**GeoScan: Information Gathering Tool**

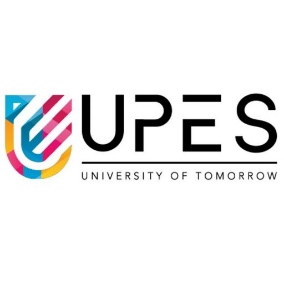
***Project Report***

*submitted in fulfillment of the   
requirements for the award of the degree of*

**BACHELOR OF TECHNOLOGY  
in  
COMPUTER SCIENCE & ENGINEERING**

**By**

|  |  |
| --- | --- |
| **Name** | **Roll No.** |
| **Suryansh Sharma** | **R2142220185** |
| **Vedansh Pundir** | **R2142220698** |
| **Kushagra Bhardwaj** | **R2142221044** |
| **Abhisekh Singla** | **R214222** |

***under the guidance of  
Dr. Akashdeep Bhardwaj***

**School of Computer Science**

**University of Petroleum & Energy Studies  
Bidholi, Via Prem Nagar, Dehradun, Uttarakhand  
November– 2024**

Table of Contents

[**CANDIDATE’S DECLARATION** 3](#_Toc183169293)

[**ACKNOWLEDGEMENT** 4](#_Toc183169294)

[**ABSTRACT** 5](#_Toc183169295)

[**INTRODUCTION** 5](#_Toc183169296)

# **CANDIDATE’S DECLARATION**

We hereby certify that the project work entitled **“ GeoScan: Information Gathering tool”** in fulfilment of the requirements for the award of the Degree of BACHELOR OF TECHNOLOGY in COMPUTER SCIENCE AND ENGINEERING with specialization in Cybersecurity and submitted to the Department of Systemics, School of Computer Science, University of Petroleum & Energy Studies, Dehradun, is an authentic record of my/ our work carried out during a period from **August**, **2024** to **November**, **2024** under the supervision of **Dr. Akashdeep Bhardwaj, Faculty Cybersecurity**.

The matter presented in this project has not been submitted by us for the award of any other degree of this or any other University.

**Vedansh Pundir R2142220698**

**Suryansh Sharma R2142220185**

**Kushagra Bhardwaj R2142221044**

**Abhishek Singla R2142220698**

This is to certify that the above statement made by the candidate is correct to the best of my knowledge.

Date:

# **ACKNOWLEDGEMENT**

We wish to express our deep gratitude to our guide **Dr. Akashdeep Bhardwaj**, for all advice, encouragement and constant support he has given us throughout our project work. This work would not have been possible without his support and valuable suggestions.

We sincerely thanks to our respected **Head of Department of Informatics** for his great support in doing our project **GeoScan: Information Gathering Tool.**

We are also grateful to Dean of **SOCS UPES** for giving us the necessary facilities to carry out our project work successfully. We also thanks to our *Course Coordinator, Dr. Keshav Sinha* for providing timely support and information during the completion of this project.

We would like to thank all our friends for their help and constructive criticism during our project work. Finally, we have no words to express our sincere gratitude to our parents who have shown us this world and for every support they have given us.

|  |  |
| --- | --- |
| **Name** | **Roll No.** |
| **Vedansh Pundir** | **R2142220698** |
| **Suryansh Sharma** | **R2142220185** |
| **Kushagra Bharadwaj** |  |
| **Abhishek Singla** |  |

# **ABSTRACT**

Gathering information about wireless-connected devices on a network can be critical in the age of network security. “**GeoScan: An Information Gathering Tool**” aims to do just that, providing a comprehensive Information Gathering tool for both network admins and security experts. The tool is able to conduct scans that can reveal the presence of wireless devices nearby, examine ports and determine type of OS. Also, GeoScan includes location-based real-time news aggregation which can be used to understand context for potential threats or if there is an event that might affect the network security. All of these features make GeoScan not only a very complete, but also changed the way to secure networks in various aspects. Forthcoming, we will be adding a Geolocation feature in which the location of the IP Address will be displayed. GeoScan can be productised in various forms to cater enterprises, governments (for securing defence infrastructure), smart cities and emergency response systems etc. GeoScan might lead the way in Information Gathering and network analysis tools by solving these problems of visibility over networks with detailed monitoring (through scanning) and situational awareness (by Geolocation and News Aggregation).

