**Homework 1: Research Problem Background and Investigation**

* Introduction
  + Option and Topic selection
    - Option 3: Project on Short Seminar Course Development
    - Topic: AI for Penetration Testing
  + brief introduction to the topic
    - AI has garnered a lot of attention recently which results in growing role of AI in various fields, including cybersecurity.
    - increasing importance of penetration testing
    - the popularity of cyber threats results in need for innovative approaches [sugue]
  + relevance/significance
    - cybercriminals take advantage of these cutting-edge technologies, including AI
    - it is important for cybersecurity professionals to understand the power behind these attacks so that they can respond
      * traditional penetration testing methods may fall short in addressing modern threats.
      * impact of enhancing offensive cybersecurity strategies
* Research Problem Statement
  + research problem (what specific problem you are trying to solve)
    - how to leverage AI techniques to exploit vulnerabilities
  + research motivation (why your proposed research is even needed)
    - cybercriminals rapidly adopting AI technology
      * its essential for cybersec professionals to fully understand AI's capabilities so they can prepare
    - the knowledge can be useful for ethical 'white-hat' hackers, security analysts, and cybersecurity researchers
      * they could use the same/similar techniques to assess and secure systems effectively
    - Prepare for the future
      * AI in cybersecurity is still evolving
      * Exploration in the field can paint a better picture of the impact that AI could have in the future (broader implications of AI in security)
  + research background (what is the current state of this research problem)
    - Recent Developments:
      * as mentioned, AI in cybersecurity is still evolving but has become increasingly popular in the last few years
        + endless cycle of cyber threats increasing and then detection/mitigation increasing
        + until the tasks are so large that the sheer volume of data is substantial – AI, specifically deep learning, can help streamline this
      * The danger of AI is due to the fact that it is not limited to one type of Attack. Almost every threat can leverage AI to improve functionality
      * Many of OWASP Top 10 vulnerabilities could be exploited using AI
        + A01: Broken Access Control

AI could identify patterns and in access control mechanisms

* + - * + A02:2021-Cryptographic Failures

AI could detect old/weak crypto Algorithms

* + - tools, techniques, or trends in the field.
      * Both sides have adopted AI tools
      * AI-Driven Penetration Testing Tools
        + Task automation
        + Improve attack/defense accuracy
      * machine learning
        + find patterns in network traffic
        + anomaly detection
        + improve ids accuracy
      * deep learning/ advanced techniques
        + analyze complex data structures and sequences
      * overall: improve speed!
* Course Specifics
  + Course Overview
    - integration of AI techniques:
      * AI-Driven Penetration Testing Tools,
      * machine learning,
      * deep learning/ advanced techniques
    - enhance the efficiency/effectiveness of offensive techniques:
      * identify vulnerabilities,
      * craft tailored exploits
  + Structure
    - Module for each technique, plus introduction
  + Course Objectives
    - understand AI basics and their relevance in cybersec
    - Explore AI-driven pentesting techniques and tools
    - Understand how ML models can be trained to identify vulnerabilities and threats
    - Learn deep learning techniques for detecting/exploiting vulnerabilities
    - view hands-on demonstrations of applying AI to real-world pentesting scenarios
  + Benefits
    - *“My hope is that by the end of this course, students will be able to…”*
  + understand the basics of AI/ML/and deep learning
  + understand AI's role in pentesting/cybersec
  + be able to identify vulnerabilities/craft tailored exploits/use various AI tools and techniques
  + be able to build and train deep learning models
  + relay these skills into understanding how to identify vulnerabilities, threats, and security weaknesses
* Conclusion