DNS LOOP

A Major Project Report
Submitted in Partial Fulfillment of the requirement for the Award of the
Degree of

BACHELOR OF TECHNOLOGY

(COMPUTER SCIENCE AND ENGINEERING)

To

Dr. A.P.J. ABDUL KALAM TECHNICAL UNIVERSITY, LUCKNOW

Submitted by:

DEVESH KESARWANI
(1900100100061)

NAMO MISHRA
(1900100100094)

NIKITA SINGH
(1900100100102)

SAUMYA YADAV
(1900100100132)

UNDER THE SUPERVISION OF

Mr. RAHUL KESHARWANI
(Assistant Professor)

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

UNITED COLLEGE OF ENGINEERING AND RESEARCH, PRAYAGRAJ

MAY 2023

CANDIDATE’S DECLARATION

We, hereby declare that the project entitled “DNS LOOP” (Group-2) submitted by us in partial fulfillment of the requirement for the award of degree of the B. Tech. (Computer Science & Engineering) submitted to Dr. A.P.J. Abdul Kalam Technical University, Lucknow at United College of Engineering and Research, Prayagraj is an authentic record of our own work carried out during the period from June, 2022 to May, 2023 under the guidance of Mr. Rahul kesharwani (Assistant Professor, Department of Computer Science & Engineering). The matter presented in this project has not formed the basis for the award of any other degree, diploma, fellowship or any other similar titles.

DEVESH KESARWANI
(1900100100061)

NAMO MISHRA
(1900100100094)

NIKITA SINGH
(1900100100102)

SAUMYA YADAV
(1900100100132)

Place: Prayagraj

Date:29/05/23

CERTIFICATE

This is to certify that the project titled “DNS LOOP” is the bonafide work carried out by DEVESH KESARWANI (1900100100061), NAMO MISHRA (1900100100094), NIKITA SINGH (1900100100102) and SAUMYA YADAV (1900100100132) in partial fulfillment of the requirement for the award of degree of the B.Tech. (Computer Science & Engineering) submitted to Dr.A.P.J Abdul Kalam Technical University, Lucknow at United College of Engineering and Research, Prayagraj is an authentic record of their own work carried out during the period from June 2022 to May 2023 under the guidance of Mr. Rahul kesharwani (Assistant Professor, Department of Computer Science & Engineering).

Signature of the Guide ________________________________

[Mr. Rahul Kesharwani]

Signature of Project Coordinator ________________________________

[Mr. Shyam Bahadur Verma]

Signature of the Head of Department ________________________________

[Dr.Vijay Kumar Dwivedi]

Place: Prayagraj

Date:29/05/23

ACKNOWLEDGEMENT

We express our sincere gratitude to the Dr. A.P.J Abdul Kalam Technical University, Lucknow for giving us the opportunity to work on the Major Project during our final year of B.Tech. (CSE) is an important aspect in the field of engineering.

We would like to thank Dr. H.P. Shukla, Principal and Dr. Vijay Kumar Dwivedi, Head of Department, CSE at United College of Engineering and Research, Prayagraj for their kind support.

We also owe our sincerest gratitude towards Rahul Kesarwani sir for his valuable advice and healthy criticism throughout our project which helped us immensely to complete our work successfully.

We would also like to thank everyone who has knowingly and unknowingly helped us throughout our work. Last but not the least, a word of thanks for the authors of all those books and papers which we have consulted during our project work as well as for preparing the report.

ABSTRACT

Our project seeks to create a software tool that enables network administrators and security experts to undertake thorough network port and service scanning and analysis. The project focuses on offering a quick and simple way to find open ports, note running services, and evaluate any security holes in a target network. In order to systematically scan a variety of IP addresses and assess the state of particular ports, our research will make use of a variety of scanning techniques and protocols. In order to meet particular scanning needs, it will offer the flexibility to customize scanning parameters, such as scan speed, port range, and service detection choices.The software will produce thorough reports detailing the findings after the scanning procedure is finished, including a list of open ports, related services, and probable vulnerabilities.

Accuracy, dependability, and performance will be given top priority in our project to ensure successful scanning operations. To reduce any potential dangers related to port scanning activities, it will take security into account and follow best practices.The project's goal is to improve network security and make proactive network infrastructure monitoring and management easier by creating this port scanning software application. It is a priceless resource for spotting potential vulnerabilities, evaluating the security posture, and putting in place the necessary safeguards to safeguard important systems and data. A well-known software development life cycle, the project will include requirements collecting, system design, implementation, testing, deployment and final maintenance phases. In relation to network scanning and security, it will take into account industry standards, protocols, and best practices.

Overall, our project's goal is to provide a reliable and effective solution that gives network administrators and security experts the tools they need to actively manage network security and reduce potential dangers.

TABLE OF CONTENT

INTRODUCTION

Chapter-1

Introduction

An essential method for finding open ports on a computer or network is port scanning. Port scanning is an essential step in network security because hackers can use these unsecured ports to gain unauthorized access to any system.

Our project's goal is to examine various port scanning techniques, their advantages and disadvantages, and their use in network security in order to identify vulnerable ports on a network. The project will go over various port scanning tools and software as well as quick and deep scanning techniques.

The initiative will also go through the moral issues with port scanning, like the chance of interfering with network traffic or harming systems.

1.1Problem Statement and Scope

This project's objective is to design and implement a port-scanning tool that can search a target network for open ports and provide comprehensive details about the services found. The program should be able to do both TCP and UDP scans and offer accurate and trustworthy results.

The primary problems to be tackled in this project are developing efficient scanning algorithms that can handle huge networks without overwhelming them, decreasing the danger of detection by intrusion detection systems, and ensuring that the tool functions within legal and ethical constraints.

The finished product ought to be simple to use and offer thorough reports on the services and ports that were scanned. It should also be designed with extensibility in mind, allowing for future improvements and updates. Overall, network administrators and security experts looking to find and fix vulnerabilities in their networks should find the port-scanning tool to be a useful tool.

The finished solution need to be simple to use and offer thorough reports on the services and ports that were scanned. It should be created with extensibility in mind to enable for upcoming updates and changes. Overall, network administrators and security experts looking to find and fix vulnerabilities in their networks should find the port-scanning tool to be a useful tool.

1.3 Motivation Of The Project

The goal of the port-scanning project is to give network administrators and security experts a practical tool for locating and repairing network vulnerabilities. Port scanning is an important part of network security since it helps to find open ports on a system, which might possibly be exploited by attackers to obtain unwanted access to the network.

Network administrators and security experts can find open ports by using a port-scanning tool and then take the required precautions to secure them, such as blocking superfluous ports, updating software versions, or applying security updates. This helps to prevent potential attacks and improve the overall security posture of the network.

Additionally, traditional manual techniques of port scanning become more and more ineffective as networks continue to expand in size and complexity.

1.4 Benefits

Network administrators and security experts may benefit from the port-scanning project in a number of ways. Here are a few of the main advantages:

1.Increased network security:

By locating open ports on a network, the port-scanning tool can assist in locating potential flaws that attackers might exploit. The results of the scan can be used by network administrators and security experts to decide what steps should be taken to secure the network, such as closing unused ports, updating software, or installing security patches.

2. Time-saving:

Manual port scanning can be laborious and unworkable, especially for larger networks. By automating the scanning procedure, the port-scanning tool can produce thorough and accurate findings more quickly and efficiently.

3. Lessened danger of network outages:

By spotting potential flaws before they are exploited, the port-scanning technology can help avoid outages and other problems brought on by security breaches.

4. Adherence to rules:

Many organizations are obligated to adhere to regulations that are specific to their business and call for recurring network vulnerability assessments. By delivering thorough reports on the scanned ports and services, the port-scanning tool can assist organizations in meeting these standards.

5. Extensibility:

The port-scanning tool can be made extensible, enabling for upcoming updates and improvements. This indicates that it can be modified to accommodate evolving network environments and security threats.

Overall, the port-scanning project can help increase network security, save time, lower the chance of network outages, guarantee regulatory compliance, and provide extensibility for upcoming updates and improvement

System Analysis

Chapter 2

2.1 Feasibility Study

A feasibility study evaluates how viable or advantageous the creation of an information system will be for a certain organization or a group. The feasibility analysis should be carried out continually throughout the life cycle of the system.

In our project, a port scanning feasibility study would typically assess the usefulness and practical ability of doing port scanning for a certain situation. The act of searching a network for open ports on a certain system is known as Port Scanning.

Feasibility study is important because if port scanning is thought to be practical, it should be carried out carefully and in accordance with all relevant rules and regulations. In order to safeguard against any potential risks or threats that might be discovered during the scanning process, it is also crucial to make sure that the proper security measures are in place.

The following factors can be used to analyse the viability of the development software:

1. Operational Feasibility
2. Technical Feasibility
3. Economic Feasibility

2.1.1 Operational Feasibility:

The application will cut down on the amount of time needed to maintain manual records and makes records maintenance less strenuous and time-consuming.

In our project, operational feasibility of port scanning refers to the practicality of conducting port scanning withing the context of an organization's existing resources, processes and infrastructure.

Conducting a port scan requires personnel with specialized knowledge of network security and scanning tools. The availability of such personnel withing the organization must be evaluated and hence the operational feasibility is assured.

2.1.1 Technical Feasibility:

Technical feasibility refers to the evaluation of whether a proposed project can be developed, implemented and operated utilizing the current technical resources and infrastructure. It determines if the technical specifications of the project can be met within the limitations of the technology and resources.

In our project, for determining the port scanning is technically feasible, the following variables should be taken into consideration:

- For the organization, to efficiently find open ports and potential vulnerabilities, scanning tools and methods must be available. To decide whether these tools and methods are appropriate for the particular network environment of the organization, their accessibility should be assessed.

- Significant amount of network traffics are produced by port scanning, which may have an effect on network performance. The organization needs to make sure that the infrastructure can handle the traffic that port scanning generates and that the scanning tools and methodologiescan be scaled to fit the network's size and complexities.

- The following pieces of hardware are necessary for our project to be technically feasible:

  - Since we are using a web application so we don’t need any processor or storage.
  - Internet connectivity
  - Database used: MySQL
  - Fronted technology used: HTML, CSS, JavaScript and Bootstrap
  - Middle framework used: JSP (Java Server Page)
  - Backend technology used: Java

2.1.2 Economic Feasibility:

Economic feasibility is the determination of whether a proposed project or system can provide an adequate return on investment to cover the associated expenditures.

Users of our system are not required to pay for any further overhead after the hardware and software criteria are met.

When determining if a port scanning project is economically feasible, the following variables should be taken into account:

- It is necessary to assess the cost of the hardware and software needed for port scanning. This includes the price of the servers, scanners, and any gear and software needed to perform port scans.

- The cost of hiring and training qualified staff to conduct scans is one of the people costs related to port scanning that must be assessed.

- It is necessary to assess the operational expenses of doing port scans, including those related to electricity, internet bandwidth, and other resources.

- It is vital to assess the cost of observing the rules and regulations pertaining to port scanning, such as paying for required licences.

- The potential advantages of performing port scans, such as finding vulnerabilities and enhancing network security, must be considered. This includes any potential financial savings brought on by avoiding security incidents and data breaches.

2.2 Module Description

There are four main modules in our project, which are:
2.2.1 Accounts
2.2.2 Listings
2.2.3 Predict
2.2.4Admin

2.2.1 Accounts:

- In our project, there are basically three parts i.e. Sign Up, Login and user dashboard in the account's section and there are four types of users in our web application – normal users, guest users, super users and the staff users.

- The guest users can access the register, search by applying filters and browsing features listings functionality but they cannot directly login or make and inquiry on a property listing until they become registered users.

- On the other hand, the normal users can access those features which are prohibited for the guest users.

- There are various authentication checks which have been applied to check the activity of the users like a user cannot login without registering, a user cannot create another account with same username and email-Id and before login and registering an inquiry on a particular property listing, it is first confirmed if the users really have the valid account or not.

2.2.2 Listings:

- In our project, the listing section comprises of the single listings page, featured listings page with pagination and the search page.

- The single listings page consists of the detailed description of the property.

- The featured listings page portrays all the property listings which have published attribute marked as true in the admin panel. Both the guest users and normal users can browse the featured listings and the single listings page.

- The search results are depicted on the search page and it provides the facility of the users to continue their search by applying various filters such as keywords in description, systems and so on.

2.2.3 Predict:

- The Predict module in our project often entails reviewing the information gathered throughout the scanning procedure in order to spot patterns and trends and generate forecasts on potential security issues or vulnerabilities in the future.

- This module can help to proactively identify potential security threats and can offer insightful information about the organization's security posture.

- predicts include examining the information gathered throughout the port scanning process, including as the categories of devices and systems examined, the quantity and seriousness of vulnerabilities found, and the frequency of scans.

- Additionally, the Predict module can be used to simulate various scenarios in order to assess the potential effects of various security threats on the organisation. For instance, the module can be used to simulate the effect of a particular vulnerability on the business operations and financial health of the organization.

2.2.4 Admin:

- In our project, the admin module is in charge of running the project and supervising its many elements. Project planning, team management, resource allocation, and collaboration with other organisational departments are among the activities included in this module.

- Creating an elaborate project plan for the admin module entails determining the project's scope, timeframe, budget, and resource needs.

- The team members' roles and responsibilities, as well as the reporting and communication procedures, should all be described in the project plan.

- The task of allocating the resources required to complete the port scanning project falls under the purview of the admin module. This involves setting aside money for hardware and software resources, as well as determining the scanning tools and technologies needed.

