# Introduction

## Background of the Course Topic

* + - a

## Importance and Relevance of the Course Topic

* + - a

# Literature Review

## Research Paper 1: Introduction of Topic

### Details

* + - * Getting pwn’d by AI: Penetration Testing with Large Language Models
      * Andreas Happe, Jürgen Cito
      * [link](https://arxiv.org/pdf/2308.00121.pdf)

### Introduction

* + - * a

### Summary

* + - * a

### Main Findings

* + - * a

### Methodologies

* + - * a

### Relevance to Your Course Content

* + - * a

## Research Paper 2: Pentesting Step 1 - Gathering Information (Module 1)

### Details

* + - * Reinforcement Learning for Intelligent Penetration Testing
      * Mohamed C. Ghanem, Thomas M. Chen
      * [link](https://ieeexplore.ieee.org/document/8611595)

### Introduction

* + - * a

### Summary

* + - * a

### Main Findings

* + - * a

### Methodologies

* + - * a

### Relevance to Your Course Content

* + - * a

## Research Paper 3: Pentesting Step 2 - Scanning (Module 2)

### Details

* + - * Penetration Testing Procedure using Machine Learning
      * Reevan Seelen Jagamogan, Saiful Adli Ismail, Noor Hafizah Hassan, Hafiza Abas
      * [link](https://ieeexplore.ieee.org/document/9870951)

### Introduction

* + - * a

### Summary

* + - * a

### Main Findings

* + - * a

### Methodologies

* + - * a

### Relevance to Your Course Content

* + - * a

## Research Paper 4: Pentesting Step 3 - Exploiting (Module 3)

### Details

* + - * An Intelligent Penetration Test Simulation Environment Construction Method Incorporating Social Engineering Factors
      * Yang Li, Yongjie Wang, Xinli Xiong, Jingye Zhang, Qian Yao
      * [link](https://www.mdpi.com/2076-3417/12/12/6186)

### Introduction

* + - * a

### Summary

* + - * a

### Main Findings

* + - * a

### Methodologies

* + - * a

### Relevance to Your Course Content

* + - * a

## Research Paper 5: Post-Breach/Exploit, Pentesting Steps 4,5, and 6 (Module 4)

### Details

* + - * Automated Post-Breach Penetration Testing through Reinforcement Learning
      * Sujita Chaudhary, Austin O’Brien, Shengjie Xu
      * [link](https://ieeexplore.ieee.org/document/9162301)

### Introduction

* + - * a

### Summary

* + - * a

### Main Findings

* + - * a

### Methodologies

* + - * a

### Relevance to Your Course Content

* + - * a

# Incorporation of Findings into the Course

## Discussion on how the findings from the literature review inform your course development.

* + - a

## Preliminary Ideas for Course Content based on the Literature Review

* + - a

# Table of Contents for the Course

## Module 1: Introduction to AI and ML in Penetration Testing

### Module Overview and Brief Description

* + - * Module 1, comprised of "Introduction to AI and ML in Penetration Testing" and "Gathering Information and Reconnaissance with AI," serves as the foundation for the course. It offers participants an in-depth introduction to the role of Artificial Intelligence (AI) and Machine Learning (ML) in the field of penetration testing. This module introduces the first step of the Penetration Testing process, Gathering Information. Through these submodules, participants will gain a comprehensive understanding of key concepts, ethical considerations, and the terminology essential for the course.

### Submodule 1.1: Introduction to AI and ML in Penetration Testing

* + - * Overview of the Course
      * Overview of Penetration Testing
        + Pentest steps/phases
      * Overview of AI
      * Overview of Machine Learning
        + Deep Learning
      * Examine Ethical Considerations
        + Discuss Ethical challenges
        + Responsible/ lawful use of AI for security assessments
      * Key concepts and terminology
        + threats, vulnerability, exploits, AI, penetration testing, Machine Learning …

### Submodule 1.2: Gathering Information and Reconnaissance with AI

* + - * Introduction to Phase 1: Gathering Information
      * Use of AI-Driven Tools for Information Gathering
        + Shodan and Censys (“Asset Discovery”)
      * Machine Learning in Data Collection and Analysis
      * Ethical Considerations in Information Gathering
      * Demonstration: Gathering Information with AI

## Module 2: Machine Learning for Vulnerability Assessment

### Module Overview and Brief Description

* + - * Module 2, consisting of "Scanning and Vulnerability Assessment with ML" and "Exploiting and AI-Enhanced Techniques," focuses on utilizing Machine Learning (ML) in the context of vulnerability assessment during penetration testing. This module offers participants an in-depth exploration of Penetration Testing Phases 2, Scanning and Phase, and 3, Exploitation. By highlighting the role of AI and ML in these critical phases, participants will learn about AI-powered vulnerability scanners, data collection and preprocessing techniques, exploit development with ML, and practical vulnerability assessment exercises.

