Project Plan: Automated Vulnerability Assessment Tool Development

1. Project / Research Summary

This project focuses on researching and analyzing automated vulnerability assessment tools used to identify and evaluate security weaknesses in networks and applications. The goal is to understand how automation improves vulnerability detection, accuracy, and efficiency while reducing manual testing workloads. By studying and testing open-source tools like OWASP Nettacker and ProjectDiscovery Nuclei, I aim to compare their design, performance, and usability.

At the end of the project, I will deliver a research report detailing findings, tool comparisons, and recommendations for building or enhancing automated vulnerability assessment systems.

---

2. Project Approach

- What I Will Do:
    - Analyze existing open-source vulnerability scanners to understand automated detection workflows.
    - Conduct limited hands-on testing using selected tools.
    - Evaluate the strengths, weaknesses, and scalability of each solution.
- Tools / Languages / Platforms:
    - Tools: OWASP Nettacker, ProjectDiscovery Nuclei
    - Languages: Python, YAML (for Nuclei templates)
    - Platforms: Kali Linux / Ubuntu VM environment
    - Supporting Tools: Docker (for setup), ChatGPT (for analysis and documentation support)
- Starting Point:
    - I will not build from scratch; instead, I'll use existing GitHub projects as research baselines to analyze architecture, automation, and accuracy.

- AI Tool Usage:
    - Use ChatGPT to summarize findings, structure reports, and refine technical writing.
    - Optionally generate testing checklists or compare tool outputs automatically.

---

3. Three Clear Goals

- Ambitious Goal:

  Prototype a simple vulnerability scanning workflow that combines Nuclei and Nettacker results into a unified reporting format.

- Realistic Goal:

  Fully analyze and document both tools, including hands-on tests and a comparative evaluation of automation features and limitations.

- Minimum Goal:

  Deliver a well-organized research paper explaining how automated vulnerability assessment tools function and their impact on modern cybersecurity testing.

---

4. Four-Week Timeline

Week 1 – Get Started and Make Progress

- Install Nettacker and Nuclei in a test environment.
- Review documentation, dependencies, and community usage.
- Begin literature review on automated vulnerability assessment.
- Deliverable: Environment setup complete; annotated list of academic and GitHub sources.

Week 2 – Push Forward

- Run both tools on a small controlled target (local or lab setup).
- Record performance, findings, and scan accuracy.
- Draft comparison notes and outline research sections.
- Deliverable: Initial tool testing results and partial analysis draft.

Week 3 – Finish and Polish

- Complete detailed tool evaluation and finalize comparisons.
- Identify automation challenges (false positives, scalability).
- Begin full report writing and integrate supporting sources.
- Deliverable: Full research draft with analysis and discussion.

Week 4 – Finalize Everything

- Proofread and finalize research report in APA format.
- Prepare a short presentation or summary slides.
- Double-check references, test results, and formatting.
- Deliverable: Completed research paper and final presentation materials.