Document Generated: 06/29/2026

Learning Style: On Demand

Technology: EC-Council

Difficulty: Intermediate

Course Duration: 40 Hours

EC-Council Certified Offensive AI Security Professional (COASP)

About This Course:

The Certified Offensive AI Security Professional (COASP) from EC-Council is an advanced AI security certification designed for cybersecurity professionals, penetration testers, and red team operators. This course equips learners with the

skills to identify, exploit, test, and defend against vulnerabilities in AI systems, Large Language Models (LLMs), and Agentic AI applications

What's Included:

- One-year access to the E-courseware
- Exam Voucher valid for one year
- One-year access to self-paced training videos

Course Objectives:

- Prompt injection and LLM jailbreaking
- Prompt chaining attacks
- AI reconnaissance and attack surface mapping
- AI vulnerability scanning and fuzzing
- Data poisoning attacks
- Model extraction and model theft
- Adversarial machine learning attacks
- Agentic AI attacks (memory corruption, tool misuse, checkpoint manipulation)
- AI infrastructure and supply chain security
- AI security testing and red teaming
- AI incident response and forensics
- OWASP LLM Top 10 and MITRE ATLAS frameworks

Audience:

- Penetration Testers
- Ethical Hackers
- Red Team Operators
- Offensive Security Engineers

- AI Security Analysts
- Threat Hunters
- AI/ML Security Researchers
- DevSecOps Professionals
- Security Architects

Prerequisites:

- EC-Council states that foundational cybersecurity knowledge is required. This is not an entry-level certification and is designed for professionals who already understand cybersecurity fundamentals.

Course Outline:

- Offensive AI & AI System Hacking Methodology
- AI Reconnaissance & Attack Surface Mapping
- AI Vulnerability Scanning & Fuzzing
- LLM Attacks & Exploitation
- Adversarial ML & Model Privacy Attacks
- Agentic AI Security
- AI Workflow Attacks
- AI Infrastructure & Supply Chain Attacks
- AI Security Testing & Hardening
- AI Incident Response & Forensic