

Offensive Security Training, Courses & Certifications

By Mike DozierSavannah River Nuclear Solutions

Archived: 2026-04-05 19:40:08 UTC

Outsmart Hackers with Real-World Offensive Security Training

As cyberthreats grow more sophisticated, it is critical to proactively identify and address vulnerabilities before adversaries exploit them. SANS Offensive Operations delivers expert-led training across the entire attack surface, covering everything from penetration testing and red teaming to exploit development and hardware hacking. Through hands-on labs and industry-recognized certifications, we equip professionals to master real-world offensive techniques and adversarial tactics.

Student Insights

In one week, my instructor built a bridge from typical vulnerability scanning to the true art of penetration testing. Thank you, SANS, for making myself and my company much more capable in information security.

Meet Your Experts





Erik Van Buggenhout

Co-Founder & Partner

NVISO co-founder and SANS Senior Instructor, leading cybersecurity education in advanced adversary tactics. Experienced in offensive security with extensive background in penetration testing and ethical hacking across Europe.

[Learn more](#)





Chris Elgee

Builder & Breaker

Chris is a senior security analyst for Counter Hack and Cyber Range Lead (S-6) for the Army National Guard's 91st Cyber Brigade. Through his work, he shares his unique insights into cyber security threats to prepare and inspire students.

[Learn more](#)





Moses Frost

Solutions Consultant

Moses has built an impressive career as a Network Architect, DevOps Engineer, and Information Security professional. Today, he works in the Offensive Operations space as a Red Team Operator and serves as the course author for SEC588.

[Learn more](#)





Jean-François is based in Portugal, where he is the CEO of Offensive Guardian, a boutique red and purple teaming shop providing freelance services to various organizations. He has worked for other noteworthy firms, including, but not limited to: Neuvik, TrustedSec, Fortra's Cobalt-Strike team, and NVISO.

[Learn more](#)





Jeff McJunkin, Rogue Valley InfoSec founder, has led Fortune 100 pen tests and shaped Core NetWars. His key role in SANS Holiday Hack Challenge and hands-on security innovations continue to elevate the industry, advancing defenses worldwide.

[Learn more](#)





Larry Pesce

Vice President of Services

Larry has revolutionized embedded device security with decades of hands-on offensive research, co-authoring SANS's flagship wireless and IoT penetration testing courses, and pioneering SBOM exploitation techniques for supply chain defense strategies.

[Learn more](#)

Explore Careers Within Offensive Operations

Upcoming Events

- Slide 1 of 5

Defending at the Speed of AI: Outpacing Tomorrow's Attackers

This talk explores the emerging landscape of AI-driven cyber threats and argues that organizations must defend at the speed of AI to survive.

Webinar Offensive Operations



- 14 Apr 2026
- 14:00 PHST
- Bryce Galbraith

[View details](#)

- Slide 2 of 5

Hackventures with Josh: Better Password Attacks with AI

The Verizon DBIR says stolen credentials cause more breaches than phishing and exploits combined. Now, AI is making these attacks even more effective. Join SANS Fellow Joshua Wright to learn what you can do

[to protect your environment.](#)

[WebinarOffensive Operations](#)



- [15 Apr 2026](#)
- [13:00 EDT](#)
- [Joshua Wright](#)

[View details](#)

- Slide 3 of 5

[**Vibe Coding Your Own Evasion Framework: AI-Assisted Red Team Tool Development**](#)

[AI can accelerate red team tool development, but only with the right approach. This hands-on workshop explores “vibe coding,” showing how to use LLMs to design, validate, and build evasion tooling step by step, resulting in a functional, AI-assisted red team framework.](#)

[WebinarOffensive Operations](#)



- [16 Apr 2026](#)
- [10:00 EDT](#)
- [Jean-François Maes](#)

[View details](#)

- Slide 4 of 5

[SANS Network Security 2026 - Featured Keynote: Offense at Machine Speed: How AI Is Reshaping the Threat Landscape](#)

[The session will demonstrate how AI can be applied as both a SAST and DAST capability for discovering and exploiting zero-day vulnerabilities in web applications, as well as its growing role in binary exploitation.](#)

[WebinarOffensive Operations](#)



- [22 Sep 2026](#)
- [18:00 PDT](#)
- [Stephen Sims](#)

[View details](#)

- Slide 5 of 5

[SANS 2026 Threat Hunting Survey: The Evolution of Threat Hunting](#)

[Threat hunting is no longer just a niche skill—it's a critical pillar of modern defense.](#)

[Webinar Offensive Operations](#)



- [23 Sep 2026](#)
- [10:30 EDT](#)
- [Josh Lemon](#)

[View details](#)

Modern Multi-Factor Authentication Bypass Techniques: A Taste of SANS SEC660

With the proliferation of multi-factor authentication, penetration testers need to apply existing tooling to manipulate even internal applications. Building attack infrastructure internally during a penetration test is resource exhausting, but modern tools like evilginx can do most of the heavy lifting for us.

Webinar

FeaturesJames Shewmaker



- Slide 1 of 2



- Slide 2 of 2



[More Insights](#)

Frequently Asked Questions

Source: <https://pen-testing.sans.org/resources/papers/gcih/real-world-arp-spoofing-105411>