2.3 System Design:

The planning and specification of the system's architecture, components, interfaces, and data structures constitute the crucial step of system design in every project. It entails converting the requirements and specifications established in the project's early stages into a comprehensive design that can be utilised for development, implementation, and testing.

There are basically two types of system design approaches:

2.3.1Top-down designing approach
2.3.2Bottom-up designing approach

2.3.1 Top-down designing approach:

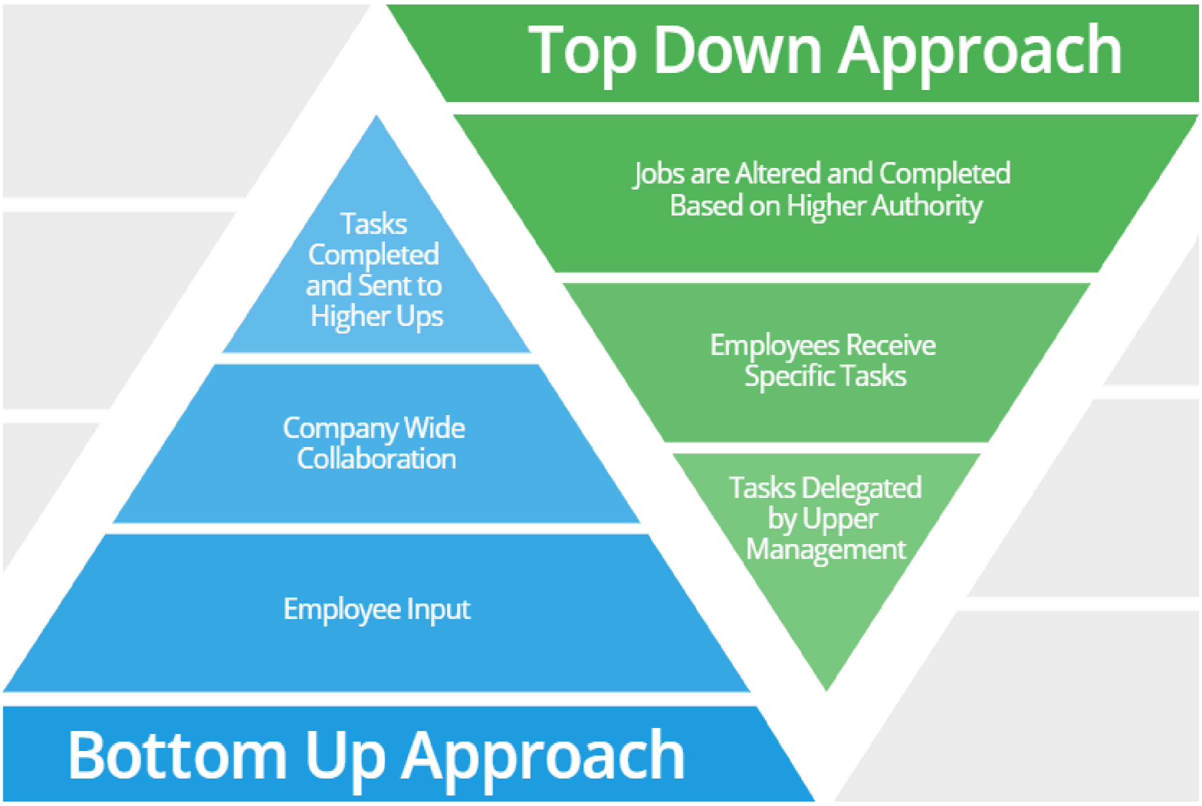
- Top-down design is a method of creating systems or software that begins with the overall system architecture and descends to the implementation's finer points. Top-down design divides the system into more manageable, smaller modules or components, and each module is created and developed independently.

- Because it enables a methodical and organised approach to development, top-down design is a common strategy in software and system design. It may be simpler to design, develop, and test each component independently if the system is divided into smaller, more manageable modules. As a result, the system as a whole may be more reliable and robust.

2.3.2 Bottom -up designing approach:

- Bottom-up design is a method of creating systems or software that begins with the creation of individual parts or modules and eventually combines them into a whole system. The bottom-up approach places more emphasis on creating the system from the ground up, beginning with the simplest and most fundamental components, as opposed to top-down design.

- When working with complex systems or utilising existing components, bottom-up design is frequently used. Prior to merging them into a broader system, it enables a concentrate on the specifics and implementation of individual components, assuring their usability and dependability. Bottom-up design has the advantage of early validation and progressive development of individual components, even though it could take longer to create a completely functional system than top-down design.


Top Down Approach
Jobs are Altered and Completed Based on Higher Authority
Employees Receive Specific Tasks
Tasks Delegated by Upper Management
Tasks Completed and Sent to Higher Ups
Company Wide Collaboration
Employee Input
Bottom Up Approach

Approach we are following:

➢ In our project, we are using the mixed approach i.e., the combination of Top-Down and Bottom-Up approach.

- For designing some of our components like our web pages, Top-Down approach had used and for backend portion we are following the bottom-Up approach.

2.4 Goals & Scope of our project:

In order to understand the goals, scope, and technical considerations involved with implementing a successful port scanning solution, system analysis on port scanning entails a thorough evaluation of the requirements, functionalities, and constraints of the port scanning system. The following aspects are typically taken into account:

2.4.1 Business Objectives:

Our project's commercial goals may change based on the organization and its unique security requirements. However, some typical commercial goals connected with port scanning include:

1. **Strengthening Network Security:**

   Finding potential weaknesses and security hazards in the network infrastructure of an organization is the main goal of our research. Organizations can prevent unauthorized access by running routine port scans to find open ports, improperly configured services, and potential entry points. By spotting and patching these holes in network security before bad actors can take advantage of them, the goal is to increase network security.

2. **Finding Vulnerabilities and Applying Fixes:**

   Our project aids businesses in locating particular security flaws in their network hardware and software. Through prompt patching, software updates, and configuration modifications, the goal is to prioritise and address these vulnerabilities. Organisations can lessen the possibility of successful cyberattacks and limit possible damage by discovering and correcting vulnerabilities.

3. **Guaranteeing Compliance:**

   Organizations must uphold a specific standard of security and compliance in order to comply with many different industries and regulatory frameworks. Our project can assist businesses in evaluating how well they adhere to security guidelines and rules. The goal is to locate any security flaws or illegal behaviour related to networks and take the necessary action to close them.

4. **Analysing Network Availability:**

   Through the identification of systems, devices, and services that may be unknown or unauthorised, our project offers insights into the network's visibility. Gaining a thorough understanding of the network architecture is the goal, along with making sure that all devices and services are authorised and accountable. This aids businesses in maintaining a strong and safe network environment.

5. **Risk management:**

   Risk management is aided by our initiatives by identifying and ranking potential security hazards. The goal is to evaluate the seriousness and potential impact of detected vulnerabilities, allowing organisations to invest resources wisely and prioritise the most serious threats. This aids businesses in risk mitigation, potential damage control, and security posture enhancement.

6. **Organising an incident response:**

   Identifying potential attack routes and access points for malicious activities is one way that our project may help incident response planning. The goal is to use the information gained from port scanning to create efficient incident response plans and processes. As a result, downtime and data breaches are reduced and organisations are able to respond to security problems quickly and effectively.

Together, these corporate goals seek to increase network security, safeguard sensitive data, guarantee legal compliance, and reduce the danger of cyberattacks. By locating vulnerabilities, enabling preventative security measures, and assisting risk management initiatives, port scanning is essential in attaining these goals.

Scope Definition:

In our project, scope definition refers to identifying the limits and breadth of port scanning operations within a network infrastructure of an organisation. It entails deciding which particular systems, gadgets, and network segments will be covered by the scanning procedure. Scope definition enables the port scanning operations to be targeted, focused, and in line with the organization's security goals.

Depending on the needs of the organisation, the complexity of the network, and the security objectives, the port scanning's scope may change. When defining the scope of port scanning, some factors to take into account are:

1.Network Infrastructure:

List the components of the network infrastructure that will be scanned, such as servers, firewalls, routers, switches, workstations, and other devices. Choose whether to monitor internal networks, external networks, or both.

2.Protocols:

Decide which ones will be inspected, such as TCP (Transmission Control Protocol) or UDP (User Datagram Protocol). Check to see if comprehensive coverage requires scanning both the TCP and UDP protocols.

3.Needs for compliance:

Take into account any particular laws or rules that may have an impact on the project's scope. There may be special requirements for network scanning operations set forth by certain standards or businesses.

4.IP Scope:

Establish the IP address range that will be covered by the port scanning operations. Choosing the beginning and ending IP addresses or designating particular subnets to be searched are examples of how to do this.

5.Exclusions:

Establish whether hardware, software, or IP addresses need to be excluded from the scanning procedure. Critical production servers, network devices that might be vulnerable to scanning, or devices that are maintained separately could all fall under this category.

6.Port Scope:

The specific ports or range of ports that will be inspected are chosen by our project. This could comprise well-known ports (like HTTP on port 80 and HTTPS on port 443) or specially created ports based on the applications and services offered by the organisation.

7.Time span:

Our project specifies the timing and frequency of port scanning operations. Establish the frequency of the scans, such as daily, weekly, or monthly, as well as the length of each scan.

Organisations may make sure that the scanning efforts are concentrated on the required network segments and devices by precisely setting the port scanning scope. This aids in accurately identifying vulnerabilities, evaluating risks, and putting in place the necessary security measures. Scope definition also assists in managing the resources needed for scanning and guarantees that scanning activities are in line with the organization's security objectives and legal requirements.

2.4.2 Functional Requirements:

In our project, functional requirements specify the particular features and functionalities that the port scanning system must have. These specifications, which are developed from the project's goals, serve as a roadmap for creating and implementing a successful port scanning solution. Typical functional specifications for a port scanning project include the following:

1. **Vulnerabilities Detections:**

The open ports and services found during scanning should allow the system to discover any possible vulnerabilities they may have. It ought to be able to compare scan results to a database of acknowledged vulnerabilities.

2. **Performance & Scalability:**

   The system ought to be built to manage extensive network environments and support expanding networks. It should be able to carry out scans quickly and effectively without having a substantial negative effect on network performance.

3. **Usability & User Interface:**

   The system ought to feature an intuitive user interface that makes it simple to configure, monitor, and understand scan results. It ought to have simple navigation, unambiguous status indications, and the option to personalise views and reports.

4. **Port Scanning Capabilities:**

   The system ought to be able to do thorough port scanning throughout the network infrastructure. It should be able to define the range of ports to be examined and support scanning for both the TCP and UDP protocols.

5. **Risk Assessment:**

   A risk assessment method for the system should be available to analyse the seriousness and potential consequences of found vulnerabilities. Each vulnerability should be given a risk score or rating based on variables like the likelihood that it will be exploited and the potential repercussions.

6. **Open Port Detection:**

   On network systems and devices, the system should be able to precisely detect and identify open ports. In order to help with vulnerability assessment, it should provide details about the services that are active on those ports and collect pertinent information, such as service banners.

7. **Reporting & Alerting:**

   The system must produce thorough reports summarising the scan findings, including open ports, discovered vulnerabilities, and their seriousness. Additionally, it must have ways to notify security teams or system administrators of serious flaws or ominous activity.

8. **Scan scheduling & Automation:**

   In order to maintain ongoing security monitoring, the system should support scheduling regular port scans at set intervals. It should be able to automate the scanning procedure, making unattended and timely scans possible.

9. **Authentication & Access Control:**

   To restrict access to its features, the system needs to offer authentication procedures. To provide accountability and traceability, it ought to support user management, role-based access control, and audit recording.

10. **Integration with existing security tools:**

    The system must be able to integrate with other security tools and platforms, such as ticketing systems, SIEM (Security Information and Event Management) solutions, or platforms for managing vulnerabilities. As a result, operations are streamlined, data communication is made easier, and effective security incident response is made possible.

These functional specifications serve as the cornerstone for creating and implementing a reliable and efficient our port scanning system. They make sure the system can carry out exhaustive scans, find vulnerabilities, produce reports that may be used, and support overall network security objectives.

2.4.3Technical Consideration:

To ensure the effectiveness and efficiency of the scanning process, numerous important criteria should be taken into account when evaluating the technical parts of our project. Here are some crucial technical factors to bear in mind when port scanning:

1.Performance & Speed:

Think about how port scanning will affect the network and target systems' performance. Improve scanning algorithms and put in place controls to lessen network traffic and prevent overtaxing the target systems. To achieve accurate and quick findings, it's crucial to strike a balance between scan speed and network effect.

2.Stealth and evasion methods:

Utilise evasive and stealth tactics to reduce the visibility of port scanning operations. This includes methods like using counterfeit IP addresses, changing packet length, and randomising scan timing. These methods can assist in preventing the activation of security safeguards and intrusion detection systems.

3.Scanning Techniques:

Analyse the various port scanning methodologies and scanning strategies, such as idle scanning, SYN scanning, idle scanning, TCP connect scanning, and SYN scanning. Depending on network infrastructures and scan objectives, be aware of the benefits, drawbacks, and acceptable use cases for each technique.

4.Firewall & IDS Considerations:

Recognise the potential effects of firewalls and intrusion detection systems (IDS) on port scanning operations. Adapt scanning methods and timing to avoid or reduce security system detection. To prevent pointless alarms or blocking, take into account these systems' setups and policies.

