Name: KATUMBIRE BOB BELLS

RegNo: S20B23/219

Project : Nsafe

TECHNICAL PLAN

1. Introduction and summary of constraints:

Nsafe is a network security system that uses different port scans and alerts to identify existing vulnerable open ports that pose a security threat to the network

Networking, also known as computer networking, is the practice of transporting and exchanging data between nodes over a shared medium in an information system. Networking comprises not only the design, construction and use of a network, but also the management, maintenance and operation of the network infrastructure, software, and policies.

Network vulnerability results from open ports on the network which leads to network insecurity by giving hackers a chance to intrude through our system. This in the end can leave a business (enterprise) unable to use their software or devices. This means their revenue stream dries up. Approximately 29% of businesses that experience a data breach lose revenue, and 38% of those companies lost more than 20% of their revenue.

(c) user requirements concerning implementation.

The system will have to cover the needs of the enterprises (users) that are facing challenges of hacking due to vulnerable ports being open on their network.)

The *Client's perspective* of the system

- Simple Registration and subscription, the clients will be required to register in their details and there will be a choice of sign-up methods such as creating a new account using an email address, google, social media address
- Various payment methods; these will include mobile money, and credit card usage. theses will mainly be used to pay the subscription fee for the registered new members
- Entering the IP address, so here there will be an option of manually entering the IP address or using the auto scan for the available network IP address with a concept like Wi-Fi.

- Port scans; the system will have a range input for the network ports that need to be scanned in order to minimize the time taken while running the ports that are not in range. There are different types of scans available in the system e.g. TCP, UDP, xmass.
- A scan report will be displayed to show the open ports on the network and the ports that are vulnerable on the network.

2. Recommended approach

Selected methodology or process model;

For the Nsafe system with different scan types, The Rapid Application Development would be the best methodology to consider using the Prototyping Model specifically

The Prototyping Model

This is a software development model in which a prototype is built, tested and reworked until an acceptable prototype is achieved.

Reason for Using Prototyping Methodology

- More understanding about the project, prototyping is a great way to not only understand the problem you're currently trying to solve, but to illuminate alternative problems you should solve instead. This process is called problem discovery, and it can help you find the root cause of your user's pain, which might be different than your originally assumed user problem.
- It also enables Users to be involved actively in the development of the software. Therefore, errors can be detected in the initial stage of the software development process
- The prototyping methodology helps gain better understanding of the customer's needs hence quicker user feedback helping one to achieve better software development solutions.

3. Tools and Technologies to be used

To build Nsafe, the following actors should be put in mind

- Customers (needs)
- payment methods
- standby help team
- Scripts

Scanning Approach

To test scan performance and ensure anonymization, during testing, the team will scan in a controlled environment against a machine that it owns. The purpose of benchmarking is to fold:

I. Ensuring that the source's IP address isn’t leaked to the target machine
II. Testing how many additional scans can be run in parallel on each machine. How adding one additional scan can increase or decrease total throughput time.