# VISVESVARAYA TECHNOLOGICAL UNIVERSITY

**Belagavi-590018,Karnataka**

**Internship report**

**ON**

# “NETWORK SCANNER WITH WIFI PASSWORD SEARCHER”

## BACHELOR OF ENGINEERING IN CSE-AIML

*Submitted by*

**JAYASRI G , 1AM21CI019**
**TARUN BALAJI KS, 1AM21CI04**

Conducted at
**INCERD**

## AMC ENGINEERING COLLEGE

Department of branch CSE-AIML

**Accredited by NAAC&NBA, New Delhi**

**AMC CAMPUS,BANNERGHATTA MAIN ROAD,BENGLURU,KARNATAKA-560083**

# AMC ENGINEERING COLLEGE

Department of CSE-AIML

**Accredited by NAAC&NBA, New Delhi**

**AMC CAMPUS,BANNERGHATTA MAIN ROAD,BENGLURU,KARNATAKA-560083**

## CERTIFICATE

This is to certify that the Internship titled **“**CYBER SECURITY**”** carried out by **Ms Jayasri G and Mr. Tarun Balaji KS** , bonafide students of AMC Engineering College, in partial fulfillment for the award of **Bachelor of Engineering**, in **CSE AIML** under Visvesvaraya Technological University,Belagavi, during the year 2022-2023. It is certified that all corrections/suggestions indicated have been incorporated in the report.

The project report has been approved as it satisfies the academic requirements in respect of Internship prescribed for the course Internship / Professional Practice (18CSI85)

**Signature of Guide** **Signature of HOD** **Signature of Principal**

# DECLARATION

We, **Jayasri G and Tarun Balaji K S**, third year student of CSE AIML, AMC Engineering College - 560 083, declare that the Internship has been successfully completed, in **INCERD**. This report is submitted in partial fulfillment of the requirements for award of Bachelor Degree in CSE AIML , during the academic year 2022-2023.

Date : 10/12/2023

Place : Bangalore

USN :1AM21CI019

:1AM21CI049

NAME : JAYASRI G

TARUN BALAJI K S

# ACKNOWLEDGEMENT

This Internship is a result of accumulated guidance, direction and support of several important persons. We take this opportunity to express our gratitude to all who have helped us to complete the Internship.

We would like to thank INCERD, for providing us an opportunity to carry out Internship and for their valuable guidance and support.

We express our deep and profound gratitude to our guide, Tarun Balaji K S, for his keen interest and encouragement at every step in completing the Internship.

We would like to thank all the coordinators for the support extended during the course of Internship.

Last but not the least, we would like to thank our parents and friends without whose constant help, the completion of Internship would have not been possible.

# ABSTRACT

In today's digitally interconnected world, the significance of cybersecurity cannot be overstated. As cyber threats continue to evolve in complexity and scale, there is a growing need for skilled professionals to safeguard digital ecosystems. This abstract delves into the experiential learning gained through a cybersecurity internship, examining the bridge between theoretical knowledge and practical application in the realm of cybersecurity.

The internship provided an immersive experience within a dynamic cybersecurity environment, offering a hands-on opportunity to apply theoretical concepts learned in academic settings. The internship covered a broad spectrum of cybersecurity domains, including but not limited to network security, penetration testing, incident response, and security policy enforcement.

Throughout the internship, emphasis was placed on the application of theoretical knowledge to real-world scenarios, enabling the development of practical skills such as vulnerability assessment, threat detection, and mitigation strategies. The intern had the opportunity to work alongside seasoned professionals, gaining insights into industry best practices and the latest advancements in cybersecurity technology.

The internship also facilitated exposure to diverse cybersecurity tools and platforms, allowing the intern to navigate through simulated cyber incidents, assess system vulnerabilities, and implement proactive security measures. The experience contributed to a deeper understanding of the challenges faced by cybersecurity professionals and the critical role they play in safeguarding sensitive information.
In essence, this abstract provides a panoramic view of cybersecurity, encapsulating its foundational principles, contemporary challenges, and the dynamic strategies employed to protect digital assets and privacy in an interconnected world.