5.Compliance & Legal Considerations:

In our project, while doing port scanning tasks, make sure you adhere to legal and regulatory standards. Recognise any limitations, permits, or notices that could be required to carry out scans legally and morally. Follow industry standards and recommendations to safeguard data integrity and privacy.

6.Resource Consumption:

When running port scans, take into account the resources needed, including CPU and memory usage as well as network bandwidth. Reduce resource usage and make sure scanning doesn't interfere with the network or target systems' normal operation by streamlining the scanning procedure.

7.Scanning Accuracy:

By using dependable scanning methods and doing a careful examination of scan findings, you can ensure the correctness of port scanning results. Reduce false positives and false negatives by correctly interpreting scan results and validating against services and vulnerabilities that are well-known.

Organisations can create and implement a robust and efficient port scanning system that supports their security goals, improves speed, and provides accurate and useful results by taking into account certain technological considerations.

2.4.3 Cost-Benefit Analysis:

An essential evaluation technique for determining the prospective costs and advantages of our project is cost-benefit analysis. By weighing the anticipated benefits against the estimated expenses, it assists organisations in deciding if the investment in our project is warranted. An overview of how cost-benefit analysis might be used in our project is given below:

1. **Identifying Costs:**

- **Licences and maintenance:**

  Take into account the price of the software licence for port scanning as well as Continuous maintenance charges.

- **Hardware and software:**

  Calculate the cost of purchasing or upgrading the gear and software required For the port scanning system.

- **Infrastructure:**

  Analyse the expenses associated with any network infrastructure improvements or upgrades needed to support port scanning activities .

- **Personnel:**

  Determine the personnel costs, such as salary, training costs, and recruitment costs, associated with setting up, running, and administering the port scanning system.

2.Determine Benefits:

- **Compliance:**

  Analyse the advantages of port scanning in establishing and maintaining compliance with industry standards and legal obligations. Benefits could include avoiding non-compliance fines and reputational harm.

- **Cost Avoidance:**

  Think about the expenses that can be prevented by anticipatorily detecting and resolving vulnerabilities before they are used against you. This covers potential expenses for system outages, data loss, potential legal problems, and loss of clientele.

- **Incident Response Efficiency:**

  By identifying potential attack vectors and entry points through port scanning, you can quantify the advantages of increased incident response capabilities. Lower recovery costs, less downtime, and less damage can all be achieved through quicker event identification and response.

- **Enhanced Security:**

  By locating and fixing open ports and incorrect configurations through routine port scanning, evaluate the possible decrease in security risks and vulnerabilities. Take into account the possible financial savings from avoiding security incidents or data breaches.

3.Quantity costs and benefits:

- To assess the costs and benefits, use prior data, industry benchmarks, professional judgement, and organisational insights. To assist the analysis, it's critical to compile trustworthy facts.

- Where possible, give monetary amounts to the stated costs and benefits. Even while estimating or approximating some qualitative advantages' financial impact with the greatest degree of accuracy can be difficult, it is crucial.

4.Consider Intangible benefits:

Even though it could be challenging to put some benefits into monetary terms, it's nevertheless necessary to take them into account. This includes intangible advantages like better organisational resilience, consumer trust, and brand reputation.

5.Compare costs & benefits:

- By contrasting the net benefits with the overall costs, you can determine the return on investment (ROI). This gives an idea of the investment's effectiveness and aids in determining whether the project is financially sustainable.

- By contrasting the net advantages and the total expenses, determine the return on investment (ROI). This offers information on the effectiveness of the investment and aids in determining if the project is financially sustainable.

Organisations can make educated judgements about the deployment of our project by completing a thorough cost-benefit analysis. It gives organisations information about potential financial gains, security enhancements, and compliance advantages, enabling them to spend resources wisely and give network security investments top priority.

Testing and Implementation

Chapter 3

3.1Testing:

For the functionality, precision, and dependability of the scanning system to be confirmed in every project, testing is essential. When doing testing for any project, it's important to take into account a number of important factors, including functional testing, testing of scanning techniques, testing of scan coverage, testing of integration, testing of performance, testing of documentation, and so forth. In our project we are using following testing modules:

3.1.1 Unit Testing

3.1.2 Integration Testing

3.1.1 Unit Testing:

A software testing technique called unit testing is used to check the functionality of individual software system units or components. It focuses on testing discrete, small-scale portions of the code, usually at the level of specific functions, methods, or classes. Unit testing is used to make sure each unit operates as intended and complies with all requirements.

Unit testing is a crucial testing strategy utilised in our project to assess the scanning system's distinct parts or units. It focuses on confirming the efficiency, accuracy, and dependability of each unit separately.

It Divides the port scanning system into smaller components or modules so that each one may be tested on its own. The scanning engine, network communication module, result analysis module, and reporting module are a few examples of components of our port scanning system.

To replicate the behaviour of external dependencies or services that the unit being tested interacts with, use mocking and stubbing techniques. As a result, the unit being tested is more effectively isolated and its functioning is independently tested.

The key characteristics of Unit Testing:

- Automated Execution
- Isolation
- Fast Execution
- Code Coverage
- Test Assertions
- Independence
- Small Scop

Benefits of unit testing:

Code maintenance and refactoring are made simpler and less risky by unit tests, which give confidence in the accuracy and stability of individual units.

Early detection of flaws and problems via unit tests makes their correction simpler and less expensive.

Unit tests act as living documentation, giving developers examples of how to use the units and explaining the expected behaviour of the code.

Regressions are avoided via unit tests, which serve as a safety net. Existing unit tests can rapidly determine whether any functionality has been unintentionally broken whenever changes are made to the code.

Code quality is raised as a result of unit testing, which pushes developers to produce modular, testable, and well-organized code.

3.1.2 Integration Testing:

The goal of the software testing technique known as "integration testing" is to evaluate how well various software system modules, components, and subsystems work together. The goal of integration testing is to find problems that might occur when various components are put together as well as to make sure the integrated system works as intended.

In our project, integration testing is used to evaluate how well the various parts and modules that make up the scanning system work together.

To ensure that data is delivered correctly, parameters are processed correctly, and communication between components is seamless, test the interfaces between the components. Check to see if the parts can reliably and accurately communicate information.

Check the data's consistency and integrity as it moves across the various components. Ascertain that data transformations, filtering, and analysis are carried out precisely, consistently, and that the outcomes accurately reflect the state of the scanned ports and services.

The key characteristics of integration testing:

- Testing Interfaces
- Component Interaction
- Performance and Scalability
- Stubbing and Mocking
- Dependency Management
- External System Integration
- Error Handling and Exception Testing

Benefits of integration testing:

Collaboration between development teams is necessary for integration testing, ensuring efficient coordination and communication among various stakeholders.

Integration testing enhances the system's overall dependability, stability, and performance by testing the integration between components.

The danger of problems or errors when deploying the software system in a production environment is decreased by thorough integration testing.

Early in the development process, integration testing assists in discovering issues like incompatible interfaces, poor communication, or inconsistent data.

Integration testing makes sure that the integrated system functions as intended as a whole and that all of its parts communicate with one another without any problems.

3.2 Implementation:

In our project, implementation refers to the process of converting the scanning system's design and specifications into an operational and executable software solution. It entails writing the relevant code, setting up the infrastructure, and configuring the system components needed to implement the port scanning capabilities.The following are the main steps in a port scanning project's implementation phase:

- ➢ **Configuration:**

  Set up the system's settings and components as necessary. Determining parameters for the port scanning system, such as the range of ports to scan, scanning methods to use, timeout values, logging choices, and any other modifiable features, may fall under this category.

- ➢ **Training and Handover:**

Transfer the port scanning system to the intended users or administrators and provide the necessary training. Make sure they are knowledgeable on the functionality, configuration possibilities, and upkeep processes of the system.

- **Development Environment Setup:**

  Create the development environment and add the tools, frameworks, and programming languages required to create the port scanning system. Installing compilers, libraries, IDEs (Integrated Development Environments), and other development dependencies may be required.

- **Network Setup:**

  Make that the network infrastructure is configured correctly to facilitate the port scanning operations. This could entail setting up switches, routers, and firewalls to permit network traffic required for port scanning. Verify that the scanning procedures adhere to any applicable network policies or rules.

- **Coding:**

  Based on the system design and specifications, write the code for each of the port scanning system's many components. The scanning engine, network communication module, result analysis module, reporting module, as well as any other pertinent functionality discovered during the system design process, must all be implemented. To guarantee code quality, readability, and maintainability, adhere to coding standards and best practises.

- **Testing:**

  Test the implemented port scanning mechanism thoroughly. To verify the functionality, performance, and stability of the system, this also comprises unit testing, integration testing, and system testing. Different scanning circumstances should be tested, mistake situations should be handled, and the system's outputs should be precise.

- **Deployment:**

  Set up the port scanning system in the target environment before deployment. This could entail setting up production servers or machines, packaging the system into deployable parts, and adhering to the project's deployment process.

- **Bug fixes and refinement:**

  Fix any problems or faults found during testing, then adjust the implementation in light of user feedback and test results. Make sure the system complies with the desired standards and requirements.

- **Integration of external libraries or APIs:**

  Integrate external libraries, frameworks, or APIs into the implementation if the port scanning system depends on them. This could entail integrating network protocols, security frameworks, or port scanning libraries from outside the system.

Requirement Analysis

Chapter 4

4.1Requirement Analysis:

Understanding and describing the particular requirements, expectations, and restrictions of the stakeholders in relation to our port scanning system are key components of requirement analysis in a port scanning project. It is an essential stage in the software development lifecycle that ensures the finished system will achieve the required goals. In our project, we are using waterfall model on the basis of our project requirements.

4.2Waterfall Model:

The Waterfall model is a well-known, linear, and systematic approach to software development. It is divided into a number of discrete phases, each of which must be finished before going on to the further step.

We may give an overview of how the Waterfall approach would be employed in our port scanning project even if it is less frequently used in contemporary software development.

There are several following phases that we are using in our project:

- Requirement Gathering
- System Design
- Implementation
- Testing
- Deployment
- Maintenance

4.2.1 Requirement Gathering:

All of the requirements needed for our port scanning system are acquired from the stakeholders in the first step. The scanning goals, target network specifications, scanning methods, reporting needs, and any other functional or non-functional requirements must all be identified.

4.2.2 System Design:

The system design phase starts as soon as the requirements are complete. For our port scanning system, the design team develops a thorough design that includes the architecture, component interactions, data flow, and any necessary algorithms or protocols to be employed.

4.2.3 Implementation:

Our project is put into place during this phase in accordance with the design requirements. The necessary functionalities and modules are created, and the coding and programming tasks are completed. Making the scanning engine, network communication module, result analysis module, reporting module, and any other necessary components are all included in this.

4.2.4 Testing:

The system is tested after the implementation is finished to make sure it works properly. This involves testing at several levels, such as system testing, unit testing, and integration testing. The testing stage seeks to find and address any flaws or problems with the port scanning system.

4.2.5 Deployment:

Our project scanning project is put into use in the production environment following a successful test run. On the target servers or computers, the system must be installed and configured. To accommodate the scanning activities, any necessary network and infrastructure changes are done.

4.2.6 Maintenance:

After the system is installed, continual maintenance and support are given to guarantee its proper operation. This can entail responding to user feedback, resolving any glitches or problems, and adding updates or improvements as required.

One of the drawbacks of the waterfall model is that once the project has moved past the requirements gathering phase, it is difficult to accommodate modifications or revisions in the requirements. As is frequently the case with software development projects, this makes it less suitable for projects where needs may change or necessitate frequent revisions.

Advantages of Waterfall Model:

The Waterfall model is straightforward and simple to comprehend. It is simple to follow and put into practise due to its sequential structure and linear flow.

The project is divided into several phases by the model, and each phase has its own deliverables and milestones. This offers a defined framework and enables better planning and progress monitoring.

The Waterfall model places a strong emphasis on gathering and outlining needs in advance. This reduces ambiguity and establishes a clear knowledge of the project's scope.

The Waterfall model uses a sequential process in order to avoid ambiguity and the chance of miscommunication between stakeholders and the development team.

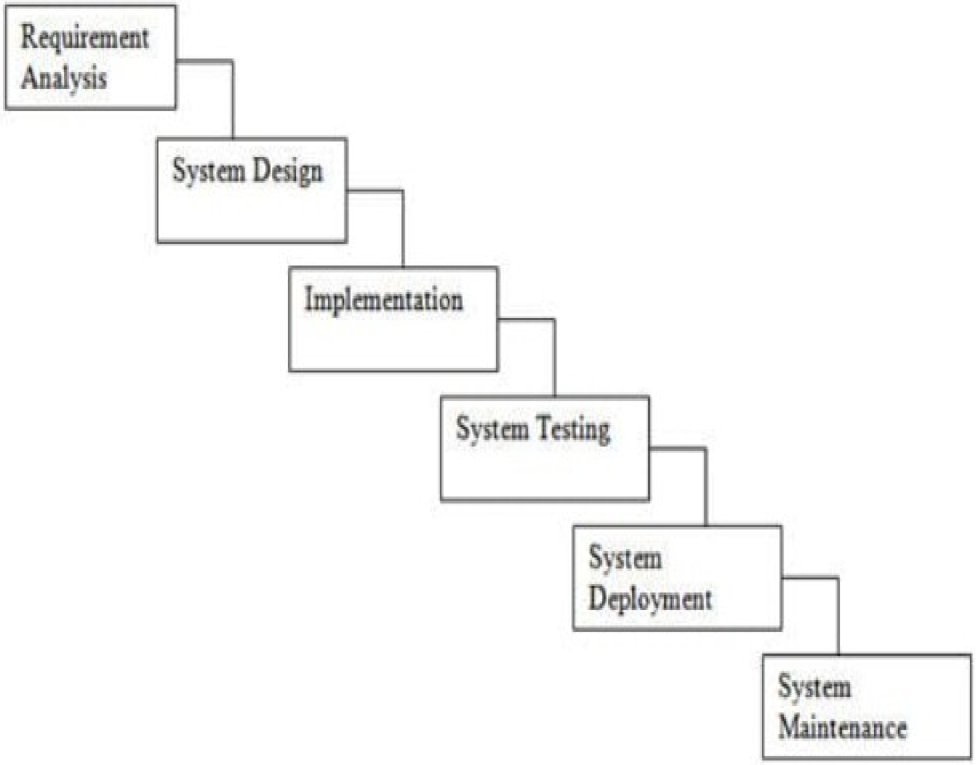
Disadvantages of Waterfall Model:

Until the later stages of the project, the Waterfall model often involves little input from clients or end users. This may result in a gap between the system that has been designed and the needs of the actual users, which may cause unhappiness or require additional effort.

