SAHYADRI
COLLEGE OF ENGINEERING & MANAGEMENT
An Autonomous Institution
MANGALURU

Department of Computer Science & Engineering

Mini-Project Synopsis - Academic Year 2023-24

1	**Title of the Project**	Network Port Scanner
2	**Team No**	CS59
3	**Department**	Department of Computer Science & Engineering
4	**Project Area/Domain**	Cyber security
5	**Project Type**	Distributed Web application
6	**Name of the Students with USN**	1. Prateek Satyavan Naik 4SF21CS110 2. Adithya Nayak K 4SF21CS007 3.Puneeth Kumar 4SF21CS117
7	**Name of Guide**	Mr. Kishore Kumar K

Abstract

The primary intent of this project is to develop a robust and efficient tool for examining open ports on a target system. Utilizing socket programming, to identify accessible entry points on a network. Port scanning involves systematically probing a range of ports on a host to discover open, closed, or filtered ports. By leveraging an API, the aim is to create a versatile and potent scanning tool, specifically focusing on port scanning.

Central to the efforts is the identification and analysis of vulnerabilities within the network. This entails a thorough exploration of potential weaknesses that could be exploited by malicious actors. The capabilities can extend beyond TCP ports, incorporating an investigation into potential vulnerabilities within UDP ports. This distributed approach enhances the tool's effectiveness in network security assessment, ensuring a thorough examination of potential risks and weaknesses, including those unveiled through the intricacies of port scanning.

Introduction

Overview: The Network Port Scanner project is rooted in the foundational principles of network security, aiming to address the growing need for accessible yet robust tools that enable the identification of potential vulnerabilities within computer networks. At its core, the project revolves around the development of a tool that leverages socket programming, multithreading, and user interface design to provide an efficient and distributed solution for port scanning.

Scope: The scope of the project extends from fundamental aspects, such as user-input handling and specifying port ranges, to advanced features, including multithreading for optimized performance and the potential for scanning UDP ports. Additionally, the project encompasses the design of an intuitive user interface and robust error-handling mechanisms, ensuring a comprehensive and adaptable tool for varying applications.

Literature Survey:

Base Papers:

Name of Paper	Publisher	Date of Publish	Source of paper	Author
Port scan detection	IEEE	2nd Feb 2009	IEEE website	Jayanth Gadge Anish Anand Paatil
Port Scanning Techniques	Research gate	2010	DBLP	Germinal Isren
Port Scanning Utility	IIT Kanpur	2015	IIT Kanpur	Sourav Khandelwal Anurag Awasthi Vismay Chintan

Problem Statement and Description

Problem Statement

To detect

- The host or hosts are alive on the target network
- What Services are running?
- What users own those services?
- The port state of target machine ports.

Explanation

The challenge is to design a tool that scans and displays open ports on a computer system, contributing to enhanced security by identifying vulnerabilities. This requires creating an efficient and user-friendly solution accessible to users of diverse technical backgrounds

Objectives:

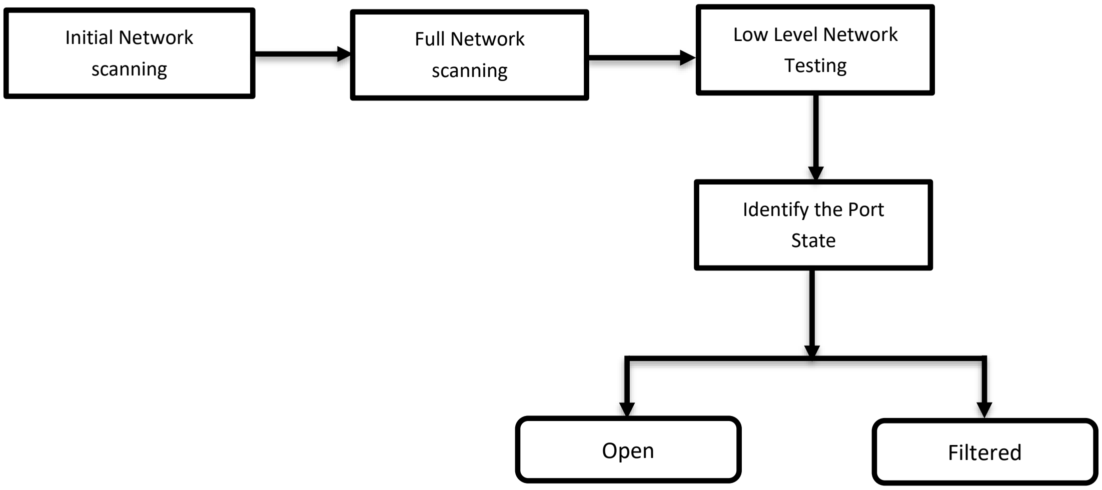
Develop a User-Friendly Interface: Create an intuitive and accessible user interface for the Network Port Scanner, allowing users of varying technical backgrounds to input target IP addresses and port ranges effortlessly.

Implement Efficient Port Scanning: Utilize socket programming and multithreading to design a scanning mechanism that ensures efficient examination of open ports, providing timely and accurate results without compromising performance.

Explore Advanced Features: Investigate the feasibility of extending the tool's capabilities to include the scanning of UDP ports, offering users a more comprehensive analysis of network services.

Promote Ethical Use: Emphasize responsible and ethical use of the Network Port Scanner by incorporating features and guidelines that encourage obtaining proper authorization before initiating scans, reinforcing a commitment to legal and ethical boundaries in cybersecurity practices.

Proposed Methodology:



The outcome of the work

Functional Tool: Develop a practical Network Port Scanner that efficiently checks open ports on a computer.

User-Friendly Frontend: The web application features an intuitive and user-friendly frontend, allowing users to easily input scanning parameters and interpret results.

Clear Port Status Output: Users receive a straightforward output detailing the status of open ports on their system, providing a concise overview of potential vulnerabilities.

Educational Impact: Provide users with insights into network security, ethical hacking, and Python programming.

Robust Security Scanning: The tool implements a robust security scanning mechanism, accurately identifying open ports and potential vulnerabilities on the user's system.

Conclusion

In conclusion, the web application delivers a potential solution for applications to evaluate their system's security. It provides user friendly interface to detect open ports, crucial for vulnerability assessment. Applications can use this information to proactively address security concerns and strengthen their systems against potential vulnerabilities.

16.	**Signature of Students**	
17.	**Signature of Guide**	
18.	**Signature of the Project Coordinator**	