SEC565

Red Team Operations and Adversary Emulation

March 2026 Update: AI Tools to Test and Improve Organizational Defenses

The latest SEC565 update modernizes SANS' Red Team operations training course for the AI-driven offensive landscape. This major refresh integrates artificial intelligence across planning, infrastructure, weaponization, and command-and-control workflows — preparing Red Team operators to emulate modern adversaries with greater speed, realism, and operational depth.

Authored by Jean-François Maes and Dave Mayer, the new version expands adversary emulation tradecraft, modernizes attack infrastructure, and introduces AI-driven tooling including Model Context Protocol (MCP) C2 operations and AI-assisted CTI analysis. Students will experience a more adaptive, realistic Red Team engagement — aligned with today's enterprise environments and emerging attack methodologies.

New Content

- AI-assisted CTI analysis and automated TTP extraction
- AI-generated social engineering pretexts
- AI-driven C2 operations using Model Context Protocol (MCP)
- Vibe coding: building custom evasion frameworks with AI
- AI-assisted restoration and modernization of legacy tooling
- Expanded integration of AI across adversary emulation lifecycle

Updated Features

- Enhanced focus on current real-world adversary tradecraft
- Consolidating regulatory frameworks (e.g., removing TIBER in favor of DORA)
- Refined operational security and infrastructure guidance
- Streamlined and modernized content flow across sections
- Removed and replaced outdated tooling

Lab Refresh

- New lab: Guardrailed execution and keyed payload deployment
- Range updates to support DLL hijacking demonstrations
- Improved Active Directory attack scenarios
- Modernized reconnaissance techniques and tooling
- Refined immersive Red Team CTF experience
- Updated lab walkthrough integrations

"Red Teaming is evolving rapidly with AI and automation. This update ensures students don't just use modern tools — they understand how to build, modify, and operationalize them safely and effectively. The goal remains the same: make defenders better by emulating real adversaries with precision and purpose." **— Jean-François Maes | SEC565 Author**