Iterations that happen frequently or feedback loops are not prioritised in the waterfall model. This means that the development team and stakeholders have few opportunities to offer input, which results in missed chances for improvement and course correction.

The sequential and linear nature of the Waterfall model limits its ability to adapt to changes. It becomes challenging and expensive to return and make adjustments to earlier phases once a phase is finished and the project goes on to the following phase.

The sequential structure of the waterfall methodology may lead to lengthier development cycles. The need that each phase be finished before going on to the next might cause project schedules to be stretched, particularly if changes or problems are discovered after the fact.


Requirement Analysis
System Design
Implementation
System Testing
System Deployment
System Maintenance

DATA FLOW DIAGRAM

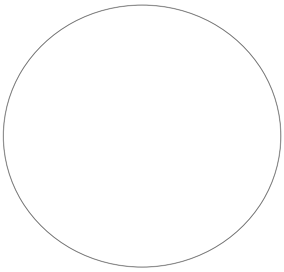
Chapter 5

5.1 Terms Used In DFD

A data flow diagram, often known as a DFD, is a graphical representation of a system or process that demonstrates the data flow between various components. In DFDs, a number of terms are frequently used. Here are some crucial words:

5.1.1 Process:

A process in a system refers to a certain activity or function. It could involve a computation, a data transformation, or data manipulation. In a DFD, processes are frequently depicted by circles or rectangles.

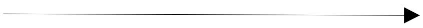


Graphical Representation

5.1.2 Data Flow:

Data flow depict the transfer of information between entities, processes, and data repositories. They show how information moves through the system. In a DFD, data

Graphical Representation



5.1.3 Entity:

An entity is a representation of an external, system-interacting entity. It could be a person, group, or system not covered by the DFD. In a DFD, rectangles are frequently used to represent entities.

5.1.4 Data Store:

A data store is a system-wide repository where data is kept. It could be a file, database, or some other kind of storage device. In a DFD, data stores are often shown as two parallel lines.

5.1.5 External Entity:

An entity that is external to the system but engages with it is referred to as an external entity. It serves as a data source or destination. Typically, external entities are shown as rectangles with lines connecting them to data.

Graphical Representation

ne

5.1.7 Control Flow:

The control or sequencing of system processes is represented by control flow. It displays how decisions are made or how processes are carried out. Labels or annotations are frequently used to illustrate control flow on data flow arrows.

5.1.8 Context Diagram:

A high-level DFD that gives an overview of the system and how it interacts with external entities is known as a context diagram. It depicts the system as a single process with external objects serving as either data sources or destinations.

5.1.9 Decomposition:

A complex DFD is divided into smaller, easier-to-manage components through the process of decomposition. For each process, lower-level DFDs must be created until a complete picture of the system is obtained.

5.1.10 Balancing:

Maintaining data consistency in a DFD is referred to as balancing. It makes sure that no data is lost or created throughout the transformation process and that the input and output data flows of a process are balanced.

These are a few of the words that appear frequently in data flow diagrams. Understanding these concepts makes it easier to analyze and record how data flows through a system or process.

5.2 Level-0 DFD

A Level 0 Data Flow Diagram (DFD) shows the key elements and interactions inside a system or process and offers a high-level overview of it. It displays how data moves between external entities, processes, and data stores and represents the system as a single process. Since it presents the context or overall view of the system, the Level 0 DFD is sometimes referred to as the context diagram.

A description of the typical elements of a Level 0 DFD is given below:

1.Processes:
The system is represented by a single process or function in the Level 0 DFD. It focuses on general functioning rather than going into specifics about how the system functions internally.

2. External Entities:
Despite being external to the system, external entities can nonetheless interact with it. They could be users, other systems, or outside companies. External entities are shown as rectangles in the Level 0 DFD, connected to the system by data flows.

3. Data Flows:
Data flows show how information is transferred among various system components. They demonstrate the entry, processing, and output of data. Typically, arrows are used to symbolize data flows, and they are labelled to show what kind of data is being conveyed.

4. Data Stores:
Data stores are the system's internal repositories for storing data. They could be files, databases, or any other kind of storage device. Data stores can be stated or labelled in the Level 0 DFD to illustrate where data is kept or retrieved, but they are typically not described in detail.

The Level 0 DFD offers a general overview of the system's boundaries, its relationships with external entities, and its main data flows. It serves as a foundation for comprehending the extent of the system and can be further broken down into lower-level DFDs to provide more specific details about each procedure or element.

Keep in mind that the Level 0 DFD's complexity and level of detail can change based on the system being implemented.

5.3 Level-1 DFD

To give a more thorough understanding of the system's operation, the processes are further divided into sub-processes in a Level 1 Data Flow Diagram (DFD). The sub-processes and their unique data flows are illustrated in the Level 1 DFD, which builds upon the Level 0 DFD.

Each process from the Level 0 DFD is transformed into a parent process in a Level 1 DFD, which is then divided into more manageable sub-processes. Within the parent process, these sub-processes reflect finer-grained operations or phases. The Level 1 DFD gives a deeper grasp of the processes involved by concentrating on the internal operations of the system.

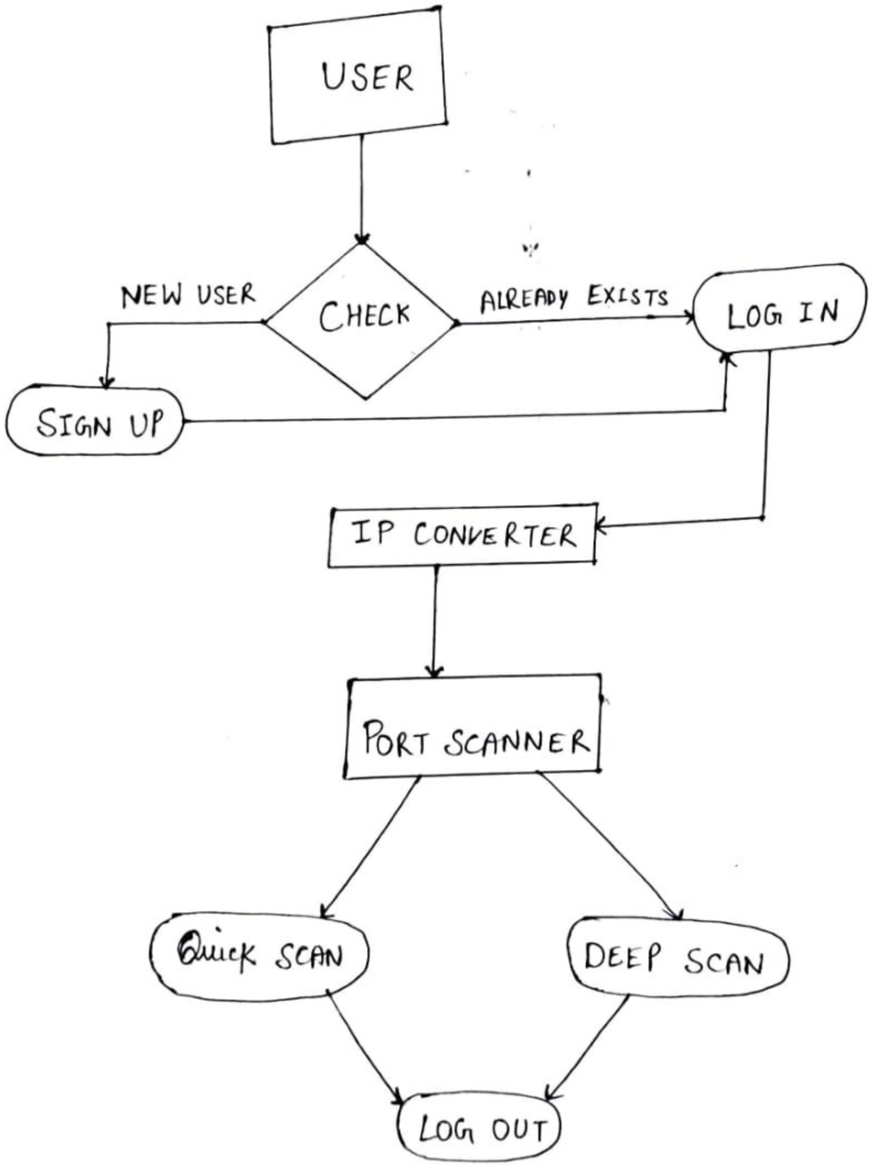
Arrows are used to represent data flows as they link the operations. The data flow between the sub-processes is shown by these arrows. Each data flow corresponds to a particular piece of information that is transferred between subprocesses.

You can learn more about the inner workings of the system, spot dependencies between sub-processes, and comprehend how data is changed and processed within the system by using a Level 1 DFD.

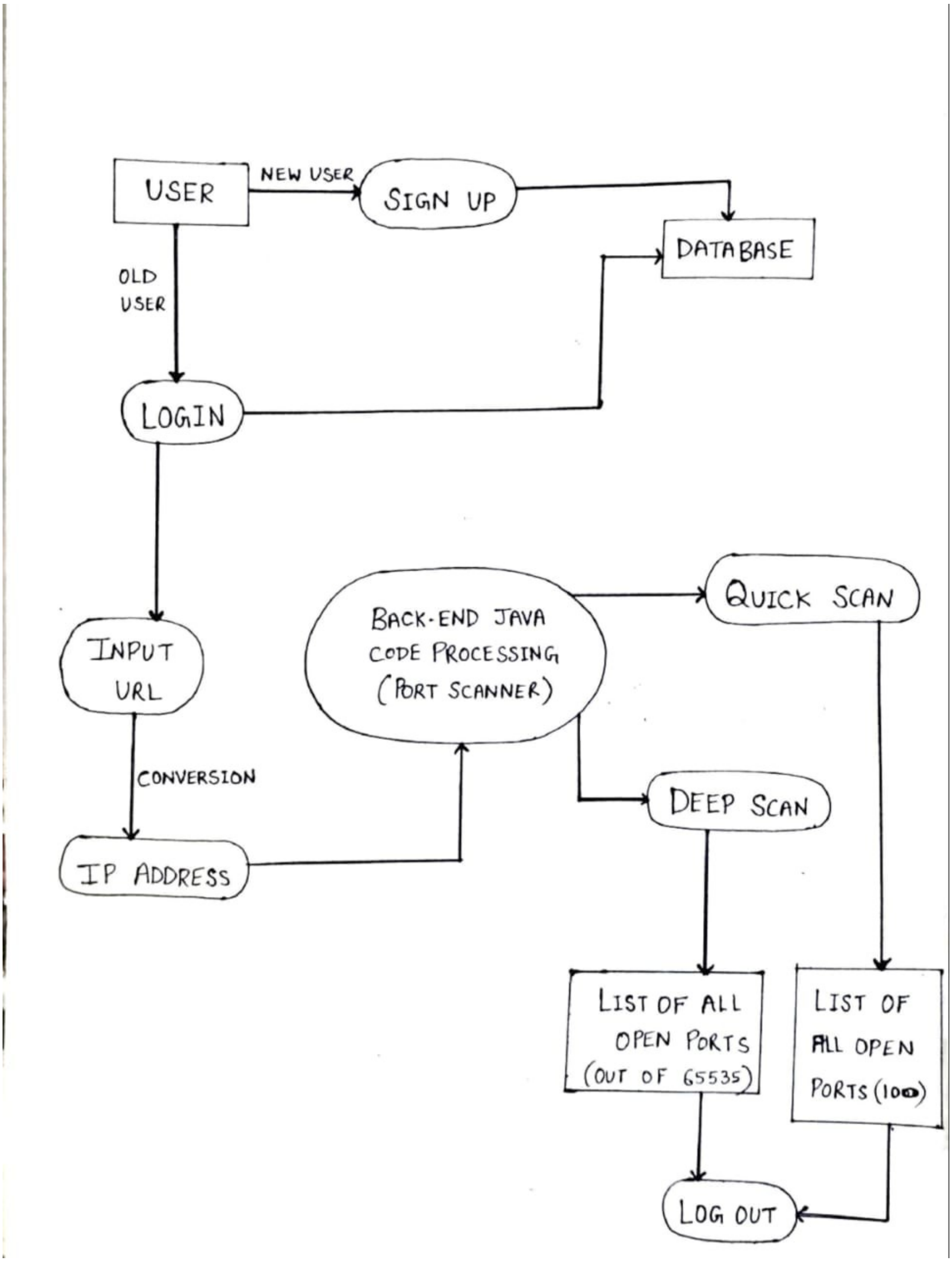
It's important to remember that the Level 1 DFD is only one level of decomposition and that more levels of decomposition (Level 2, Level 3, and so on) may be built depending on how complex the system is to provide even more in-depth insights into the system's processes.