### Submodule 2.1: Scanning and Vulnerability Assessment with ML

* + - * Introduction to Phase 2: Scanning
      * Using Machine Learning for Vulnerability Assessment
      * AI-Powered Vulnerability Scanners
      * Data Collection and Preprocessing for ML
        + NLP
      * Practical Exercise: Vulnerability Assessment with ML

### Submodule 2.2: Exploiting and AI-Enhanced Techniques

* + - * Introduction to Phase 3: Exploitation
      * AI-Driven Exploitation Tools and Frameworks
      * Machine Learning for Exploit Development
      * Real-World Examples of AI-Enhanced Exploits
      * Demonstration: AI-Powered Exploitation

## Module 3: Post-Exploitation AI and ML Techniques

### Module Overview and Brief Description

* + - * Module 3, "Post-Exploitation AI and ML Techniques," delves into the advanced phases of penetration testing, Maintaining Connection, Covering Tracks, and Reporting. By highlighting the role of AI and ML in these critical post-exploitation phases, participants will gain insights into enhancing evasion techniques, streamlining reporting and documentation through AI-generated reports, and applying advanced AI-enhanced post-exploitation and privilege escalation strategies. This module equips participants with advanced skills and insights into the transformative power of AI and ML in post-exploitation scenarios, enhancing their ability to navigate and assess cybersecurity landscapes effectively.

### Submodule 3.1: Maintaining Connection, Covering Tracks, and Reporting

* + - * Overview of Maintaining Connection and Covering Tracks
      * Role of AI and ML in Evasion and Stealth Techniques
      * Reporting and Documentation with AI-Generated Reports
      * Practical Exercise: Maintaining Connection and Covering Tracks with AI

### Submodule 3.2: AI-Enhanced Post-Exploitation and Privilege Escalation

* + - * Techniques for Post-Exploitation with AI
      * AI-Driven Privilege Escalation Strategies
      * Realistic Scenario Simulations with AI
      * Demonstration:

## Module 4: Deep Learning and Advanced Techniques

### Module Overview and Brief Description

* + - * Module 4, "Deep Learning and Advanced Techniques," concludes the course, focusing on cutting-edge topics in penetration testing. Participants will explore the potential of Deep Learning, AI, and ML in advanced penetration testing techniques. This module wraps up the course by revisiting key concepts, exploring future trends in AI and ML within penetration testing, and offering additional insights and suggested references for further exploration in this dynamic field.

### Submodule 4.1: Deep Learning and Advanced Techniques

* + - * Introduction to Deep Learning
      * Deep Learning Applications in Penetration Testing
      * Advanced AI-Enhanced Techniques
      * Machine Learning for Zero-Day Exploits
      * AI-Driven Red Team Operations
      * Demonstration:

### Submodule 4.2: Review/Conclusion

* + - * Review Key Concepts
      * Future Trends in AI and ML in Penetration Testing
      * Additional Insights
        + Discuss References and Further Reading

## References and Further Reading

* + - a

# Key Components of the Newly Developed Course

## Learning Objectives

* + - *outline what students should be able to achieve or demonstrate by the end of the course*
    - Understand fundamental concepts of pentesting, AI, and ML
    - Understand penetration testing phases
    - Familiarity with various pentesting tools

## Target Audience

* + - *group of individuals or professionals for whom the course is designed*

## Assessment Strategies

* + - *how students' knowledge and skills will be evaluated and measured throughout the course*
    - A quiz at the end of each module to test for understanding
    - Assorted practical exercises

## Supplementary Materials

* + - *“description of what you intend to include in your future final deliverable”*
    - reading materials
      * e.g., online technical blogs, articles, whitepapers
      * about any topics, tools, and related concepts mentioned
    - official tutorials of some
      * software and/or hardware tools mentioned/ used

# Conclusion

## Summary of Key Insights

* + - a

## Potential Impact of the Course

* + - a

# References

# Additional Facts

* + “cybercriminals are increasingly doubling the effectiveness of their attack tools for half the cost every few months”
    - <https://ieeexplore.ieee.org/abstract/document/8963730>

# Additional Resources to Consider

* + Reinforcing Penetration Testing Using AI
    - <https://ieeexplore.ieee.org/abstract/document/9843459>
  + Reinforcement Learning for Intelligent Penetration Testing
    - <https://ieeexplore.ieee.org/document/8611595>
  + Survey On The Applications Of Artificial Intelligence In Cyber Security \*\*
    - https://www.researchgate.net/profile/Aaron-Achi/publication/355119649\_Survey\_On\_The\_Applications\_Of\_Artificial\_Intelligence\_In\_Cyber\_Security/links/623c6b5991e0810f44d62f22/Survey-On-The-Applications-Of-Artificial-Intelligence-In-Cyber-Security.pdf