AI-Powered Cybersecurity:

Advanced Training for Modern Threats

Duration: 40 hours (5 days)

Module 1: Foundations of AI and Cybersecurity

1. **Introduction to AI in Cybersecurity:**
   - Key concepts: AI, ML, and DL in cybersecurity.
   - Types of AI systems (rule-based, supervised, unsupervised, and reinforcement learning).
   - Differences between traditional cybersecurity and AI-driven approaches.
2. **Role of AI in Cybersecurity Domains:**
   - Threat detection and response.
   - Predictive analytics for attack prevention.
   - Behavioural analysis and anomaly detection.
3. **AI in Network Traffic Analysis:**
   - Common attacks detectable via AI (DDoS, spoofing, port scans).
   - Features extraction for network traffic using packet analysers (e.g., Wireshark).
4. **Hands-On Lab:**
   - Setting up a network traffic dataset.
   - Preprocessing the data for training AI models using Python and pandas.

Module 2: Machine Learning for Threat Detection

1. **Supervised Learning in Cybersecurity:**
   - Training classifiers to detect malware, phishing, and fraud.
   - Using decision trees, random forests, and support vector machines (SVM).
2. **Unsupervised Learning:**

- Clustering techniques for anomaly detection.
- Applications in insider threat detection and zero-day attack identification.

3. **Data Preparation for ML Models:**
   - Handling imbalanced datasets (e.g., oversampling with SMOTE).
   - Feature selection using mutual information or principal component analysis (PCA).
4. **Hands-On Lab:**
   - Build a supervised ML model for intrusion detection using a public dataset (e.g., KDDCup99 or UNSW-NB15).
   - Implement a clustering algorithm (e.g., K-means) for anomaly detection.

Module 3: Advanced Deep Learning Applications in Cybersecurity

1. **Deep Learning Fundamentals for Cybersecurity:**
   - Architectures: Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), and Transformers.
   - How deep learning enhances malware detection and email classification.
2. **AI for Endpoint Security and Fraud Detection:**
   - Endpoint vulnerability detection using DL models.
   - Fraud detection techniques with recurrent models.
3. **Phishing Email Detection with Natural Language Processing (NLP):**
   - Using pretrained NLP models (e.g., BERT, GPT) for phishing classification.
   - Tokenization and text vectorization for cybersecurity datasets.
4. **Hands-On Lab:**
   - Train and fine-tune a neural network for phishing detection.
   - Use a malware dataset to train a CNN for malware classification.

Module 4: Securing AI Systems and Ethical Hacking with AI

1. **AI Vulnerabilities and Adversarial Attacks:**
   - Types of attacks on AI models (e.g., poisoning, evasion).

- Adversarial examples and how attackers exploit AI systems.

2. **Techniques to Secure AI Models:**
    - Defensive distillation and adversarial training.
    - Role of explainable AI (XAI) in improving model robustness.
3. **Using AI for Penetration Testing:**
    - AI-driven tools for vulnerability scanning and exploitation (e.g., Metasploit with ML extensions).
    - Predicting attack vectors using AI models.
4. **Hands-On Lab:**
    - Simulate adversarial attacks on a pre-trained AI model and implement mitigation strategies.
    - Conduct AI-powered penetration testing on a virtual environment.

Module 5: Real-World AI Cybersecurity Solutions and Capstone Project

1. **AI Cybersecurity Tools and Frameworks:**
    - Tools like IBM Watson for Cybersecurity, Darktrace, and Splunk with AI modules.
    - Frameworks for building AI models (TensorFlow, PyTorch, Scikit-learn).
2. **Emerging Trends in AI Cybersecurity:**
    - AI in quantum cryptography.
    - The rise of generative AI in crafting and detecting cyber threats.
3. **Capstone Project:**
    - Build an end-to-end AI-based cybersecurity solution:
        - Dataset collection and preprocessing.
        - Model training for anomaly detection.
        - Deploy a proof-of-concept (PoC) in a simulated environment.