In comparison to higher-level diagrams like the Level 0 DFD, a Level 1 DFD provides a more thorough insight of the system's core processes and data flows.

ER- Diagram


USER
NEW USER
CHECK
ALREADY EXISTS
LOG IN
SIGN UP
IP CONVERTER
PORT SCANNER
Quick SCAN
DEEP SCAN
LOG OUT

Level 1- DFD

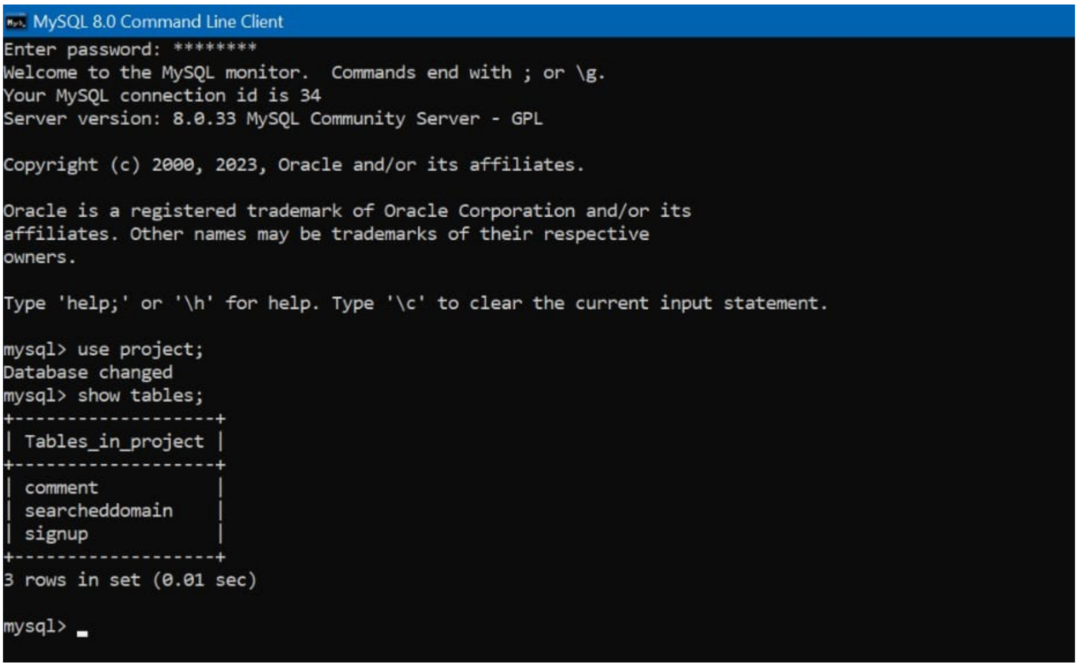

USER
NEW USER
SIGN UP
DATABASE
OLD USER
LOGIN
INPUT URL
CONVERSION
IP ADDRESS
BACK-END JAVA CODE PROCESSING (PORT SCANNER)
QUICK SCAN
DEEP SCAN
LIST OF ALL OPEN PORTS (OUT OF 65535)
LIST OF ALL OPEN PORTS (1000)
LOG OUT

DATABASE TABLES

Chapter 6

a. Database Tables:

In our project, following snapshots are showing the database tables that are used to store and manage relevant information in our project:



```
Enter password: ********
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 34
Server version: 8.0.33 MySQL Community Server - GPL

Copyright (c) 2000, 2023, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> use project;
Database changed
mysql> show tables;
+-------------------+
| Tables_in_project |
+-------------------+
| comment           |
| searcheddomain    |
| signup            |
+-------------------+
3 rows in set (0.01 sec)

mysql>
```

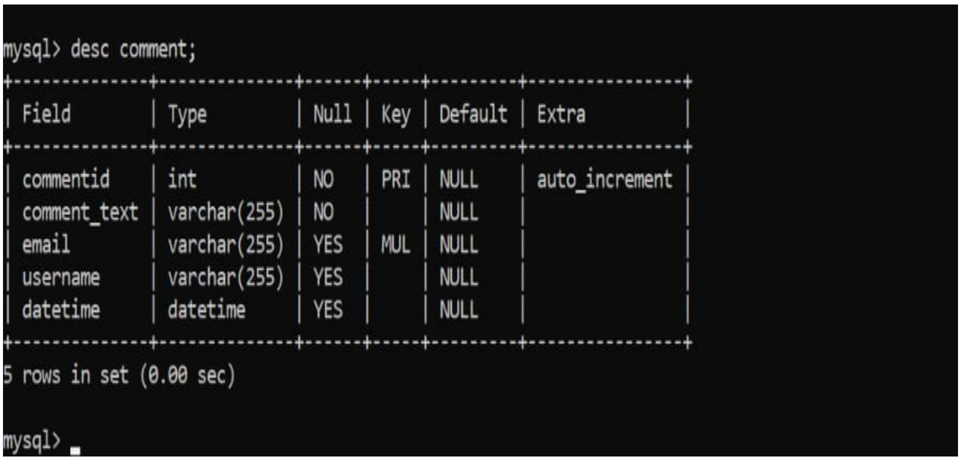
As showing in the picture, there are basically three tables that are used:

6.1.1Comment Table

6.1.2Searcheddomain Table

6.1.3Signup Table

6.1.1 Comment Table:

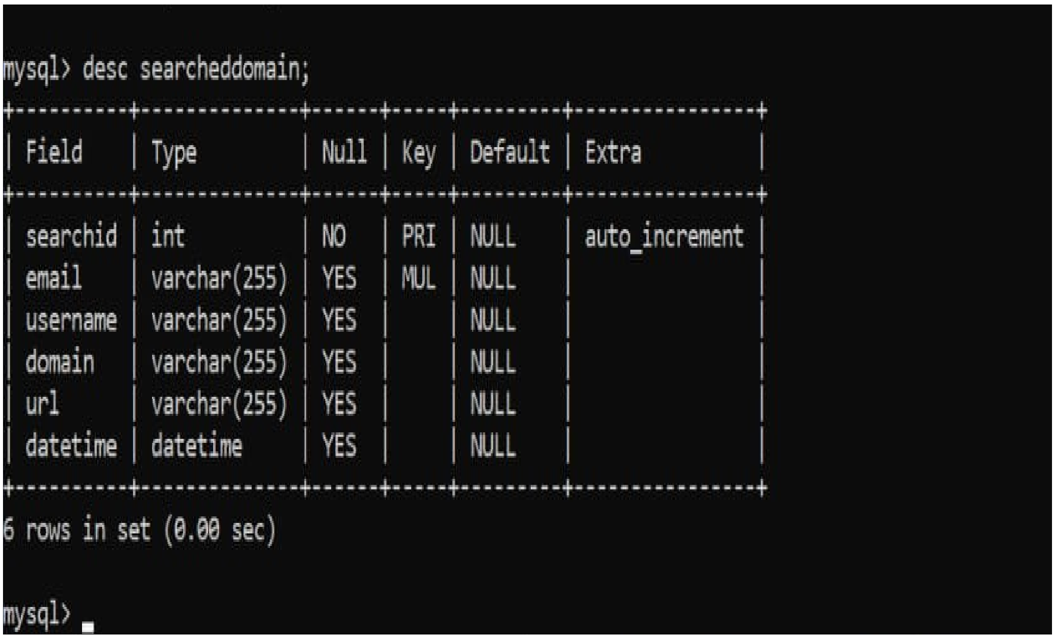


```
mysql> desc comment;
+--------------+--------------+------+-----+---------+----------------+
| Field        | Type         | Null | Key | Default | Extra          |
+--------------+--------------+------+-----+---------+----------------+
| commentid    | int          | NO   | PRI | NULL    | auto_increment |
| comment_text | varchar(255) | NO   |     | NULL    |                |
| email        | varchar(255) | YES  | MUL | NULL    |                |
| username     | varchar(255) | YES  |     | NULL    |                |
| datetime     | datetime     | YES  |     | NULL    |                |
+--------------+--------------+------+-----+---------+----------------+
5 rows in set (0.00 sec)

mysql>
```

Comment table allows users to add comment in our web application and the comment will be displayed in the comment section with username and time that when comment was added.

6.1.2 Searcheddomain Table:

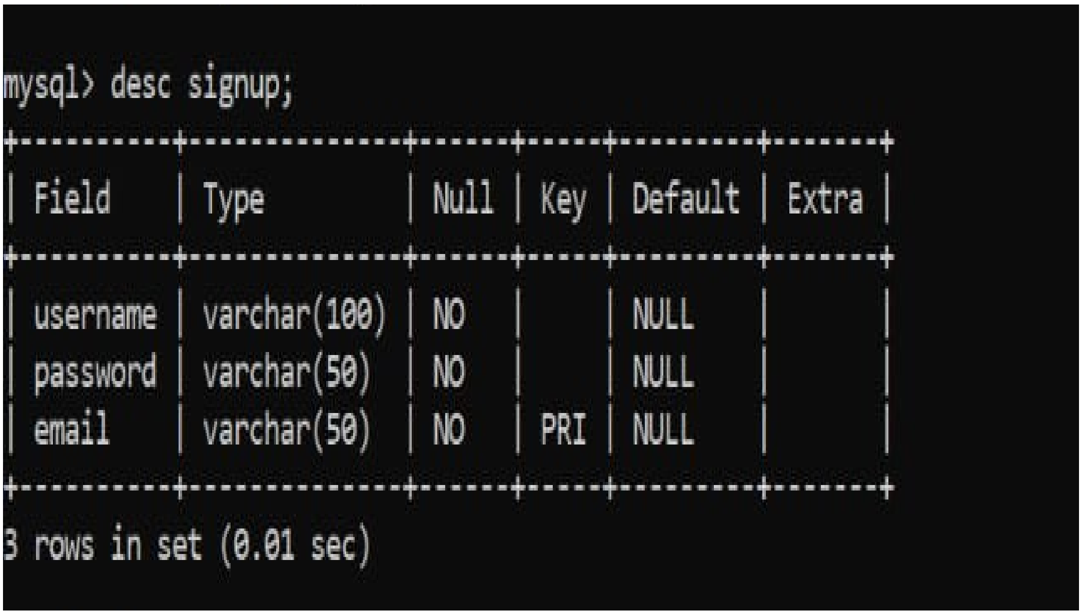


```
mysql> desc searcheddomain;
+----------+-------------+------+-----+---------+----------------+
| Field    | Type        | Null | Key | Default | Extra          |
+----------+-------------+------+-----+---------+----------------+
| searchid | int         | NO   | PRI | NULL    | auto_increment |
| email    | varchar(255)| YES  | MUL | NULL    |                |
| username | varchar(255)| YES  |     | NULL    |                |
| domain   | varchar(255)| YES  |     | NULL    |                |
| url      | varchar(255)| YES  |     | NULL    |                |
| datetime | datetime    | YES  |     | NULL    |                |
+----------+-------------+------+-----+---------+----------------+
6 rows in set (0.00 sec)

mysql> _
```

Searcheddomain Table used to keep information and history about the domain that are searched by the user during the scanning process.

6.1.3 Signup Table:



```
mysql> desc signup;
+----------+--------------+------+-----+---------+-------+
| Field    | Type         | Null | Key | Default | Extra |
+----------+--------------+------+-----+---------+-------+
| username | varchar(100) | NO   |     | NULL    |       |
| password | varchar(50)  | NO   |     | NULL    |       |
| email    | varchar(50)  | NO   | PRI | NULL    |       |
+----------+--------------+------+-----+---------+-------+
3 rows in set (0.01 sec)
```

Signup table used to contain all the data of the users who sign up and register their selves for accessing our services in the port scanning application. For sign up the user need to provide their username password and email.

