



The most trusted source for cybersecurity training, certifications, degrees, and research

# Offensive Operations East

June 8–14, 2025

Baltimore, MD & Virtual (ET)



## Pen Testing in The Modern Era

Attend In-Person in Baltimore or Live Online (ET)

Whether you're just starting in penetration testing or a seasoned operator, **Offensive Operations East 2025** offers immersive, hands-on training tailored for all experience levels across every offense-focused area. Throughout the week, you'll learn directly from expert practitioners, engage in real-world lab exercises, and forge connections with fellow security professionals at evening events. This training event is designed to equip you with unique skills that immediately benefit your organization's security posture.

Immerse yourself in a learning environment that features industry-leading hands-on labs, simulations, and exercises, all geared towards practical application in your professional endeavors. Seize the opportunity to hone your skills during bonus sessions and activities, backed by SANS unwavering commitment to excellence and expertise.

### SANS Offensive Operations East 2025 Features

#### Offensive Ops Workshops Gratis

Sunday, June 8 | 10:00 AM–5:15 PM

- Artificial Infection: Using AI to Write Malware
- Follow the SSRF Rabbit
- Active Directory Privilege Escalation Workshop
- SANS Villages



- **Thought leadership panel and receptions:** Join the discussion—in partnership with local community organizations and alumni, network with industry professionals and discuss issues facing the industry today.
- **Coin-a-palooza:** Your chance to earn challenge coins you may have missed out on previously!
- **Central hotel location:** Courses will be held at The Royal Sonesta Harbor Court Baltimore

### Ways to Train

#### In-Person: The All-Access Experience in Baltimore, MD

Dive into the future of offensive operations, participate in live discussions, and engage in critical dialogs. Don't miss this chance to influence the conversation and connect with top cybersecurity leaders! There's no better way to gain insights than hearing directly from those steering the industry. Get ready to spark your curiosity through hands-on workshops, @Night talks, and more!

#### Live Online SANS

Live Online training offers live, interactive streaming sessions delivered directly from your instructor. Features of Live Online training include networking via chat channels and live access to top SANS instructors. Live Online is a flexible and fun way to learn—from anywhere!



CORE

**NETWORKS**

June 12 & 13 | 6:30–9:30 PM

**Attendance Options:** In-Person

Participation is free with any 4–6 day course purchase!



Explore the Event

[www.sans.org/cyber-security-training-events/offensive-operations-east-2025](https://www.sans.org/cyber-security-training-events/offensive-operations-east-2025)

☎ 301-654-SANS (7267) ✉ [support@sans.org](mailto:support@sans.org) ✎ @SANSInstitute

## Confirmed Courses

**SEC467: Social Engineering for Security Professionals™**

**SEC504: Hacker Tools, Techniques, and Incident Handling™**

**GCIH**

**GIAC Certified Incident Handler**  
giac.org/gcih



**SEC542: Web App Penetration Testing and Ethical Hacking™**

**GWAPT**

**GIAC Web Application Penetration Tester**  
giac.org/gwapt



**SEC556: IoT Penetration Testing™**

**SEC560: Enterprise Penetration Testing™**

**GPEN**

**GIAC Penetration Tester**  
giac.org/gpen



**SEC565: Red Team Operations and Adversary Emulation™**

**GRTF**

**GIAC Red Team Professional**  
giac.org/grtp



**SEC575: iOS and Android Application Security Analysis and Penetration Testing™**

**GMOB**

**GIAC Mobile Device Security Analyst**  
giac.org/gmob



**SEC588: Cloud Penetration Testing™**

**GCPN**

**GIAC Cloud Penetration Tester**  
giac.org/gcpn



**SEC598: Security Automation for Offense, Defense, and Cloud™** **NEW**

**SEC599: Defeating Advanced Adversaries – Purple Team Tactics & Kill Chain Defenses™**

**GDAT**

**GIAC Defending Advanced Threats**  
giac.org/gdat



**SEC617: Wireless Penetration Testing and Ethical Hacking™**

**GAWN**

**GIAC Assessing and Auditing Wireless Networks**  
giac.org/gawn



**SEC660: Advanced Penetration Testing, Exploit Writing, and Ethical Hacking™**

**GXPEN**

**GIAC Exploit Researcher & Advanced Penetration Tester**  
giac.org/gxpn



**SEC670: Red Teaming Tools – Developing Windows Implants, Shellcode, Command and Control™**

**SEC699: Advanced Purple Teaming – Adversary Emulation & Detection Engineering™**

**SEC760: Advanced Exploit Development for Penetration Testers™**