CYBERSECURITY RESEARCH & TRAINING

4th March 2025

CERTIFICATE

This is to certify that **Sreejith M Varma** (Reg.No: NSS22CS060) Department of Computer Science & Engineering student of **NSS COLLEGE OF ENGINEERING, PALAKKAD** has visited and attended a session on Cyber Security at **EHACKIFY CYBERSECURITY RESEARCH & TRAINING - KOCHI** on 4th March 2025 as the part of industry visit program.

Regards

Silpa Mohandas

Head of Operations

Ehackify Cybersecurity Research & Training

Ehackify Cybersecurity Research & Training
Shenoy Road
Kaloor,
Kochi-682017

+91 9745 1111 63
+91 9745 1111 65
info@ehackify.com
www.ehackify.com
Shenoy Road, Kaloor
Kochi, Kerala - 682017

Fig 1.2. Sample Certificate issued by Ehackify Cybersecurity Research & Training

Name	University regNo
Abhinanda M S	NSS22CS002
Abhishek S	NSS22CS006
Adeela farshana A	NSS22CS007
Ameesha. T	NSS22CS014
Anjali VM	NSS22CS016
Anjithkrishnan K	NSS22CS018
Brighty Jobin	NSS22CS026
Fathima lana EK	NSS22CS031
Kanishka C	NSS22CS036
Mihikka S	NSS22CS039
munawir muhammed p	NSS22CS042
Naviya p	NSS22CS045
Nidha Shameer TS	NSS22CS047
Riya S	NSS22CS055
Riyas PK	NSS22CS056
Rohan C Alben	NSS22CS057
Sasank M	NSS22CS059
Sreejith M Varma	NSS22CS060
S Thejaswini	NSS22CS061
Vaisakh V	NSS22CS065
vaishnav gopal	NSS22CS066
Shamil A	PKD22CS056
Nandhana C S	LNSS22CS070
Phoenix lal P T	LNSS22CS071
Rajeev R	LNSS22CS072
Sam James	LNSS22CS073

Visited students list

CONCLUSION

Our visit to Ehackify Cybersecurity Research & Training, Kochi was an insightful experience that deepened our understanding of cybersecurity threats and defense mechanisms. Through hands-on demonstrations, we explored the risks associated with data breaches, USB-based attacks, wireless security threats, and physical security vulnerabilities. The sessions on Flipper Zero, USBKill, and lock picking highlighted how ethical hackers and security professionals assess and strengthen both digital and physical security systems. This visit emphasized the growing importance of cyber awareness, ethical hacking, and proactive security measures in today's digital landscape. The knowledge gained from these sessions will be invaluable in identifying vulnerabilities, preventing cyber threats, and implementing stronger security practices in real-world scenarios

BIBLIOGRAPHY

- https://ehackify.com/ - EHACKIFY CYBERSECURITY RESEARCH & TRAINING