AI + Ethical Hacker

Duration: 120Hrs
Days: 20
Exam Code: AT-220

Day 1: Module 1 - Foundations of Ethical Hacking (6 hours)

Module 1: Foundations of Ethical Hacking
• Topic 1.1: Introduction to Ethical Hacking

- Defining Ethical Hacking and its importance
- Knowledge and skill requirements for Ethical hacking
- Types of hackers: white, black, grey hats
- Role and responsibilities of ethical hackers
- Overview of threat landscape
- **Use-cases**
- **Case study**

• Topic 1.2: Legal and Ethical Considerations

- Laws and Regulations: Navigate legal frameworks in Ethical Hacking with AI such as GDPR, HIPAA, Computer Fraud & Abuse Act
- Concepts: Consent, authorization, and disclosure
- Organizational policies and ethical boundaries
- Reporting and Documentation
- Scoping and rules of engagement
- **Use-cases**
- **Case study**

• Topic 1.3: Ethical Hacking Methodology

- Phases of Ethical Hacking: Reconnaissance, Scanning, Gaining Access, Maintaining Access, Covering Tracks
- Importance of Ethical Hacking Phases
- Information Gathering Techniques
- Enumeration Techniques
- Importance & Application of Enumeration Techniques
- **Use-cases**
- **Case study**
- **Hands-on**

✅ **Day 2: Module 2 - Reconnaissance and Footprinting with AI (6 hours)**

Module 2: Reconnaissance and Footprinting with AI

• Topic 2.1: Passive Information Gathering

- Importance of Passive Information Gathering
- Application of Passive Information Gathering
- OSINT tools: Shodan, Maltego
- WHOIS, DNS, social media analysis
- Website mirroring and metadata extraction
- **Use-cases**
- **Case study**
- **Hands-on**

• Topic 2.2: Active Reconnaissance & Footprinting

- Importance of Active Information Gathering
- Application of Active Information Gathering
- DNS enumeration, ping sweeps, traceroutes
- Banner grabbing, service fingerprinting
- AI for pattern recognition in recon data
- **Use-cases**
- **Case study**
- **Hands-on**

• Topic 2.3: Countermeasures and Ethics

- Defense techniques: deception, segmentation
- Ethical boundaries in reconnaissance
- AI-generated risk scores from footprinting
- **Use-cases**
- **Case study**
- **Hands-on**

✅ **Day 3: Module 3 - Supervised Learning for Cybersecurity (6 hours)**

Module 3: Supervised Learning for Cybersecurity

• Topic 3.1: Introduction to Supervised Learning

- Machine Learning (ML) Concepts
- Machine Learning Working Model
- Types of ML Algorithms
- Supervised Learning and its application
- Types of Supervised Learning Algorithms-Classification and regression
- Model types: Decision trees, SVM, Random Forest

- **Use-cases**
- **Case study**
- **Hands-on**

• Topic 3.2: Threat Detection with Supervised Models

- Threat Hunting basic Concepts and its application
- Supervised Models for Email and URL classification
- Supervised Models in anti-virus systems
- Model evaluation (Confusion Matrices, Accuracy, Precision, Recall, MCC, F1-Score, ROC, ROCAUC Curve)
- **Use-cases**
- **Case study**
- **Hands-on**

• Topic 3.3: Model Optimization & Tuning

- Model Optimization and its importance
- Types of Model Optimization techniques-Cross-validation, Grid search
- Overfitting and underfitting
- Regularization
- Hyperparameter tuning techniques
- **Use-cases**
- **Case study**
- **Hands-on**

✅ **Day 4: Module 4 - Unsupervised Learning and Anomaly Detection (6 hours)**

Module 4: Unsupervised Learning and Anomaly Detection

• Topic 4.1: Introduction to Unsupervised Learning

- Unsupervised Learning and its importance
- Application of Unsupervised Learning
- Types of Unsupervised Learning Algorithms
- Clustering algorithms: K-means, DBSCAN
- Dimensionality reduction: PCA, t-SNE
- Data preprocessing techniques
- **Use-cases**
- **Case study**
- **Hands-on**

• Topic 4.2: Anomaly Detection Techniques

- Anomaly Detection Techniques Concepts
- Importance of Anomaly Detection

- Application of Anomaly Detection
- Statistical methods for anomaly detection
- Autoencoders for detecting anomalies
- Threshold setting and evaluation metrics
- **Use-cases**
- **Case study**
- **Hands-on**

• Topic 4.3: Integrating Anomaly Detection in Security Systems

- Real-time anomaly detection systems
- Alert generation and incident response
- Challenges and limitations
- **Use-cases**
- **Case study**
- **Hands-on**