# **INTRODUCTION**

We live in an era where our world is highly connected and this makes network security a must. As wireless devices become more prevalent, the need to protect networks from threats increases. “GeoScan: An Information Gathering Tool" ensures the network security as well to get complete information about wireless networks and devices and its related help. The data collected by this tool is crucial and includes the version of a device, an IP address and of what type it happens to be, open ports, geolocation and location-based news.

# **PROBLEM STATEMENT**

Existing Information Gathering or Network Scanning tools often rely on external libraries, limiting their applicability in environments requiring independent implementations. The challenge lies in creating a comprehensive information gathering solution that can accurately identify device details, open ports, while also providing advanced features like geolocation-based mapping and location-based news. This project addresses this gap by developing a tool, GeoScan: An Information Gathering Tool, which integrates these capabilities natively, enhancing security and analysis across diverse network environments.

# **Introduction**

**Purpose**

This is the SRS for the GeoScan software which has been designed as a minor project for BTech in Computer Science & Engineering with specialization in Cyber Security. This document enlists and describes all functionalities, constraints along with features of GeoScan to communicate properly while developing it.

**Scope**

GeoScan scans and analyzes the number of devices that are connected wirelessly in your local network. The scanning tool should give detailed information about each device with the IP address, open ports, geolocation, version check, type of device, and many more news related to the locations of devices to be made available in a friendly user interface dashboard.

1. **Overall Description**

**Product Perspective**

GeoScan is a standalone network scanning tool, targeting local network usage. It uses the existing protocols and APIs to collect and present data regarding associated equipment. GeoScan is programmed in C++ and leverages third-party services for geolocation and news aggregation.

**Product Functions**

GeoScan offers the following main functions:

**Network Scan:**

Automates a scan on all devices it could connect with located within the same local network, listing all of them out.

**Device Information Scanning:**

* **IP Device:** It will display the IP address connected to every device.
* **Port Scanning:** Scans and reports open ports in ready use for each device where active services are running.
* **Version Scan:** It senses the software or firmware in use within any device.
* **Device Type:** It detects the type of a device, e.g., it will identify whether it is a router, smartphone, or a laptop. (If applicable)
* **Geolocation:** It retrieves geolocation data from the IP addresses of the devices.

**User Characteristics**

GeoScan is intended for use by:

* For network device monitoring and management.
* Cybersecurity professionals whose role includes measuring network security and pointing out possible vulnerabilities.
* IT Students to get a basic idea of scanning on the network and security application.

**Constraints**

* **Operating System**: Developed primarily for Windows due to the use of Winsock.
* **Programming Language**: Implemented in C++.
* **Permissions**: Requires administrative privileges to perform raw socket operations and network scanning.
* **Network Environment**: Assumes devices are connected within the same local network or subnet.

**Assumptions and Dependencies**

* **Network Configuration**: The local network uses IPv4 addressing.
* **Firewall Settings**: Firewalls are configured to allow ICMP and other necessary traffic for scanning.
* **External Services**: Geolocation and news aggregation rely on third-party APIs.
* **Hardware Resources**: Adequate system resources are available to perform network scans without significant performance degradation.

1. **Specific Requirements**  
   1. **Functional Requirements:**

**Network Discovery**

* The system shall automatically detect the local machine’s IP address and subnet.
* The system shall generate a list of all possible IP addresses within the detected subnet range.
* The system shall perform a ping sweep to identify active devices on the network.

**Device Information Retrieval**

* The system shall retrieve and display the IP address of each active device with open ports.
* The system shall perform version checks to identify software or firmware versions running on each device.

**Port Scanning**

* The system shall scan a predefined range of ports (e.g., 1-1024) on each active device.
* The system shall identify and list open ports.

**Geolocation**

* The system shall retrieve geographical information (e.g., country, city) based on each device’s IP address using an external geolocation API.
* The system shall display the geolocation data on the dashboard.
  1. **Non-Functional Requirements:**

**Performance**

* The system shall complete a full network scan of a typical local subnet (e.g., 192.168.1.1 - 192.168.1.254) with fast efficiency.

**Usability**

* The dashboard shall have an intuitive and user-friendly interface, requiring minimal training for new users.
* The system shall provide clear and informative error messages in case of failures or exceptions.

**Reliability**

* The system shall handle network interruptions gracefully, ensuring that partial scan results are saved and can be resumed.
* The system shall maintain accuracy in device detection and information retrieval.

