**Final Report**

# 1.Introduction

## 1.1 Project Overview

Cyber security is crucial in the modern digital world. This project explores various cyber threats and their impact while providing effective solutions to safeguard digital assets.

## 1.2 Purpose

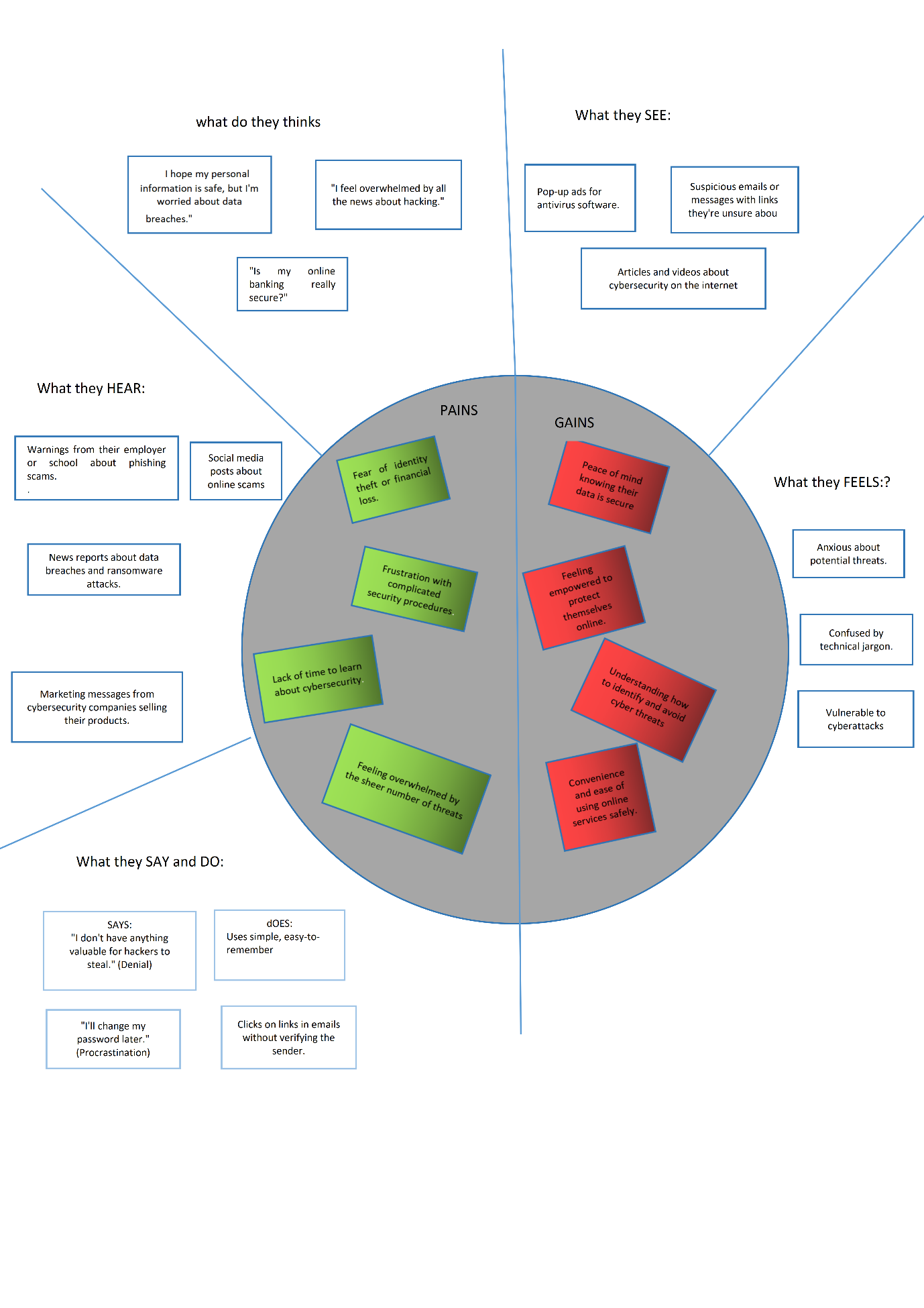
The purpose of this project is to create awareness about cyber security, identify common threats, and provide practical solutions to mitigate risks. It also aims to help individuals and organizations secure their digital presence.

# 2. Ideation Phase

## 2.1 Problem Statement

With the rise of technology, cyber threats have become more advanced and widespread. This project focuses on understanding these threats and providing solutions to counter them effectively.