✅ **Day 5: Module 5 - Deep Learning for Cybersecurity (6 hours)**

Module 5: Deep Learning for Cybersecurity

• Topic 5.1: Introduction to Deep Learning

- Neural networks basics
- Deep learning and its importance
- Activation functions and architecture
- Training deep learning models
- **Use-cases**
- **Case study**
- **Hands-on**

• Topic 5.2: Recurrent Neural Networks (RNNs) and Reinforcement Learning in Security

- Understanding RNNs and LSTMs
- Working model of RNNs and LSTMs in security
- Sequence modeling for log analysis
- Understanding Reinforcement Learning and its application in security
- **Use-cases**
- **Case study**
- **Hands-on**

• Topic 5.3: Generative Adversarial Networks (GANs) and Security

- GAN architecture and training
- Importance of GAN
- Types of GANs

- Applications in generating synthetic data
- **Use-cases**
- **Case study**
- **Hands-on**

✅ **Day 6: Module 6 - Network Scanning and Enumeration (6 hours)**

Module 6: Network Scanning and Enumeration
• Topic 6.1: Network Scanning Techniques

- Understanding of Network Scanning
- Importance of Network Scanning
- Types of Network Scanning and their applications
- Types of scans: SYN, UDP, ACK
- Tools: Nmap, Wireshark
- **Use-cases**
- **Case study**
- **Hands-on**

• Topic 6.2: Enumeration Methods

- Understanding Enumeration concepts
- Importance of Enumeration Techniques
- Types of Enumeration techniques and their applications in security
- Banner grabbing and service identification
- SNMP, LDAP, and NetBIOS enumeration
- **Use-cases**
- **Case study**
- **Hands-on**

• Topic 6.3: AI in Scanning and Enumeration

- Automating scanning processes with AI
- Predictive analysis of scan data
- Application of AI in Scanning and Enumeration techniques in security
- **Use-cases**
- **Case study**
- **Hands-on**

✅ **Day 7: Module 7 - Vulnerability Analysis and Exploitation (6 hours)**

Module 7: Vulnerability Analysis and Exploitation

• Topic 7.1: Vulnerability Assessment Tools

- Understanding Vulnerability concepts and its impact
- Understanding Vulnerability Assessment and its importance
- Vulnerability Assessment Tools and its uses
- Interpreting vulnerability reports
- **Use-cases**
- **Case study**
- **Hands-on**

• Topic 7.2: Exploitation Techniques

- Understanding Exploitation Techniques
- Types of Exploitation Techniques
- Exploit frameworks: Metasploit
- Buffer overflows, privilege escalation
- **Use-cases**
- **Case study**
- **Hands-on**

• Topic 7.3: AI in Vulnerability Analysis

- Understanding Vulnerability Analysis
- Predictive modeling for vulnerability prioritization
- Machine learning for zero-day detection
- **Use-cases**
- **Case study**
- **Hands-on**

✅ **Day 8: Module 8 - Web Application Security (6 hours)**

Module 8: Web Application Security

• Topic 8.1: Common Web Vulnerabilities

- Application of AI in Web Application Security
- Web Application Security tools
- SQL injection, XSS, CSRF
- **Use-cases**
- **Case study**
- **Hands-on**

• Topic 8.2: Secure Coding Practices

- Best practices for secure coding to prevent vulnerabilities
- AI technologies assist in code analysis

- Session management and error handling
- **Use-cases**
- **Case study**
- **Hands-on**

• Topic 8.3: AI in Web Security

- Application of AI in Web Security
- Key features of AI in Web Security
- AI for detecting web attacks
- Automated code review using machine learning
- **Use-cases**
- **Case study**
- **Hands-on**

✅ **Day 9: Module 9 - Wireless Network Security (6 hours)**

Module 9: Wireless Network Security
• Topic 9.1: Wireless Network Fundamentals

- Wireless Network Fundamentals
- Importance of Wireless Network Security
- Wi-Fi standards and encryption protocols
- Common wireless attacks: de-authentication, rogue Aps
- **Use-cases**
- **Case study**
- **Hands-on**

✅ **Day 10: Module 10 - AI for Malware and Threat Intelligence** (6 hours)

Module 10: AI for Malware and Threat Intelligence
• Topic 10.1: AI for Malware Detection

- Malware and Threat Intelligence concepts
- Applications of AI in Malware Detection
- AI in Malware Analysis
- Static and dynamic analysis
- Malware signature generation
- AI-driven sandboxing techniques
- **Use-cases**

