EMPATHY MAP

Says
What have we heard them say?
What can we imagine them saying?

"We need better vulnerability management strategies."

"What other tools should I consider for threat detection?"

"How do I use Nessus effectively for scanning?"

Gain
What are their wants, needs, hopes, and dreams?
What other thoughts might influence their behavior?

Mastery of Nessus and other vulnerability scanning tools.

Staying ahead in the cybersecurity field with updated knowledge.

Improved security posture for their organization.

cyber security
Understanding cyber threats: Exploring the nessus and beyond scanning tools

Are our systems secure from cyber threats?

Does
What behavior have we observed?
What can we imagine them doing?

Experimenting with Nessus and other scanning tools.

Attending cybersecurity webinars or training sessions.

Looking for best practices and case studies in vulnerability scanning.

Will learning these tools improve my cybersecurity skills?

How effective is Nessus compared to other scanning tools?

Feels
What are their fears, frustrations, and anxieties?
What other feelings might influence their behavior?

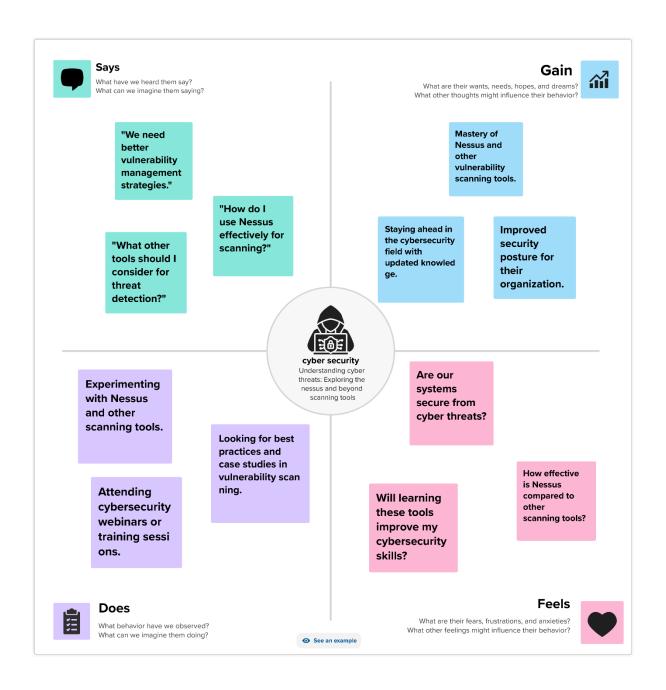See an example

PROBLEM STATEMENT

2.1 The Thought Behind the project:

Various Ideas

sravani

Conduct extensive literature research on cyber threats and vulnerability scanning techniques.	Provide detailed explanations of Nessus, other scanning tools, and their effectiveness.
Integrate real-world case studies of cyberattacks where vulnerability scanning could have mitigated the damage.	

Teja prasanth

Select a few commonly used vulnerability scanning tools (e.g., Nessus, OpenVAS, Qualys, Nexpose).	Walk through the process of scanning a system for vulnerabilities with Nessus.
Analyze the results of the scan, including high, medium, and low-risk vulnerabilities.	

Ganesh

Select a few commonly used vulnerability scanning tools (e.g., Nessus, OpenVAS, Qualys, Nexpose).	Set up each tool in a similar test environment and perform vulnerability scans on the same systems.
Analyze and compare the results based on scan speed, ease of use, accuracy, and comprehensiveness.	

Fransis

Create a test environment with multiple known vulnerabilities (e.g., outdated software, misconfigured network settings).	Perform vulnerability scanning using Nessus and other tools as part of a penetration testing framework.
Identify weaknesses in the system using the results from the scans and exploit them to demonstrate the impact of these vulnerabilities.	