AI RED TEAMER IN CYBER SECURITY

Certificate of Completion: AI Red Teamer in Cyber Security

Course Code: IT_HM_I_007/25

Duration: 40 Hours

Delivery Format: Hybrid

Target Audience:

This course is specifically designed for students who:

- Are pursuing or have completed degrees in Computer Science, Cybersecurity, Information Technology, or related fields.
- Have a foundational understanding of computer networking, operating systems, and basic cybersecurity principles.
- Possess an interest in specializing in the intersection of AI and cybersecurity.
- Aspire to develop skills in ethical hacking, penetration testing, and AI vulnerability assessment.
- Are keen to learn practical skills in using cybersecurity tools and programming languages (like Python) for security analysis and AI model manipulation.

Program Objectives:

- Understand fundamental cybersecurity principles and threats.
- Learn the basics of AI and machine learning and their application in cybersecurity.
- Apply AI techniques for threat detection, malware analysis, and network security.
- Utilize AI for security analytics, SIEM systems, and risk assessment.
- Address the ethical and legal challenges of AI in cybersecurity.
- Develop AI-powered cybersecurity solutions.

Detailed Syllabus

Module 1 (8 hours): Introduction to Cybersecurity

Objective: To provide a foundation in cybersecurity concepts, threats, and tools.

Session 1 (4 hours): Basics of Cybersecurity

Topics:

- What is Cybersecurity? - Definitions, importance, and current landscape
- Types of Cybersecurity Threats - Malware, phishing, ransomware, APTS, DDoS
- Security Fundamentals - Confidentiality, Integrity, Availability (CIA Triad)
- Defensive Security Layers - Perimeter defense, network security, endpoint security
- Regulatory and Compliance Frameworks - GDPR, HIPAA, NIST, ISO 27001

Activities:

- Mini-Project: Cyber Threat Report - Analyze and report on a real-world cybersecurity incident.

Session 2 (4 hours): Cybersecurity Tools & Techniques

Topics:

- Common Security Tools - Firewalls, IDS/IPS, Antivirus, SIEM tools
- Network Defense Basics - VPNs, proxies, NAT, and encryption
- Endpoint Protection & Incident Response - EDR, malware detection, and forensic analysis

Activities:

- Hands-on Lab: Using Wireshark & Snort for network traffic analysis
- Project: Threat Hunting Challenge - Use Wireshark & Snort to detect an intrusion attempt.

Module 2 (8 hours): Introduction to AI & Machine Learning for Security

Objective: To introduce the basics of AI and machine learning in the context of cybersecurity.

Session 3 (4 hours): Basics of AI & Machine Learning

Topics:

- What is AI & Machine Learning? - Overview of key concepts and terminology
- Types of Machine Learning - Supervised, unsupervised, reinforcement learning
- Common AI Algorithms - Decision trees, KNN, SVM, neural networks
- Hands-on with AI Tools - Python, TensorFlow, Scikit-learn, Keras

Activities:

- Mini Coding Task: Write a simple Python script to classify spam emails using Scikit-learn.

Session 4 (4 hours): AI in Cybersecurity & Data Protection

Topics

- AI in Threat Detection – AI-driven malware analysis, anomaly detection
- AI and Encryption - AI-enhanced cryptographic techniques
- AI for Fraud Prevention and Behavioural Analytics
- Challenges of AI in Security - AI bias, adversarial AI attacks

Activities:

- Project: Anomaly Detection with AI - Build a basic anomaly detection model using Python & Scikit-learn.

Module 3 (8 hours): Security Principles & Architecture

Objective: To establish fundamental security principles and understand security models and frameworks.

Session 5 (4 Hours): Security Models and Frameworks

Topics:

- The CIA Triad in Practice - Implementing security principles
- Risk Management Framework (RMF) - Identifying and mitigating risks
- Security Control Frameworks - NIST, ISO 27001, COBIT
- Cloud & IoT Security - Challenges in securing cloud and IoT environments

Activities:

- Project: AI for Risk Assessment - Use AI tools to classify security risks based on severity.

Session 6 (4 Hours): Network Security & Hands-on Labs

Topics:

- Network Security Basics - Routers, switches, firewalls
- Principles of Network Defense - Defense in depth, least privilege
- Network Security Protocols - TCP/IP, VPN, SSL/TLS

Activities:

- Hands-on Lab: Configure a Firewall using pfSense
- Project: Simulating a Cyber Attack - Use Kali Linux & Metasploit to test network security.

Module 4 (8 hours): Advanced AI-Powered Cybersecurity

Objective: To delve into advanced AI techniques and their application in specific cybersecurity domains.

Session 7 (4 Hours): Deep Learning in Cybersecurity

Topics:

- Introduction to Deep Learning - Neural networks, CNNs, RNNs
- AI for Malware Classification - Using deep learning to detect threats
- Adversarial AI Attacks - Focusing AI-based security systems

Activities:

- Hands-on: Running a pre-trained deep learning model for malware detection
- Project: Deep Learning for Phishing Detection - Train an AI model to classify phishing emails.

Session 8 (4 Hours): AI for Security Analytics & SIEM

Topics:

- What is SIEM? - Security Information & Event Management
- Integrating AI into SIEM Systems - AI-driven threat detection
- Predictive Analytics for Cybersecurity - Risk assessment with AI

Activities:

- Hands-on: Using Splunk or IBM QRadar for threat analytics
- Project: Building an AI-Based SIEM Alert System - Implement a basic alerting system using AI.

Module 5 (4 hours): Ethics & Legal Challenges of AI in Cybersecurity

Objective: To address the ethical and legal considerations of using AI in cybersecurity.

Session 9 (4 Hours): Ethics & Compliance in AI Cybersecurity

Topics:

- Ethical Dilemmas in AI & Cybersecurity - Privacy, surveillance, AI bias
- Legal Challenges in AI Cybersecurity - Compliance & liability issues
- Cybersecurity Laws & Regulations - GDPR, CCPA, AI governance
- Case Studies - Real-world security failures and ethical concerns

Activities:

- Project: AI Ethics Case Study - Analyze a controversial AI security incident and propose solutions.

Module 6 (4 hours): Capstone Project - AI-Powered Cybersecurity Solution

Objective: To develop a final AI-powered cybersecurity solution.

Activities:

Final Project: Develop an AI-Powered Security Solution

- Choose an area (Threat detection, fraud prevention, anomaly detection)
- Train a simple AI model in Python for threat detection or risk assessment
- Deploy and test the model using real or simulated security logs
- Present findings and demonstrate effectiveness

Learning Objectives

By the end of this course, learners should be able to:

- Explain fundamental concepts of Artificial Intelligence (AI) and Machine Learning (ML) and their specific applications within the cybersecurity domain.
- Identify and describe various threats and vulnerabilities that are unique to AI and ML systems, such as adversarial attacks and data poisoning.
- Apply the principles and techniques of red teaming to evaluate the security of AI-powered systems.
- Design and execute basic simulated attacks against AI systems to identify potential weaknesses and vulnerabilities.
- Analyze the results of simulated attacks and other evaluations to assess the overall security posture of AI systems.