SEC588
Cloud Penetration Testing

Fall 2025 Update: Modern Cloud, Modern Offense

The all-new SEC588: Cloud Penetration Testing has been completely updated for today's cloud-first world. This 2025 refresh expands coverage across AWS, Azure, Microsoft 365, and Kubernetes, with 24 hands-on labs and modern attack simulations.

Co-authored by Moses Frost and Aaron Cure, the course dives into current adversary tradecraft, including identity abuse, IaC exploitation, and multi-cloud persistence. Students will learn to assess, attack, and report on complex, hybrid environments that blend on-premise, cloud, and containerized systems.

> "The misuse of valid accounts emerged as the primary initial access vector for cloud environments, accounting for 35% of cloud incidents in the first half of 2024."
> (Source: CrowdStrike 2025 Global Threat Report)

This major update reflects the evolving offensive landscape — from legacy data centers moving into cloud-native architectures — ensuring students leave ready to test tomorrow's IT environments.

New Content

- Expanded coverage across AWS, Azure, Microsoft 365, and Kubernetes.
- New section on Identity Systems featuring Microsoft Entra ID, malicious app consents, Microsoft Graph, FIDO2/Passkeys, and attacker-in-the-browser scenarios.
- Enhanced focus on Infrastructure as Code (IaC), CI/CD pipeline attacks, serverless exploitation, and datalakes/LLMs as data sources.
- Added coverage for Azure Arc, AssumeRole/Confused Deputy in AWS, and Modern C2 for cloud command and control.
- Expanded container and Kubernetes assessments including persistence and lateral movement techniques.

Updated Features

- 24 hands-on labs simulating end-to-end cloud attacks across AWS, Azure, Microsoft 365, and Kubernetes.
- 4 months of lab access plus OnDemand video walkthroughs and MP3 audio for extended practice.
- Enhanced lab environments featuring real-world offensive tooling such as CursedChrome, GraphRunner, GraphSpy, and Roadtools.
- Modernized methodology aligning with today's adversary behavior in hybrid and multi-cloud ecosystems.
- Updated course books and exercises for immediate, real-world application.

Lab Refresh

- New End-to-End AWS Attack Lab featuring AssumeRole and Confused Deputy privilege escalation paths.
- Microsoft Entra ID lab suite exploring malicious app consents, Graph API exfiltration, and attacker-in-the-browser scenarios.
- Azure VM and Azure Arc labs demonstrating real-world lateral movement and code execution.
- IaC and CI/CD Hijacking labs covering Terraform misconfigurations and polluted pipeline execution.
- Serverless and Database labs exploring SSRF, RCE, and data exfiltration in modern stacks.
- Container and Kubernetes labs on breakout, pivoting, and persistence techniques.
- Three new Docker breakout labs challenge students to exploit real misconfigurations and break out from containers to the host, simulating one of today's most critical cloud-native threats.

"As cloud adoption accelerates, so must our offensive readiness. The latest SEC588 equips security professionals to test, understand, and defend the environments that define modern business — because attackers aren't waiting for you to catch up. Ultimately, I hope this class will continue to empower both the red and blue teams to build stronger defenses and enhance the security of these environments." — Moses Frost | Course Author and Senior Instructor

For more information: sans.org/SEC588

SANS | GIAC CERTIFICATIONS