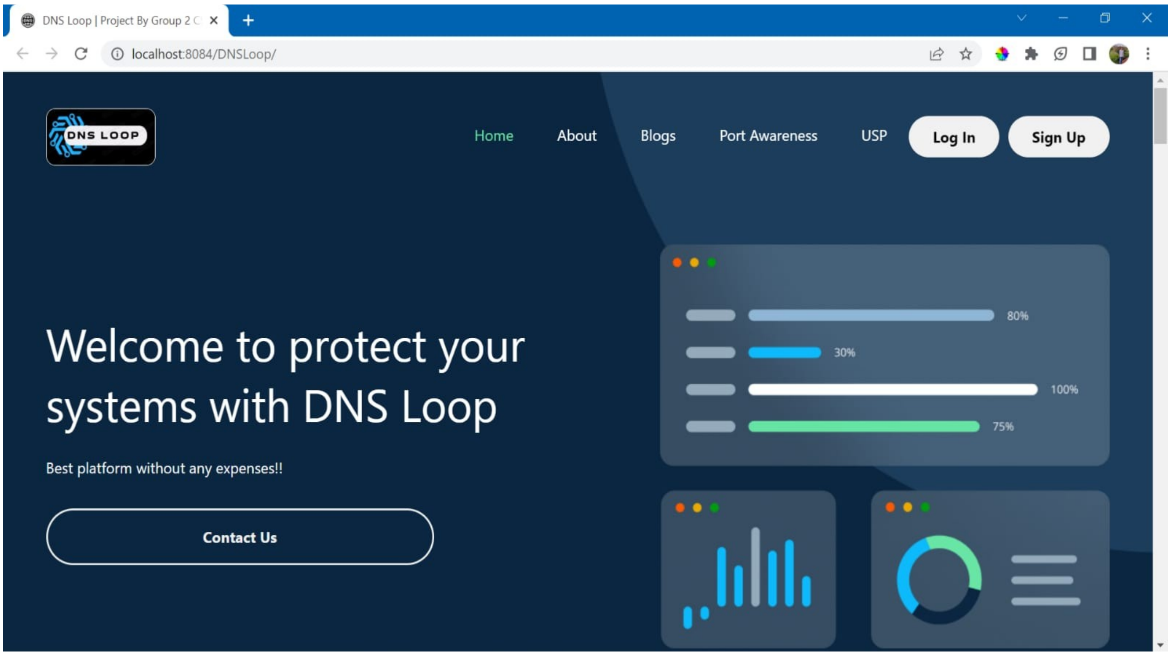
SNAPSHOTS

Chapter 7

7.1Homepage:

There are three sections in our homepage:

Top View of homepage:

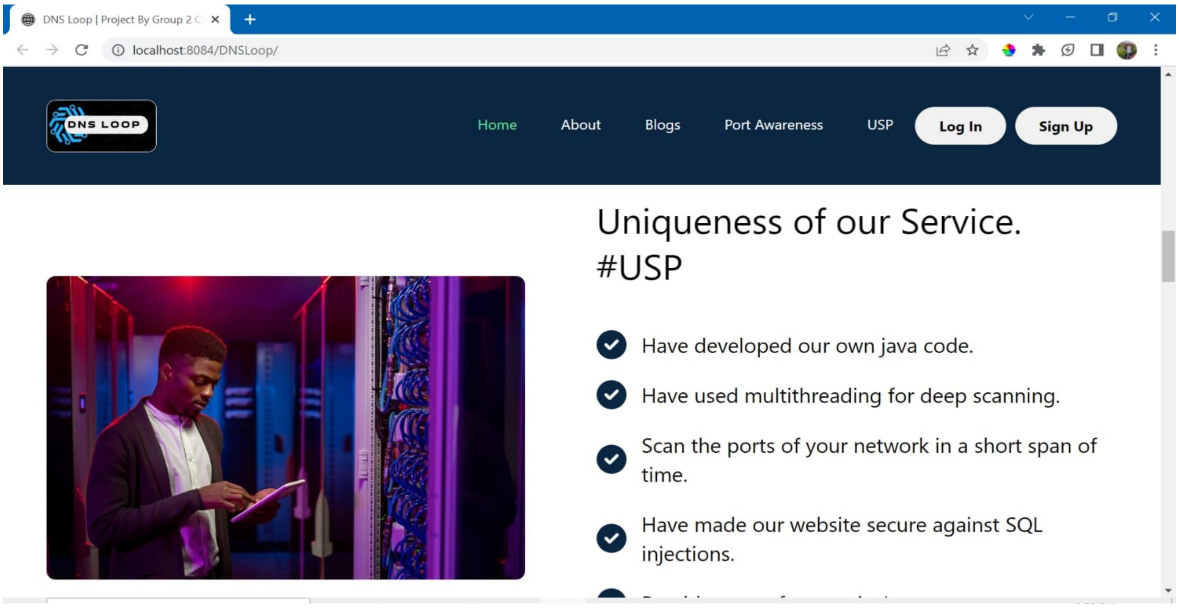


DNS Loop | Project By Group 2 C
localhost:8084/DNSLoop/
DNS LOOP
Home
About
Blogs
Port Awareness
USP
Log In
Sign Up
Welcome to protect your systems with DNS Loop
Best platform without any expenses!!
Contact Us
80%
30%
100%
75%

Middle View of homepage:

There are two sections in middle view of homepage:

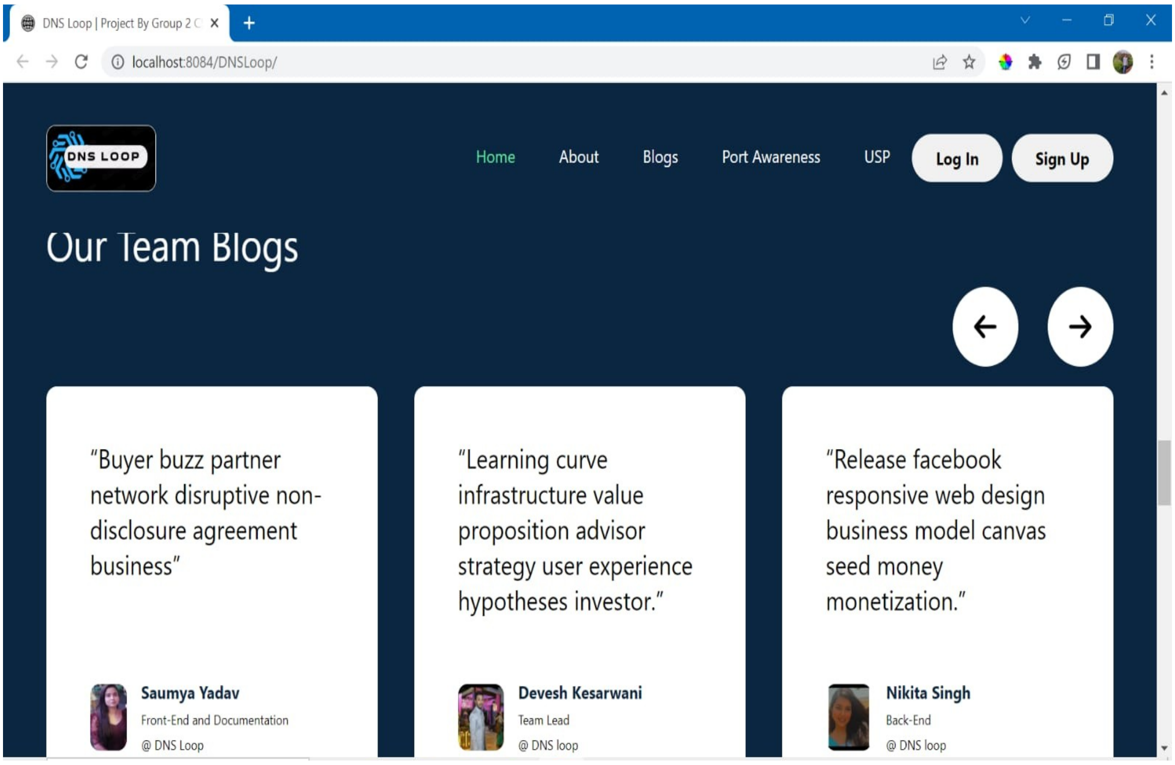
Section 1:



Uniqueness of our Service. #USP

- ✓ Have developed our own java code.
- ✓ Have used multithreading for deep scanning.
- ✓ Scan the ports of your network in a short span of time.
- ✓ Have made our website secure against SQL injections.

Section 2:



Our Team Blogs

"Buyer buzz partner network disruptive non-disclosure agreement business"

Saumya Yadav
Front-End and Documentation
@ DNS Loop

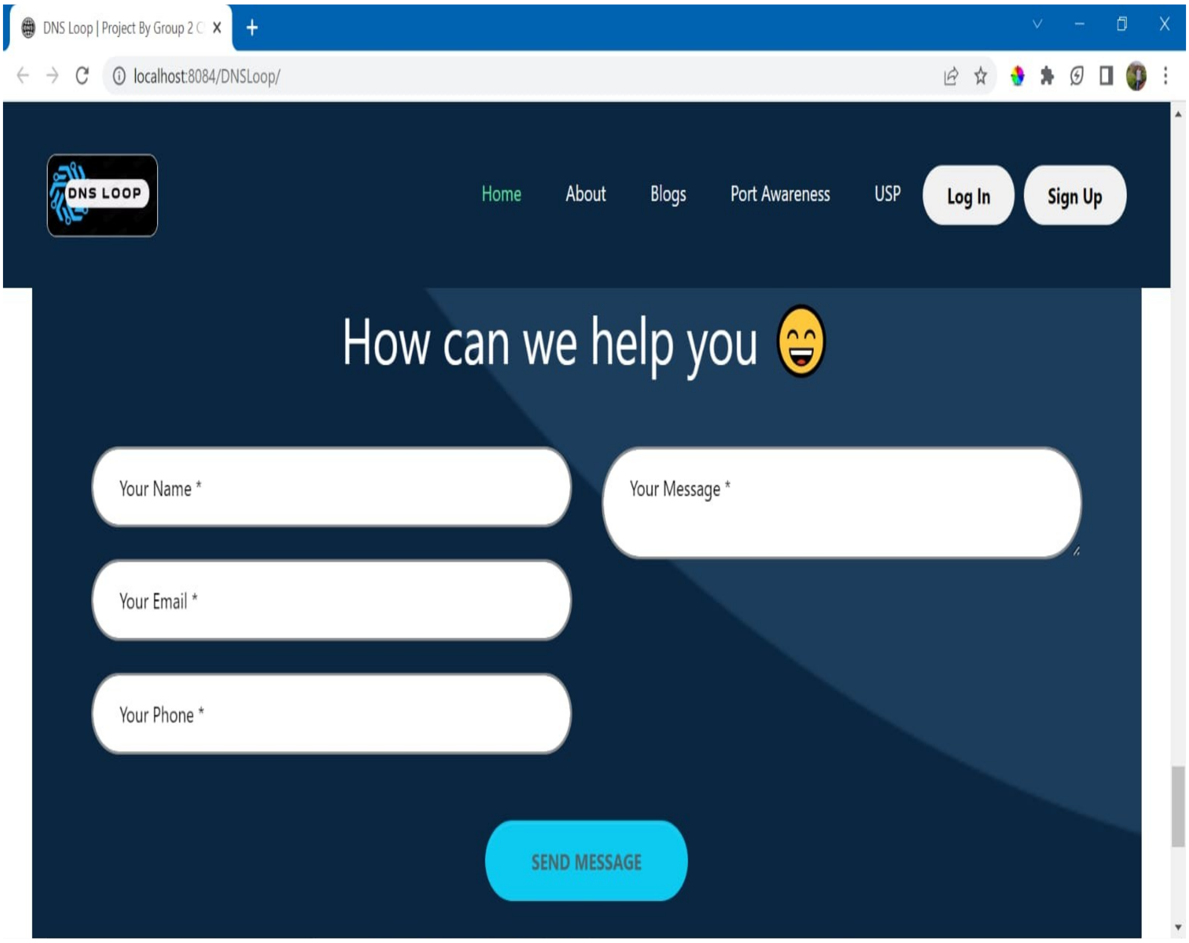
"Learning curve infrastructure value proposition advisor strategy user experience hypotheses investor."

Devesh Kesarwani
Team Lead
@ DNS loop

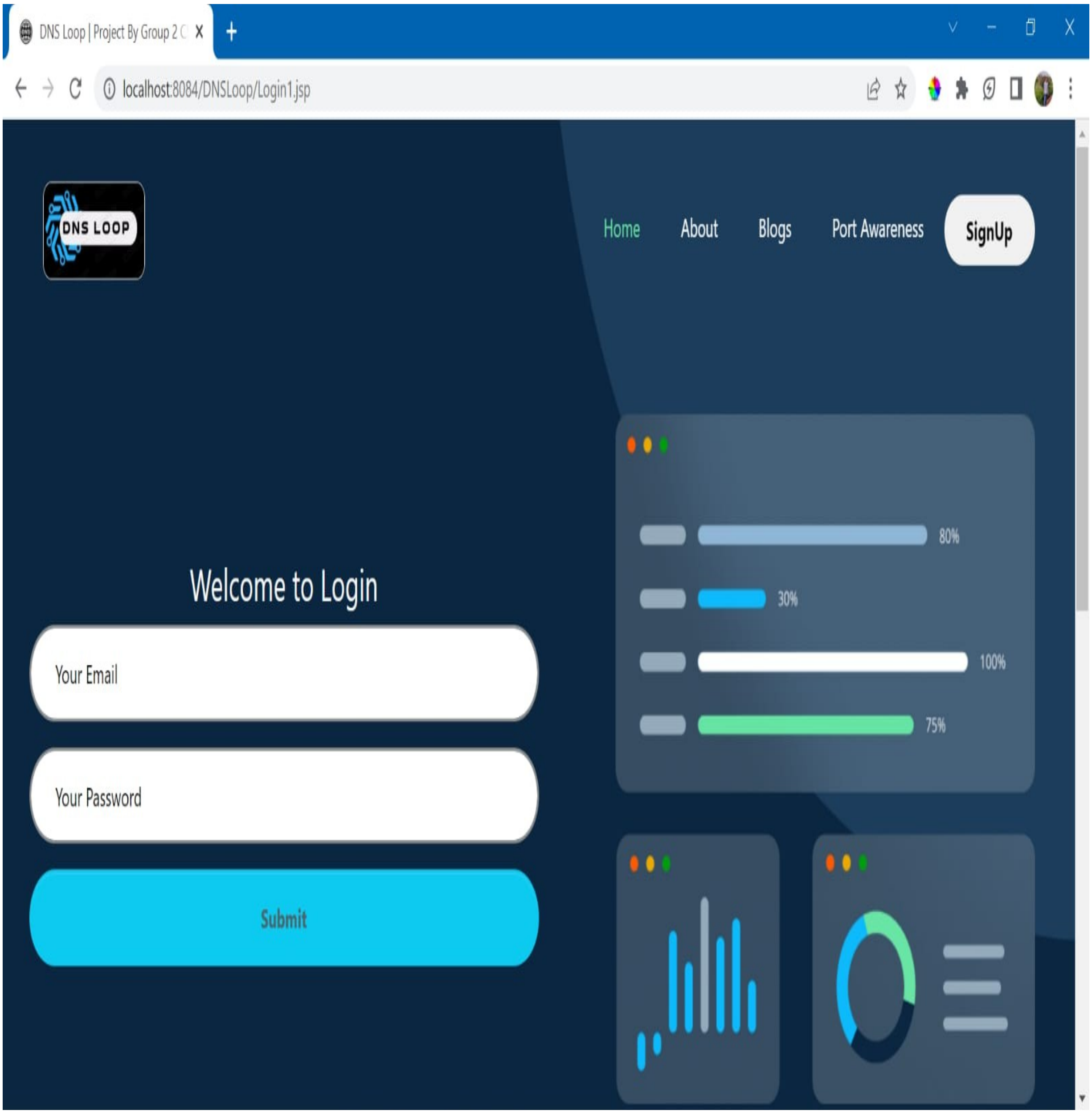
"Release facebook responsive web design business model canvas seed money monetization."