- **Case study**
- **Hands-on**

• Topic 10.2: Threat Intelligence Automation

- AI enhances predictive threat intelligence
- Automation of threat intelligence processes using machine learning algorithms
- Machine learning in threat data aggregation
- Real-time feed parsing and pattern matching
- Natural language processing for threat reports
- AI in threat hunting and its role
- **Use-case**
- **Case study**
- **Hands-on**

• Topic 10.3: Cognitive Security Tools

- Cognitive Security Tools
- Functionalities of Cognitive Security Tools
- Benefits of Cognitive Security Tools
- Features: automated decision-making, pattern detection
- Integration with SIEM and incident response tools
- **Use-cases**
- **Case study**
- **Hands-on**

✅ **Day 11: Module 11 - AI in Cloud, IoT, and Smart Systems Security (6 hours)**

Module 11: AI in Cloud, IoT, and Smart Systems Security
• Topic 11.1: Securing IoT and Smart Homes

- Securing IoT
- Benefits of Securing IoT and Smart Homes
- Threats to consumer IoT
- Federated learning and privacy
- **Use-cases**
- **Case study**

• Topic 11.2: AI in Cloud Security

- AI in Cloud Security
- Benefits of AI in Cloud Security
- Monitoring cloud workloads with ML
- Detecting misconfigurations in AWS/Azure
- **Use-cases**

- **Case study**
- **Hands-on**

• Topic 11.3: AI for Industrial Systems & Smart Cities

- Application of AI for Industrial Systems & Smart Cities
- Benefits of AI for Industrial Systems & Smart Cities
- AI in SCADA, ICS, and OT
- Secure telemetry with edge AI
- **Use-cases**
- **Case study**

✅ **Day 12: Module 12 - Blockchain and AI Security (6 hours)**

Module 12: Blockchain and AI Security

• Topic 12.1: AI for Fraud Detection in Blockchain

- Fraud Detection
- Application of AI for Fraud Detection
- Benefits of AI for Fraud detection in blockchain
- Detecting anomalous blockchain transactions
- AI in cryptocurrency security
- **Use-cases**
- **Case study**

• Topic 12.2: Smart Contracts & AI Security

- Smart Contracts
- AI-based tools to detect vulnerabilities in smart contracts
- Engineering AI Systems for Malicious Smart Contract Detection
- Detecting malicious logic using ML
- Leveraging AI for Automated Smart Contract Auditing
- **Use-cases**
- **Case study**

• Topic 12.3: AI-Enhanced Consensus & Integrity

- Application of AI techniques to enhance consensus algorithms
- AI-Based Techniques for Improving Consensus Mechanisms
- AI in Proof-of-Stake and Byzantine fault tolerance
- AI and Blockchain for Secure Decision-Making Systems
- **Use-cases**
- **Case study**

✅ **Day 13: Module 13 - Secure AI Design and Adversarial ML (6 hours)**

Module 13: Secure AI Design and Adversarial ML

• Topic 13.1: Adversarial Attacks on AI Models

- Adversarial Attacks and their impact
- Adversarial Attacks on AI Systems
- Detecting and Defending Against Adversarial Attacks
- Adversarial Attacks on AI Systems
- Evasion and poisoning attacks
- Model inversion and extraction
- **Use-cases**
- **Case study**
- **Hands-on**

• Topic 13.2: Defense Mechanisms

- Adversarial training and gradient masking
- Adversarial Training for Model Robustness
- Adversarial Attacks in Phishing Detection and their defense approach
- **Use-cases:**
- **Case study**
- **Hands-on**

• Topic 13.3: Secure AI Engineering Practices

- Secure AI Engineering
- Cryptographic protection of ML models
- Model explainability with SHAP, LIME
- **Use-cases**
- **Case study**
- **Hands-on**

✅ **Day 14: Module 14 - AI in Identity, Access & Behavioral Analytics (6 hours)**

Module 14: AI in IAM & Behavior Analytics

• Topic 14.1: AI-Driven Identity & Access Management (IAM)

- IAM and its benefits
- AI-Driven User Authentication Techniques
- AI-Based Anomaly Detection in IAM
- Implementing AI in IAM
- AI in biometric MFA
- Risk-based authentication models

- **Use-cases**
- **Case study**
- **Hands-on**

• Topic 14.2: UEBA & Behavioral Biometrics

- Fundamentals of UEBA
- UEBA detection techniques
- UEBA Models for Threat Hunting
- Challenges and Considerations in Behavioral Analysis
- **Use-cases**
- **Case study**
- **Hands-on**

• Topic 14.3: Real-Time Threat Profiling

- Threat Profiling
- Threat Profiling techniques
- Real-time behavioral threat scoring
- Real Time AI in Threat profiling
- **Use-cases**:
- **Case study**
- **Hands-on**

