IDEATION PHASE

The ideation phase sets the foundation for our cybersecurity project by fostering creative thinking, understanding user perspectives, and clearly defining the problem to be solved. This phase consists of three main components: Brainstorming, Empathy Map, and Problem Statement.

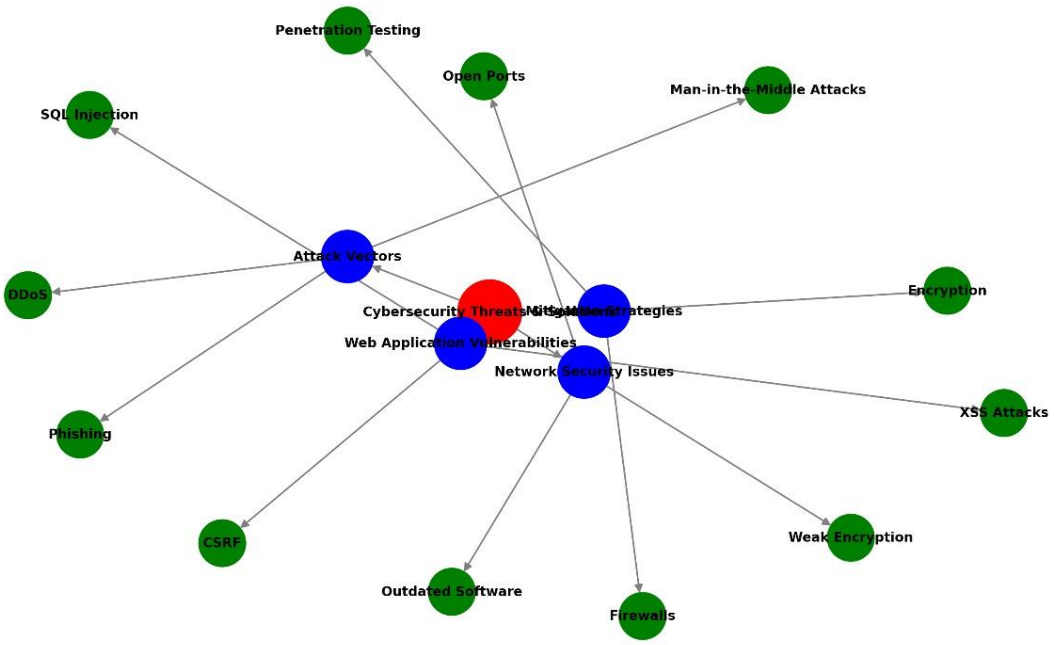
Brainstorming

During our brainstorming sessions, the team generated ideas based on our past experiences and understanding of known attack vectors. The focus areas included:

- Identifying potential cybersecurity threats (e.g., malware, phishing, ransomware, etc.).
- Discussing innovative approaches to detect vulnerabilities such as Insecure Direct Object References (IDOR), Cross-Site Request Forgery (CSRF), security misconfigurations, unvalidated redirects, and XML External Entity (XXE) injections.
- Engaging in collaborative discussions, incorporating insights from academic research and industry case studies.
- Outlining a combination of testing methodologies that use both automated scanning (e.g., Nessus) and manual testing (e.g., OWASP ZAP, Burp Suite, and Wireshark).

Outcome:

- A prioritized list of potential vulnerabilities.
- Preliminary testing ideas and strategies for a comprehensive cybersecurity assessment.



Empathy Map

An empathy map was created to capture the perspectives of end users and stakeholders. This tool helped us ensure that our solution addresses real-world concerns. Key aspects include:

User Needs:

- Secure and reliable access to data.
- Assurance that personal and sensitive information is protected.

Stakeholder Concerns:

