INTRODUCTION TO AI AND ML IN PENETRATION TESTING

Harnessing Artificial Intelligence for Penetration Testing

COURSE OVERVIEW

goals

Explore	Explore Artificial Intelligence, Machine Learning, and Penetration Testing
Engage	Actively Engage with Automated Tools
Reflect	Reflect on Ethical Considerations
Examine	Examine the Broader Implications of AI
Encourage	Encourage Critical and Creative Thinking

COURSE OVERVIEW

general outline

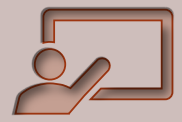
Module 1	Introduction to AI and ML in Penetration Testing
Module 2	Machine Learning for Vulnerability Assessment
Module 3	Post-Exploitation AI and ML Techniques
Module 4	Deep Learning and Advanced Techniques

COURSE OVERVIEW

assessment strategies

Reflective Questions

Capture The Flag / Practical Exercises



Final Seminar Project

PENETRATION TESTING

"A method of evaluating the security of computer systems or networks by simulating an attack by a malicious individual" [1]

- Uncover Weak Points
- Understand Potential Attack Scenarios
- Analyze Vulnerability Severity

PENETRATION TESTING

- Splunk
  - Log Management
  - Historical Analysis
  - Reporting and Documentation Features
  - So Much More!
- Phases
  - Preparation
  - Implementation
  - Analysis

PENETRATION TESTING

- Phases
  - Gather Information
  - Scanning — *Preparation*
  - Exploitation — *Implementation*
  - Maintaining Access
  - Covering Tracks
  - Reporting and Documentation — *Analysis*

MACHINE LEARNING

Develop Algorithms that Mimic 'Human Cognition' Abilities to Solve Complex Problems without Explicit Programming

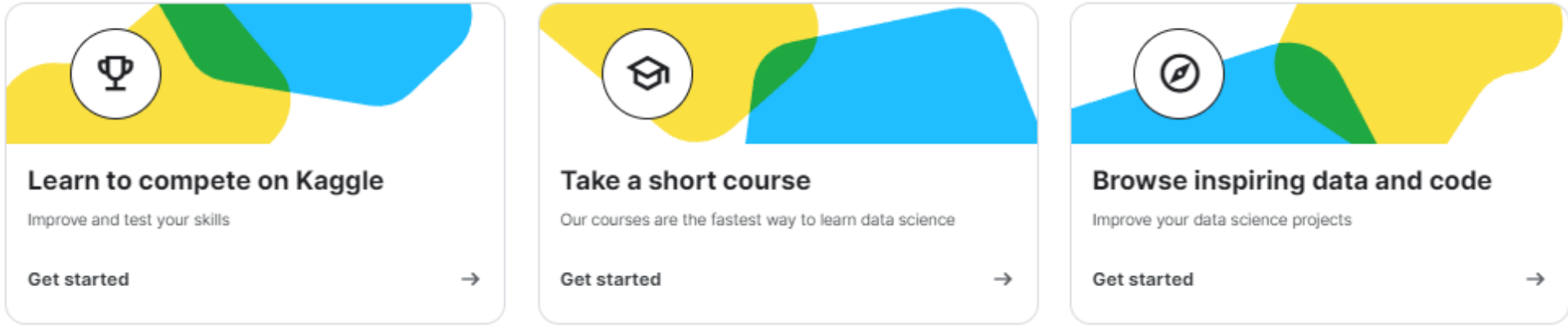
MACHINE LEARNING

- Supervised Learning
  - Predict New Data from Labeled Data
  - Prediction, Classification
- Unsupervised Learning
  - Predict New Data from Patterns in Unlabeled Data
  - Pattern Recognition, Clustering