Nikita Singh
Back-End
@ DNS loop

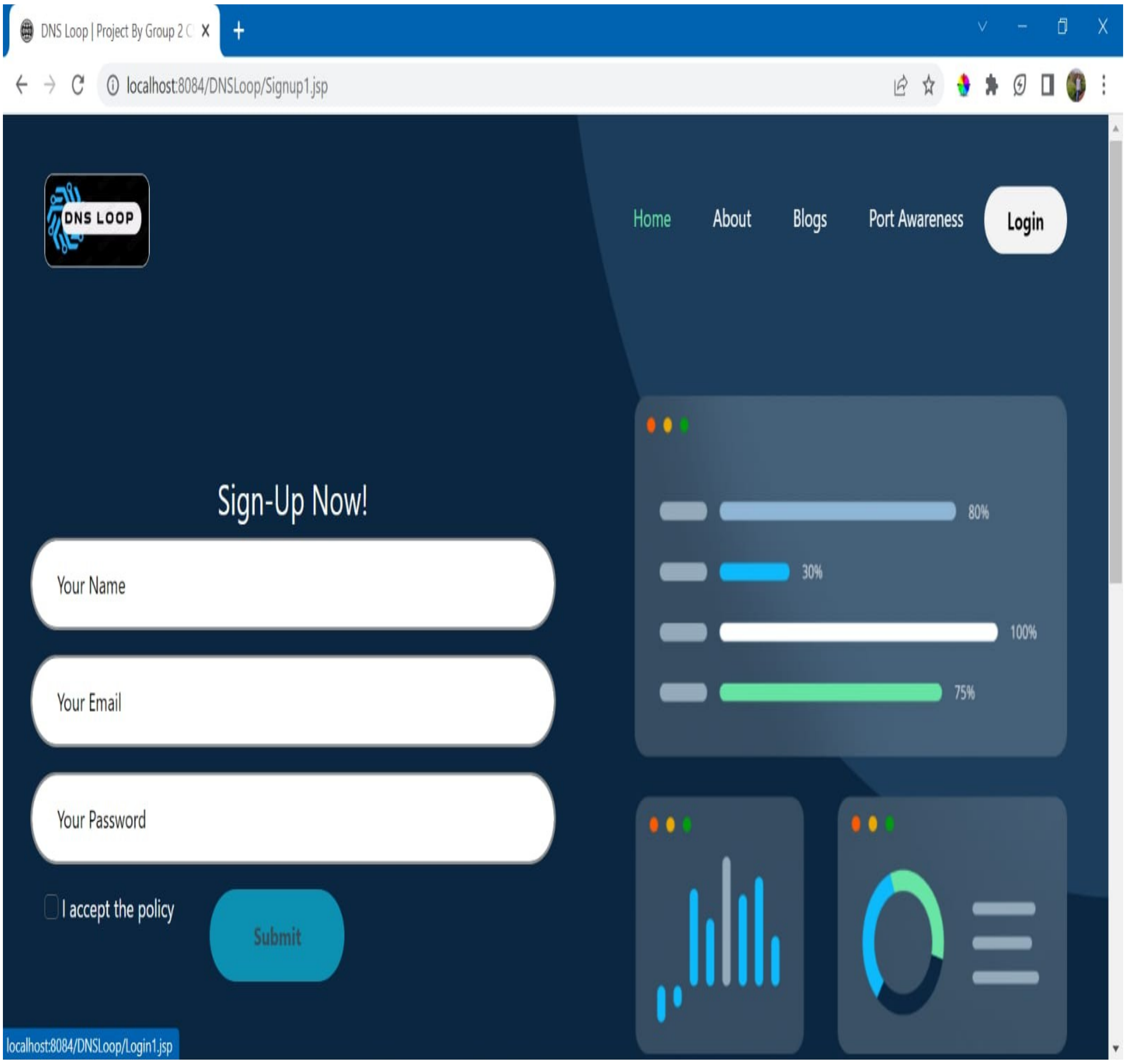
End View of Homepage:



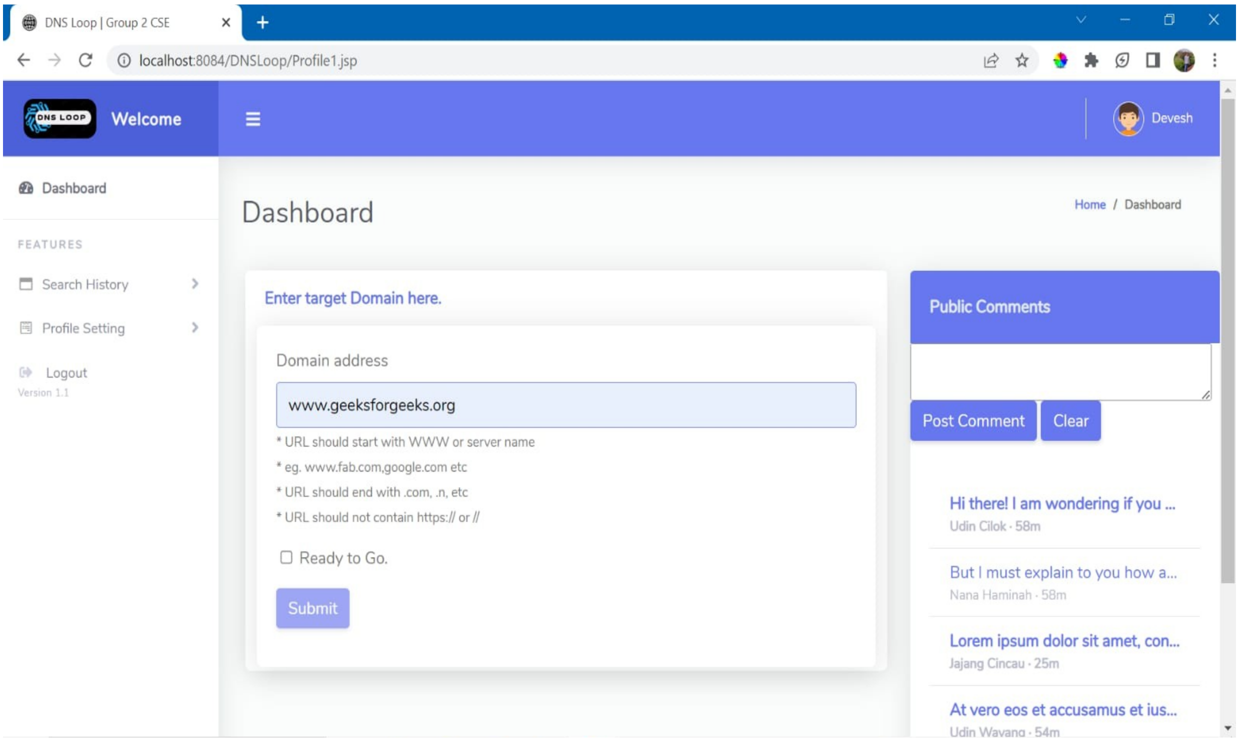
7.2 Login Page:



7.3 Signup Page:



7.4 Profile Page:



Dashboard

Enter target Domain here.

Domain address

www.geeksforgeeks.org

* URL should start with WWW or server name

* eg. www.fab.com,google.com etc

* URL should end with .com, .n, etc

* URL should not contain https:// or //

□ Ready to Go.

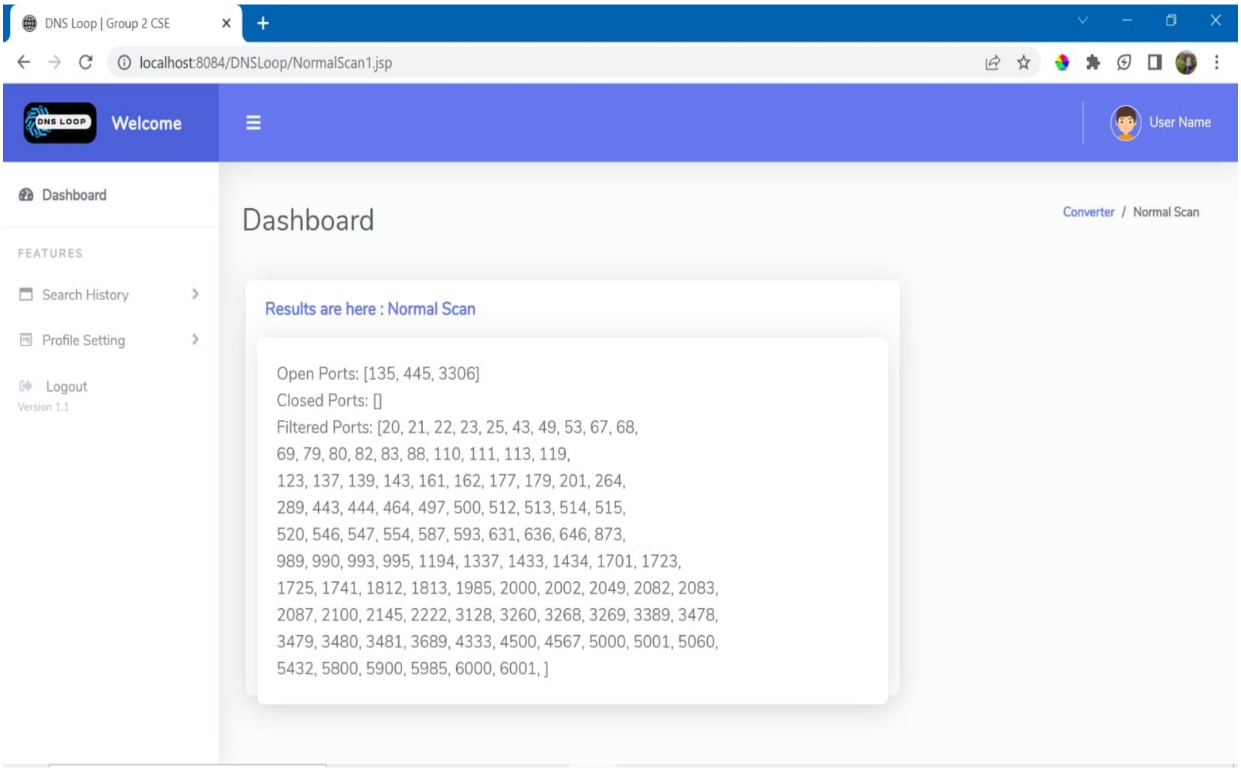
Hi there! I am wondering if you ...
Udin Cilok · 58m

But I must explain to you how a...
Nana Haminah · 58m

Lorem ipsum dolor sit amet, con...
Jajang Cincau · 25m

At vero eos et accusamus et ius...
Udin Wayang · 54m

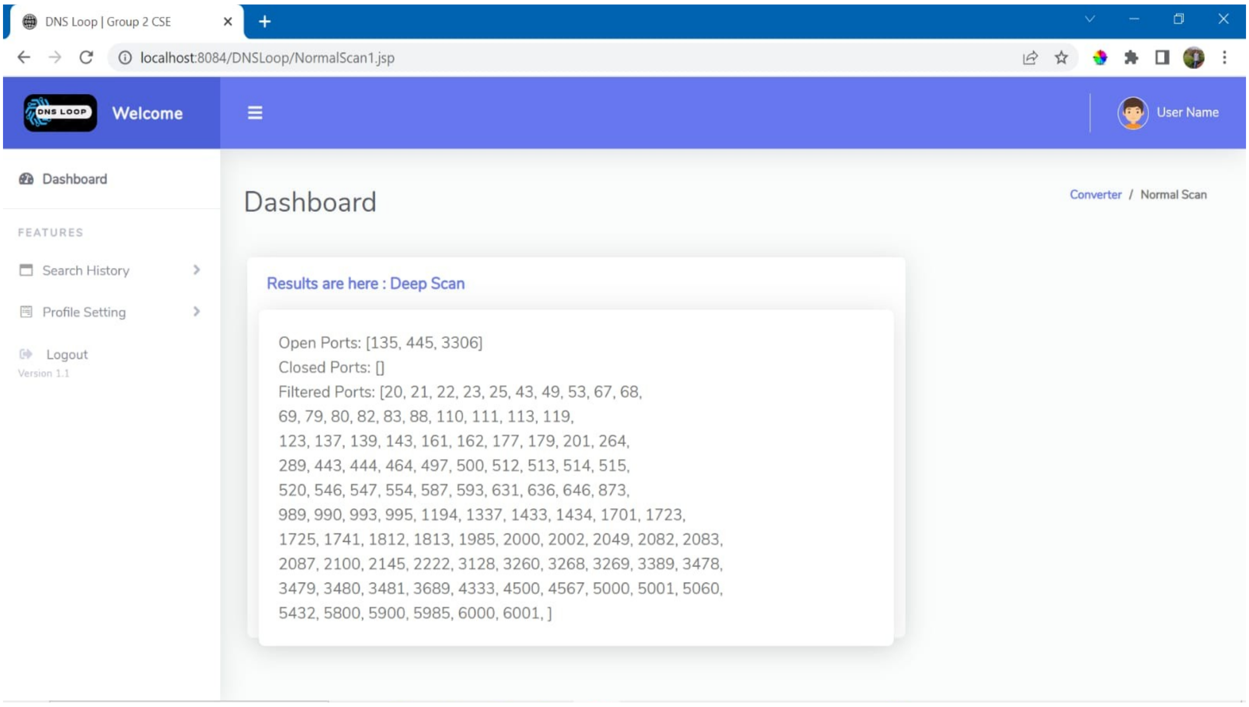
7.5 Normal Scan:



