SEC504

Hacker Tools, Techniques, and Incident Handling

Fall 2025 Update: The AI Era of Offensive Readiness

The latest SEC504 update redefines the industry's flagship incident handling and offensive operations course for the AI-driven age. This 2025 refresh integrates artificial intelligence throughout the labs and workbook, preparing students to detect, analyze, and counter modern adversary tactics across Windows, Linux, and cloud environments.

Authored by Joshua Wright, the new version introduces advanced content on Offensive AI, API Attacks, and Prompt Injection, plus redesigned hands-on labs and AI-enabled workbook features. Students will experience a more interactive, adaptive learning journey — with tools, threats, and techniques that mirror today's fast-evolving attack landscape.

"The World Economic Forum (WEF) released findings that 60% of organizations cite geopolitical tensions as having impacted their cybersecurity strategy. The report elaborates that while 66% of organizations expect the pressures of AI adoption to exacerbate security challenges, only 37% report having processes in place to assess whether these tools are safe for employees to use."

(Source: SC Media | Turning a cybersecurity breach into a win: Steps to take in the first 24 hours)

New Content

- Expanded coverage of AI in incident response, adversarial use, and defense strategies
- New modules: Offensive AI, API Attacks, and Prompt Injection Attacks
- Enhanced focus on attacker use of AI, LLM guardrail evasion, and AI-driven exploitation
- Modernized Network Investigation module featuring RITA as a powerful NDR tool
- Updated examples and vulnerabilities through 2025, including Passkey attacks and Hashcat 7.0

Updated Features

- AI-integrated workbook tools: Explain, Ask, Explore, and Quiz powered by frontier AI models
- Streamlined, modernized content designed to appeal to different individual learning styles
- AI-enhanced playbooks for IR acceleration and adversarial analysis
- Inclusive learning design across visual, kinesthetic, and analytical styles
- Overhauled learning environment with lab targets from multiple industry verticals, adapted from real-world breaches and pen tests

Lab Refresh

- New AI-powered labs: Accelerating Incident Response with AI, Offensive AI Attacks, API Attack, and Prompt Injection Attack
- Gamified learning: Office Infiltrator, Lightning Labs, Linux and PowerShell bootcamp events
- Revamped Network Investigation and Metasploit labs with 2025 tools and attack paths
- All labs rewritten for concise instructions, clear formatting, and modernized environments
- Expanded Capture-the-Flag capstone event to apply what you learned in a rigorous compromise scenario

"As offensive operations evolve with AI and automation, security professionals must evolve too. The new SEC504 helps you master modern adversary tactics and integrate AI into every stage of detection and response. AI doesn't change the need for expertise — it raises the bar for what expertise looks like." — Joshua Wright | SEC504 Author and Faculty Fellow

For more information: sans.org/SEC504

SANS | GIAC CERTIFICATIONS