AI+ Ethical Hacker™

Duration: 40 hours

Course Overview

The AI+ Ethical Hacker certification delves into the intersection of cybersecurity and artificial intelligence, a pivotal juncture in our era of rapid technological progress. Tailored for budding ethical hackers and cybersecurity experts, it offers comprehensive insights into AI's transformative impact on digital offense and defense strategies. Unlike conventional ethical hacking courses, this program harnesses AI's power to enhance cybersecurity approaches. It caters to tech enthusiasts eager to master the fusion of cutting-edge AI methods with ethical hacking practices amidst the swiftly evolving digital landscape. The curriculum encompasses four key areas, from course objectives and prerequisites to anticipated job roles and the latest AI technologies in Ethical Hacking.

Course Prerequisites

- Programming Proficiency: Knowledge of Python, Java, C++, etc for automation and scripting.
- Networking Fundamentals: Understanding of networking protocols, subnetting, firewalls, and routing.
- Operating Systems Knowledge: Proficiency in using Windows and Linux operating systems.
- Cybersecurity Basics: Familiarity with fundamental cybersecurity concepts, including encryption, authentication, access controls, and security protocols
- Machine Learning Basics: Understanding of machine learning concepts, algorithms, and basic implementation.
- Web Technologies: Understanding of web technologies, including HTTP/HTTPS protocols, and web servers.

Course Agenda

Module 1: Foundation of Ethical Hacking Using Artificial Intelligence (AI)

- Introduction to Ethical Hacking
- Ethical Hacking Methodology
- Legal and Regulatory Framework
- Hacker Types and Motivations
- Information Gathering Techniques
- Footprinting and Reconnaissance

- Scanning Networks
- Enumeration Techniques

Module 2: Introduction to AI in Ethical Hacking

- AI in Ethical Hacking
- Fundamentals of AI
- AI Technologies Overview
- Machine Learning in Cybersecurity
- Natural Language Processing (NLP) for Cybersecurity
- Deep Learning for Threat Detection
- Adversarial Machine Learning in Cybersecurity
- AI-Driven Threat Intelligence Platforms
- Cybersecurity Automation with AI

Module 3: AI Tools and Technologies in Ethical Hacking

- AI-based Threat Detection Tools
- Machine Learning Frameworks for Ethical Hacking
- AI-Enhanced Penetration Testing Tools
- Behavioral Analysis Tools for Anomaly Detection
- AI-Driven Network Security Solutions
- Automated Vulnerability Scanners
- AI in Web Application
- AI for Malware Detection and Analysis
- Cognitive Security Tools

Module 4: AI-Driven Reconnaissance Techniques

- Introduction to Reconnaissance in Ethical Hacking
- Traditional vs. AI-Driven Reconnaissance
- Automated OS Fingerprinting with AI

- AI-Enhanced Port Scanning Techniques
- Machine Learning for Network Mapping
- AI-Driven Social Engineering Reconnaissance
- Machine Learning in OSINT
- AI-Enhanced DNS Enumeration and AI-Driven Target Profiling

Module 5: AI in Vulnerability Assessment and Penetration Testing

- Automated Vulnerability Scanning with AI
- AI-Enhanced Penetration Testing Tools
- Machine Learning for Exploitation Techniques
- Dynamic Application Security Testing (DAST) with AI
- AI-Driven Fuzz Testing
- Adversarial Machine Learning in Penetration Testing
- Automated Report Generation using AI
- AI-Based Threat Modeling
- Challenges and Ethical Considerations in AI-Driven Penetration Testing

Module 6: Machine Learning for Threat Analysis

- Supervised Learning for Threat Detection
- Unsupervised Learning for Anomaly Detection
- Reinforcement Learning for Adaptive Security Measures
- Natural Language Processing (NLP) for Threat Intelligence
- Behavioral Analysis using Machine Learning
- Ensemble Learning for Improved Threat Prediction
- Feature Engineering in Threat Analysis
- Machine Learning in Endpoint Security
- Explainable AI in Threat Analysis

Module 7: Behavioral Analysis and Anomaly Detection for System Hacking

- Behavioral Biometrics for User Authentication
- Machine Learning Models for User Behavior Analysis
- Network Traffic Behavioral Analysis
- Endpoint Behavioral Monitoring
- Time Series Analysis for Anomaly Detection
- Heuristic Approaches to Anomaly Detection
- AI-Driven Threat Hunting
- User and Entity Behavior Analytics (UEBA)
- Challenges and Considerations in Behavioral Analysis

Module 8: AI Enabled Incident Response Systems

- Automated Threat Triage using AI
- Machine Learning for Threat Classification
- Real-time Threat Intelligence Integration
- Predictive Analytics in Incident Response
- AI-Driven Incident Forensics
- Automated Containment and Eradication Strategies
- Behavioral Analysis in Incident Response
- Continuous Improvement through Machine Learning Feedback
- Human-AI Collaboration in Incident Handling

Module 9: AI for Identity and Access Management (IAM)

- AI-Driven User Authentication Techniques
- Behavioral Biometrics for Access Control
- AI-Based Anomaly Detection in IAM
- Dynamic Access Policies with Machine Learning
- AI-Enhanced Privileged Access Management (PAM)
- Continuous Authentication using Machine Learning

- Automated User Provisioning and De-provisioning
- Risk-Based Authentication with AI
- AI in Identity Governance and Administration (IGA)

Module 10: Securing AI Systems

- Adversarial Attacks on AI Models
- Secure Model Training Practices
- Data Privacy in AI Systems
- Secure Deployment of AI Applications
- AI Model Explainability and Interpretability
- Robustness and Resilience in AI
- Secure Transfer and Sharing of AI Models
- Continuous Monitoring and Threat Detection for AI

Module 11: Ethics in AI and Cybersecurity

- Ethical Decision-Making in Cybersecurity
- Bias and Fairness in AI Algorithms
- Transparency and Explainability in AI Systems
- Privacy Concerns in AI-Driven Cybersecurity
- Accountability and Responsibility in AI Security
- Ethics of Threat Intelligence Sharing
- Human Rights and AI in Cybersecurity
- Regulatory Compliance and Ethical Standards
- Ethical Hacking and Responsible Disclosure

Module 12: Capstone Project

- Case Study 1: AI-Enhanced Threat Detection and Response
- Case Study 2: Ethical Hacking with AI Integration
- Case Study 3: AI in Identity and Access Management (IAM)

- Case Study 4: Secure Deployment of AI Systems