

SEC535: Offensive AI – Attack Tools and Techniques™



GOAA
Offensive AI Analyst
giac.org/goaa

3
Day Course

18
CPEs

Laptop
Required

You Will Be Able To

- Engineer AI-Powered Pentesting GPTs
- Perform Patch Diffing with AI-Driven Analysis
- Supercharge OSINT analysis with AI Automation
- Weaponize AI for Social Engineering Attacks
- Craft Custom AI Generated Malware
- Design AI Optimized Exploits

Business Takeaways

- Reduce organizational risk from AI-enabled cyber threats
- Improve detection capabilities against novel attack vectors
- Enhance security team readiness for emerging AI threats
- Protect critical assets from advanced persistent threats
- Strengthen compliance posture for AI security controls
- Create robust security architecture resistant to AI attacks
- Decrease incident response time for AI-powered attacks

Prerequisites

- Students should be comfortable with HTTP APIs and familiar with general web and application security concepts. An AI or ML background is helpful but not required. Python experience is useful for customizing payloads and tooling but is not a prerequisite.

Attackers are already using AI to push past traditional defenses. They automate reconnaissance, craft convincing social engineering campaigns, and even generate custom malware designed to bypass security controls.

This course is built for security professionals who need to understand how offensive teams apply AI at every stage of an attack. Over three days, you'll examine the same tools and techniques adversaries use to map networks, manipulate human targets, and build evasive payloads. Through labs based on real-world scenarios, you'll see firsthand how these tactics unfold and learn to anticipate them. By studying offensive AI through the eyes of the attacker, you will build the insight and hands-on experience needed to outpace these evolving threats and protect what matters most when it counts, while preparing you for the GOAA certification exam.

Preparing for AI-Enabled Cyber Threats

Today's threat landscape is no longer composed of traditional threats. AI-driven attacks have become a reality, and they have shattered the barrier to entry that was keeping so many unsophisticated threat actors at bay. Staying one step ahead of these AI-fueled adversaries hinges on your ability to adopt their tools, tactics, and techniques before they exploit those capabilities against your organization.

SEC535 equips you with practical offensive AI strategies, including bypassing security guardrails, automating reconnaissance, and delivering AI-driven malware. Through immersive labs, you will apply real-world TTPs like deepfake phishing and automated vulnerability discovery to simulate advanced attacks. By adopting the attacker's mindset and mastering cutting-edge techniques, you will stay ahead of evolving threats and fortify your security posture.

Author Statement

"The cyberattack space is evolving, and so should the penetration testers. In this new era of AI-driven attacks it is critical that cybersecurity professionals from blue teams, red teams, and everything in between familiarize themselves with the tactics, techniques, and procedures of these new attackers. In SEC535: Offensive AI we will fully embrace the adversarial mindset as we dive into the dark psychological tricks of social engineering and evaluate how AI can be used to bolster them, as well as looking at automating reconnaissance techniques, using AI for exploit development and utilization, as well as the process of writing novel malware with AI. As a former SANS Institute MSISE program graduate I am proud to return to the SANS ecosystem to give back to an organization that gave so much to me. When I was a cybersecurity instructor previously, I had one simple motto: Knowledge is forged by action. This sentiment was embodied during my time at SANS, and I wanted to make sure I continued that legacy with this course by introducing a large number of labs, all culminating in a massive capture the flag event on the last day of class. I love this area of study, and I'm excited to share that passion and knowledge with all of you."

—Foster Nethercott

Section Descriptions

SECTION 1: Introduction to Offensive AI and Vulnerability Exploitation

Discover how threat actors leverage AI to gather intelligence and exploit vulnerabilities. Students explore advanced OSINT tools enhanced by machine learning, examine RAG-powered penetration testing workflows, and exploit vulnerabilities using AI.

TOPICS:

- Introduction to Artificial Intelligence
- Introduction to AI Models and Capabilities
- OSINT AI For Penetration Testers
- Network Reconnaissance and Vulnerability Exploitation
- Web Exploitation Using AI

SECTION 3: Malware Development and Security Control Evasion

Explore cutting-edge AI applications in malware engineering and defense evasion. Students learn how neural networks transform malware development, grasp how attackers circumvent AI safety guardrails, demonstrate sophisticated evasion techniques powered by machine learning, and examine living-off-the-land tactics enhanced through computational intelligence.

TOPICS:

- Fundamentals of Malware
- Writing Malware with AI
- Hiding, Obscuring, and Trojanizing Persistent Malware
- Agentic Malware
- Bypassing Security Controls

SECTION 2: Social Engineering Attacks

In this section, we'll explore the art of developing convincing phishing content, as well as how to supplement it with both audio and video deepfake content. We will then finish the day by performing patch diffing with AI.

TOPICS:

- Introduction to Social Engineering
- Creating AI-Powered Phishing Emails
- Creating Audio Deepfakes
- Creating Image and Video Deepfakes
- Patch Diffing

Who Should Attend

- Penetration testers
- Red Team operators
- Security consultants
- SOC personnel
- Security architects
- AI and machine learning enthusiasts
- Incident responders
- Security engineers
- Security managers, directors, and CISOs looking to broaden their knowledge in the current attack space



GOAA

Offensive AI Analyst
giac.org/goaa

GIAC Offensive AI Analyst Certification

The GIAC Offensive AI Analyst (GOAA) certification validates ability to apply practical, real-world offensive artificial intelligence techniques to modern cybersecurity challenges. Certified professionals prove their proficiency in applying advanced tactics such as deepfake-enabled phishing, automated vulnerability discovery, and AI-driven attack simulations to emulate sophisticated adversaries.

- AI-powered reconnaissance & OSINT automation
- AI-aided vulnerability discovery, patch diffing, and exploit generation
- Malware development with AI
- Bypassing security controls and guardrails
- Designing and deploying AI-driven phishing
- Legal, ethical, and OPSEC considerations