**Maintainability**

* The codebase shall be modular, allowing easy updates and maintenance.
* The system shall include comprehensive documentation for future developers and users.
  1. **External Interface Requirements**

**User Interfaces**

* A graphical dashboard interface developed using HTML, CSS, JavaScript, and AngularJS.

**Software Interfaces**

* Integration with external APIs for geolocation and news aggregation.
* Interaction with the Windows API for network scanning functionalities.

**Communication Interfaces**

* Utilization of TCP/IP protocols for network communication.
* Use of HTTP/HTTPS protocols for API interactions.

**System Features:**

**Network Discovery Feature**

**Description**: Automatically detects and lists all devices connected to the same local network.

* **Input**: Local machine’s IP address and subnet.
* **Processing**: Generates a list of IP addresses within the subnet and performs ping sweeps.
* **Output**: List of active devices with their IP addresses.

**Device Information Retrieval Feature**

**Description**: Gathers detailed information about each active device.

* **Input**: IP addresses of active devices.
* **Processing**: Performs version checks.
* **Output**: Detailed device information including IP, open ports and software versions.

**Port Scanning Feature**

**Description**: Scans and lists open ports on each active device.

* **Input**: IP addresses of active devices.
* **Processing**: Scans predefined port ranges using TCP connections.

**Geolocation Feature**

**Description**: Retrieves geographical information based on device IP addresses.

* **Input**: IP addresses of active devices.
* **Processing**: Sends requests to geolocation APIs and processes responses.
* **Output**: Geographical data such as country, region, and city.

**News Aggregation Feature**

**Description**: Fetches and displays news related to device locations.

* **Input**: Geographical data of device locations.
* **Processing**: Queries news APIs based on location data.
* **Output**: Relevant news articles categorized by location.

**Dashboard Visualization Feature**

**Description**: Presents all collected data in an interactive dashboard.

* **Input**: Data from network discovery, device information, port scanning, geolocation, and news aggregation.
* **Processing**: Organizes and formats data for visualization.

**User Authentication Feature**

**Description**: Secures access to the GeoScan dashboard.

* **Input**: User credentials (username and password).
* **Processing**: Validates credentials against a secure database.
* **Output**: Access granted or denied based on authentication results

1. **Other Requirements:**

**Database Requirements**

* The system shall use a secure database to store user credentials for authentication.
* The database shall store scan results for future reference and reporting.

**Documentation Requirements**

* Provide comprehensive user manuals and guides for operating GeoScan.
* Include detailed developer documentation for future maintenance and feature additions.

**Quality Assurance Requirements**

* Perform thorough testing and user acceptance tests to ensure system reliability.
* Implement error handling and logging mechanisms to track and resolve issues promptly.

**Literature Review**

**Inference from Literature**

1. **Network Scanning Techniques (Kaushik et al., 2019)**
   * Efficient device identification and IP retrieval, inspired by NMAP and NBTSCAN methodologies, enhancing network discovery within GeoScan.
2. **Port Scanning and Detection (Vurgin et al., 2020)**
   * GeoScan’ s open port retrieval uses proven techniques from this study, improving detection of vulnerabilities through real-time port scanning.
3. **Data Analysis for Red Teamers (Sivasangari et al., 2023)**
   * Structured data collection and analysis for efficient IP and MAC address retrieval, enhancing the tool’s reconnaissance capabilities.
4. **EH and Reconnaissance (Barman et al., 2023)**
   * Adoption of ethical reconnaissance practices, ensuring secure and compliant information gathering in GeoScan.

**Reference**

1. [**https://github.com/Lissy93/web-check**](https://github.com/Lissy93/web-check)
2. **Kaushik, S., Bhutto, A., & Pandey, B. (2019). Efficient Information Gathering using NMAP and NBTSCAN: Case study on 172.19.19.0 IP Address. Indian Journal of Science and Technology, 12(28), 1–13.** [**https://doi.org/10.17485/ijst/2019/v12i28/147004**](https://doi.org/10.17485/ijst/2019/v12i28/147004)
3. **Barman, F., Alkaabi, N., Almenhali, H., Alshedi, M., & Ikuesan, R. (2023). A Methodical Framework for Conducting Reconnaissance and Enumeration in the Ethical Hacking Lifecycle. European Conference on Cyber Warfare and Security, 22(1), 54–64**[**https:/doi.org/10.34190/eccws.22.1.1438**](https://doi.org/10.34190/eccws.22.1.1438)
4. **Vugrin, E. D, et al. (2020). Cyber threat modeling and validation: Port Scanning and Detection** [**https://doi.org/10.1145/3384217.3385626**](https://doi.org/10.1145/3384217.3385626)
5. **Sivasangari, A., B, P., M, K., Ajitha, P., Gomathi, R., & Vignesh, N. (2023). Dart | Data Analysis For Red Teamers.** [**https://doi.org/10.1109/ictbig59752.2023.10456020**](https://doi.org/10.1109/ictbig59752.2023.10456020)