MACHINE LEARNING

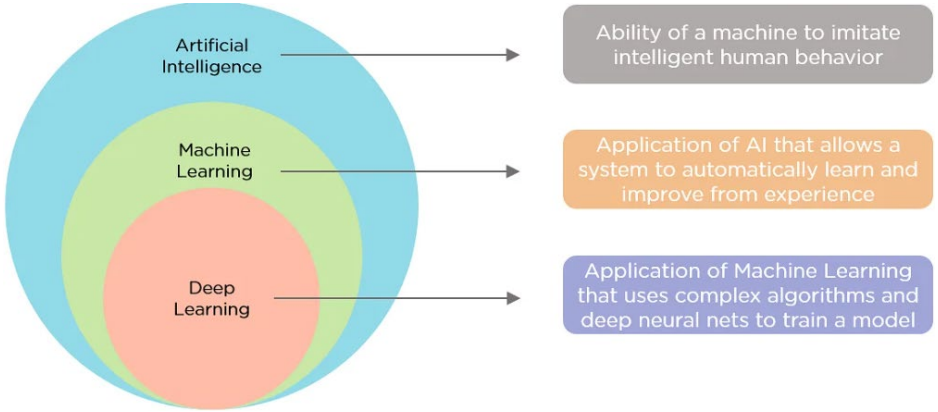
- Reinforcement Learning
  - Autonomously learns through Action And Reward
  - Maximizes Cumulative Rewards Over Time
  - Q-Learning
  - Deep Q-Learning

www.Kaggle.com



ARTIFICIAL INTELLIGENCE

The Creation of Machines to Mimic Intelligent Human Behavior



- Weak (Narrow) AI
  - Single Task
  - Siri, Alexa, Image Recognition, LLM
- Strong (General) AI
  - Meet or Surpass Human Intelligence
  - Theoretical

AUTOMATED PT

overview

- Constantly Evolving Threats
- Modern Network Complexity
  - IoT
  - The Cloud
  - BYoD/ Remote Work
- Critical Shortage of Cybersecurity Experts
  - Reduce Workload
  - Address Understaffed/trained
  - Minimize human Errors
- Traditional PT Methods Fall Short
  - Manual
  - Repetitive

AUTOMATED PT

information gathering

- Automate Data Collection
- Target Profiling
- Identifying Assets
- Predicting Vulnerabilities
- Examples
  - Natural Language Processing (NLP)
  - Reinforcement Learning (RL)

AUTOMATED PT

scanning

- Continuous Monitoring
- Prioritization
- GyoiThon
  - Collect Data from Target URLs

AUTOMATED PT

exploitation

- Traditional Methods
  - Rigid
  - Exhaustive
  - Resource Intensive
- Real-Time Adaptability
  - Reinforcement Learning
  - Experience Replay
- Social Engineering
  - Phishing
  - Large Language Model (LLM)

AUTOMATED PT

post-exploitation

- Counteract Detection and Mitigation
  - Emulates Normal Network Traffic Patterns
  - Counteracts Anomaly Detection
  - Erases Log Files To Cover Tracks
- Report Generation

RESEARCH QUESTION

What are some key advantages of using AI in the information gathering phase, and how does it enhance the accuracy and efficiency of the process?

REFERENCES

1) S. Watts , Penetration Testing: Practical Introduction & Tutorials, 2022.
2) "Market Research Report," Fortune Business Insights, 2022.
3) Market Research Report, MarketsandMarkets, 2022.
4) H. M. Z. A. Shebli and B. D. Beheshti, "A study on penetration testing process and tools," in Long Island Systems, Applications and Technology Conference (LISAT), Farmingdale, 2018.
5) N. Duggal, What is Artificial Intelligence: Types, History, and Future, 2023.
6) S. Shah and B. M. Mehtre , "An overview of vulnerability assessment and penetration testing techniques," Journal of Computer Virology and Hacking Techniques, pp. 27-49, 18 November 2014.
7) S. Morgan, Cybersecurity Jobs Report: 3.5 Million Unfilled Positions In 2025, Sausality, California, 2023.
8) N. Kühl, M. Schemmer, . M. Goutier and G. Sat, Artificial intelligence and machine learning, 2022, pp. 2235-2244.
9) S. Morgan, 2023 Cybersecurity Almanac: 100 Facts, Figures, Predictions, And Statistics, Sausality, California, 2023.
10) A. Almajali, . L. Al-Abed, R. Mutleq, Z. Samamah, A. Issa Abu Shhadeh, B. Jamil Mohd and K. M. Ahmad Yousef , "Vulnerability Exploitation Using Reinforcement Learning," in Jordan International Joint Conference Electrical Engineering and Information Technology, 2023.