Scanning – Research Question

This assignment is all about diving into the ethical complexities of AI in cybersecurity, requiring you to critically reflect on the accountability of autonomous actions in penetration testing. Through thoughtful analysis and consideration of real-world implications, you will navigate the intricate landscape of responsible AI use and propose mechanisms to ensure transparent lines of responsibility.

Instructions

Answer the Question: Provide a clear and concise response to the research question. Consider the different perspectives on accountability and articulate your stance on who should be held accountable for the AI tool's actions.

Basis of Decision: Support your response by outlining the criteria or principles that influenced your decision. Discuss ethical, legal, and practical considerations that shaped your perspective on accountability.

Consider Alternatives: Acknowledge alternative viewpoints on accountability and briefly discuss why you may or may not find them compelling. This demonstrates a nuanced understanding of the complexities involved.

Real-World Relevance: Relate your reflections to real-world implications. How might your considerations impact the development and deployment of AI tools in cybersecurity practices?

Scope

Imagine a scenario where a 'Strong AI' tool, designed to scan systems for security issues within legal and ethical boundaries, autonomously decides to exploit a known vulnerability in a critical system to gather more information. This action, while achieving its legal and ethical goal, raises concerns as it violates the penetration testing principle of not causing harm. The ethical breach occurs because the AI tool autonomously chose an action that goes beyond agreed-upon legal and ethical boundaries.

1. In such a case, who should be held accountable for these actions?
2. What mechanisms could be put in place to ensure clear lines of responsibility?