# Table of Contents

# CHAPTER 1

# INTRODUCTION

# 1.INTRODUCTION

A network scanner with a WiFi password searcher is a tool designed to analyze and explore wireless networks. It scans for available networks, provides essential information about them, and, in some cases, attempts to find or crack their passwords. This type of tool is often used for network troubleshooting, security testing, or by individuals seeking unauthorized access to WiFi networks. It's crucial to note that using such tools for unauthorized access is illegal and unethical, emphasizing the importance of responsible and lawful use in any network-related activities.

This versatile tool finds applications across a spectrum of scenarios, serving as an indispensable asset for legitimate network troubleshooting, optimization endeavors, and rigorous security assessments to identify potential vulnerabilities. Nevertheless, it is of utmost importance to underscore the ethical and legal considerations that accompany its use. Engaging in unauthorized activities, including attempts to access WiFi networks without proper authorization or compromise their passwords, not only violates legal frameworks but also contradicts ethical standards. Therefore, responsible and lawful utilization is not only a prudent choice but an imperative one to uphold the integrity and legality of all network-related activities.

While network scanners with WiFi password searchers are powerful tools for network management, their usage raises ethical considerations. It is imperative to emphasize that these tools should only be employed for legitimate and authorized purposes, such as network maintenance, security assessments, and troubleshooting. Unauthorized use, including attempting to access networks without permission, is a violation of privacy and legal standards.

# CHAPTER 2

# SOFTWARE REQUIREMENTS AND SPECIFICATIONS

# 2.SOFTWARE REQUIREMENTS AND SPECIFICATIONS

## SOFTWARE REQUIREMENTS:

1.**Programming Language**: Choose a language like Python, Java, or C++ based on your preference and platform compatibility.

2.**Network Scanning Library**: Utilize a library like Scapy (Python), jpcap (Java), or pcap (C++) for network scanning capabilities.

3.**WiFi Password Retrieval**: Implement tools like Aircrack-ng or Wifite to search for and retrieve WiFi passwords.

4. **Operating System Compatibility**: Consider the compatibility of your software with different operating systems (Windows, Linux, macOS).

## TECHNICAL SPECIFCATIONS:

1**.WiFi Password Searching**: Implement a script to search for default credentials or vulnerabilities.Use tools like Aircrack-ng for WiFi password cracking

2**.Compliance**: Ensure your project complies with local laws and regulations.

3.**Ethical Use**: Emphasize responsible and ethical use of the tool to avoid legal consequences.

4.**Network Scanning** Software:Use tools like Nmap or custom scripts to scan and identify devices on the network.

# CHAPTER 3

# PROJECT PLAN

# 3.PROJECT PLAN

1. **Define Requirements:**

- Define the purpose of the project: Building a network scanner with the ability to search for WiFi passwords.
- Specify the target platforms (e.g., desktop, mobile).

2. **Technology Stack :**

- Choose programming languages and frameworks suitable for network scanning and WiFi password retrieval.
- Determine if any third-party libraries or tools will be utilized.

3. **System Architecture**

- Design the overall architecture of the network scanner, outlining how components will interact.
- Identify modules for network scanning and WiFi password searching.

4. **User Interface Design**

- Create wireframes or mockups for the user interface.
- Ensure a user-friendly design for both network scanning and password retrieval.

5. **Network Scanning Implementation**

- Develop the functionality to scan and enumerate devices on the network.
- Implement features for identifying connected devices.

6. **WiFi Password Retrieval Implementation**

- Develop methods to retrieve WiFi passwords from connected devices.
- Ensure security measures to protect user privacy and comply with legal considerations.

# CHAPTER 4
# DESIGN STARTEGY

# 4.Design Strategy

- Clearly define the project's purpose, emphasizing ethical use and legal boundaries.
- Focus on network security assessment rather than unauthorized access.
- Ensure compliance with local and international laws related to network scanning and data privacy.
- Clearly communicate to users that the tool should only be used on networks they own or have explicit permission to assess.
- Implement robust user authentication to control access to the tool and its features.
- Develop a scanning module to identify active devices on the network.
- Include features for discovering open ports and services on each device.
- Only include this feature if it aligns with ethical considerations and legal requirements.
- Implement a secure method for retrieving and displaying Wi-Fi passwords, ensuring access is limited to authorized users.
- Implement encryption for communication between the tool and the scanned devices.
- Regularly update the tool to address security vulnerabilities.
- Provide clear documentation on the ethical use of the tool.
- Emphasize responsible usage and respect for privacy.
- Implement comprehensive logging mechanisms to track tool usage.
- Allow administrators to audit and review the tool's activities.
- Implement a notification system to alert network owners of the scanning activities, fostering transparency.
- Encourage open-source development and peer review to ensure transparency and security.
- Consider community input to refine and enhance the tool's functionality.