✅ **Day 15: Module 15 - AI in Security Testing & DevSecOps (6 hours)**

Module 15: AI in Security Testing & DevSecOps
• Topic 15.1: AI in DAST and SAST

- Applications of AI in DAST
- Benefits of AI in DAST
- AI for Static and Dynamic Application Security Testing
- AI-enhanced static analysis tools
- Real-time vulnerability discovery
- **Use-cases**
- **Case study**
- **Hands-on**

• Topic 15.2: AI for DevSecOps Pipelines

- DevSecOps Pipelines
- Integrating AI into DevSecOps Pipelines
- AI-Driven DevSecOps in Continuous Delivery
- AI in continuous compliance
- **Use-cases**

- **Case study**

• Topic 15.3: Fuzzing and Exploitation with AI

- Fuzzing and Exploitation
- AI fuzzers and test case generation
- ML models in exploit chaining
- Dynamic exploit simulation
- **Use-cases**
- **Case study**

✅ **Day 16: Module 16 - Compliance, Privacy & AI Governance (6 hours)**

Module 16: Compliance, Privacy & AI Governance

• Topic 16.1: Legal & Regulatory Standards

- Understanding Legal & Regulatory Standards
- Importance of Legal and Regulatory Standards
- Regulatory Compliance
- Ethical Standards for AI Security
- **Use-cases**
- **Case study**
- **Hands-on**

• Topic 16.2: Privacy-Preserving AI

- Understanding of Privacy Preserving in AI
- Privacy-preserving threat analytics
- **Use-cases**
- **Case study**

• Topic 16.3: Ethics and Governance in AI Security

- Understanding of Ethics and Governance in AI Security
- Responsible AI principles
- Ethics audit of AI threat model
- Bias, transparency, accountability
- **Use-cases**
- **Case study**
- **Hands-on**

✅ **Day 17: Module 17 - Advanced Threat Detection Architectures (6 hours)**

Module 17: Advanced Threat Detection Architectures

• Topic 17.1: CNNs and RNNs in Intrusion Detection

- CNN and RNN Concepts
- Application of CNN and RNN in security
- CNN for packet inspection
- CNN for encrypted traffic
- RNN/LSTM for sequential pattern detection
- **Use-cases**
- **Case study**
- **Hands-on**

• Topic 17.2: Autoencoders for Anomaly Detection

- Autoencoders basic concepts
- Application of Autoencoders for Anomaly Detection
- Variational autoencoders for rare threats
- Insider threat detection via autoencoder
- Zero-day exploit identification via autoencoder
- **Use-cases**
- **Case study**
- **Hands-on**

• Topic 17.3: AI at the Edge

- IoT anomaly detection at the edge
- Model compression and efficiency
- Lightweight endpoint threat detection
- **Use-cases**
- **Case study**

✅ **Day 18: Module 18 - Red Teaming with AI & AI Threat Simulation (6 hours)**

Module 18: Red Teaming with AI

• Topic 18.1: AI-Powered Edge

- Understanding of Penetration Testing
- Machine Learning in Penetration Testing
- Limitations and Challenges
- AI in Penetration Testing
- AI Red Team vs Blue Team simulation
- Augmenting Penetration Testing with AI
- **Use-cases**
- **Case study**

• Topic 18.2: Adversarial AI Simulation

- Understanding of Adversarial AI
- Types of Adversarial Attacks
- GAN and LLM based threat simulation
- Adversarial AI against AI testing
- Tools for Adversarial AI Attack Simulation
- Red-teaming phishing detection systems
- **Use-cases**
- **Case study**
- **Hands-on**

✅ **Day 19: Module 19 - Capstone Project Engineering (6 hours)**

Module 19: Capstone Project – Engineering AI Systems for Security
• Topic 19.1: Problem Identification and Scope Definition

- Identifying real-world security problems
- Understanding Scope, requirements, and objectives

• Topic 19.2: System Design and Data Engineering

- Selecting datasets
- Understanding and applying EDA
- Understanding Feature engineering & preprocessing

• Topic 19.3: Model Training and Integration

- Identifying and applying Training security models
- Evaluating the Models
- Analyzing the inference or insights

✅ **Day 20: Module 20 - Capstone Project Presentation and Review (6 hours)**

Module 20: Capstone Review & Presentation
• Topic 20.1: Capstone Projects

- Captone Project-1
- Captone Project-2
- Captone Project-3
- Captone Project-4
- Captone Project-5

• Topic 20.2: Project Presentation & Documentation

- Understanding Project Presentation approaches
- Project Presentation
- Final report creation
- Lessons and improvements