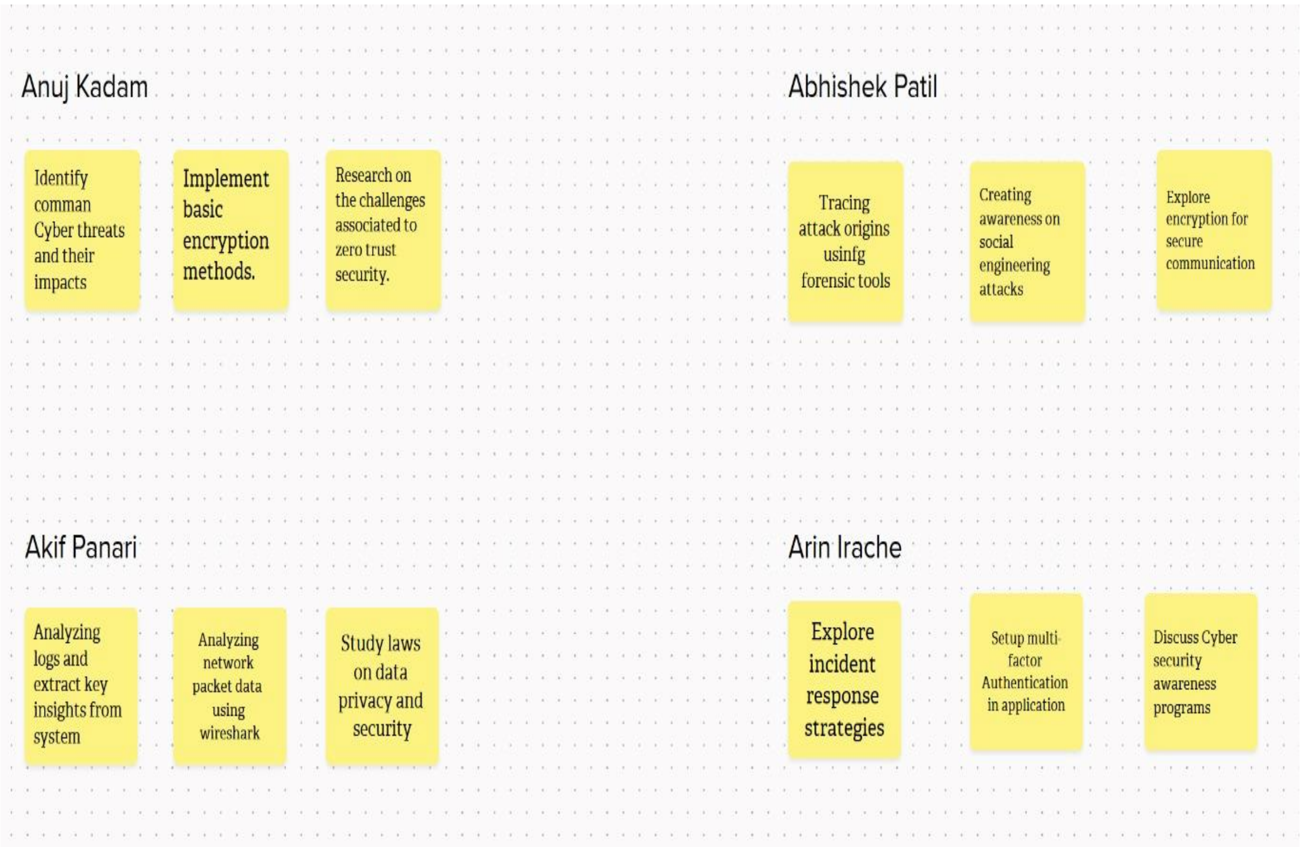
- Safeguarding critical business information.
- Meeting regulatory requirements and maintaining customer trust.

Pain Points:

- The risk of data breaches leading to financial loss.
- Damage to reputation due to security incidents.

Desired Gains:

- Enhanced security protocols to reduce vulnerability risks.
- Increased confidence in the system's integrity and overall cybersecurity posture.



Anuj Kadam

Identify comman Cyber threats and their impacts

Implement basic encryption methods.

Research on the challenges associated to zero trust security.

Abhishek Patil

Tracing attack origins usinfg forensic tools

Creating awareness on social engineering attacks

Explore encryption for secure communication

Akif Panari

Analyzing logs and extract key insights from system

Analyzing network packet data using wireshark

Study laws on data privacy and security

Arin Irache

Explore incident response strategies

Setup multi-factor Authentication in application

Discuss Cyber security awareness programs

Problem Statement

In today's rapidly evolving digital landscape, cyber attacks are becoming increasingly sophisticated, exposing critical vulnerabilities in web applications and network systems. The primary challenges we aim to address include:

- Vulnerability Identification: Detecting security flaws such as IDOR, CSRF, security misconfigurations, unvalidated redirects, and XXE injections.
- Impact Evaluation: Assessing the business impact of these vulnerabilities on system integrity and user trust.

- Remediation Development: Proposing effective, actionable strategies that include: • Secure coding practices. • Advanced encryption methods (AES, RSA). • Implementation of multi-factor authentication. • Continuous monitoring and real-time threat detection.

Overall Goal:

To develop a robust cybersecurity framework that not only identifies and analyzes vulnerabilities but also provides clear and targeted remediation strategies to protect digital assets in the modern threat landscape.