# CHAPTER 5
# IMPLEMENTATION

# 5.**Implementation**

The network scanner with a WiFi password searcher project involves several key components and considerations.

Firstly, the network scanning aspect typically employs techniques like ARP (Address Resolution Protocol) scanning to identify devices on the network. This helps create a list of active devices by mapping IP addresses to corresponding MAC addresses. The tool may also employ ping sweeps or other methods to discover devices that might not respond to ARP requests.

Once the active devices are identified, the tool may attempt to gather more information about them, such as open ports, services running, and potentially vulnerable areas. This phase often requires a balance between thorough scanning and respecting privacy and security concerns.

The WiFi password searching functionality usually focuses on accessing the router's admin panel. This step requires knowledge of the router's IP address and valid login credentials. While default credentials are sometimes successful, users often change them for security reasons. Therefore, the tool may need to employ techniques like dictionary attacks or brute force attacks, though ethical considerations and legal regulations strongly discourage such methods.

It's crucial to emphasize responsible and ethical use of this tool. Unauthorized access to networks, devices, or data is illegal and unethical. Developers and users should prioritize obtaining proper authorization and consent before using such tools, and be aware of the potential legal consequences associated with unauthorized access.

In summary, the project involves network scanning to identify devices and extracting information, coupled with an attempt to access the router's admin panel to retrieve the WiFi password. Ethical considerations, legal compliance, and user consent are integral aspects of the development and usage of such tools.

# CHAPTER 6
# FUTURE WORK

# 6.Future Work

**1.Enhanced Security Features:**

- Implement robust encryption techniques to ensure the security of scanned networks and passwords.

**2.User-Friendly Interface:**

- Improve the app's UI for a more intuitive and user-friendly experience, making it accessible for users with varying technical backgrounds.

**3.Database Integration**:

- Incorporate a secure database to store and manage scanned network details, providing users with a history of connected networks.

**4.Cross-Platform Compatibility:**

- Develop versions for multiple platforms (Windows, macOS, Linux, iOS, Android) to cater to a broader audience.

**5.Automated Updates:**

- Integrate an automatic update system to keep the application current with the latest security standards and features.

**6.Community Feedback Integration:**

- Include a feedback mechanism for users to report issues and suggest improvements, fostering community engagement.

**7. Security Auditing Tools:**

- Integrate tools for users to assess the security of their own networks and identify potential vulnerabilities.

**8. Educational Resources:**

- Include guides or tooltips to educate users about network security best practices and responsible usage of such tools.

**9. Permission Handling:**

- Implement fine-grained permission controls to ensure the app adheres to privacy standards and regulations.

**10. Multi-Language Support:**

- Translate the app into multiple languages to make it accessible to a global audience.

# CHAPTER 7
# CONCLUSION

# 7.**CONCLUSION**

Attempting to extract Wi-Fi passwords using network scanners or related tools is not the primary function of these utilities. While certain techniques within specialized software like Kali Linux may aid in capturing data that could lead to identifying or cracking Wi-Fi passwords, this should only be done ethically and legally with proper authorization. Unauthorized access to networks or attempts to obtain passwords without permission are illegal and unethical.

It's important to prioritize ethical and legal considerations when using tools like network scanners or penetration testing platforms. These tools are designed for security testing, but their misuse can lead to legal consequences. Always ensure you have proper authorization and permission before attempting any form of network scanning or security testing, especially when it involves accessing or attempting to obtain passwords or sensitive information. Responsible and ethical use of these tools is crucial to ensure the security and privacy of networks and systems.

Responsible use of network scanning tools involves strict adherence to ethical and legal standards, refraining from unauthorized attempts to access networks or extract passwords without explicit consent. Prior authorization is pivotal before initiating any security assessments or network scans. While network scanners primarily identify devices and vulnerabilities without directly revealing Wi-Fi passwords, specialized platforms like Kali Linux may contain functionalities aiding in data capture for password identification. However, their primary intent remains security testing and vulnerability assessment. It's imperative to deploy these tools responsibly, focusing on legitimate purposes, respecting privacy, and prioritizing network security while continuously staying informed about legal implications and ethical considerations associated with their use.