1-Week Beginner-Level AI Penetration Testing Training Plan

# Day 1: Understanding AI Security Landscape

Objective: Familiarize participants with the basics of AI and its security challenges.

## Session 1: Introduction to AI and Cybersecurity (2 hours)

Overview of AI in modern systems  
AI in cybersecurity  
Why AI systems need security

## Session 2: Current AI Threat Landscape (2 hours)

Types of threats against AI systems (adversarial attacks, data poisoning, model evasion)  
Real-world case studies on AI security incidents

## Session 3: Understanding AI-Specific Attack Vectors (2 hours)

Differences between traditional and AI system attacks  
Attacks on AI models: evasion, inference, and poisoning  
Vulnerabilities in training data

## Practical Lab: AI Landscape Overview (2 hours)

Case study analysis of AI vulnerabilities  
Review of known AI-related cyber incidents

# Day 2: Basic AI Penetration Testing Fundamentals

Objective: Build foundational knowledge in AI penetration testing techniques.

## Session 1: Introduction to AI Penetration Testing (2 hours)

Understanding the penetration testing process for AI systems  
Tools for AI penetration testing

## Session 2: Threat Modeling for AI Systems (2 hours)

Basics of threat modeling  
Identifying high-risk areas in AI pipelines (data, models, algorithms)

## Session 3: Methodologies for Assessing AI Systems (2 hours)

Differences between assessing traditional vs. AI systems  
Common testing frameworks: OWASP, ATLAS, and ART

## Practical Lab: Setting Up Penetration Testing Environment (2 hours)

Setting up basic testing tools (open-source tools)  
Testing basic AI models for vulnerabilities

# Day 3: Vulnerability Assessment and Exploitation Basics

Objective: Understand how to identify and exploit vulnerabilities in AI models.

## Session 1: Vulnerability Assessment for AI Systems (2 hours)

Identifying and analyzing vulnerabilities in AI models  
Understanding risk analysis for AI models

## Session 2: Common AI Vulnerabilities (2 hours)

Adversarial machine learning attacks  
Vulnerabilities in AI data pipelines

## Session 3: Exploiting AI Vulnerabilities (2 hours)

Basics of AI model exploitation  
Real-world examples of AI vulnerabilities

## Practical Lab: Exploiting AI Models (2 hours)

Performing adversarial attacks on simple machine learning models  
Real-world case study simulations

# Day 4: Securing AI Applications

Objective: Learn how to protect AI systems from common attacks.

## Session 1: Securing AI Applications (2 hours)

Best practices for securing AI systems  
Securing data, model, and application layers

## Session 2: Implementing Defensive Strategies in AI (2 hours)

Defending against adversarial attacks  
Secure development lifecycle for AI models

## Session 3: Data Privacy and AI Security (2 hours)

Understanding how data privacy interacts with AI  
Secure data collection and usage in AI pipelines

## Practical Lab: Securing an AI System (2 hours)

Hands-on labs on how to secure AI model environments  
Securing APIs and data storage in AI applications

# Day 5: Advanced Concepts Introduction

Objective: Transition to advanced AI security techniques to bridge to the next level.

## Session 1: Introduction to AI-Driven Security Countermeasures (2 hours)

Overview of AI-enabled security mechanisms  
Introduction to AI-based anomaly detection and behavioral analysis

## Session 2: AI-Enabled Endpoint Security (2 hours)

How AI can be used for endpoint security and threat detection  
Tools and platforms for AI-driven endpoint security

## Session 3: Introduction to Machine Learning in Cybersecurity (2 hours)

How machine learning is changing the field of cybersecurity  
Examples of machine learning techniques in security

## Practical Lab: Applying AI in Security Systems (2 hours)

Basic setup of machine learning for intrusion detection  
Practical exploration of AI-driven threat analysis tools

# Day 6: Introduction to Automation and AI Tools

Objective: Introduce the concept of automation in AI penetration testing.

## Session 1: Automation in AI Penetration Testing (2 hours)

How automation can assist in AI security testing  
Tools for automated penetration testing of AI systems

## Session 2: Automated AI Exploits and Case Studies (2 hours)

Real-world case studies of automated AI attacks  
Deep learning-based penetration testing tools

## Session 3: Tools for AI Security Audits (2 hours)

Automated security audit tools for AI systems  
Best tools for AI system vulnerability scanning

## Practical Lab: Automating Penetration Testing Tasks (2 hours)

Setting up automated penetration testing for AI applications  
Working with deep exploit and similar tools

# Day 7: Closing, Evaluation, and Transition to Advanced Topics

Objective: Summarize key concepts and introduce participants to advanced topics.

## Session 1: Review of Key Concepts (2 hours)

Summarizing the core principles of AI security and penetration testing  
Key takeaways from vulnerability assessments, exploitation, and defenses

## Session 2: Bridging the Gap to Advanced AI Penetration Testing (2 hours)

Overview of advanced topics (AI-guided penetration testing, quantum CNNs)  
Next steps for further learning

## Session 3: Final Practical Lab and Evaluation (2 hours)

Final practical testing of AI models for vulnerabilities  
Participants work on mini-projects to demonstrate what they've learned

## Closing Evaluation: Knowledge Assessment (2 hours)

Participants complete an evaluation quiz to assess knowledge gained  
Feedback session to tailor future training paths