Results are here : Normal Scan

```
Open Ports: [135, 445, 3306]
Closed Ports: []
Filtered Ports: [20, 21, 22, 23, 25, 43, 49, 53, 67, 68,
69, 79, 80, 82, 83, 88, 110, 111, 113, 119,
123, 137, 139, 143, 161, 162, 177, 179, 201, 264,
289, 443, 444, 464, 497, 500, 512, 513, 514, 515,
520, 546, 547, 554, 587, 593, 631, 636, 646, 873,
989, 990, 993, 995, 1194, 1337, 1433, 1434, 1701, 1723,
1725, 1741, 1812, 1813, 1985, 2000, 2002, 2049, 2082, 2083,
2087, 2100, 2145, 2222, 3128, 3260, 3268, 3269, 3389, 3478,
3479, 3480, 3481, 3689, 4333, 4500, 4567, 5000, 5001, 5060,
5432, 5800, 5900, 5985, 6000, 6001, ]
```

7.6 Deep scan:



Results are here : Deep Scan

```
Open Ports: [135, 445, 3306]
Closed Ports: []
Filtered Ports: [20, 21, 22, 23, 25, 43, 49, 53, 67, 68,
69, 79, 80, 82, 83, 88, 110, 111, 113, 119,
123, 137, 139, 143, 161, 162, 177, 179, 201, 264,
289, 443, 444, 464, 497, 500, 512, 513, 514, 515,
520, 546, 547, 554, 587, 593, 631, 636, 646, 873,
989, 990, 993, 995, 1194, 1337, 1433, 1434, 1701, 1723,
1725, 1741, 1812, 1813, 1985, 2000, 2002, 2049, 2082, 2083,
2087, 2100, 2145, 2222, 3128, 3260, 3268, 3269, 3389, 3478,
3479, 3480, 3481, 3689, 4333, 4500, 4567, 5000, 5001, 5060,
5432, 5800, 5900, 5985, 6000, 6001, ]
```

FUTURE SCOPE
OF
PROJECT

Chapter 8

In future port scanning projects may have different scopes depending on a number of variables. Here are a few things to think about:

1.Security testing and vulnerability analysis:
Port scanning is essential to these processes. New attack methods and weaknesses often appear as technology develops. As a result, port scanning initiatives' purview will probably broaden to include developing technologies and the security dangers they pose.

2. Devices for the Internet of Things (IoT):
In terms of security, the spread of IoT devices offers both benefits and difficulties. Future port scanning studies may concentrate on finding open ports, analysing potential vulnerabilities in network interfaces of IoT devices, and uncovering and evaluating the security posture of these devices.

3. Cloud-Based Infrastructure:
Port scanning initiatives may broaden to incorporate cloud-based environments as cloud computing and infrastructure-as-a-service (IaaS) platforms gain popularity. Such projects might include crucial components like evaluating the security of cloud infrastructure, spotting errors, and monitoring open ports in virtual networks.

4. Emerging Protocols and Services:
Port scanning programmes will need to adjust to these changes as new network

protocols and services continue to appear. For instance, port scanning projects may need to support scanning and analysing IPv6 networks and services as IPv6 adoption rises.

5. Changing danger Environment:

New attack types and sophisticated evasion tactics are always being developed, resulting in a constantly changing danger environment. In order to remain ahead of attackers, future port scanning initiatives might need to implement sophisticated scanning methods and detection systems.

6. Compliance and Regulatory Requirements:

Organisations have a serious concern about adhering to industry standards and regulations. In order to ensure that the required security evaluations are carried out to comply with these standards, port scanning initiatives may need to be aligned with specific compliance requirements, such as PCI DSS (Payment Card Industry Data Security Standard) or HIPAA (Health Insurance Portability and Accountability Act).

7. Automation and Integration:

Port scanning initiatives may benefit from automation and integration with other security tools and platforms as technology develops. The effectiveness and efficiency of port scanning operations can be increased through integration with security information and event management (SIEM) systems, vulnerability management programmes, and threat intelligence platforms.

It's crucial to keep in mind that any project's scope can change depending on its unique objectives, goals, and context. In order to prevent any unlawful or unauthorised operations, it is also essential to always conduct port scanning ethically and with the appropriate licence.

CONCLUSION

Chapter 9

Following a thorough port scanning project, we have learned important details about the target system's network architecture and security. Our research and conclusions shed light on the system's possible weaknesses and advantages. The following conclusions can be drawn from the results:

1.Network Security Assessment: Through port scanning, we were able to evaluate the network security of the target machine. We acquired insight into the system's exposure to external networks by finding open ports, closed ports, and filtered ports. This analysis is an essential first step in determining how secure the network architecture is overall.

2. Open Ports Have Been Found: The identification of open ports brings to light potential entry points that malevolent actors might use. To stop unauthorised access or prospective assaults, these open ports should be thoroughly reviewed and locked. To reduce any risks related to these open ports, appropriate security measures should be put in place, such as firewall rules, access controls, and routine patching.

3. Closed and Filtered Ports: The existence of closed and filtered ports shows that the system is purposefully restricting access to specific services or ports. Filtered ports can imply the presence of a firewall or other security measures, but closed ports are inaccessible and typically pose a smaller risk. However, additional investigation is required to identify the precise causes of the closure or filtering the ports.

4. Service Identification: By scanning open ports, we were able to determine which services were present there. Understanding the software and protocols exposed to the network and determining the potential attack surface both depend on this information. System administrators can concentrate on securing and updating these services to stop known vulnerabilities from being exploited by understanding the precise services that

are being used.

5. Vulnerability Assessment: Port scanning serves as a starting point for additional vulnerability analyses. Specific vulnerability scanning tools can be used to evaluate the target system's security faults and weaknesses once the open ports and related services have been found. Following up on these evaluations is crucial in order to find any vulnerabilities and fix them.

6. Recommendations: The following actions are advised based on the results of the port scanning project:

- Regular patching: To reduce known vulnerabilities, make sure that all software, operating systems, and services are current with the most recent security patches.

- Access control: To prevent unauthorised access to the network and services, put in place stringent access controls, such as firewall policies and robust authentication procedures.

- Intrusion Detection/Prevention Systems: Install an intrusion detection or prevention system to keep an eye on network activity, spot unusual activity, and defend against prospective assaults.

- Security awareness training: Inform system administrators and users on the best ways to secure a network, including avoiding phishing emails, creating strong passwords, and reporting suspicious activity.

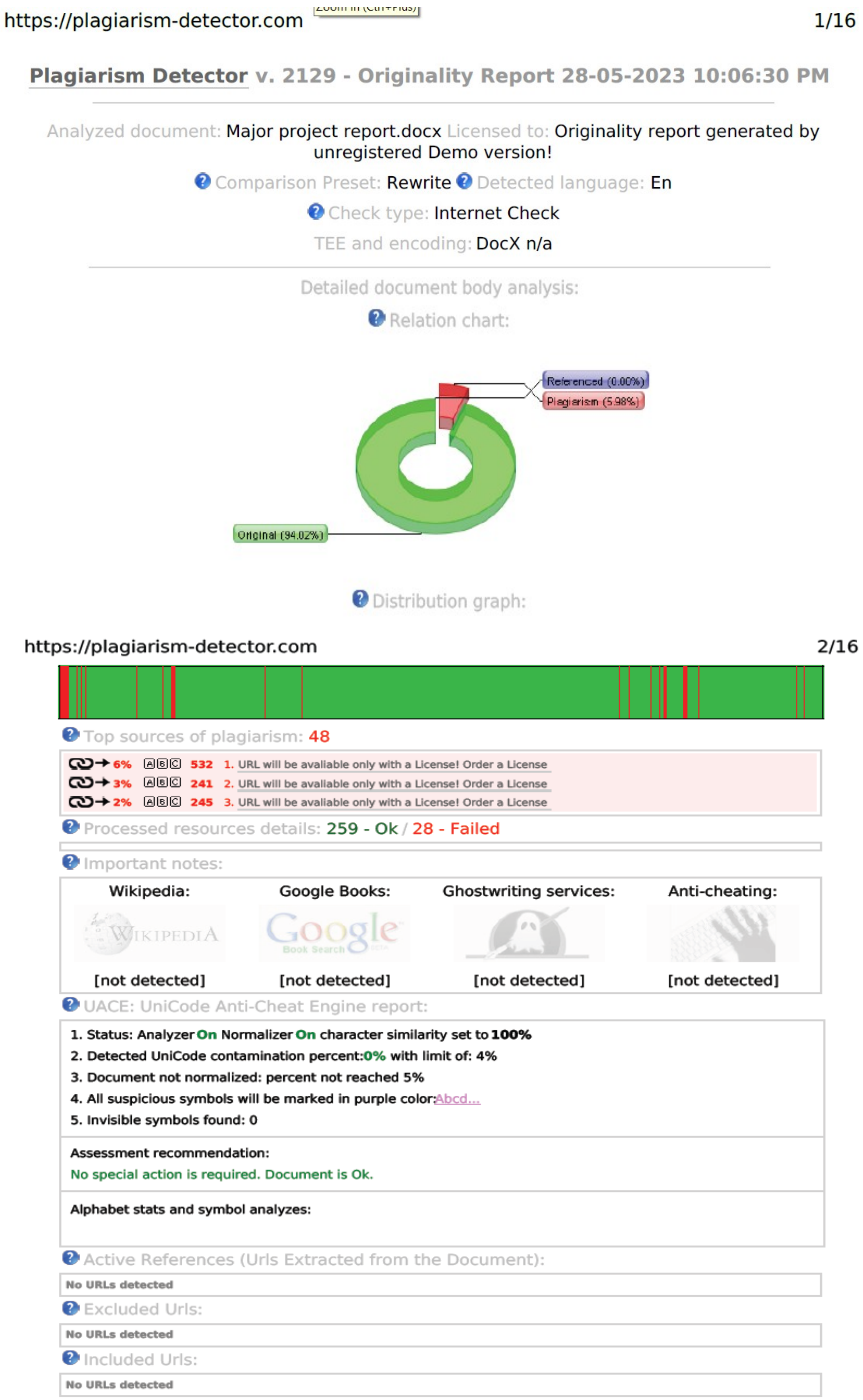
- Periodic security audits: Conduct periodic security audits to spot any modifications to the network infrastructure, revise security policies, and confirm adherence to security standards.

In conclusion, the port scanning project has given useful information about the target system's security and network architecture. The conclusions form the basis for additional vulnerability analyses and the application of crucial security controls to safeguard against potential dangers and reduce vulnerabilities. To maintain a safe network environment, regular updates, continuous monitoring, and adherence to best practices are essential.

References

- https://www.softwaretestinghelp.com/waterfall-model/
- https://www.geeksforgeeks.org/
- https://www.fortinet.com/resources/cyberglossary/what-is-port-scan
- https://www.tutorialspoint.com/
- www.portswigger.com
- nmap.org

Plagiarism Report



https://plagiarism-detector.com 1/16

Plagiarism Detector v. 2129 - Originality Report 28-05-2023 10:06:30 PM

Analyzed document: Major project report.docx Licensed to: Originality report generated by unregistered Demo version!

Comparison Preset: Rewrite Detected language: En

Check type: Internet Check

TEE and encoding: DocX n/a

Detailed document body analysis:

Relation chart:

Distribution graph:

https://plagiarism-detector.com 2/16

Top sources of plagiarism: 48

6%	532	1.	URL will be available only with a License! Order a License
3%	241	2.	URL will be available only with a License! Order a License
2%	245	3.	URL will be available only with a License! Order a License

Processed resources details: 259 - Ok / 28 - Failed

Important notes:

Wikipedia:	Google Books:	Ghostwriting services:	Anti-cheating:
[not detected]	[not detected]	[not detected]	[not detected]

UACE: UniCode Anti-Cheat Engine report:

1. Status: Analyzer On Normalizer On character similarity set to **100%**
2. Detected UniCode contamination percent:0% with limit of: 4%
3. Document not normalized: percent not reached 5%
4. All suspicious symbols will be marked in purple color:Abcd...
5. Invisible symbols found: 0

Assessment recommendation:

No special action is required. Document is Ok.

Alphabet stats and symbol analyzes:

Active References (Urls Extracted from the Document):

No URLs detected

Excluded Urls:

No URLs detected

Included Urls:

No URLs detected