SEC535: **Offensive AI – Attack Tools and Techniques™**

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

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

The first day of SEC535 focuses on AI-driven reconnaissance and social engineering attacks, equipping you with the tools and techniques modern adversaries use to infiltrate organizations. We kick off with Open Source Intelligence (OSINT) gathering using AI, leveraging powerful tools like Spiderfoot and Bbot to uncover valuable intelligence such as DNS records, employee emails, and internal phone numbers at the notional company "Meridian Systems." From there, we explore how an AI Pentest Assistant powered by a Retrieval-Augmented Generation (RAG) database can streamline network enumeration and optimize vulnerability discovery to enhance penetration testing workflows.

Armed with this intelligence, we will transition to exploiting the vulnerabilities using AI with Metasploit, and performing SQL Injection attacks.

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 2: Social Engineering Attacks

In this section, we explore how AI is transforming traditional social engineering and targeted exploitation. We start by examining the social engineering attack surface and the psychology behind manipulation, then build practical campaigns using tools like GoPhish and SET. You will develop and tune PhishGPT to generate tailored phishing emails, leverage sentiment analysis for profiling, and automate large-scale attacks through N8N workflows. Moving deeper, we uncover how attackers create convincing audio deepfakes with platforms like ElevenLabs and Voice.ai to enable advanced vishing scenarios. From there, we step into visual deepfakes, applying face swapping, motion transfer, and lip syncing to craft realistic video lures. Finally, we shift focus to vulnerability research with AI-assisted patch diffing. You will use tools such as DeepBinDiff and ChatGPT to identify silent patches, evaluate exploitability through zero-shot techniques, and refine prompts that accelerate finding new attack paths before they are widely known. Finally, we introduce AI-automated patch diffing, where AI-driven agents perform binary comparisons to detect security fixes, rank exploitability, and generate working exploits before vulnerabilities are publicly disclosed.

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

SECTION 3: Malware Development and Security Control Evasion

In this section, we examine how AI is reshaping the creation and deployment of modern malware. We begin by breaking down the fundamental components of malicious software and exploring how attackers build anti-analysis capabilities to evade detection. From there, you will use AI to develop custom malware, starting with generating proof-of-concept payloads and progressively layering in quality-of-life and stealth features. We also highlight curious, sometimes unpredictable behaviors that emerge when tools like ChatGPT assist in crafting malicious code. Moving forward, you will learn techniques for hiding, obscuring, and embedding persistent malware using alternate data streams, wrapped execution, dynamic attribute access, and encoding substitutions. You will automate obfuscation, implement WMI persistence, build malicious DLLs, and use AI to trojanize payloads. Finally, we cover advanced agentic malware, leveraging AI assistants and frameworks like GNAW to rewrite code in memory, deploy subordinate programs, and bypass security controls by disabling Defender, defeating tamper protection, and writing AMSI bypasses.

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

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