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

For my cumulative project in CSC 786 - Cyber Problems, I have selected Option 3, which involves the development of a short seminar course. The central theme of this course will involve leveraging Artificial Intelligence (AI) for penetration testing. Due to the growing prominence of AI technology in recent years, many fields experienced a significant surge in innovative applications and techniques. This is especially true in today's rapidly evolving cybersecurity landscape, whose complex and labor intensive strategies greatly benefit from AI's capabilities. The importance of integrating AI into penetration testing, a linchpin of proactive cybersecurity, lies in its ability to level the playing field, which enables defenders to effectively anticipate and mitigate threats. In my course, I intend to explore these threats comprehensively. This exploration will involve leveraging various AI techniques, such as machine learning and potentially deep learning, and integrating them into the practice of penetration testing.

To accomplish this task, it is important to address a fundamental question: How can AI techniques be effectively harnessed to exploit vulnerabilities in the realm of cybersecurity? Due to its powerful nature, AI has become a popular tool for cybercriminals, who harness cognitive computing to unleash increasingly sophisticated threats. In response, cybersecurity professionals must urgently keep up with the rapid integration of AI, as continued reliance on traditional penetration testing methods may leave them ill-equipped to effectively address these modern threats.

As such, this course could be valuable not only for defenders of cybersecurity but also for ethical "white-hat" hackers, security analysts, and cybersecurity researchers. By providing insight into popular tools and techniques to effectively employ AI, these key players can refine their ability to assess and secure systems efficiently. Additionally, as AI's role continues to evolve, it becomes increasingly important to delve deeper to gain a comprehensive understanding of the future implications of AI as it pertains to security.

Within the current research landscape, the influence of AI is unmistakable. It has created a cyclical pattern, with the propagation of cyber threats followed closely by advancements in detection and mitigation techniques. AI, specifically the deep learning subset, helps streamlines these tasks, especially as they become increasingly complex.

One of the most dangerous facets of AI implementations pertains to its adaptability; almost every threat can leverage it and potentially improve their functionality. This is evident when reviewing the OWASP Top 10 vulnerabilities list which reveals that AI could play a pivotal role in almost all of their exploitations. For example, Broken Access Control (A01) could be exploited by AI by identify patterns and in access control mechanisms and Cryptographic Failures (A02:2021) could be exploited by detecting old or weak cryptographic algorithms.

In the field, both offensive and defensive actors have integrated AI tools into their arsenals. Some of the most popular subsets of AI used are AI-Driven Penetration Testing Tools, machine learning algorithms, and deep learning. AI-driven penetration testing offer task automation and improves the precision of both offensive attacks and defensive strategies. Machine learning, another facet of AI, serves as an instrumental tool in identifying intricate patterns within network traffic, facilitating anomaly detection, and enhancing the accuracy of intrusion detection systems (IDS).

Furthermore, deep learning techniques, along with advanced AI methods, prove invaluable in analyzing complex data structures and sequences. These advancements translate to substantial improvements in processing speed, a critical factor in staying ahead in the dynamic landscape of cybersecurity.

* 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

rotating door/ cyclical pattern

* + - * + 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
  + In this dynamic landscape, embracing AI is no longer just an option - it's a necessity for staying ahead of an ever-evolving adversary