## 2.2 Empathy Map Canvas



### 2.3 Brainstroming

Pratiksha Satavekar Akshaya Chavan

|  |
| --- |
| Analyzing the  Evoiution of Ransomware |

|  |
| --- |
| IOT  Vulnerabilities |

|  |
| --- |
| Cloud  Security  Breaches |

|  |
| --- |
| Insider  Threat |

|  |
| --- |
| Deepfakes and  Social  Engineering |

|  |
| --- |
| The Threat of AI-Powered cyberattacks |

Priyanshi Kalra Anuja Bodhale

|  |
| --- |
| AI Driven Threat detection |

|  |
| --- |
| Zero Trust  Security  Implementation |

|  |
| --- |
| Blockchain for Cyber Security |

|  |
| --- |
| Security  Automation and  Orchestration |

|  |
| --- |
| Quantum  Cryptography |

|  |
| --- |
| Phishing and smashing trends |

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |

**3. Requirement Analysis**

## 3.1 Technology stack

* Programming Languages: Python, Java
* Security Tools: Wireshark, Metasploit, Nessus
* Encryption: AES, RSA
* Secure Protocols: HTTPS, TLS

# 4. PROJECT DESIGN

## 4.1 Problem-Solution Fit

* Problem: Increasing cyber threats targeting individuals and organizations.
* Solution: Implementing security practices to prevent attacks and mitigate risks.

## 4.2 Proposed Solution

* Conduct security audits and risk assessments
* Implement strong security policies
* Educate users about cyber threats

**4.3 Solution Architecture**

Threat landscape analysis

Security Controls

Incident Response plan

Exploring the threat solutions

Data Measure Protection

Vulnerability Management

Cloud Security

Network Security

User Authentication

# 5. Project planning

|  |  |  |
| --- | --- | --- |
| **Day** | **Phase** | **Task** |
| **1-2** | **Research** | **Study cyber threats and attack methods** |
| **3-4** | **Documentation** | **Write about key cybersecurity concepts** |
| **5-6** | **Analysis** | **Case studies on real-world cyber attacks** |
| **7-8** | **Review** | **Proofreading and improving documentation** |
| **9-10** | **Finalization** | **Preparing project presentation / report** |

# 6. FUNCTIONAL AND PERFORMANCE TESTING

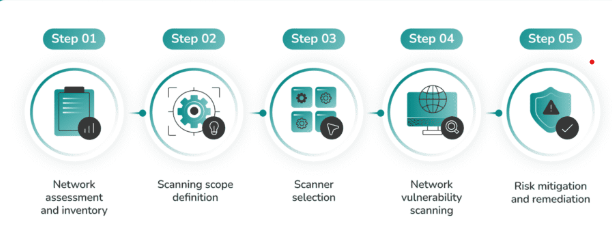
## 6.1 Performance Testing

* Vulnerability Scanning: Identify weaknesses in a system.
* Penetration Testing: Simulate real-world cyber-attacks.
* Load Testing: Check the system's ability to handle multiple requests.

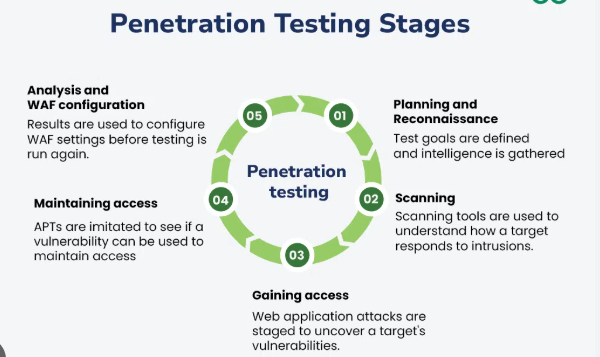
**7. Results**

**7.1 Screenshots (testing phase related)**

**Vulnerability scanning:**



**Penetration Testing:**



**Load Testing:**

****

# 8. ADVANTAGES & DISADVANTAGES

## Advantages

* Protects sensitive data
* Reduces financial losses due to cyber-attacks
* Enhances trust in digital systems
* Improves overall security awareness

## Disadvantages

❌ Requires continuous updates and monitoring

❌ Initial setup cost can be high

❌ Complexity in managing multiple security tools

# 9. CONCLUSION

Cyber security is an essential aspect of the digital age. By understanding threats and implementing effective solutions, individuals and organizations can protect their data and ensure a safer online experience.

# 10. FUTURE SCOPE

* AI-driven cyber security solutions
* Blockchain for enhanced security
* Quantum cryptography
* Advanced intrusion detection systems

**11. Appendix**