**SWOT Analysis**

**Strengths**

* Comprehensive data collection: GeoScan gathers extensive information about each device.
* Geolocation and elevation data: Unique features that enhance the security assessment process.
* Real-time news integration: Allows for situational awareness based on the device's location.

**Weaknesses**

* Potential for high resource consumption: The extensive scanning process may require significant computational resources.
* Dependency on external services: Geolocation and news aggregation depend on third-party APIs.

**Opportunities**

* Increasing demand for network security tools: Growing cybersecurity concerns create a large market for tools like GeoScan.
* Expansion into IoT security: The tool can be adapted to monitor IoT devices, which are often vulnerable to attacks.

**Threats**

* Competition from existing tools: Established Information Gatheringtools may offer similar features.
* Privacy concerns: Detailed data collection might raise privacy issues, especially regarding geolocation and news aggregation.

**Objective**

1. **Optimized Device Scanning**

* To design and implement a time-efficient device scanning process that identifies all active devices on the network. The system must ensure that scanning is done swiftly without compromising accuracy or overloading network resources.

1. **Accurate Device Information Retrieval**

* To develop a robust mechanism that captures detailed device information, such as IP addresses, MAC addresses, and open ports. Each piece of data must be collected in a secure manner and presented clearly in the user interface, facilitating seamless interaction for network administrators.

1. **Secure and Scalable Architecture**

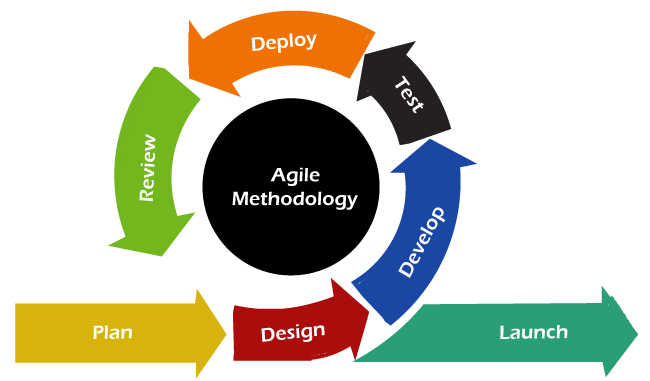
* To build a secure foundation for handling device information, ensuring no data leakage or unauthorized access. The architecture should be scalable to accommodate future features such as geolocation and elevation mapping, while maintaining security standards.

**Methodology**

**Reference Software model**

The **Agile Development Model** is suitable for the GeoScan project:-

* **Iterative Development**: Ideal for building and refining complex features like device scanning, geolocation, and news integration.
* **Adaptability:** Agile supports changes and enhancements throughout the development process.
* **Frequent Feedback**: Regular iterations ensure that feedback can be quickly incorporated.
* **Collaboration:** Close collaboration between personals ensure that the project meets its goals effectively.



**Steps**

1. **Requirement Analysis:**
   * Identify project objectives and gather detailed requirements.
   * Define technical specifications and desired outcomes.
2. **Design & Planning:**
   * Architect the system structure and data flow.
   * Plan the development phases and set milestones.
3. **Development & Implementation:**
   * Code the core features including device discovery, port scanning, geolocation, and news aggregation.
   * Integrate modules and ensure system cohesion.
4. **Testing & Validation:**
   * Conduct unit, integration, and system testing.
   * Validate results with real-world scenarios and adjust as needed.
5. **Deployment & Maintenance:**
   * Deploy the tool in a controlled environment.
   * Monitor performance and provide ongoing updates and bug fixes.

**Results**

**Attained Deliverable**

Device Information Collected

* IP Address
* MAC Address
* Version
* Open Ports
* Geolocation
* Latitude and Longitude

**Input Format**

* IP Address Range: Defines the scope for network scanning.
* Port List: Predefined list of ports to scan (e.g., 22, 80, 443).
* Geolocation Data: IP-to-location mapping dataset.